Didactiques
Mathématiques

Un cours d'algèbre constructive

Ray Mines – Fred Richman – Wim Ruitenburg

Édition anglaise originale : 1988

Traduction française par Henri Lombardi

révisée par Stefan Neuwirth

Presses universitaires de Franche-Comté

Un cours d'algèbre constructive

Ray Mines Fred Richman Wim Ruitenburg

Édition anglaise originale : 1988

Traduction française par Henri Lombardi
révisée par Stefan Neuwirth

28 novembre 2020

Dédié à Errett Bishop

Préface

L'approche constructive aux mathématiques a connu une renaissance, en grande partie grâce à la parution du livre d'Errett Bishop *Foundations of constructive analysis* en 1967, et aussi grâce à l'influence subtile de la prolifération d'ordinateurs avec de grandes capacités de calcul. Bishop a démontré que les mathématiques pures peuvent être développées d'un point de vue constructif tout en maintenant la continuité avec la terminologie et l'esprit classiques ; une bien plus grande partie des mathématiques classiques a pu être préservée par rapport à ce que l'on pouvait croire possible, et aucun théorème faux en mathématiques classiques n'en a résulté, comme cela avait été le cas pour d'autres écoles constructives, comme le constructivisme russe ou l'intuitionnisme. Les ordinateurs ont créé une conscience largement partagée de la notion intuitive de procédure effective, et de celle de calculs exécutables en principe. Ils ont en outre stimulé l'étude de l'algèbre constructive en vue de son implémentation, ainsi que du point de vue de la théorie des fonctions récursives.

En analyse, les problèmes de constructibilité apparaissent immédiatement parce que nous devons commencer avec les nombres réels, et qu'il n'y a pas de procédure finie pour décider si deux nombres réels sont égaux ou pas (les nombres réels ne forment pas un ensemble discret). Le principal obstacle pour les mathématiques constructives était en direction de l'analyse, alors que plusieurs mathématiciens, notamment Kronecker et van der Waerden, avaient fait d'importantes contributions à l'algèbre constructive. Heyting, travaillant en algèbre intuitionniste, s'est concentré sur les problèmes liés aux structures algébriques sur les nombres réels ; il y a développé une partie de l'analyse plutôt qu'une théorie des structures algébriques discrètes. De manière paradoxale, c'est en algèbre que le plus souvent nous nous heurtons à des arguments sauvagement non constructifs comme ceux qui établissent l'existence d'idéaux maximaux, ou l'existence de plus que deux automorphismes du corps des nombres complexes.

Dans ce livre, nous présentons les notions de base de l'algèbre moderne d'un point de vue constructif. Les sujets les plus avancés ont été dictés par nos préférences et par nos limitations, et par la disponibilité de traitements constructifs dans la littérature. Quoique le livre soit par nécessité à peu près auto-contenu, il n'est pas censé être une première introduction à l'algèbre moderne ; le lecteur est présumé avoir quelque familiarité avec le sujet classique.

Il est important de garder à l'esprit que l'algèbre constructive est de l'algèbre ; en fait, c'est une généralisation de l'algèbre classique en ce que nous ne supposons pas la loi du tiers exclu, exactement comme la théorie des groupes est une

généralisation de la théorie des groupes abéliens en ce que la commutativité n'est plus supposée. Une démonstration constructive d'un théorème est en particulier une démonstration de ce théorème. Tout théorème dans ce livre peut être compris comme se référant à l'univers conventionnel du discours mathématique, et les démonstrations sont acceptables dans cet univers (aux fautes éventuelles de raisonnement près). Nous ne nous limitons pas à une classe restreinte d'« objets constructifs » comme le font les théoriciens des fonctions récursives et nous n'introduisons pas non plus de principes classiquement faux comme le font les intuitionnistes.

Nous exprimons nos remerciements à Abraham Seidenberg, Gabriel Stolzenberg, Larry Hughes, Bill Julian et Steve Merrin pour leurs suggestions.

Ray Mines
Fred Richman
New Mexico State University

Wim Ruitenburg
Marquette University

Préface du traducteur

Il me faut avant tout remercier Fred Richman pour sa collaboration bienveillante à cette traduction. Il m'a fourni le fichier source latex de la version originale du livre en anglais, et il a répondu à toutes mes demandes d'éclaircissements.

Je remercie aussi chaleureusement Stefan Neuwirth, un collaborateur qui a relu avec une précision remarquable la traduction une fois terminée. Le nombre d'erreurs que je suis capable de commettre sans les déceler lors d'une relecture personnelle m'a véritablement impressionné. Sa relecture nous a aussi permis de préciser certains points délicats dans plusieurs démonstrations.

J'ai introduit un certain nombre de « notes du traducteur » en bas de page, notées **NdT**. Souvent il s'agit de préciser la terminologie anglaise pour un terme dont la traduction française est assez éloignée. Quand c'était possible, j'ai utilisé comme terminologie française de référence celle de Bourbaki.

D'autres fois, j'ai utilisé une note de bas de page pour ajouter une précision que j'estimais utile pour mieux comprendre le texte.

Par ailleurs les rares fois où j'ai un tout petit peu corrigé le texte, hormis quelques fautes de frappe évidentes, je l'ai fait en accord avec Fred Richman.

Après la traduction proprement dite du livre, je fais figurer une postface où je commente certains des aspects particulièrement marquants, notamment certaines divergences par rapport au livre de Bishop.

Enfin Stefan Neuwirth a réalisé le chapitre final sur la réception de l'édition originale de l'ouvrage. Il donne une liste bibliographique des travaux qui ont cité le livre depuis sa parution.

Henri Lombardi
Université de Franche-Comté

Table des matières

I. Ensembles

Sommaire

1 Mathématiques constructives vs. mathématiques classiques

Le point de vue classique sur les mathématiques est essentiellement descriptif : on essaie de décrire des faits à propos d'un univers statique. Ainsi par exemple on admet qu'un polynôme de degré impair admet toujours une racine, et qu'il y a une décimale qui apparait une infinité de fois dans le développement décimal de π. On a un point de vue opposé en mathématiques constructives, elles concentrent leur attention sur l'interaction dynamique entre l'individu et l'univers mathématique ; dans les termes de Hao Wang, il s'agit d'une mathématique du faire plutôt que d'une mathématique de l'être. Le mathématicien constructif doit montrer comment construire une racine d'un polynôme de degré impair, et comment on peut trouver une décimale qui apparait une infinité de fois dans le développement décimal de π.

Nous imaginons un mathématicien idéalisé U qui interagit avec l'univers mathématique ; c'est lui le « vous » qui trouve le δ et à qui un ϵ est donné lorsque nous disons « étant donné un ϵ vous devez trouver δ ». Les phrases « il existe » et « vous devez trouver » signifient que U doit réaliser les constructions souhaitées. Puisque « P_1 ou P_2 » signifie qu'il existe $i \in \{1, 2\}$ tel que P_i est vrai, la signification du « ou » découle de la signification du « il existe », et c'est

l'interprétation de cette dernière phrase qui est fondamentale en mathématiques constructives.

Les mathématiques classiques peuvent être elles aussi décrites dans cette image ; la différence réside dans le pouvoir que nous attribuons à U. Un U omniscient peut décider si une assertion mathématique donnée est vraie ou fausse ; ainsi par exemple U peut inspecter la suite des décimales de π et déterminer quelles décimales apparaissent une infinité de fois. Avec un omniscient U, notre image est simplement un portrait plus dynamique, anthropomorphique, des mathématiques classiques.

En mathématiques constructives nous supposons que U peut seulement réaliser des constructions finies en nature. Comme le dit Errett Bishop, « la seule manière de démontrer qu'un objet existe est de donner une procédure finie pour le trouver ». Dans ce cadre, nous n'avons pas le droit de dire qu'une décimale apparait une infinité de fois dans le développement de π tant que nous ne sommes pas prêts à exhiber une telle décimale ou au moins à produire un algorithme qui calculera cette décimale.

Nous considérons que U est capable de réaliser n'importe quelle construction spécifiée par un algorithme, mais nous n'excluons pas la possibilité qu'il sache faire d'autres choses – y compris qu'il puisse être omniscient. Le tableau qui résulte du fait de restreindre les capacités de U à des constructions finies est l'**interprétation calculatoire** des mathématiques. Comme toute assertion qui admet une preuve constructive est vraie dans l'interprétation calculatoire, nous disons que les mathématiques constructives ont une signification numérique ; comme toute assertion qui admet une preuve constructive est vraie dans l'interprétation classique, nous disons que les mathématiques constructives sont une généralisation des mathématiques classiques.

Les mathématiques constructives sont les mathématiques pures faites de manière algorithmique de façon à respecter l'interprétation calculatoire. La notion centrale de processus fini, ou d'algorithme, est prise comme une notion primitive. Toute tentative de définir ce qu'est un algorithme implique en dernière analyse la notion d'existence – par exemple nous pourrions demander qu'il existe une étape à laquelle un certain programme de calcul produit une réponse. Si le terme « exister » est pris dans son sens classique ici, nous échouons à capturer la notion même d'algorithme. Si le terme est utilisé dans son sens constructif, la définition est circulaire.

Considérez la distinction entre l'usage classique et l'usage constructif du « ou ». Pour prouver « P_1 ou P_2 » de manière constructive, nous devons construire un algorithme qui soit prouve P_1, soit prouve P_2, et en exécutant cet algorithme nous (le mathématicien idéalisé) pouvons déterminer laquelle des deux conditions est vraie. Pour prouver « P_1 ou P_2 » de manière classique, il suffit de montrer que P_1 et P_2 ne peuvent être simultanément fausses. Par exemple considérons

l'assertion P_1 :

il existe des entiers strictement positifs x, y, z, et n tels que :

$$x^{n+2} + y^{n+2} = z^{n+2},$$

et soit P_2 le fameux théorème de Fermat, la négation de P_1. Si P_1 est faux alors P_2 est vrai, donc « P_1 ou P_2 » est classiquement prouvable ; mais tant que le théorème de Fermat n'est pas démontré, nous ne savons pas laquelle des deux assertions P_1 ou P_2 est vraie, et nous n'avons pas de preuve constructive de « P_1 ou P_2 ».

Une démonstration constructive d'un théorème prouve plus qu'une démonstration classique : une démonstration constructive du fait qu'une suite de nombres réels converge implique que nous pouvons calculer une vitesse de convergence ; une démonstration constructive du fait qu'un espace vectoriel est de dimension finie implique que nous pouvons calculer une base de cet espace vectoriel ; et une démonstration constructive du fait qu'un polynôme est un produit de polynômes irréductibles implique que nous pouvons construire ces polynômes irréductibles.

Deux assertions peuvent être classiquement équivalentes sans l'être constructivement. Soit P l'affirmation selon laquelle tout sous-groupe de $\mathbb{Z}$ est cyclique. Cela signifie que nous pouvons à partir d'une spécification du sous-groupe trouver un générateur de ce sous-groupe. Soit Q l'affirmation selon laquelle aucun sous-groupe G de $\mathbb{Z}$ ne peut avoir la propriété que pour chaque $m \in G$, il y a un entier dans G qui n'est pas multiple de m. Les affirmations P et Q sont de manière immédiate équivalentes en mathématiques classiques, mais très différentes d'un point de vue constructif. L'affirmation Q est vraie : comme 0 est dans G, il y a un entier non nul n dans G ; comme n est dans G, il y a un diviseur strict de n dans G ; et ainsi de suite jusqu'à ce que nous arrivions à une contradiction. Mais il n'est pas du tout crédible que P soit vraie, comme nous pouvons nous en rendre compte en considérant le sous-groupe de $\mathbb{Z}$ engendré par les nombres parfaits : pour construire un générateur de G nous devons construire un nombre parfait impair ou démontrer que tous les nombres parfaits sont pairs.

D'un autre côté, deux assertions constructivement équivalentes sont classiquement équivalentes ; en effet, tout théorème de mathématiques constructives est aussi un théorème de mathématiques classiques : une démonstration constructive est une démonstration.

Supposons que nous essayions de trouver une démonstration constructive pour une assertion P qui est classiquement vraie. Après de nombreuses tentatives infructueuses nous pourrions être tentés de chercher un contre-exemple. Mais nous ne pouvons espérer prouver la négation de P, ce qu'un contre-exemple de bonne foi impliquerait, car $\neg P$ est classiquement fausse. Comme cette voie nous

est fermée, nous avons besoin d'une autre alternative quand nous persistons à vouloir contredire P.

Une approche consiste à fixer un langage formel dans lequel la propriété P peut être exprimée, à préciser dans ce langage formel quelles sont les suites de mots qui constituent une démonstration, et à démontrer qu'aucune preuve formelle de P ne peut être construite (éventuellement en considérant une interprétation inattendue du langage formel et en montrant que dans cette interprétation la propriété est fausse). Un tel programme de travail est éclairant, mais on peut souvent mettre en doute que le système formel choisi reflète de manière adéquate la réalité mathématique. Une objection plus sérieuse consiste à dire que mettre en œuvre de tels arguments d'indépendance réclame un changement de point de vue drastique. Une procédure qui se situerait plus près du sujet à traiter semble préférable. À cette fin nous introduisons les idées de *principe d'omniscience* et d'*exemple brouwerien*.

Une règle qui à chaque entier naturel n fait correspondre un élément α_n de $\{0,1\}$ est appelée une **suite binaire** [1]. Un **principe d'omniscience** est une affirmation vraie classiquement, de la forme « $P(\alpha)$ est vraie pour toutes les suites binaires α », mais qui n'est pas considérée pouvoir être prouvée constructivement. Par exemple classiquement pour toute suite α, ou bien

(P) il existe un n pour lequel $\alpha_n = 1$, ou bien

(Q) pour tout n, $\alpha_n = 0$.

L'affirmation selon laquelle P ou Q a bien lieu est appelée le **petit principe d'omniscience (LPO)** [2]. Étant donné que Q est la négation de P, le petit principe d'omniscience est une forme de la **loi du tiers exclu** : l'affirmation selon laquelle pour n'importe quelle propriété P on a « P ou non P ». Le petit principe d'omniscience, et à fortiori la loi du tiers exclu, ne sont pas acceptés dans l'approche constructive car personne ne croit sérieusement que l'on puisse construire un algorithme qui, étant donnée une suite α, choisisse l'alternative correcte P ou Q. Un autre argument contre LPO est que si on se limite à certains types d'algorithmes, comme c'est le cas pour l'école constructiviste russe, alors on peut prouver que LPO est faux. On fixe un langage de programmation capable d'exprimer les fonctions usuelles sur les entiers naturels ainsi que les manipulations symboliques ordinaires. On peut alors démontrer qu'il n'existe aucun programme d'ordinateur qui accepte en entrée des programmes de calcul et qui, appliqué à un programme qui calcule une suite binaire, retourne 1 si la suite contient 1 et 0 si la suite n'en contient pas. Ainsi si nous demandons que nos règles de calcul [3] soient toutes données par des programmes d'ordinateur,

1. **NdT.** De manière générale dans cet ouvrage, les auteurs utilisent une casse grasse pour indiquer qu'il donne une définition.

2. **NdT.** Limited principle of omniscience.

3. **NdT.** Celles utilisées pour produire des suites binaires, et celles utilisées pour produire le test souhaité.

on peut démontrer que LPO est faux. Ceci est un argument contre l'acceptation de LPO, parce que tout algorithme informel que nous produisons sera sans aucun doute programmable, ainsi nos théorèmes doivent être vrais dans l'interprétation où les algorithmes sont des programmes d'ordinateur ; mais nous ne nous restreignons pas à cette interprétation car elle interdit d'interpréter nos théorèmes en mathématiques classiques : et en effet LPO est classiquement vrai.

Lorsque l'on peut montrer qu'une affirmation P implique LPO, nous abandonnons la recherche d'une preuve constructive de P. Mais nous n'affirmons pas pour autant que P est fausse : après tout, P peut admettre une preuve classique. Les assertions telles que LPO doivent plutôt être considérées comme *indépendantes* en ce sens que ni elles ni leurs négations ne sont valides.

Considérez par exemple la propriété P valide en mathématiques classiques selon laquelle tout sous-ensemble des entiers naturels est vide ou contient un élément. Étant donnée une suite binaire α, définissez $A = \{1\}$ et $B = \{\, \alpha_n : n \in \mathbb{N} \,\}$. Alors $A \cap B$ est un sous-ensemble des entiers naturels. S'il contient un élément, ce doit être 1, et selon la définition de B, il existe un entier n tel que $\alpha_n = 1$; si $A \cap B$ est vide, pour tout entier n, $\alpha_n = 0$. Ainsi, si la propriété P est vraie alors on a également LPO.

Un principe d'omniscience plus faible est le **mini principe d'omniscience (LLPO)**[1] qui affirme qu'une suite binaire $(\alpha_n)_{n\in\mathbb{N}}$ qui contient au plus un élément 1, ou bien est nulle pour tout n impair, ou bien est nulle pour tout n pair. Cela implique que dans une suite binaire nous pouvons dire à priori que dans le cas où un élément 1 apparait, sa première apparition sera pour un indice pair ou impair. Comme dans le cas du principe LPO, si nous limitons nos algorithmes à ceux qui sont programmables sur ordinateur, nous pouvons réfuter LLPO. Si vous pensez à la suite binaire α comme à une boite noire qui retourne α_n lorsque vous lui donnez l'entier n en entrée, il est tout à fait clair que vous ne pouvez espérer établir ni LPO ni LLPO. Considérez la suite α définie comme suit :

$\alpha_{2n} = 1$	si, et seulement si, il y a 100 décimales consécutives de π égales à 6 dans les n premières décimales de π ;
$\alpha_{2n+1} = 1$	si, et seulement si, il y a 100 décimales consécutives de π égales à 7 dans les n premières décimales de π.

Comme on sait calculer les décimales de π, il y a un algorithme qui calcule la suite α. Mais à moins que nous tombions par chance sur 100 décimales de π consécutives égales à 6 ou à 7, nous aurons du mal à trouver un algorithme qui décide que si cela arrive, pour la première fois ce sera avec un entier m pair ou avec un entier impair.

Un **exemple brouwerien** E est une construction $E(\alpha)$ basée sur une suite binaire arbitraire α. Nous disons que l'exemple brouwerien E **satisfait la condi-**

1. **NdT.** Lesser limited principle of omniscience.

tion C si $E(\alpha)$ satisfait la condition C pour chaque α ; nous disons que l'exemple E **ne satisfait pas la condition** C s'il y a un principe d'omniscience « $P(\alpha)$ pour tout α » tel que chaque fois que $E(\alpha)$ satisfait C, $P(\alpha)$ est valide. Un **contre-exemple brouwerien** à une affirmation du type « C_1 implique C_2 » est un exemple brouwerien qui satisfait C_1 mais ne satisfait pas C_2.

Notre construction précédente $A \cap B$ est un exemple brouwerien d'un sous-ensemble des entiers naturels qui, ni ne contient un élément, ni n'est vide. Nous construisons maintenant une suite croissante bornée de nombres réels qui n'admet pas de borne supérieure. Pour chaque suite binaire α soit $E(\alpha)$ la suite β de nombres réels définie par $\beta_n = \sup_{k=1}^{n} \alpha_k$. Alors $E(\alpha)$ est une suite bornée croissante de nombres réels. Soit C la condition pour une suite de nombres réels qu'elle admette une borne supérieure. Nous allons montrer que E ne satisfait pas la condition C. Soit $P(\alpha)$ la propriété que, ou bien α est identiquement nulle, ou bien il y a un entier n tel que $\alpha_n = 1$, et supposons que E satisfasse la condition C. Si la borne supérieure de $E(\alpha)$ est < 1 alors α est identiquement nulle. Si la borne supérieure de $E(\alpha)$ est > 0 alors il y a un entier n tel que $\alpha_n > 0$, donc $\alpha_n = 1$. Ainsi $P(\alpha)$ est valide.

Exercices

1. Montrer que LPO implique LLPO.
2. Tout sous-ensemble de $\{0, 1\}$ contient 0, 1 ou 2 éléments. Construisez un contre-exemple brouwerien pour cette affirmation.
3. Construisez un exemple brouwerien pour un ensemble d'entiers naturels qui ne contient pas de plus petit élément.
4. Construisez un exemple brouwerien pour un sous-groupe de $\mathbb{Z}$ qui n'est pas cyclique.
5. Construisez un exemple brouwerien de deux suites binaires dans la somme contient une infinité de 1, mais cependant aucune des deux ne contient une infinité de 1.
6. Dites qu'une assertion est **simplement existentielle** si elle est de la forme « il existe un entier n tel que $\alpha_n = 1$ » pour une certaine suite binaire α. Montrer que LLPO est équivalent à
   $$\neg(A \text{ et } B) \text{ si, et seulement si, } \neg A \text{ ou } \neg B$$
   pour toute paire d'assertions simplement existentielles A et B.
7. Le **petit principe d'omniscience faible** (**WLPO**) est l'affirmation selon laquelle, pour toute suite binaire, ou bien elle est identiquement nulle, ou bien il est impossible qu'elle soit identiquement nulle. Montrer que LPO implique WLPO et que WLPO implique LLPO.
8. Soit S l'ensemble des suites finies d'entiers strictement positifs. Par un **arbre finitaire** nous entendons un sous-ensemble T de S tel que

(i) pour chaque $s \in S$, $s \in T$ ou $s \notin T$,

(ii) si $(x_1, \ldots, x_n) \in T$, $(x_1, \ldots, x_{n-1}) \in T$,

(iii) pour tout $(x_1, \ldots, x_n) \in T$, il y a un $m \in \mathbb{N}$ tel que si $(x_1, \ldots, x_n, z) \in T$, alors $z \leqslant m$.

Une **branche infinie** de T est une suite $\{x_i\}_{i \in \mathbb{N}}$ d'entiers strictement positifs tels que $(x_1, \ldots, x_n) \in T$ pour chaque n. Le **lemme de Kőnig** affirme que si T est infini (s'il a des sous-ensembles arbitrairement grands), il a une branche infinie. Montrer que le lemme de Kőnig implique LLPO.

2 Ensembles, sous-ensembles, fonctions

Nous travaillons avec deux types de collections d'objets mathématiques, les ensembles et les catégories. Notre notion de ce qu'est un **ensemble** est une notion plutôt libérale.

Définition 2.1. Un ensemble S est défini lorsque nous décrivons comment construire ses éléments à partir d'objets déjà construits, ou qui pourraient l'avoir été, avant S lui-même, et lorsque nous expliquons ce que signifie pour deux éléments de S qu'ils sont égaux.

À la suite de Bishop nous regardons la **relation d'égalité** sur un ensemble comme conventionnelle : quelque chose à préciser lorsque l'ensemble est défini, et qui est soumis à la seule contrainte d'être une relation d'équivalence, c'est-à-dire d'être

réflexive : $a = a$,
symétrique : si $a = b$, alors $b = a$,
transitive : si $a = b$ et $b = c$, alors $a = c$.

Une **relation** n-aire sur un ensemble S est une propriété P qui concerne les n-uplets d'éléments de S, et qui est **extensionnelle** en ce sens que si $x_i = y_i$, pour $i = 1, \ldots, n$, alors $P(x_1, \ldots, x_n)$ si, et seulement si, $P(y_1, \ldots, y_n)$. Notez que l'égalité est une relation binaire en ce sens. La relation P est **décidable** si pour chaque n-uplet $x_1, \ldots, x_n$, ou bien $P(x_1, \ldots, x_n)$ est valide, ou bien elle ne l'est pas.

Une relation unaire P sur S définit un **sous-ensemble** $A = \{\, x \in S : P(x) \,\}$ de S : un élément de A est un élément de S qui satisfait la propriété P, et deux éléments de A sont égaux si, et seulement si, ils sont égaux comme éléments de S. Si A et B sont des sous-ensembles de S, et si chaque élément de A est un élément de B, nous disons que A est **contenu** dans B, et nous écrivons $A \subseteq B$. Deux sous-ensembles A et B d'un ensemble S sont **égaux** si $A \subseteq B$ et $B \subseteq A$; ceci est clairement une relation d'équivalence sur les sous-ensembles de S. Nous avons décrit comment construire un sous-ensemble de S, et ce que cela

signifie d'être égaux pour deux sous-ensembles de S. Donc nous avons défini l'ensemble tous les sous-ensembles, encore appelé l'**ensemble des parties** de S. Un sous-ensemble de S est **non vide** s'il contient un élément.

La **réunion** de deux sous-ensembles A et B de S est le sous-ensemble de S défini par $A \cup B = \{\, x \in S : x \in A \text{ ou } x \in B \,\}$. Le « ou » dans cette définition doit être interprété constructivement, de sorte que, étant donné un x dans $A \cup B$, nous puissions déterminer un des ensembles dans lequel il se trouve (même si nous ne pouvons savoir s'il est dans les deux à la fois). En termes d'existence, $x \in A \cup B$ signifie qu'il existe $i \in \{1, 2\}$ tel que si $i = 1$, alors $x \in A$, et si $i = 2$, alors $x \in B$. L'**intersection** de A et B est le sous-ensemble $A \cap B = \{\, x \in S : x \in A \text{ et } x \in B \,\}$.

Nous regardons la relation d'**inégalité** comme conventionnelle, comme n'étant pas nécessairement la négation de l'égalité ; l'interprétation du symbole $a \neq b$ dépendra du contexte. Sur chaque ensemble la relation de **non-égalité** est définie par $a \neq b$ si $a = b$ est impossible. Certains ensembles admettent une relation d'inégalité plus naturelle : si a et b sont des suites binaires, alors la bonne interprétation de $a \neq b$ est qu'il existe un n tel que $a_n \neq b_n$. Si l'on n'a pas spécifié une inégalité sur un ensemble, nous interprétons $a \neq b$ comme étant la non-égalité. Nous employons la terminologie usuelle concernant l'inégalité : dire que a et b sont **distincts** signifie $a \neq b$; dire que a est **non nul** signifie $a \neq 0$.

Une inégalité sur un ensemble peut être

consistante : $a \neq a$ est impossible ;
symétrique : si $a \neq b$, alors $b \neq a$;
cotransitive : si $a \neq c$, alors pour tout b, $a \neq b$ ou $b \neq c$;
étroite : si $a \neq b$ est impossible, alors $a = b$.

Nous voulons presque toujours qu'une inégalité soit symétrique parce que $a \neq b$ est supposée contenir l'idée que a et b sont distincts, ce qui devrait être une relation symétrique. Il est également naturel de demander la consistance, mais en pratique cette propriété est rarement nécessaire. Une inégalité symétrique, consistante et cotransitive est appelée une **relation de séparation** ; l'inégalité que nous avons décrite précédemment pour l'ensemble des suites binaires est une relation de séparation étroite, et il en va de même pour la relation d'inégalité standard sur les nombres réels (voir II.3). La non-égalité n'est pas nécessairement une relation de séparation, et elle n'est pas non plus nécessairement étroite.

On dit qu'une inégalité est **standard** si l'on peut démontrer qu'elle est équivalente à la relation de non-égalité en utilisant la loi du tiers exclu. Une inégalité étroite et consistante est standard parce que $\neg\neg(a \neq b)$ est équivalent à $\neg(a = b)$. La non-égalité est trivialement standard. Mise à part une importante exception (pour les anneaux locaux), nous serons intéressés uniquement par des inégalités standards. Il faut noter cependant que l'exigence qu'une inégalité soit standard possède très peu de contenu constructif : on ne peut même pas démontrer

que toute inégalité standard sur l'ensemble à un élément est consistante (une affirmation qui peut être réfutée en utilisant la loi du tiers exclu n'est pas nécessairement réfutable).

Un ensemble S avec une inégalité consistante est appelé **discret** si, étant donnés deux éléments a et b de S, on a $a = b$ ou $a \neq b$; si S n'a pas une inégalité spécifiée, nous disons que S est discret s'il est discret pour la relation de non-égalité. L'inégalité d'un ensemble discret est la non-égalité, et c'est une relation de séparation étroite. Cependant, l'affirmation selon laquelle un ensemble est discret ne fait pas à priori référence à la relation de non-égalité, mais plutôt à n'importe quelle inégalité qui arrive naturellement avec S : dire qu'un ensemble S de suites binaires est discret signifie que pour tous a et $b \in S$, ou bien $a = b$ ou bien il existe un n tel que $a_n \neq b_n$.

L'ensemble $\mathbb{Z}$ des entiers est discret. L'ensemble $\mathbb{Q}$ des nombres rationnels est également discret : un nombre rationnel est un couple d'entiers m/n avec $n \neq 0$, deux nombres rationnels m_1/n_1 et m_2/n_2 étant considérés comme égaux lorsque que $m_1 n_2 = m_2 n_1$. Un autre exemple d'ensemble discret est l'anneau $\mathbb{Z}_{12}$ des entiers modulo 12 : ses éléments sont des entiers et deux entiers sont considérés comme égaux lorsque leur différence est divisible par 12. Comme nous savons décider si un entier est divisible par 12 ou pas, l'ensemble $\mathbb{Z}_{12}$ est discret.

Si $x \in S$ et si A est un sous-ensemble de S, nous définissons $x \notin A$ comme signifiant que $x \neq a$ pour tout $a \in A$; si l'inégalité sur S est la non-égalité, ou si S n'a pas d'inégalité spécifiée, alors on a $x \notin A$ si, et seulement si, x ne peut pas appartenir à A. Le **complémentaire** de A dans S est l'ensemble $S \setminus A = \{\, x \in S : x \notin A \,\}$.

Un sous-ensemble A d'un ensemble S est **propre** s'il existe un élément x de S tel que $x \notin A$. Il est **détachable** si pour tout élément x de S on a $x \in A$ ou $x \notin A$.

Étant donnés des ensembles $S_1, S_2, \ldots, S_n$ nous définissons leur **produit cartésien** $S_1 \times S_2 \times \cdots \times S_n$ comme l'ensemble des n-uplets $(x_1, x_2, \ldots, x_n)$ où $x_i \in S_i$ pour chaque i. Deux tels n-uplets $(x_1, x_2, \ldots, x_n)$ et $(y_1, y_2, \ldots, y_n)$ sont égaux si $x_i = y_i$ pour chaque i. Les relations peuvent être identifiées avec les sous-ensembles de produits cartésiens : une relation binaire sur S est un sous-ensemble de $S \times S$.

Si A et B sont des ensembles, alors une **fonction** de A vers B est une règle qui fait correspondre à tout élément a de A un élément $f(a)$ de B, et qui est **extensionnelle** en ce sens que $f(a_1) = f(a_2)$ chaque fois que $a_1 = a_2$. Nous écrivons $f\colon A \to B$ pour indiquer que f est une fonction de A vers B. Deux fonctions f et g de A vers B sont **égales** si $f(a) = g(a)$ pour chaque $a \in A$. La **fonction identité** $f\colon A \to A$ est définie en posant $f(a) = a$ pour chaque $a \in A$. Pour construire une fonction de A vers B il suffit de construire un sous-ensemble S du produit cartésien $A \times B$ qui satisfait les propriétés

(i) pour chaque $a \in A$, il existe un $b \in B$ tel que $(a, b) \in S$,

(ii) si (a, b_1) et (a, b_2) sont des éléments de S, alors $b_1 = b_2$.

Dans l'interprétation calculatoire, l'algorithme pour la fonction provient de (i), qui spécifie la construction d'un élément b dépendant du paramètre a. En l'absence de (ii), cependant, l'algorithme implicite dans (i) n'est pas nécessairement extensionnel. Le fait qu'un sous-ensemble S de $A \times B$ qui satisfait (i) et (ii) détermine une fonction f telle que $(a, f(a)) \in S$ pour chaque $a \in A$ est connu comme l'**axiome du choix unique**.

Considérons une fonction f de A vers B. Nous disons que f est

injective [1] si $a_1 = a_2$ chaque fois que $f(a_1) = f(a_2)$,
surjective [2] si pour chaque $b \in B$ il existe un $a \in A$ tel que $f(a) = b$,
fortement extensionnelle si $a_1 \neq a_2$ chaque fois que $f(a_1) \neq f(a_2)$.

Notez que toute fonction entre deux ensembles munis de la non-égalité est fortement extensionnelle.

Si $S \subseteq A$, l'**image** de S par f est l'ensemble

$$f(S) = \{\, b \in B : b = f(a) \text{ pour un } a \in A \,\}.$$

Ainsi f est surjective si, et seulement si, $f(A) = B$. Si $S \subseteq B$, l'**image réciproque** de S par f est l'ensemble

$$f^{-1}(S) = \{\, a \in A : f(a) \in S \,\}.$$

Deux ensembles **ont la même cardinalité** si l'on a des fonctions f de A vers B, et g de B vers A telles que fg est la fonction identité sur B et gf est la fonction identité sur A ; nous disons que les fonctions f et g sont **inverses** l'une de l'autre, et que chacune est une **bijection**. Si A et B ont la même cardinalité, nous écrivons $\#A = \#B$. L'axiome du choix unique implique qu'une fonction qui est à la fois injective et surjective est une bijection (exercice 6). En mathématiques classiques on pense à des ensembles de même cardinalité simplement comme à des ensembles qui ont la même *taille* ; d'un point de vue constructif il est plus exact d'y penser comme à des ensembles qui ont la même *structure*. Quand nous parlons de la **cardinalité** d'un ensemble nous entendons l'ensemble lui-même en ignorant toute structure autre que l'égalité qu'il pourrait avoir. La distinction entre parler d'un ensemble et parler de sa cardinalité est avant tout une question d'intention : quand nous parlons de sa cardinalité nous ne voulons prêter aucune attention à toutes caractéristiques de l'ensemble qui ne seraient pas partagées par tous les ensembles qui ont la même cardinalité. Par exemple si x est un élément d'un groupe, alors l'ensemble $S = \{1, x, x^2, x^3, \ldots\}$

1. **NdT.** One-to-one.
2. **NdT.** Onto. Dans le livre anglais, « onto » est utilisé soit comme adjectif, dans le sens de « surjectif », soit comme préposition dans le sens usuel de « sur » : une fonction de A sur B est une fonction de A vers B qui est surjective.

est le sous-monoïde engendré par x, tandis que la cardinalité de S est l'ordre de x. C'est comme la distinction entre être une fraction et être un nombre rationnel. Une manière usuelle pour traiter ce genre de situation est d'introduire les *classes d'équivalence* mais, à la suite de Bishop (1967), nous préférons traiter directement avec la relation d'équivalence et ne pas introduire de nouvelles entités bien encombrantes.

Si un ensemble A possède la même cardinalité que $\{1, \ldots, n\}$ (est vide si $n = 0$) pour un entier naturel n, alors nous disons que A est un **ensemble à n éléments**, ou que A est de cardinalité n, et nous écrivons $\#A = n$. Un ensemble **fini** A est un ensemble discret qui a la cardinalité n pour un entier naturel n. Rappelons qu'un ensemble discret doit être discret pour son inégalité spécifiée, s'il y en a une, de sorte qu'un ensemble peut avoir une cardinalité finie sans être fini ; de tels ensembles sont quelque peu pathologiques, ce qui est la raison pour laquelle nous préférons les nommer de manière plus longue.

Un ensemble A est **finiment énumérable** s'il est vide ou s'il existe une fonction de $\{1, \ldots, n\}$ sur A. Notez qu'un ensemble finiment énumérable est discret si, et seulement si, il est fini. Nous disons que A **possède au plus n éléments** si chaque fois que $a_0, \ldots, a_n \in A$, il existe des éléments $0 \leqslant i < j \leqslant n$ tels que $a_i = a_j$. Un ensemble est **borné en nombre**, ou **borné**,s'il a au plus n éléments pour un certain n. Un ensemble est **infini** s'il contient des sous-ensembles finis arbitrairement grands.

Un ensemble A est **dénombrable** [1] s'il existe une fonction depuis un sous-ensemble détachable de l'ensemble des entiers naturels sur A. Ainsi l'ensemble vide est dénombrable, de même que l'ensemble des nombres parfaits impairs. Les ensembles dénombrables non vides sont les images de fonctions définies sur l'ensemble des entiers strictement positifs, de sorte que leurs éléments peuvent être énumérés (éventuellement avec des répétitions) sous la forme $a_1, a_2, \ldots$.

Une **suite** d'éléments d'un ensemble A, ou une **suite dans** A, est une fonction depuis l'ensemble des entiers naturels $\mathbb{N}$ vers A. Nous dirons également que les fonctions depuis les entiers strictement positifs sont des suites.

Une **famille d'éléments** de A, **indexée par** un ensemble I, est une fonction f de I vers A ; l'image de i dans A par f est habituellement notée f_i plutôt que $f(i)$. Ainsi une suite est une famille indexée par les entiers naturels $\mathbb{N}$.

Une **famille finie d'éléments** de A est une famille d'éléments de A indexée par $\{1, \ldots, n\}$ pour un entier strictement positif n.

Si $\{A_i\}_{i \in I}$ est une famille de sous-ensembles de S, alors sa **réunion** est définie par $\bigcup_{i \in I} A_i = \{\, x \in S : \text{il existe un } i \in I \text{ tel que } x \in A_i \,\}$, et son **intersection** est définie par $\bigcap_{i \in I} A_i = \{\, x \in S : x \in A_i \text{ pour tout } i \in I \,\}$.

Si S est un ensemble muni d'une inégalité et si X est un ensemble, alors l'ensemble S^X des fonctions de X vers S hérite depuis S de l'inégalité obtenue en posant $f \neq g$ s'il existe un $x \in X$ tel que $f(x) \neq g(x)$.

1. **NdT.** Countable.

Théorème 2.2. *Soit S un ensemble muni d'une inégalité et soit X un ensemble. Si l'inégalité sur S est consistante, symétrique, cotransitive, ou étroite, alors il en va de même, respectivement, pour l'inégalité sur S^X.*

Démonstration. La consistance et la symétrie sont claires. Supposons que l'inégalité sur S est étroite. Si $f_1 \neq f_2$ est impossible, alors il ne peut pas exister de $x \in S$ tel que $f_1(x) \neq f_2(x)$. Ainsi, étant donné x, il est impossible que $f_1(x) \neq f_2(x)$, donc $f_1(x) = f_2(x)$ pour chaque x, et par suite $f_1 = f_2$. Supposons maintenant que l'inégalité sur S est cotransitive. Si $f_1 \neq f_3$, alors pour un certain x nous avons $f_1(x) \neq f_3(x)$ de sorte que $f_1(x) \neq f_2(x)$ ou $f_2(x) \neq f_3(x)$ et donc $f_1 \neq f_2$ ou $f_2 \neq f_3$. □

Pour illustrer le théorème 2.2, prenons pour S l'ensemble discret $\{0, 1\}$ et pour X l'ensemble des entiers naturels. Alors S^X est l'ensemble des suites binaires. Comme $\{0, 1\}$ est discret, l'inégalité sur $\{0, 1\}$ est une relation de séparation consistante étroite, par suite l'inégalité sur l'ensemble des suites binaires est aussi une relation de séparation consistante étroite. Cependant, si l'ensemble des suites binaires était discret, nous pourrions démontrer LPO.

Exercices

1. Donner un exemple (pas un exemple brouwerien) d'une relation de séparation consistante qui ne soit pas étroite.
2. Montrer que l'ensemble des suites binaires est discret si, et seulement si, LPO est valide.
3. *Une non-égalité qui n'est pas une relation de séparation.* Soit A l'ensemble des suites binaires. Pour x et $y \in A$ on dit que $x = y$ s'il existe un entier N tel que $x_n = y_n$ pour tout $n \geqslant N$, et l'on note $x \neq y$ la non-égalité correspondante. Montrer que si cette inégalité est une relation de séparation, alors on a WLPO ; montrer que si c'est une relation de séparation étroite, alors on a LPO.
4. *Un problème de négations.* Une **relation de différence** est une inégalité symétrique telle que l'une de ces conditions soit vérifiée :

   (i) $x \neq z$ implique $\neg(\neg x \neq y$ et $\neg y \neq z)$

   (ii) $\neg x \neq y$ et $\neg y \neq z$ implique $\neg x \neq z$

   (iii) $x \neq z$ et $\neg x \neq y$ implique $\neg\neg y \neq z$.

   Montrer que ces conditions sont équivalentes et qu'une relation de séparation est une relation de différence.
5. Définir une relation de séparation étroite naturelle sur l'ensemble des parties détachables d'un ensemble. Montrer qu'un sous-ensemble A d'un

ensemble S est détachable si, et seulement si, il possède une **fonction caractéristique**, c'est-à-dire une fonction f de S vers $\{0,1\}$ telle que

$$A = \{\, s \in S : f(s) = 1 \,\}.$$

6. Montrer qu'une fonction est une bijection si, et seulement si, elle est à la fois surjective et injective.
7. Montrer qu'un ensemble finiment énumérable discret est fini. Construire un exemple brouwerien d'un ensemble finiment énumérable, avec une relation de séparation étroite, qui n'est pas fini. Montrer qu'un ensemble finiment énumérable est borné en nombre. Construire un exemple brouwerien d'un ensemble borné en nombre mais qui n'est pas finiment énumérable.
8. Montrer qu'un ensemble non vide A est dénombrable si, et seulement si, il existe une fonction de $\mathbb{N}$ sur A. Montrer qu'un ensemble discret est dénombrable si, et seulement si, il a la même cardinalité qu'un sous-ensemble détachable de $\mathbb{N}$.
9. Montrer qu'un sous-ensemble A de $\mathbb{N}$ est dénombrable si, et seulement si, il existe un sous-ensemble détachable S de $\mathbb{N} \times \mathbb{N}$ tel que $A = \pi S$, où π est la projection de $\mathbb{N} \times \mathbb{N}$ sur son premier facteur.
10. Montrer que l'ensemble des fonctions depuis un ensemble borné discret A vers $\{0,1\}$ n'est pas nécessairement discret. (Suggestion : soit A l'image d'une suite binaire).
11. Montrer que si un ensemble S est borné en nombre, alors toute fonction injective de S vers S est surjective.
12. Donner un exemple brouwerien d'un sous-ensemble A de $\mathbb{N}$ tel que A ne peut pas être fini, et cependant A n'est pas infini.
13. Soit S un ensemble non vide muni d'une relation de séparation, et soit n un entier strictement positif. Montrer que les propriétés suivantes sont équivalentes.

    (i) Il existe des éléments $x_0, \ldots, x_n$ de S tels que $x_i \neq x_j$ pour $i \neq j$.

    (ii) Étant donnés des éléments $y_1, \ldots, y_n$ de S, il existe un $z \in S$ tel que $z \neq y_i$ pour $i = 1, \ldots, n$.

14. On dit qu'un ensemble avec inégalité est **Dedekind-infini** lorsqu'il est isomorphe, en tant qu'ensemble avec inégalité, à un sous-ensemble propre de lui-même. Montrer qu'un ensemble Dedekind-infini satisfait la propriété (i) de l'exercice 13 pour chaque n.
15. On dit qu'un ensemble S est **ω-borné** lorsque, pour chaque suite $\{s_i\}$ dans S, il existe un $m \neq n$ tel que $s_m = s_n$. Montrer que si S est un

ensemble ω-borné, si $\{s_i\}$ est une suite dans S et si m est un entier strictement positif, alors il existe un ensemble fini I formé de m entiers strictement positifs tel que $s_i = s_j$ pour i et $j \in I$. Montrer que si A et B sont des ensembles ω-bornés discrets, alors il en va de même pour l'ensemble $A \times B$.

3 L'axiome du choix

L'axiome du choix affirme l'existence d'une fonction qui possède une certaine propriété, en conséquence sa validité sera probablement plus douteuse en mathématiques constructives, où les fonctions doivent être interprétées comme des algorithmes. Nous formulons l'axiome du choix comme suit :

> **Axiome du choix.** *Soient A et B des ensembles, et S un sous-ensemble de $A \times B$ tel que pour tout $a \in A$ on a un $b \in B$ tel que $(a, b) \in S$. Alors il existe une fonction $f\colon A \to B$ telle que $(a, f(a)) \in S$ pour chaque $a \in A$.*

L'axiome du choix peut être critiqué de deux manières d'un point de vue calculatoire. La première objection concerne le fait que nous puissions trouver un *algorithme* f (non nécessairement extensionnel) avec la propriété requise. Nous avons déjà rencontré ce problème avec l'axiome du choix unique, et nous avons adopté la position selon laquelle un algorithme est inhérent à l'interprétation de la phrase « pour tout $a \in A$ il existe un $b \in B$ ».

Une objection plus sérieuse est que même si nous pouvons trouver un algorithme f nous ne pouvons sans doute pas trouver une *fonction*. En fait, nous pouvons construire un contre-exemple brouwerien pour l'axiome du choix.

Exemple 3.1. Soit α une suite binaire et soit $A = \{x, y\}$ muni de l'inégalité obtenue en posant $x = y$ si, et seulement si, il existe un n tel que $\alpha_n = 1$, et enfin soit $B = \{0, 1\}$. Considérons le sous-ensemble $S = \{(x, 0), (y, 1)\}$ de $A \times B$. Supposons que $f\colon A \to B$ satisfasse $(a, f(a)) \in S$ pour chaque $a \in A$. Si $f(x) = f(y)$, alors $\alpha_n = 1$ pour un n ; si $f(x) \neq f(y)$, alors $\alpha_n = 0$ pour tout n. □

Il y a deux versions affaiblies de l'axiome du choix qui sont communément acceptées en mathématiques constructives. La plus faible est la suivante.

> **Axiome du choix dénombrable.** *Il s'agit de l'axiome du choix lorsque l'on prend pour A l'ensemble $\mathbb{N}$ des entiers naturels.*

Si A est l'ensemble des entiers naturels, il n'y a pas de réelle distinction entre un algorithme et une fonction dans l'interprétation calculatoire car chaque entier naturel a une représentation canonique. En conséquence cet axiome résulte de l'interprétation de la phrase « pour tout $a \in A$ il existe un $b \in B$ » comme

signifiant l'existence d'un algorithme qui transforme tout élément de A en un élément de B.

Une version plus forte que l'axiome du choix dénombrable est la suivante.

> **Axiome du choix dépendant.** *Soient A un ensemble non vide et R un sous-ensemble de $A \times A$ tels que pour chaque $a \in A$ on ait un élément $a' \in A$ avec $(a, a') \in R$. Alors il existe une suite $a_0, a_1, \ldots$ d'éléments de A telle que $(a_i, a_{i+1}) \in R$ pour chaque i.*

L'axiome du choix dépendant implique l'axiome du choix dénombrable de la manière suivante. Supposons que S est un sous-ensemble de $\mathbb{N} \times B$ tel que pour chaque $n \in \mathbb{N}$ on a un élément $b \in B$ tel que $(n, b) \in S$. Soit A l'ensemble formé des suites finies $b_0, b_1, \ldots, b_m$ dans B telles que $(i, b_i) \in S$ pour tout i, et soit R l'ensemble formé par tous les couples (α, α') d'éléments de A tels que, en supprimant le dernier élément de α', on obtienne α. L'axiome du choix dépendant appliqué à R fournit une suite dans A dont les derniers éléments sont la suite requise dans B.

L'argument en faveur de l'axiome du choix dépendant est essentiellement le même que celui pour le choix dénombrable. Nous utiliserons librement ces deux axiomes, même si en général nous signalerons les moments où nous les utilisons.

Nous aurons l'occasion de nous référer à la forme suivante de l'axiome du choix pour laquelle nous n'avons pas de contre-exemple brouwerien, même si nous pensons que cette variante faible n'est pas démontrable dans le contexte des mathématiques constructives.

> **Axiome du choix le plus simple du monde.** *Soit A un ensemble d'ensembles à deux éléments tel que si $a_1 \in A$ et $a_2 \in A$, alors $a_1 = a_2$. Alors il existe une fonction f de A vers $\{\, x : x \in a \text{ pour un } a \in A \,\}$ tel que $f(a) \in a$ pour chaque $a \in A$.*

Exercices

1. Modifier l'exemple 3.1 de façon à montrer que l'axiome du choix implique la loi du tiers exclu.
2. Montrer que LLPO, avec l'axiome du choix dépendant, implique le lemme de Kőnig (voir l'exercice 1.7).
3. Montrer que l'axiome du choix implique l'axiome du choix le plus simple du monde.
4. Un ensemble P est dit **projectif** lorsque chaque fois que l'on a deux applications $\pi\colon A \to B$ surjective et $f\colon P \to B$, il existe une application $g\colon P \to A$ telle que $\pi g = f$. Montrer que les ensembles finis sont projectifs. Montrer que les ensembles dénombrables discrets sont projectifs si, et seulement si, l'axiome du choix dénombrable est valide. Montrer que si les ensembles discrets sont projectifs, alors l'axiome du choix le plus simple du monde est valide.

4 Catégories

La collection des suites binaires forme un ensemble parce que nous savons ce que signifie pour deux suites binaires le fait d'être égales. Par ailleurs étant donnés deux groupes, ou deux ensembles, il est en général incorrect de demander s'ils sont égaux ; la question pertinente est de savoir s'ils sont ou ne sont pas isomorphes, ou plus généralement quels sont les morphismes entre eux.

Une **catégorie** est une collection d'objets (comme l'est un ensemble). Une relation d'égalité sur un ensemble construit, pour deux objets a et b de cet ensemble, une *proposition* « $a = b$ ». Pour spécifier une catégorie $\mathcal{C}$, nous devons montrer comment construire, pour deux objets A et B de $\mathcal{C}$, un *ensemble* $\mathcal{C}(A, B)$. Dans les catégories concrètes, les objets de $\mathcal{C}$ sont des structures mathématiques d'un certain type, et l'ensemble $\mathcal{C}(A, B)$ est l'ensemble des applications de A vers B qui respectent cette structure : si $\mathcal{C}$ est la catégorie des ensembles, alors $\mathcal{C}(A, B)$ est l'ensemble des fonctions de A vers B ; si $\mathcal{C}$ est la catégorie des groupes, alors $\mathcal{C}(A, B)$ est l'ensemble des homomorphismes de A vers B. De manière plus générale nous appellerons **flèche** ou **morphisme** un élément de l'ensemble $\mathcal{C}(A, B)$.

La notion de composition d'applications, présente dans ces situations concrètes, est abstraite sous la forme suivante dans les catégories plus générales : chaque fois que nous avons trois objets A, B et C dans une catégorie $\mathcal{C}$, nous devons avoir une fonction de $\mathcal{C}(A, B) \times \mathcal{C}(B, C)$ vers $\mathcal{C}(A, C)$, appelée **composition** et notée par la juxtaposition, et nous devons avoir aussi un élément $1_B \in \mathcal{C}(B, B)$, tels que si $f \in \mathcal{C}(C, D)$, $g \in \mathcal{C}(B, C)$ et $h \in \mathcal{C}(A, B)$, les propriétés suivantes sont satisfaites.

(i) $1_B h = h$ et $g1_B = g$,

(ii) $(fg)h = f(gh)$.

Tout ensemble S peut être considéré comme une catégorie en posant

$$S(a, b) = \{\, x \in \{0\} : a = b \,\}.$$

La réflexivité de l'égalité donne l'élément 1_B, et la transitivité donne l'item (ii).

Les ensembles et fonctions introduites dans les sections précédentes constituent une catégorie : les **objets** de cette catégorie sont les ensembles et les **flèches** sont les fonctions entre ensembles. Nous pouvons aussi considérer la catégorie dont les objets sont les ensembles avec inégalité et dont les flèches sont les fonctions fortement extensionnelles.

L'idée de la théorie des catégories est d'oublier la structure interne des objets et de se concentrer sur la manière dont les flèches se combinent par composition. Par exemple, une fonction f de A vers B est injective si $a_1 = a_2$ chaque fois que $f(a_1) = f(a_2)$. Cette définition s'appuie sur la structure interne des ensembles A et B, c'est-à-dire sur les éléments de ces ensembles et les relations d'égalité sur

ces ensembles. La propriété catégorique qui correspond au fait qu'une fonction f est injective est la suivante : si g et h sont des flèches depuis n'importe quel ensemble C vers A et si $fg = fh$, alors $g = h$; c'est-à-dire f est **simplifiable à gauche** (on dit aussi **régulier à gauche**). Le fait qu'une fonction f est injective si, et seulement si, elle est simplifiable à gauche, est une démonstration purement routinière.

Une fonction f de A vers B est surjective si pour chaque $b \in B$ il existe un $a \in A$ tel que $f(a) = b$. La propriété catégorique correspondante est que f est **simplifiable à droite**, c'est-à-dire que si g et h sont des flèches de B vers n'importe quel ensemble C et si $gf = hf$, alors $g = h$. Le fait qu'une fonction f est surjective si, et seulement si, elle est simplifiable à droite, est une démonstration moins routinière que la démonstration du résultat correspondant pour les flèches simplifiables à la gauche.

Théorème 4.1. *Une fonction est simplifiable à droite dans la catégorie des ensembles si, et seulement si, elle est surjective.*

Démonstration. Supposons que $f\colon A \to B$ est surjective et que $gf = hf$. Pour tout $b \in B$ il existe un $a \in A$ tel que $f(a) = b$. Donc $g(b) = g(f(a)) = h(f(a)) = h(b)$, et $g = h$. Réciproquement supposons que $f\colon A \to B$ est simplifiable à droite, et soit Ω l'ensemble des sous-ensembles de $\{0\}$. Définissons $g\colon B \to \Omega$ par $g(b) = \{0\}$ pour tout b, et définissons $h\colon B \to \Omega$ par

$$h(b) = \{\, x \in \{0\} : b = f(a) \text{ pour un } a \,\}.$$

Donc $h(b)$ est le sous-ensemble de $\{0\}$ tel que $0 \in h(b)$ si, et seulement si, il existe un a tel que $b = f(a)$. Clairement $gf = hf$ est la fonction qui fait correspondre à tout élément de A le sous-ensemble $\{0\}$. Donc $g = h$, et par suite $0 \in h(b)$, ce qui signifie que $b = f(a)$ pour un a. □

Un **isomorphisme** entre deux objets A et B d'une catégorie $\mathcal{C}$ est un élément f de $\mathcal{C}(A, B)$ tel qu'il existe un $g \in \mathcal{C}(B, A)$ pour lequel on a $fg = 1_B$ et $gf = 1_A$. La flèche g est appelée l'**inverse** de f ; on montre facilement que g est unique. Une bijection entre ensembles est un isomorphisme dans la catégorie des ensembles. Nous disons que A et B sont **isomorphes**, et nous écrivons $A \simeq B$ s'il y a un isomorphisme entre A et B.

Nous serons surtout intéressés par les catégories dont les objets sont les ensembles munis d'une structure algébrique, et dans lesquelles les flèches sont les fonctions qui préservent la structure algébrique. Dans ce cas les flèches sont appelées des **homomorphismes**. Si un homomorphisme est injectif, on l'appelle un **monomorphisme** ; s'il est surjectif on l'appelle un **épimorphisme** [1].

1. **NdT.** Les épimorphismes au sens catégorique habituel sont les flèches simplifiables à droite. Dans la catégorie des anneaux commutatifs ils ne sont pas tous surjectifs. Le mot « épimorphisme » ici est donc pris dans un sens plus restreint, correspondant à une structure quotient dans les catégories données avec un foncteur d'oubli vers la catégorie des ensembles.

Un homomorphisme d'un objet vers lui-même est appelé un **endomorphisme**, et un endomorphisme qui est un isomorphisme est appelé un **automorphisme**.

Un **foncteur** T depuis une catégorie $\mathcal{A}$ vers une catégorie $\mathcal{B}$ est une règle qui fait correspondre à tout objet $A \in \mathcal{A}$ un objet $T(A) \in \mathcal{B}$, et qui à chaque flèche $f \in \mathcal{A}(A_1, A_2)$ fait correspondre une flèche $T(f) \in \mathcal{B}(T(A_1), T(A_2))$, telle que

(i) $T\colon \mathcal{A}(A_1, A_2) \to \mathcal{B}(T(A_1), T(A_2))$ est une fonction,

(ii) $T(fg) = T(f)T(g)$,

(iii) $T(1_A) = 1_{T(A)}$.

Un foncteur entre deux ensembles, lorsqu'on les considère comme des catégories, est simplement une fonction. Notons que si f est un isomorphisme, alors il en va de même pour $T(f)$.

En utilisant la notion de foncteur nous pouvons étendre notre définition d'une famille d'éléments dans un ensemble à celle d'une famille d'objets dans une catégorie $\mathcal{C}$. Soit I un ensemble. Une **famille** A **d'objets de** $\mathcal{C}$ **indexée par** I est un foncteur depuis I, vu comme une catégorie, vers la catégorie $\mathcal{C}$. Nous notons souvent une telle famille par $\{A_i\}_{i\in I}$. Si $i = j$, la flèche de A_i vers A_j est notée A^i_j, et c'est un isomorphisme.

Un élément de la **réunion disjointe** d'une famille d'ensembles $\{A_i\}_{i\in I}$ est un couple (i, x) tel que $i \in I$ et $x \in A_i$. Deux éléments (i, x) et (j, y) de la réunion disjointe sont **égaux** si $i = j$ et $A^i_j(x) = y$. Nous identifions A_i avec le sous-ensemble $\{\, (i, x) : x \in A_i \,\}$ de la réunion disjointe. Ainsi, une fois construite la réunion disjointe, nous pouvons considérer la famille $\{A_i\}_{i\in I}$ comme une famille d'éléments de l'ensemble des parties de la réunion disjointe.

Soit $\{A_i\}_{i\in I}$ une famille d'ensembles et soit P un ensemble. Alors une fonction de P vers A_i peut être identifiée avec une fonction f de P vers la réunion disjointe de la famille $\{A_i\}_{i\in I}$ telle que $f(P) \subseteq A_i$. Notons F l'ensemble des fonctions f de P vers la réunion disjointe des $\{A_i\}_{i\in I}$ telles que $f(P) \subseteq A_i$ pour un $i \in I$. Une **famille de fonctions** π_i **de** P **vers les** A_i est par définition une famille π d'éléments de F telle que $\pi_i(P) \subseteq A_i$ pour chaque $i \in I$.

Soit $\{A_i\}_{i\in I}$ une famille d'objets dans une catégorie $\mathcal{C}$. Un **produit catégorique** de la famille $\{A_i\}$ est un objet P avec une famille $\{\pi_i\}_{i\in I}$ de flèches (appelées projections) de P vers A_i telles que pour chaque objet S et chaque famille de flèches f_i de S vers A_i, il existe une unique flèche f de S vers P telle que $\pi_i f = f_i$ pour chaque $i \in I$. Un produit catégorique est unique à un isomorphisme près en ce sens que si (P', π') en est un autre, alors il existe un (unique) isomorphisme θ de P vers P' tel que $\pi'_i\theta = \pi_i$ pour chaque i. Si $\mathcal{C}$ est la catégorie des ensembles, on vérifie facilement que l'ensemble de toutes les fonctions λ de I vers la réunion disjointe de la famille $\{A_i\}_{i\in I}$ telles que $\lambda(i) \in A_i$ pour chaque i, avec $\pi_i(\lambda)$ définie comme étant $\lambda(i)$, est un produit catégorique des A_i : nous le considérons comme *le* produit des A_i et nous le notons $\prod_{i\in I} A_i$.

Si $I = \{1, \ldots, n\}$, le produit des ensembles A_i est le produit cartésien $A_1 \times \cdots \times A_n$. Si $A_i = S$ pour chaque $i \in I$, nous écrivons le produit, qui est l'ensemble des fonctions de I vers S, sous la forme S^I, ou S^n si $I = \{1, \ldots, n\}$.

Exercices

1. Montrer qu'une fonction f est injective si, et seulement si, elle est simplifiable à gauche.
2. Montrer que le produit catégorique d'une famille d'objets dans une catégorie est unique à un isomorphisme près.
3. Montrer que, dans la catégorie des ensembles, l'ensemble de toutes les fonctions λ de I vers la réunion disjointe de la famille $\{A_i\}_{i\in I}$, telles que $\lambda(i) \in A_i$ pour chaque i, est un produit catégorique des $\{A_i\}_{i\in I}$.
4. Soit I l'ensemble des suites binaires, et, pour chaque $i \in I$, soit $A_i = \{\, x \in \{0,1\} : x \geqslant i_j \text{ pour tout } j \,\}$. Montrer que l'application naturelle de $\prod_i A_i$ vers A_0 est surjective si, et seulement si, WLPO est valide.
5. Considérons la catégorie des ensembles avec inégalité, avec pour flèches les fonctions fortement extensionnelles. Montrer que le produit $\prod_i A_i$ dans cette catégorie est le produit dans la catégorie des ensembles muni de l'inégalité définie par $\lambda \neq \mu$ s'il existe un i tel que $\lambda(i) \neq \mu(i)$. Généraliser le théorème 2.2 dans ce contexte.
6. Soit a un objet dans une catégorie $\mathcal{A}$. Montrer comment $T(b) = \mathcal{A}(a, b)$ est un foncteur de $\mathcal{A}$ vers la catégorie des ensembles. Un tel foncteur T est appelé un foncteur **représentable**.
7. Si $\mathcal{C}$ est une catégorie, alors la **catégorie duale** $\mathcal{C}'$ est définie comme ayant les mêmes objets que $\mathcal{C}$, mais $\mathcal{C}'(a, b) = \mathcal{C}(b, a)$. Le **coproduit** d'une famille d'objets de $\mathcal{C}$ est le produit dans la catégorie duale $\mathcal{C}'$. Décrire de manière directe le coproduit. Quel est le coproduit dans la catégorie des ensembles ?
8. *Limites directes.* Un **système direct** est une suite d'objets A_n et de flèches $f_n \colon A_n \to A_{n+1}$. Une borne supérieure d'un système direct est un objet B avec des flèches $b_n \colon A_n \to B$ telles que $b_{n+1} f_n = b_n$ pour chaque n. Une **limite directe** d'un système direct est une borne supérieure L telle que, pour n'importe quelle borne supérieure B, on a une unique flèche $\mu \colon L \to B$ telle que $\mu \ell_n = b_n$ pour chaque n.

   (i) Montrer que deux limites directes sont isomorphes.

   (ii) Montrer que la limite directe dans la catégorie des ensembles est la réunion disjointe des A_n avec l'égalité engendrée par les égalités $a = f_n(a)$ pour chaque $a \in A_n$.

(iii) Montrer qu'une limite directe d'ensembles discrets n'est pas nécessairement un ensemble discret, mais qu'il est discret si toutes les fonctions sont injectives.

5 Ensembles ordonnés et treillis

Un **ensemble (partiellement) ordonné** est un ensemble P muni d'une relation $a \leqslant b$ telle que :

(i) $a \leqslant a$,

(ii) si $a \leqslant b$ et $b \leqslant c$, alors $a \leqslant c$,

(iii) si $a \leqslant b$ et $b \leqslant a$, alors $a = b$.

Un **morphisme** entre deux ensembles ordonnés P_1 et P_2 est une fonction f de P_1 vers P_2 telle que si $a \leqslant b$, alors $f(a) \leqslant f(b)$. Nous serons la plupart du temps intéressés par les ensembles ordonnés discrets ; dans ce cas nous écrirons $a < b$ pour $a \leqslant b$ et $a \neq b$.

Soient a, b et c des éléments d'un ensemble ordonné P. Nous disons que c est la **borne inférieure**, ou l'**infimum**, de a et b, et nous écrivons $c = a \wedge b$, lorsque pour chaque $x \in L$ nous avons $x \leqslant c$ si, et seulement si, $x \leqslant a$ et $x \leqslant b$. On voit facilement qu'un tel c est unique, s'il existe. De même $c = a \vee b$ est la **borne supérieure**, ou le **supremum**, de a et b si pour chaque $x \in L$ nous avons $c \leqslant x$ si, et seulement si, $a \leqslant x$ et $b \leqslant x$.

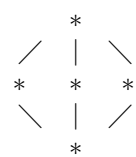
Un **treillis** est un ensemble ordonné dans lequel deux éléments arbitraires ont un infimum et un supremum. Si S est un ensemble, alors l'ensemble de tous les sous-ensembles de S, ordonné par inclusion, forme un treillis : le supremum de A et B est $A \cup B$ et l'infimum est $A \cap B$. L'ensemble des entiers strictement positifs, ordonné en posant $a \leqslant b$ si b est un multiple de a, est un treillis : le supremum de a et b est leur plus petit commun multiple, l'infimum est leur plus grand commun diviseur. Notez que la relation $a \leqslant b$ est décidable dans un treillis discret parce qu'elle est équivalente à $a \wedge b = a$.

Si un treillis admet un plus petit élément, alors nous notons cet élément 0 ; s'il admet un plus grand élément, nous le notons 1.

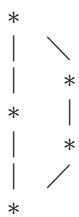
Un treillis est **distributif** lorsqu'il satisfait l'identité

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c).$$

Le treillis des sous-ensembles d'un ensemble est distributif. Le treillis ci-dessous avec cinq éléments n'est pas distributif.



Un treillis est **modulaire** si $a \vee (b \wedge c) = b \wedge (a \vee c)$ chaque fois que $a \leqslant b$. On voit facilement qu'un treillis distributif est modulaire ; le treillis non distributif à cinq éléments décrit précédemment est modulaire. Si G est un groupe abélien fini, alors l'ensemble de ses sous-groupes finis est un treillis modulaire, il est distributif seulement si G est cyclique. Plus généralement l'ensemble des sous-modules d'un R-module forme un treillis modulaire. Le plus simple des treillis non modulaires est le treillis à cinq éléments décrit ci-dessous.



Si $a \leqslant b$ dans un ensemble ordonné P, alors nous utilisons la notation d'intervalle $[a, b]$ pour indiquer l'ensemble $\{ x \in P : a \leqslant x \leqslant b \}$. Si P est un treillis alors $[a, b]$ est un treillis avec les mêmes suprema et infima que dans P. Un fait essentiel à propos des treillis modulaires est que $[a \wedge d, d]$ et $[a, a \vee d]$ sont des treillis isomorphes, pour n'importe quels éléments a et d. Nous démontrons ce fait sous une forme légèrement déguisée.

Lemme 5.1. *Soient $a \leqslant b$ et $c \leqslant d$ des éléments d'un treillis modulaire L. Définissons*

$$f(x) = a \vee (b \wedge x) = b \wedge (a \vee x)$$

$$g(y) = c \vee (d \wedge y) = d \wedge (c \vee y).$$

Alors la fonction g envoie l'intervalle $[f(c), f(d)]$ isomorphiquement sur l'intervalle $[g(a), g(b)]$ avec f pour fonction inverse.

Démonstration. Il suffit de démontrer que si $c \leqslant x \leqslant d$, alors $fgf(x) = f(x)$. Nous pouvons écrire $fgf(x)$ sous la forme

$$fgf(x) = b \wedge (a \vee c \vee (d \wedge b \wedge (a \vee x))) \qquad (*)$$

ou encore sous la forme

$$fgf(x) = a \vee (b \wedge d \wedge (c \vee a \vee (b \wedge x))). \qquad (**)$$

Pour montrer que $f(x) \leqslant fgf(x)$, nous utilisons $(*)$ et $f(x) = a \vee (b \wedge x)$. Pour montrer que $fgf(x) \leqslant f(x)$, nous utilisons $(**)$ et $f(x) = b \wedge (a \vee x)$. □

En prenant $b = a \vee d$ et $c = a \wedge d$ dans le lemme 5.1 nous voyons que $[a \wedge d, d]$ et $[a, a \vee d]$ sont isomorphes.

Un sous-ensemble C d'un ensemble ordonné P est appelé une **chaine** si pour chaque a et $b \in C$, on a $a \leqslant b$ ou $b \leqslant a$; si P lui-même est une chaine, nous disons que P est **totalement ordonné** [1]. Une **chaine maximale** dans un ensemble ordonné est une chaine C telle que $C \cup \{a\}$ est une chaine seulement si $a \in C$. Le treillis non modulaire le plus simple défini précédemment contient deux chaines maximales finies, l'une de longueur 2 et l'autre de longueur 3. Pour les treillis modulaires ceci ne peut pas se produire. Nous disons que deux ensembles totalement ordonnés C et D sont **isomorphes par morceaux** s'il existe des éléments $c_1, \dots, c_n$ et $d_1, \dots, d_n$ tels que

(i) $\{\, x \in C : x \leqslant c_1 \,\}$ est isomorphe à $\{\, x \in D : x \leqslant d_1 \,\}$,

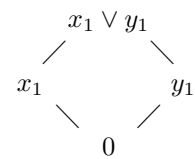
(ii) $\{\, x \in C : x \geqslant c_n \,\}$ est isomorphe à $\{\, x \in D : x \geqslant d_n \,\}$,

(iii) il existe une permutation σ de $\{1, \dots, n-1\}$ telle que $[c_i, c_{i+1}]$ est isomorphe à $[d_{\sigma i}, d_{1+\sigma i}]$ pour chaque $i < n$.

Nous laissons la preuve que la relation d'isomorphisme par morceaux est transitive en exercice (n° 4). Si C et D sont des ensembles totalement ordonnés discrets isomorphes par morceaux, alors C et D ont la même cardinalité (exercice 5).

Théorème 5.2 (Jordan-Hölder-Dedekind)**.** *Si un treillis modulaire contient une chaine maximale finiment énumérable X, alors toute chaine finiment énumérable est contenue dans une chaine maximale finiment énumérable qui est isomorphe par morceaux à X.*

Démonstration. Soit $x_0 \leqslant x_1 \leqslant \cdots \leqslant x_m$ la chaine maximale X ; nous dirons que m est la **longueur formelle** de X. Soit $y_1 \leqslant \cdots \leqslant y_n$ une chaine Y. Comme X est maximale on voit tout de suite que $x_0 = 0$, $x_m = 1$ et $x_1 \wedge y_1 = 0$ ou x_1. Si $x_1 \wedge y_1 = x_1$, alors Y est contenue dans le treillis $[x_1, 1]$. Par récurrence sur m, la chaine Y est contenue dans une chaine maximale finiment énumérable de $[x_1, 1]$ qui est isomorphe par morceaux à $x_1 \leqslant \cdots \leqslant x_m$, et par suite Y est contenue dans une chaine maximale finiment énumérable isomorphe par morceaux à X. Si $x_1 \wedge y_1 = 0$ et nous sommes dans la situation suivante



où $[y_1, x_1 \vee y_1]$ est isomorphe à $[0, x_1]$, et $[x_1, x_1 \vee y_1]$ est isomorphe à $[0, y_1]$. Par récurrence sur m la chaine $x_1 \leqslant x_1 \vee y_1$ est contenue dans une chaine finiment énumérable de $[x_1, 1]$, de longueur formelle $m-1$, formée d'une chaine maximale finiment énumérable C de $[x_1, x_1 \vee y_1]$ de longueur formelle ℓ, et d'une chaine

1. **NdT.** Linearly ordered.

maximale finiment énumérable D de $[x_1 \vee y_1, 1]$ de longueur formelle $m - \ell - 1$. La chaine $\{y_1\} \cup D$ est une chaine maximale de $[y_1, 1]$ de longueur formelle au plus $m - \ell$, de sorte que, par récurrence sur m, Y est contenue dans une chaine maximale de $[y_1, 1]$ isomorphe par morceaux à $\{y_1\} \cup D$. Le lemme 5.1 montre que la chaine C est isomorphe à une chaine maximale de $[0, y_1]$. Ainsi Y est contenue dans une chaine maximale isomorphe par morceaux à X. □

Du théorème 5.2 on déduit que si un treillis modulaire discret contient une chaine maximale finie de longueur n, alors toute chaine finie est contenue dans une chaine maximale de longueur n.

On dit que l'ensemble ordonné P satisfait la **condition de chaine ascendante** si pour chaque suite $p_1 \leqslant p_2 \leqslant p_3 \leqslant \cdots$ d'éléments de P, on a un n tel que $p_n = p_{n+1}$; la **condition de chaine descendante** est définie de manière analogue. En mathématiques classiques, si P satisfait la condition de chaine ascendante, nous pouvons trouver un n tel que $p_m = p_n$ pour chaque $m \geqslant n$. D'un point de vue constructif, même l'ensemble à deux éléments $\{0, 1\}$ ne satisfait pas cette forme de la condition de chaine ascendante.

Nous disons qu'un élément p d'un ensemble ordonné P est **de profondeur au plus** n si chaque fois que $p = p_0 \leqslant p_1 \leqslant p_2 \leqslant \cdots \leqslant p_{n+1}$, alors $p_i = p_{i+1}$ pour un $i \leqslant n$. Si P est discret, nous disons que p est **de profondeur au moins** n s'il contient une chaine $p = p_0 < p_1 < \cdots < p_n$. Un élément a une **profondeur bornée** s'il a une profondeur au plus n pour un certain n, il a une **profondeur finie** s'il a une profondeur au plus n, et au moins n, pour un certain n. Des définitions analogues sont obtenues en remplaçant *profondeur* par **hauteur** [1].

Exercices

1. Montrer qu'un treillis est discret si, et seulement si, la relation $a \leqslant b$ est décidable.
2. Montrer qu'un treillis est distributif si, et seulement si, il satisfait l'identité $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.
3. Soit L un treillis modulaire qui contient une chaine maximale finie (pour la non-égalité). Montrer que L est discret.
4. Montrer que si deux ensembles totalement ordonnés sont isomorphes par morceaux à un troisième, alors ils sont isomorphes par morceaux entre eux.
5. Montrer que si deux ensembles totalement ordonnés discrets sont isomorphes par morceaux, ils ont la même cardinalité.

1. **NdT.** La hauteur est la profondeur pour l'ordre opposé.

6. Deux intervalles A et B d'un treillis modulaire sont appelés **transposés** s'ils sont de la forme $[a, a \vee d]$ et $[a \wedge d, d]$ (ou vice versa), **projectifs** [1] si l'on a une suite $A = I_1, \ldots, I_n = B$ d'intervalles telle que I_i et I_{i+1} sont transposés pour $i = 1, \ldots, n-1$. Montrer que deux chaines maximales finiment énumérées dans un treillis modulaire sont projectives par morceaux.
7. Montrer qu'un ensemble ordonné peut être considéré comme une catégorie $\mathcal{C}$ dans laquelle l'ensemble des flèches $\mathcal{C}(a, b)$ est égal à $\{ x \in \{0\} : a \leqslant b \}$. Quelle est la description catégorique de l'infimum de deux éléments ?
8. Supposons que pour chaque suite binaire $a_1 \leqslant a_2 \leqslant a_3 \leqslant \cdots$ nous puissions trouver un m tel que $a_n = a_m$ chaque fois que $n \geqslant m$. En déduire que LPO est valide.

6 Ensembles bien fondés et ordinaux

Soit W un ensemble muni d'une relation $a < b$. Un sous-ensemble S de W est dit **héréditaire** si $w \in S$ chaque fois que $w' \in S$ pour tout $w' < w$. L'ensemble W, ou la relation $a < b$, est dite **bien fondée** si tout sous-ensemble héréditaire de W est égal à W. Un ensemble ordonné discret est dit bien fondé si la relation $a < b$ (i.e. $a \leqslant b$ et $a \neq b$) est bien fondée. Un **ordinal**, ou **ensemble bien ordonné**, est un ensemble totalement ordonné discret et bien fondé.

Les ensembles bien ordonnés fournissent l'environnement pour les arguments par induction généraux. Le prototype d'un ensemble bien ordonné est l'ensemble des entiers naturels $\mathbb{N}$, avec la relation d'ordre usuelle.

Théorème 6.1. *L'ensemble des entiers naturels est bien fondé.*

Démonstration. Soit S un sous-ensemble héréditaire de $\mathbb{N}$. Alors $0 \in S$ parce que l'hypothèse $w' \in S$ pour chaque $w' < 0$ est évidemment valide (il n'y a aucun $w' < 0$). De $0 \in S$ nous déduisons $1 \in S$, de $0 \in S$ et $1 \in S$ nous déduisons $2 \in S$, etc. □

L'ensemble des entiers naturels $\mathbb{N}$, vu comme un ordinal, est noté ω. Nous observons tout d'abord que tout sous-ensemble d'un ensemble bien fondé est lui-même bien fondé. Plus généralement nous avons le théorème suivant.

Théorème 6.2. *Soient P et W des ensembles, chacun avec une relation $a < b$, et supposons que W est bien fondé. Soit φ une application de P vers W telle que $\varphi(a) < \varphi(b)$ chaque fois que $a < b$. Alors P est bien fondé.*

1. **NdT.** Je n'ai pas trouvé la terminologie française correspondant au « projective » de [CCA].

Démonstration. Soit S' un sous-ensemble héréditaire de P, et soit $S = \{ w \in W : \varphi^{-1}(w) \subseteq S' \}$. Nous allons montrer que S est héréditaire, d'où $S = W$ et par suite $S' = P$. Supposons que $v \in S$ chaque fois que $v < w$. Si $x \in \varphi^{-1}(w)$ et $y < x$, alors $\varphi(y) < w$ de sorte que $\varphi(y) \in S$, et donc $y \in S'$. Comme S' est héréditaire, cela implique que $x \in S'$ pour chaque $x \in \varphi^{-1}(w)$, d'où $w \in S$. Ainsi S est héréditaire. □

En particulier, tout sous-ensemble de ω est un ordinal. L'image d'une suite binaire fournit un exemple d'un ordinal pour lequel il peut être impossible de trouver un premier élément. Le théorème 6.2 implique que toute sous-relation d'une relation bien fondée est elle-même bien fondée.

Nous disons qu'une relation $x < y$ est **transitive** si $a < b$ et $b < c$ impliquent $a < c$. Un ensemble bien fondé $(S, <)$ est **transitif** si la relation $x < y$ est transitive. Un exemple d'une relation bien fondée sur $\mathbb{N}$ qui n'est pas transitive est obtenu en définissant $a < b$ comme $a + 1 = b$. Cette relation est bien fondée d'après le théorème 6.2. Un argument d'induction par rapport à cette relation est la démonstration par récurrence telle qu'elle est ordinairement définie ; un argument d'induction par rapport à la relation usuelle $a < b$ est parfois appelé une démonstration par induction complète, ou par récurrence complète.

Un ensemble bien fondé discret et transitif admet une relation d'ordre naturelle définie en posant $a \leqslant b$ si $a < b$ ou $a = b$; la seule chose non triviale à vérifier est que $a = b$ si $a \leqslant b$ et $b \leqslant a$, cela résulte de ce que $a < a$ est impossible dans tout ensemble bien ordonné (exercice 1). Réciproquement la relation $a < b$ sur un ensemble ordonné discret est transitive.

On peut construire un ensemble bien fondé en additionnant des ensembles bien fondés déjà construits : on obtient l'ordinal $\omega + \omega$ en disposant deux copies des entiers naturels l'une après l'autre. Plus généralement, soit I un ensemble bien fondé et soit $\{A_i\}_{i \in I}$ une famille d'ensembles bien fondés indexée par I. Alors la réunion disjointe $\sum_{i \in I} A_i = \{ (a, i) : a \in A_i \text{ et } i \in I \}$ peut être munie de la relation naturelle suivante :

$$(a, i) < (b, j) \text{ si } i < j \text{ ou si } i = j \text{ et } a < b.$$

Si $I = \{1, \ldots, n\}$, avec la relation d'ordre habituelle, nous écrivons $A_1 + \cdots + A_n$. Notez que si I et tous les A_i sont discrets et transitifs (et totalement ordonnés), alors il en va de même pour $\sum_{i \in I} A_i$.

Théorème 6.3. *Si I est un ensemble bien fondé et si $\{A_i\}_{i \in I}$ est une famille d'ensembles bien fondés indexée par I, alors $W = \sum_{i \in I} A_i$ est un ensemble bien fondé.*

Démonstration. Soit S un sous-ensemble héréditaire de W. Pour chaque $i \in I$, nous posons $A'_i = \{ a \in A_i : (a, i) \in S \}$ et $I' = \{ i \in I : A'_i = A_i \}$. Nous allons montrer que I' est héréditaire, d'où $I' = I$, i.e. $S = W$. Supposons que

$i' \in I'$ pour chaque $i' < i$. Nous établissons $A'_i = A_i$ en démontrant que A'_i est héréditaire. Supposons que $a' \in A'_i$ pour chaque $a' < a$. Alors $w' \in S$ pour chaque $w' < (a, i)$, d'où $(a, i) \in S$ et donc $a \in A'_i$. Par suite $A'_i = A_i$ car A_i est bien fondé, et donc $i \in I'$. □

Soit $\{A_i\}_{i\in I}$ une famille d'ensembles bien fondés indexée par un ensemble discret I. Nous disons qu'un élément f de $\prod_{i\in I} A_i$ a un **support fini** si l'on a un sous-ensemble fini J de I tel que pour tout $i \in I$, ou bien [1] $i \in J$, ou bien $a < f_i$ est impossible pour $a \in A_i$ (c'est-à-dire que f_i est un élément minimal de A_i). Notez que si I est fini, alors tout élément de $\prod_{i\in I} A_i$ a un support fini, tandis que si un élément a un support fini, alors tous les A_i ont des éléments minimaux, à l'exception d'un nombre fini d'entre eux. Si I est un ensemble bien fondé, alors les éléments à support fini de l'ensemble produit $\prod_{i\in I} A_i$ sont munis d'une relation de **dernière différence** définie comme suit : $f < g$ si

(i) il existe un $i \in I$ tel que $f_i < g_i$, et

(ii) pour chaque $i \in I$, ou bien $f_i = g_i$, ou bien $f_j < g_j$ pour un $j \geqslant i$.

Si I et tous les A_i sont des ordinaux, cette relation peut être décrite en disant que deux éléments distincts doivent être ordonnés selon la dernière place où ils diffèrent (ordre lexicographique inverse).

Théorème 6.4. *Soit I un ordinal, et soit $\{A_i\}_{i\in I}$ une famille d'ensembles bien fondés indexée par I. Alors l'ensemble des éléments à support fini dans $\prod_{i\in I} A_i$ est bien fondé pour la relation de dernière différence.*

Démonstration. Nous commençons par remarquer que le théorème est vrai lorsque $I = \{1, 2\}$; dans ce cas $F = A_1 \times A_2 = \sum_{b\in B} A(b)$ où $B = A_2$ et $A(b) = A_1$ pour tout $b \in B$. Ainsi d'après le théorème 6.3 le produit $A_1 \times A_2$ est bien fondé pour la relation de dernière différence si A_1 et A_2 sont bien fondés. En ajoutant un plus grand élément ∞ à l'ensemble ordonné I et en posant $A_\infty = \{0\}$ on ne change rien, et nous pouvons donc supposer que I a un plus grand élément ∞. Soit F_i l'ensemble des éléments à support fini dans $\prod_{j\leqslant i} A_j$ et soit $I' = \{\, i \in I : F_i \text{ est bien fondé} \,\}$. Nous allons montrer que le sous-ensemble I' est héréditaire, donc égal à I, et par suite $F = F_\infty$ est bien fondé.

Supposons que $k \in I'$ pour chaque $k < i$. Soit F_i^* l'ensemble des éléments à support fini dans $\prod_{j<i} A_j$. Alors $F_i = F_i^* \times A_i$, donc F_i est bien fondé si F_i^* est bien fondé. Écrivons $F_i^* = \bigcup_{k<i} G_k$ où G_k est l'ensemble des éléments de $\prod_{j<i} A_j$ avec un support fini J tel que $j \leqslant k$ pour tout $j \in J$. La projection de G_k sur F_k préserve la relation $x < y$, de sorte que G_k est bien fondé en vertu

1. **NdT.** Quand nous raisonnons constructivement, nous utilisons l'expression « ou bien..., ou bien... » avec le sens du « ou » constructif, *mais pas exclusif*. Cela signifie donc simplement que « l'une des deux alternatives présentées est certifiée par un algorithme ». Cela facilite beaucoup la rédaction.

du théorème 6.2. Si S est un sous-ensemble héréditaire de F_i^*, alors $S \cap G_k$ est un sous-ensemble héréditaire de G_k pour chaque $k < i$, et donc $F_i^* = S$. Ainsi F_i^*, et par suite F_i, est bien fondé, d'où $i \in I$. □

Si I est un ensemble arbitraire et si A_i est un ensemble ordonné pour $i \in I$, le **produit catégorique** des A_i est l'ensemble $\prod_i A_i$ muni de la relation d'ordre suivante :

$$f \leqslant g \text{ si } f_i \leqslant g_i \text{ pour tout } i \in I.$$

Si $I = \{1, \ldots, n\}$ et si chaque A_i est discret et bien fondé, alors l'application identique du produit catégorique vers le produit muni de la relation de dernière différence préserve l'ordre (mais pas le non-ordre), par suite le produit catégorique est bien fondé d'après le théorème 6.2.

Si α est un ordinal et si β est un ensemble bien fondé, alors l'ensemble bien fondé des fonctions à support fini de α vers β sera noté β^α.

Pour des ordinaux λ et μ on définit un **plongement** de λ dans μ comme une fonction ρ de λ vers μ telle que si $a < b$ alors $\rho a < \rho b$, et si $c < \rho b$, alors on a un $a \in \lambda$ tel que $\rho a = c$. Nous allons montrer qu'il y a au plus un plongement de λ vers μ.

Théorème 6.5. *Si λ et μ sont des ordinaux et si ρ et σ sont des plongements de λ dans μ, alors $\rho = \sigma$.*

Démonstration. Soit $S = \{\, a \in \lambda : \rho a = \sigma a \,\}$, et supposons que $a \in S$ pour tout $a < b$. Si $\sigma b < \rho b$, alors on a un $a \in \lambda$ tel que $\rho a = \sigma b < \rho b$, donc $a < b$, d'où $\rho a = \sigma a$; mais $\rho a = \sigma b > \sigma a$, une contradiction. De la même manière, nous ne pouvons avoir $\rho b < \sigma b$. Par suite $\rho b = \sigma b$, et donc $b \in S$; ainsi S est héréditaire, et $S = \lambda$. □

Lorsque l'on a un plongement de l'ordinal λ dans l'ordinal μ, nous écrivons $\lambda \leqslant \mu$. Clairement, une composition de plongements est un plongement, donc cette relation est transitive. Le théorème 6.5 implique que si $\lambda \leqslant \mu$ et $\mu \leqslant \lambda$, alors λ et μ sont isomorphes, i.e. il y a une bijection de λ vers μ qui préserve et réfléchit l'ordre. Il est naturel de dire que deux ordinaux isomorphes sont **égaux**.

Exercices

1. Montrer que $a < a$ est impossible dans un ensemble bien fondé.
2. Si $a < b$ est une relation sur un ensemble W, on définit la clôture transitive $a <^* b$ de cette relation par : $a < b$ ou il existe $x_1, \ldots, x_n$ tels que $a < x_1 < x_2 < \cdots < x_n < b$. Montrer que $a <^* b$ est bien fondée si $a < b$ est bien fondée (mimer la démonstration que la récurrence ordinaire sur $\mathbb{N}$ implique l'induction complète sur $\mathbb{N}$).

3. Une relation $a < b$ est **acyclique** si $a <^* a$ est impossible pour n'importe quel a (voir l'exercice 2). Montrer qu'une relation acyclique sur un ensemble à deux éléments est bien fondée. Montrer qu'une relation acyclique sur un ensemble borné en nombre est bien fondée.
4. Montrer qu'un ensemble ordonné discret bien fondé satisfait la condition de chaine descendante.
5. Soit W un ensemble bien fondé. Soit S un sous-ensemble de W tel que, pour tout $w \in W$, ou bien $w \in S$, ou bien il existe un $w' < w$ tel que $w \in S$ si $w' \in S$. Montrer que $S = W$.
6. Montrer qu'un ensemble ordonné discret qui satisfait l'exercice 5 pour chaque sous-ensemble W satisfait la condition de chaine descendante.
7. Montrer la réciproque de l'exercice 6 (cela utilise l'axiome du choix dépendant).
8. Soit W l'ensemble des entiers naturels avec la relation $a < b$ définie par : $a \leqslant b$ et $b - a$ est impair. Montrer que cette relation $a < b$ est bien fondée mais n'est pas transitive.
9. Montrer que le produit catégorique d'ensembles ordonnés tel qu'il est défini dans la section précédente est effectivement un produit catégorique dans la catégorie des ensembles ordonnés (avec pour flèches les morphismes d'ensembles ordonnés).
10. Montrer que si tout ordinal non vide possède un plus petit élément, alors LPO est valide.
11. Une **relation de rang** sur un ensemble ordonné discret W est un ordinal A avec un sous-ensemble R de $W \times A$ qui satisfait les propriétés suivantes :

    (i) pour chaque $w \in W$ il y a un $a \in A$ tel que $(w, a) \in R$,

    (ii) si $v < w$ et $(w, a) \in R$, alors on a un $b < a$ tel que $(v, b) \in R$.

    Démontrer le théorème 6.4 pour un ensemble ordonné discret bien fondé avec une relation de rang.
12. Un **ordinal de Grayson** est un ensemble W muni d'une relation bien fondée $a < b$ qui satisfait les propriétés suivantes :

    (i) si $a < b$ et $b < c$, alors $a < c$ (transitivité),

    (ii) si $c < a$ est équivalent à $c < b$ pour tout c, alors $a = b$ (extensionnalité).

    Définissons $a \leqslant b$ sur un ordinal de Grayson comme signifiant que $c < a$ implique $c < b$ pour tout c. Montrer que lorsque la relation $a < b$ est décidable, alors W est un ordinal de Grayson si, et seulement si, W est un ordinal. (Suggestion : démontrer que $a < b$ ou $a = b$ ou $b < a$ dans un ordinal de Grayson décidable).

13. Soit α une suite binaire, et soit $S = \{x, y, z\}$ avec $x = y$ si α est identiquement nulle. On définit une relation $u < v$ sur S en posant
    (i) $y < z$
    (ii) $x < y$ si $\alpha_n = 1$ pour un n
    (iii) $x < z$ si $x = y$ ou $x < y$.

    Montrer que cela fait de S un exemple brouwerien pour un ordinal de Grayson avec des éléments tels que $x \leqslant y < z$ sans que l'on ait $x < z$.

7 Notes

Bishop (1967, page 8) définit quand on peut considérer qu'un objet existe.

L'idée selon laquelle la notion d'algorithme est une notion primitive a aussi été avancée par les mathématiciens russes Uspenskii et Semenov (1981) :

> "*Le concept d'algorithme comme celui d'ensemble ou de nombre naturel est un concept si fondamental qu'il ne peut pas être expliqué à travers d'autres concepts et qu'il devrait être regardé comme impossible à définir.*"

Les tentatives d'expliquer l'existence constructive en termes classiques sont toujours en quelque sorte peu satisfaisantes, mais la notion classique d'existence n'est pas moins mystérieuse que la notion constructive, nous sommes simplement plus familiers avec la notion classique. Quelle est la signification qu'il existe un bon ordre sur les nombres réels ? ou une base des réels comme espace vectoriel sur les rationnels ? ou un automorphisme des nombres complexes qui envoie e sur π ? ou une fonction qui ne soit pas calculable ? Des systèmes formels qui spécifient l'usage correct du « il existe » sont disponibles pour le mathématicien constructif aussi bien que pour son alter ego classique.

Notre définition d'un **ensemble** est une combinaison des formulations que l'on trouve dans [Bridges 1979, page 2] et [Heyting 1971, 3.2.1]. Beaucoup d'auteurs utilisent le terme positif **habité** pour décrire les ensembles non vides ; cela évite la confusion avec la notion d'un ensemble qui ne peut pas être vide. La notion de **relation de séparation** [1] (étroite) se trouve dans [Heyting 1971, 4.1.1]. La terminologie « étroite » est due à Scott (1979). Troelstra et van Dalen utilisent le terme « pre-apartness » pour désigner ce que nous appelons une relation de séparation. La partie du théorème 2.2 qui affirme que si une inégalité sur S est étroite alors il en va de même pour l'inégalité sur $S^{\mathbb{N}}$, est essentiellement donnée par [Bishop 1967, Lemma 5, page 24], qui dit que l'inégalité naturelle sur les nombres réels est étroite.

Une inégalité standard sur l'ensemble $\{0\}$ est obtenue en posant $0 \neq 0$ si LPO est faux. Comme LPO est réfutable dans deux branches principales des

1. **NdT.** Apartness.

mathématiques constructives – l'intuitionnisme et le constructivisme russe – nous ne pouvons pas démontrer que cette inégalité est consistante. Pour plus d'informations sur l'intuitionnisme et le constructivisme russe du point de vue des mathématiques constructives, veuillez consulter [Bridges-Richman 1987].

Les **relations de différence**[1] sont des relations d'inégalité symétriques qui satisfont l'implication

$$\neg x \neq y \text{ et } \neg y \neq z \text{ implique } \neg x \neq z.$$

Elles sont étudiées par van Rootselaar (1960) et par Olson (1977).

Nous pourrions demander que tout ensemble arrive avec une inégalité, en mettant l'inégalité et l'égalité sur le même plan ; ce serait alors naturel de demander que toutes les fonctions soient fortement extensionnelles. Avec une telle approche, chaque fois que nous construisons un ensemble, nous devons le munir d'une inégalité, et nous devons vérifier que nos fonctions sont fortement extensionnelles. Ceci est encombrant et facile à oublier, d'où résulteront des constructions incomplètes et des démonstrations incorrectes. Voici un exemple de ces complications : si H est un sous-groupe d'un groupe abélien G, alors l'inégalité sur G/H en tant que groupe peut différer de l'inégalité sur G/H en tant qu'ensemble parce que la loi de groupe sur G/H n'est pas nécessairement extensionnelle par rapport à cette dernière (à moins que l'inégalité sur G soit décidable) – voir l'exercice II.1.6.

Notre définition d'un **sous-ensemble** est en accord avec le traitement informel donné dans [Bishop 1967, page 32]. Une définition catégorique d'un **sous-ensemble** se trouve dans [Bishop 1967, page 63] où un sous-ensemble d'un ensemble S est défini comme donné par un ensemble A et par une application injective de A vers S. La définition catégorique est attrayante pour les mathématiques constructives, dans lesquelles il est important de garder à l'esprit qu'un élément d'un sous-ensemble, du fait même qu'il appartient au sous-ensemble, comporte implicitement l'information additionnelle qui établit son appartenance au sous-ensemble. L'approche catégorique nous permet de rendre cette information additionnelle explicite. Par exemple, si S est l'ensemble des suites binaires, et si A est l'ensemble des suites α telles que $\alpha_m = 1$ pour un certain m, alors pour spécifier un élément de A, nous ne devons pas seulement construire une suite dans S, mais également un entier m pour lequel $\alpha_m = 1$. Ainsi un élément de A peut être vu comme un couple (α, m), deux couples (α, m) et (α', m') étant égaux si $\alpha = \alpha'$. L'application de A vers S qui envoie (α, m) sur α est injective mais n'est pas réellement une inclusion puisqu'elle oublie la donnée additionnelle m. Nous trouvons l'approche informelle plus naturelle.

L'**axiome du choix unique** nous permet d'identifier une fonction avec son graphe ; Myhill l'a appelé l'**axiome du non-choix**. On voit facilement que cet

1. **NdT.** Difference relation.

axiome du choix unique est équivalent à l'une quelconque des deux propriétés suivantes.

(i) Toute fonction bijective admet une inverse.

(ii) Si S est un ensemble et si S^* est l'ensemble des sous-ensembles à un élément de S, alors S^* possède une fonction de choix : c'est-à-dire une fonction f de S^* vers S telle que $f(x) \in x$ pour chaque $x \in S^*$.

Bishop utilise la notion de fonction non extensionnelle ou **opération**. Dans presque tous les cas où cette notion est utilisée, on peut considérer une opération de l'ensemble A vers un ensemble B comme une fonction de A vers l'ensemble des parties non vides de B.

Notre définition d'un ensemble **fini** diffère de celles de [Bishop 1967], [Bridges 1979] et [Bishop-Bridges 1985] en ce que nous considérons qu'un ensemble vide est fini. Une autre différence plus subtile est que nous demandons que les ensembles finis soient discrets par rapport à leur propre inégalité. Ainsi un ensemble S de fonctions entre deux ensembles discrets est fini seulement si pour chaque f et $g \in S$, ou bien $f = g$, ou bien il existe un x tel que $f(x) \neq g(x)$.

Les fonctions que nous appelons **onto** [1] sont appelées **surjectives** dans [Bishop 1967] où le mot **onto** est réservé pour une application f de A vers B qui admet une section, c'est-à-dire pour laquelle il existe une fonction g de B vers A telle que fg est l'application identique sur B.

Dans [Bishop 1967] un ensemble finiment énumérable est appelé **sous-fini** [2], et un ensemble est réputé avoir **au plus** n **éléments** s'il peut être écrit sous la forme $\{x_1, \ldots, x_n\}$. Le terme « sous-fini » suggère pour nous un sous-ensemble d'un ensemble fini, tandis que l'utilisation du « au plus » dans [Bishop 1967] exclut que l'on puisse dire que tout sous-ensemble de $\{1, \ldots, n\}$ contienne au plus n éléments.

Greenleaf (1981) examine du point de vue constructif la question de la cardinalité des ensembles, ainsi que certaines questions reliées à cette notion.

Notre définition d'ensemble *dénombrable* [3] diffère de celles de [Bishop 1967], [Bridges 1979] et [Bishop-Bridges 1985] en ce que nous ne demandons pas qu'un ensemble dénombrable soit non vide (ou même que nous puissions décider s'il est vide ou pas) ; dans le cas des ensembles discrets notre définition est équivalente à celle de [Brouwer 1981].

Il semble improbable que nous soyons capables de construire un exemple brouwerien pour un sous-ensemble de $\mathbb{N}$ qui ne serait pas dénombrable. Néanmoins toute démonstration acceptable du théorème T selon lequel toute partie de $\mathbb{N}$ est dénombrable pourrait sans doute être transformée en une preuve que

1. **NdT.** Nous traduisons l'expression « map onto » de [CCA] par « fonction surjective », autrement dit nous utilisons la terminologie de Bishop. Bishop utilise quant à lui « map onto » avec une signification constructivement plus forte.
2. **NdT.** Subfinite.
3. **NdT.** Countable.

toute partie de $\mathbb{N}$ est récursivement énumérable, ce qui est faux. Une variante bien connue de T est le **schéma de Kripke**, selon lequel pour toute proposition P il existe une suite binaire α telle que P est valide si, et seulement si, $\alpha_n = 1$ pour un certain n. Le schéma de Kripke a une certaine plausibilité dans le cadre de la théorie du sujet créatif de Brouwer, dans laquelle nous imaginons le mathématicien idéalisé en train d'effectuer une suite qui n'est pas prédéterminée de tentatives de démontrer P, et lorsque nous gardons à l'esprit le critère intuitionniste selon lequel démontrer $\neg P$ revient à transformer toute preuve de P en une contradiction.

Bishop utilise *non* ou *ne pas* en italique pour indiquer l'existence d'un contre-exemple brouwerien. Par exemple nous dirions « il existe une inégalité qui *n'est pas* une relation de séparation » pour signifier que « si toute inégalité était une relation de séparation alors LPO serait valide ». Nous n'utiliserons *pas* cette convention.

Le **mini principe d'omniscience** (LLPO) a été introduit dans [Bishop 1973]. Aussi bien LPO que LLPO ont des interprétations simples en termes de nombres réels : LPO est équivalent à l'affirmation selon laquelle tout nombre réel x est $\leqslant 0$ ou > 0 ; LLPO est équivalent à l'affirmation selon laquelle tout nombre réel x est $\leqslant 0$ ou $\geqslant 0$.

Le **principe de Markov** affirme que si α est une suite binaire, et si $\alpha_n = 0$ pour tout n est impossible, alors il existe un n tel que $\alpha_n = 1$. L'idée est que nous pouvons construire le nombre n en calculant successivement α_1, α_2, α_3, ... jusqu'à ce que nous obtenions un 1. Le principe de Markov est utilisé par l'école constructive russe, qui est une forme constructive des mathématiques récursives ; pour plus de détails voir [Bridges-Richman 1987]. Un argument contre le principe de Markov est que nous n'avons aucune borne à priori, dans quelque sens que ce soit, sur la longueur du calcul qui est demandé pour construire n. Nous regardons le principe de Markov comme un principe d'omniscience.

Le point de vue selon lequel l'affirmation « pour tout $a \in A$ il existe un $b \in B$ » implique l'existence d'un algorithme (non nécessairement extensionnel) de A vers B est suggéré par l'affirmation dans [Bishop 1967, page 9] que « le fait qu'une fonction de choix existe en mathématiques constructives est une conséquence de la signification véritable de l'existence ». Bishop *définit* le fait qu'une fonction f de B vers A est surjective par l'existence d'un algorithme g de A vers B tel que $f(g(a)) = a$ pour tout $a \in A$.

Notre contre-exemple brouwerien de l'axiome du choix, ainsi que l'exercice 3.1 selon lequel l'axiome du choix implique la loi du tiers exclu, est dû à Myhill et Goodman (1978). Une démonstration qui a précédé, dans le cadre de la théorie des topos, a été donnée par Diaconescu (1975), qui démontre que l'axiome du choix implique que tout sous-ensemble A d'un ensemble B possède un **complémentaire** en ce sens qu'il existe un sous-ensemble A' tel que $B = A \cup A'$ et $A \cap A' = \emptyset$.

Fourman et Scedrov (1982) ont démontré en utilisant des méthodes de la théorie des topos que l'**axiome du choix le plus simple du monde** n'est pas démontrable dans la théorie des ensembles intuitionniste avec choix dépendant.

Les arguments contre l'axiome du choix dénombrable et l'axiome du choix dépendant doivent s'appuyer sur un socle plus fondamental que celui que nous avons utilisé contre l'axiome du choix. En fait, nous devons questionner l'interprétation de la phrase « pour tout a il existe un b » selon laquelle elle implique l'existence d'un algorithme qui transforme les éléments de A en des éléments de B. Une raison de rejeter cette interprétation est que ce faisant nos théorèmes seront aussi des théorèmes dans d'autres modèles (inattendus) qui apparaissent dans la théorie des topos, et qui possèdent un intérêt en mathématiques classiques (voir par exemple [Scedrov 1986]). Une autre raison, plus pertinente peut-être, est que des arguments qui s'appuient de manière essentielle sur cette interprétation nous laissent un sentiment d'insatisfaction concernant une « complétion à l'infini » un peu arbitraire quand, en présence d'une infinité potentielle d'items d'information, nous les réunissons tous en un seul algorithme.

Une **fonction de rang** [1] sur un ensemble bien fondé W est une application φ de W vers un ordinal A tel que $\varphi(x) < \varphi(y)$ chaque fois que $x < y$. Il semble improbable que nous puissions toujours construire une telle fonction de rang même si en mathématiques classiques tout ensemble bien fondé possède une unique fonction de rang minimale. L'induction sur le rang est une technique usuelle dans la théorie classique (voir l'exercice 6.11).

1. **NdT.** Rank function.

II. Algèbre de base

Sommaire

1 Groupes

Un **monoïde** est un ensemble G avec une application (ou loi de composition) φ de $G \times G$ vers G, habituellement écrite sous la forme $\varphi(a, b) = ab$, et un élément spécifié de G, habituellement noté 1, tel que pour tous a, b, $c \in G$

(i) $(ab)c = a(bc)$ (associativité),

(ii) $1a = a1 = a$ (élément neutre).

L'application φ est appelée la **multiplication** et l'élément 1 le **neutre**. L'associativité de la multiplication nous permet d'ignorer les parenthèses dans les produits $a_1 a_2 \cdots a_n$. Le monoïde est dit **abélien**, ou **commutatif**, lorsque $ab = ba$ pour tous éléments a et b. Dans un monoïde abélien, la loi φ est souvent appelée **addition** et écrite sous la forme $\varphi(a, b) = a + b$; l'élément neutre est alors noté 0. Dans ce cas nous parlons d'un monoïde **additif**, en opposition à un monoïde **multiplicatif**. Dans un monoïde multiplicatif, nous écrivons le produit itéré n fois $aa \cdots a$ sous la forme a^n pour chaque entier strictement positif n, et nous posons $a^0 = 1$; dans un monoïde additif, nous écrivons la somme itérée n fois $a + a + \cdots + a$ sous la forme na et nous écrivons $0a = 0$.

Si X est un ensemble, l'ensemble des fonctions de X vers X forme un monoïde : la multiplication est la composition des fonctions, et l'élément neutre est la fonction identique. L'ensemble des entiers naturels $\mathbb{N}$ est un monoïde commutatif pour l'addition, avec 0 pour élément neutre.

Un **homomorphisme de monoïdes** est une fonction f d'un monoïde G vers un monoïde H telle que $f(1) = 1$ et $f(ab) = f(a)f(b)$ pour tous a et $b \in G$. Si G est un monoïde multiplicatif, et $a \in G$, alors l'application de $\mathbb{N}$ vers G qui envoie n sur a^n est un homomorphisme. Un homomorphisme f est **non trivial** si $\{1\}$ est un sous-ensemble propre de im f. Un sous-ensemble H d'un monoïde G est un **sous-monoïde** si $1 \in H$ et si H est stable pour la multiplication. Si S est un sous-ensemble du monoïde G, alors l'ensemble formé par 1 et tous les produits finis d'éléments de S est un sous-monoïde de G appelé le **sous-monoïde engendré par** S. Le sous-monoïde de $\mathbb{N}$ engendré par $\{3, 4\}$ est $\mathbb{N} \setminus \{1, 2, 5\}$.

Soit X un ensemble. Définissons X^* comme l'ensemble des suites finies d'éléments de X, y compris la suite vide. Les éléments de X^* sont appelés des **mots**. Deux mots $u \equiv x_1 x_2 \cdots x_m$ et $v \equiv y_1 y_2 \cdots y_n$ sont **égaux** si $m = n$ et $x_i = y_i$ pour $i = 1, 2, \cdots, m$. Si u et v sont égaux dans X^* nous écrirons $u \equiv v$. On définit une **multiplication** (appelée aussi **concaténation**) sur X^* en posant $uv \equiv x_1 \cdots x_m y_1 \cdots y_n$. Cette multiplication est associative et le mot vide est l'élément neutre, de sorte que X^* est un monoïde, appelé le **monoïde libre sur l'ensemble** X. Si X est un ensemble à un élément, X^* est isomorphe au monoïde additif des entiers naturels.

Si a et b sont des éléments d'un monoïde et si $ab = 1$, alors disons que a est un **inverse à gauche** de b et que b est un **inverse à droite** de a. Si b a un inverse à gauche a et un inverse à droite c, alors $a = a(bc) = (ab)c = c$; dans ce cas nous disons que a est l'**inverse** de b et nous écrivons $a = b^{-1}$. Si b a un inverse nous disons que b est une **unité**, ou que b est **inversible**.

Un **groupe** est un monoïde G dans lequel tout élément est inversible. Dans un groupe additif, l'inverse de a est noté $-a$ plutôt que a^{-1}. Pour un entier strictement positif n nous définissons a^{-n} comme $(a^{-1})^n$; les lois usuelles pour les exposants sont valables. Dans un groupe additif, cette définition prend la forme $(-n)a = n(-a)$, et les lois de distributivité et d'associativité s'appliquent (voir la définition d'un R-module dans la section 3). Le prototype d'un groupe abélien est le groupe des entiers $\mathbb{Z}$ pour l'addition.

L'**ordre** d'un élément a d'un groupe est la cardinalité de l'ensemble $\{\, a^n : n \in \mathbb{N} \,\}$. L'ordre de a est $n \in \mathbb{N}$ si, et seulement si, $a^n = 1$ et $a^m \neq 1$ pour $m = 1, \ldots, n-1$. Dans le groupe $\mathbb{Z}$ l'élément 0 est d'ordre 1, comme l'élément neutre dans n'importe quel groupe, et tout élément non nul est d'ordre infini. Dans un groupe discret l'ordre d'un élément a est la cardinalité de l'ensemble $\{\, n \in \mathbb{N} : a^m \neq 1$ pour tous les m tels que $0 < m \leqslant n \,\}$ (cet ensemble contient 0), et par suite c'est un ordinal $\beta \leqslant \omega$.

Si G et H sont des groupes et si f est un homomorphisme de monoïdes de G

vers H, alors $f(a^{-1}) = f(a)^{-1}$ et $f(a^{-1})f(a) = f(a^{-1}a) = f(1) = 1$. Par suite un homomorphisme de monoïdes entre deux groupes préserve toute la structure de groupe : multiplication, élément neutre et inverse. Si G est un groupe et si $a \in G$, alors l'application qui envoie $x \in G$ sur axa^{-1} est un automorphisme de G, comme on le voit facilement ; un tel automorphisme est appelé **intérieur**.

Si G et H sont des groupes abéliens, alors l'ensemble $\mathrm{Hom}(G, H)$ des homomorphismes de G vers H a une structure naturelle de groupe abélien obtenue en posant $(f_1 + f_2)(x) = f_1(x) + f_2(x)$. Les groupes $\mathrm{Hom}(\mathbb{Z}, H)$ et H sont naturellement isomorphes en considérant l'application qui envoie $f \in \mathrm{Hom}(\mathbb{Z}, H)$ sur $f(1) \in H$. Si h est un homomorphisme de H vers H', alors h induit un homomorphisme de $\mathrm{Hom}(G, H)$ vers $\mathrm{Hom}(G, H')$ qui envoie f sur hf ; c'est-à-dire que l'on a $h(f_1 + f_2) = hf_1 + hf_2$. De la même manière un homomorphisme $g\colon G' \to G$ induit un homomorphisme de $\mathrm{Hom}(G, H)$ vers $\mathrm{Hom}(G', H)$ qui envoie f sur fg.

Une catégorie $\mathcal{C}$ comme la catégorie des groupes abéliens, telle que $\mathcal{C}(G, H)$ est un groupe abélien pour chaque couple d'objets G et H de $\mathcal{C}$, et telle que les fonctions induites de $\mathcal{C}(G, H)$ vers $\mathcal{C}(G, H')$ par une flèche $H \to H'$, et de $\mathcal{C}(G, H)$ vers $\mathcal{C}(G', H)$ par une flèche $G' \to G$, sont des homomorphismes de groupes, est appelée une **catégorie pré-additive**.

Une **permutation** d'un ensemble X est une bijection de X sur lui-même. L'ensemble des permutations de X est un groupe appelé le **groupe symétrique** sur X. Si $x_1, \ldots, x_n$ sont des éléments distincts dans un ensemble discret X, alors nous notons $(x_1, \ldots, x_n)$ la permutation π de X telle que

$$\pi x_i = x_{i+1} \text{ pour } i = 1, \ldots, n-1, \quad \pi x_n = x_1, \quad \pi x = x \text{ sinon.}$$

Une telle permutation est appelée un n-**cycle** de **support** $\{x_1, \ldots, x_n\}$, et deux cycles sont appelés **disjoints** si leurs supports sont disjoints. Si X est un ensemble fini, alors toute permutation est un produit de cycles disjoints. Comme $(x_1, \ldots, x_n) = (x_1, x_n) \cdots (x_1, x_3)(x_1, x_2)$, toute permutation d'un ensemble fini est un produit de 2-cycles (non nécessairement disjoints). Une permutation qui peut être écrite comme un produit d'un nombre pair de 2-cycles est appelée une permutation **paire**, et sinon **impaire**. Si π est une permutation d'un ensemble fini nous définissons

$$\operatorname{sgn} \pi = \begin{cases} 1 & \text{si } \pi \text{ est paire} \\ -1 & \text{si } \pi \text{ est impaire.} \end{cases}$$

Le produit d'un nombre pair de 2-cycles ne peut pas être égal au produit d'un nombre impair de 2-cycles (exercice 7). Par suite la signature est bien définie et $\operatorname{sgn} \pi_1\pi_2 = (\operatorname{sgn} \pi_1)(\operatorname{sgn} \pi_2)$ (exercice 8).

Un **sous-groupe** d'un groupe est un sous-monoïde stable pour le passage à l'inverse. Si G est un groupe, G et $\{1\}$ sont des sous-groupes de G ; nous notons

souvent le sous-groupe $\{1\}$ par 1. Si S est un sous-ensemble d'un groupe G, alors l'ensemble

$$\langle S\rangle = \{1\} \cup \{\, s_1 s_2 \cdots s_k : s_i \in S \cup S^{-1},\, k \geqslant 1 \,\}$$

de tous les produits finis d'éléments de S, ou d'inverses d'éléments de S, est un sous-groupe de G appelé le **sous-groupe engendré par** S. Si $\langle S\rangle = G$, alors S est appelé un **ensemble de générateurs**, ou un **système générateur** pour G. Un groupe est **de type fini** s'il possède un système générateur finiment énumérable, **cyclique** s'il possède un système générateur à un élément. Le groupe additif $\mathbb{Q}$ des nombres rationnels n'est pas de type fini ; en fait, tout sous-groupe de type fini de $\mathbb{Q}$ est cyclique (on voit facilement que tout sous-groupe de type fini de $\mathbb{Q}$ est *contenu dans* un sous-groupe cyclique).

Un sous-groupe H d'un groupe G est **normal** si $ghg^{-1} \in H$ pour tous $g \in G$ et $h \in H$. Tout sous-groupe d'un groupe abélien est normal. Si f est un homomorphisme de G vers H, alors on voit facilement que le **noyau** de f,

$$\ker f = \{\, x \in G : f(x) = 1 \,\} = f^{-1}(1)$$

est un sous-groupe normal de G. La taille du noyau de f nous dit dans quelle mesure f échoue à être injectif, comme le montre l'équivalence des propriétés suivantes :

— $f(a) = f(b)$,
— $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = 1$,
— $ab^{-1} \in \ker f$,

de sorte que f est un monomorphisme si, et seulement si, $\ker f = 1$. Nous étudierons les structures algébriques qui sont des groupes abéliens avec une structure additionnelle. Dans ces cas le noyau d'un homomorphisme f signifie le noyau de f en tant qu'homomorphisme de groupes ; si le groupe est écrit additivement, comme c'est normalement le cas pour ces structures plus complexes, on a $\ker f = f^{-1}(0)$.

Tout sous-groupe normal H d'un groupe G est le noyau d'un homomorphisme construit comme suit. L'ensemble G/H a les mêmes éléments que G, mais l'égalité est définie en posant $a = b$ si $ab^{-1} \in H$. Quand il est nécessaire de distinguer entre les deux égalités sur G et sur G/H nous écrivons $a = b \bmod H$ pour noter l'égalité dans G/H. La multiplication et le passage à l'inverse restent des fonctions par rapport à l'égalité de G/H, et donc G/H est un groupe, appelé le **groupe quotient** de G par H. Le prototype d'un groupe quotient est obtenu en prenant pour G le groupe $\mathbb{Z}$ des entiers et en prenant pour H le sous-groupe de $\mathbb{Z}$ formé par les multiples d'un entier donné n ; le groupe quotient G/H est alors le groupe $\mathbb{Z}_n$ des entiers modulo n.

Les faits essentiels qui relient les sous-groupes normaux et les groupes quotients sont réunis dans le théorème suivant.

Théorème 1.1. *Soient N un sous-groupe normal d'un groupe G et f un homomorphisme de G vers un groupe L avec $f(N) = 1$. Alors f est un homomorphisme de G/N vers L. Si f est surjectif et si le noyau de f est N, alors f est un isomorphisme de G/N sur L.*

Démonstration. Si $a = b \pmod N$, alors $ab^{-1} \in N$, d'où $f(a) = f(b)$; par suite f est une fonction sur G/N, qui est clairement un homomorphisme. Réciproquement si $f(a) = f(b)$, alors $f(ab^{-1}) = 1$, de sorte que $ab^{-1} \in N$ et $a = b \pmod N$. Par suite, si $\ker f = N$, alors f est une fonction injective de G/N vers L ; et donc, si $f\colon G \to L$ est surjective, la fonction $f\colon G/N \to L$ possède un inverse g. Clairement g est aussi un homomorphisme. □

Soit N un sous-groupe normal du groupe G. Un sous-groupe (normal) de G/N est un sous-groupe (normal) H de G qui est un sous-ensemble de G/N, c'est-à-dire, si $a \in H$ et $a = b \pmod N$, alors $b \in H$. On voit facilement qu'un sous-groupe H de G est un sous-ensemble de G/N exactement dans le cas où $N \subseteq H$. La différence entre un sous-groupe H de G contenant N et un sous-groupe H de G/N est la relation d'égalité sur H. Nous faisons la distinction entre H comme un sous-groupe de G et H comme un sous-groupe de G/N en écrivant H/N pour ce dernier. Si H est un sous-groupe normal de G qui contient N, alors $(G/N)/(H/N)$ est isomorphe à G/H ; en fait, les éléments des deux groupes sont simplement les éléments de G, et les égalités sont les mêmes.

Théorème 1.2. *Soient H et K des sous-groupes du groupe G. Si K est normal, alors*

(i) *l'ensemble $HK = \{\, hk : h \in H \text{ et } k \in K \,\}$ est un sous-groupe,*

(ii) *le sous-groupe $H \cap K$ est normal dans H, et*

(iii) *les groupes quotients HK/K et $H/(H \cap K)$ sont isomorphes.*

Démonstration. Exercice. □

Dans un groupe additif, le sous-groupe HK est écrit sous la forme $H + K$.

Si $a \in G$ et si H est un sous-groupe de G, alors $Ha = \{\, ha : h \in H \,\}$ est appelé une **classe à droite** de H, tandis que $aH = \{\, ah : h \in H \,\}$ est appelée une **classe à gauche** de H. Le passage à l'inverse induit une bijection entre classes à gauche et à droite de H qui envoie aH sur Ha^{-1}, et nous pouvons donc parler sans ambigüité de la cardinalité de l'ensemble des classes de H dans G. Cette cardinalité est appelée l'**indice** de H dans G et nous le notons $[G : H]$. Si H est normal, alors $Ha = aH$ pour chaque élément a de G.

Exercices

1. Montrer que dans un monoïde fini, si a possède un inverse à droite ou à gauche, alors $a^n = 1$ pour un entier strictement positif n, de sorte que

l'élément peut avoir au plus un inverse à droite ou à gauche. Donner un exemple d'un élément dans un monoïde qui admet deux inverses à gauche distincts ; deux inverses à droite distincts.

2. Montrer qu'un monoïde peut être identifié avec une catégorie à un seul objet, et que les homomorphismes de monoïdes sont des foncteurs entre les catégories correspondantes. Parmi ces catégories, lesquelles correspondent à des groupes ?

3. Montrer que l'ensemble des unités d'un monoïde est un groupe.

4. Montrer que l'ensemble S des suites binaires forme un groupe abélien G pour l'addition des coordonnées modulo 2. Soit $a \in S$ et définissons $b, c \in S$ par $b_n = 1$ si, et seulement si, $a_n = 1$ et $a_m = 0$ pour tous les $m < n$, et $c_n = 1$ si, et seulement si, $b_{n-1} = 1$. Montrer que si le sous-groupe de G engendré par b et c est engendré par un sous-ensemble fini de G, alors, ou bien $a = 0$, ou bien $a \neq 0$.

5. Soit G un groupe multiplicatif avec une inégalité. L'inégalité est dite **invariante par translation** si $x \neq y$ implique $zx \neq zy$ et $xz \neq yz$. Étant donnée une inégalité invariante par translation, montrer que

   (i) le passage à l'inverse qui envoie x sur x^{-1} est fortement extensionnel si, et seulement si, l'inégalité est symétrique.

   (ii) l'inégalité est cotransitive si, et seulement si, la multiplication est fortement extensionnelle (l'inégalité sur $G \times G$ est donnée par $(x_1, x_2) \neq (y_1, y_2)$ si $x_1 \neq y_1$ ou $x_2 \neq y_2$).

   Enfin, démontrer que si l'inégalité est consistante et si la multiplication est fortement extensionnelle, alors l'inégalité est invariante par translation.

6. En regardant une inégalité sur G comme un sous-ensemble de $G \times G$, montrer que la réunion d'une famille d'inégalités sur un groupe G pour lesquelles la loi de groupe est fortement extensionnelle est elle-même une inégalité de cette sorte. Montrer qu'il existe une unique inégalité sur G/N qui rend le théorème 1.1 vrai dans la catégorie des groupes avec inégalité, avec pour flèches les homomorphismes fortement extensionnels. Montrer que si G est l'ensemble des suites binaires avec pour addition l'addition des coordonnées modulo 2 et si $N = \{\, x \in G : \text{il y a un } m \text{ tel que } x_n = 0 \text{ pour tous } n \geqslant m \,\}$, alors $x \neq 0$ dans G/N si, et seulement si, $x_n = 1$ une infinité de fois et LPO est valide.

7. Soient $x_1, \ldots, x_m, y_1, \ldots, y_n$ des éléments distincts d'un ensemble fini X, soit G le groupe symétrique sur X, et soit $1 \leqslant i < j \leqslant m$. Vérifiez les deux égalités suivantes sur G.

   (i) $(x_i, x_j)(x_1, \ldots, x_m) = (x_1, \ldots, x_{i-1}, x_j, \ldots, x_m)(x_i, \ldots, x_{j-1})$

   (ii) $(x_1, y_1)(x_1, \ldots, x_m)(y_1, \ldots, y_n) = (y_1, \ldots, y_n, x_1, \ldots, x_m)$.

Pour $\pi \in G$, nous pouvons écrire π d'une manière essentiellement unique comme un produit de cycles disjoints dont les supports recouvrent X [1]. Soit N_π le nombre de cycles dans un tel produit. En utilisant (i) et (ii), montrer que si τ est un 2-cycle, alors $N_{\tau\pi} = N_\pi \pm 1$. En conclure qu'une permutation paire ne peut pas être écrite comme produit d'un nombre impair de 2-cycles.

8. Montrer que la fonction sgn est un homomorphisme du groupe symétrique d'un ensemble fini vers le groupe multiplicatif $\{-1, 1\}$.
9. Donner un exemple brouwerien d'un sous-groupe d'un groupe abélien fini qui est engendré par un sous-ensemble dénombrable mais qui n'est pas de type fini.
10. Montrer que l'ensemble des sous-groupes normaux d'un groupe est un treillis modulaire.

2 Anneaux et corps

Un **anneau** est un groupe abélien additif R qui est aussi un monoïde multiplicatif, les deux structures étant reliées par les **lois de distributivité** :

$$\begin{aligned} a(b+c) &= ab+ac, \\ (a+b)c &= ac+bc. \end{aligned}$$

Un anneau est **trivial** si $0 = 1$. Si la structure de monoïde multiplicatif est commutative, alors R est un **anneau commutatif**. Une **unité** de R est une unité du monoïde multiplicatif de R. On dit qu'un anneau a des **unités détachables** lorsque ses unités forment d'un sous-ensemble détachable.

Si A est un groupe abélien, alors l'ensemble des endomorphismes $\mathrm{E}(A) = \mathrm{Hom}(A, A)$ est un anneau (en prenant pour multiplication la composition) appelé l'**anneau des endomorphismes** de A. Plus généralement, si $\mathcal{C}$ est une catégorie pré-additive, $\mathcal{C}(A, A)$ est un anneau pour chaque objet A de $\mathcal{C}$.

Un anneau non trivial k est un **anneau à division** [2] (ou un **corps gauche**) si, pour chaque a et $b \in k$,

$$a \neq b \text{ si, et seulement si, } a - b \text{ est une unité.}$$

Nous rappelons à la lectrice que l'interprétation du symbole $a \neq b$ dépend du contexte : si k possède une inégalité, alors $a \neq b$ fait référence à cette inégalité, et sinon $a \neq b$ fait référence à la non-égalité. Une conséquence immédiate de la définition est que si k est un anneau à division, alors l'inégalité sur k est

1. **NdT.** Ici, pour recouvrir X, nous acceptons les cycles (a), de support $\{a\}$, tous égaux à la permutation identité.
2. **NdT.** Division ring.

symétrique et **invariante par translation** : si $a \neq b$, alors $a + c \neq b + c$. Notez que la non-égalité est automatiquement invariante par translation parce que l'addition est une fonction.

Naturellement, nous pourrions définir l'inégalité $a \neq b$ sur un anneau arbitraire comme signifiant que $a - b$ est une unité et, techniquement, nous aurions alors un anneau à division ; de sorte que la théorie générale des anneaux à division contient la théorie des anneaux. Cependant, l'idée est d'utiliser le symbole $a \neq b$ pour représenter des relations qui peuvent être raisonnablement appelées des inégalités : si vous prenez une inégalité stupide et que vous obtenez un anneau à division stupide, ne nous blâmez pas. Comme règle de conduite, vous pouvez choisir une inégalité standard. Pour l'essentiel, nous serons intéressés par des anneaux à division qui sont discrets, et, dans une moindre mesure, par des anneaux à division avec une relation de séparation étroite.

Les éléments non nuls d'un anneau à division sont exactement les unités ; dans le cas discret c'est une propriété caractéristique des anneaux à division (exercice 3). Un **corps** est un anneau à division commutatif. Un **corps de Heyting** est un corps avec une relation de séparation étroite. Dans un corps de Heyting ou plus généralement dans un corps avec une inégalité cotransitive, les opérations arithmétiques sont fortement extensionnelles (exercice 5). Les nombres rationnels $\mathbb{Q}$ forment un corps discret ; les nombres réels (section suivante) forment un corps de Heyting. Les quaternions rationnels (exercice 4) forment un anneau à division discret et non commutatif.

Un sous-ensemble d'un anneau est un **sous-anneau** si c'est un sous-groupe additif et un sous-monoïde multiplicatif. Soit S un sous-anneau d'un anneau commutatif R, et soient $a_1, \ldots, a_n$ des éléments de R. Alors l'ensemble des sommes d'éléments de R de la forme

$$s a_1^{m_1} a_2^{m_2} \cdots a_n^{m_n},$$

avec $s \in S$ et $m_i \in \mathbb{N}$, est un sous-anneau de R que l'on note $S[a_1, \ldots, a_n]$; il est contenu dans tout sous-anneau de R qui contient $S \cup \{a_1, \ldots, a_n\}$. Si S et R sont des corps, alors $S(a_1, \ldots, a_n)$ désigne l'ensemble des quotients f/g avec $f, g \in S[a_1, \ldots, a_n]$ et $g \neq 0$. On voit facilement que $S(a_1, \ldots, a_n)$ est un corps contenu dans chaque sous-corps de R qui contient $S \cup \{a_1, \ldots, a_n\}$.

Un **anneau intègre**, ou encore un **domaine d'intégrité** est un anneau avec inégalité qui est isomorphe à un sous-anneau d'un corps ; de manière plus informelle, un anneau intègre est simplement un sous-anneau d'un corps. Si R est un sous-anneau d'un corps, alors l'ensemble $\{\, ab^{-1} : a, b \in R \text{ et } b \neq 0 \,\}$ est un corps qui contient R, appelé le **corps de fractions** de R. Le corps de fractions d'un anneau intègre est essentiellement unique (exercice 6).

Si R est un anneau intègre discret, alors, pour chaque a et $b \in R$,

$$\text{si } a \neq 0 \text{ et } b \neq 0, \text{ alors } ab \neq 0. \qquad (*)$$

Inversement, si R est un anneau commutatif intègre discret qui satisfait la condition $(*)$, alors nous pouvons **immerger** [1] R dans un corps discret k en imitant la construction du corps des nombres rationnels $\mathbb{Q}$ à partir de l'anneau des nombres entiers $\mathbb{Z}$. Soit $k = \{\,(a,b) \in R \times R : b \neq 0\,\}$ avec $(a,b) = (c,d)$ si $ad = bc$. Nous définissons la multiplication sur k par $(a,b)\cdot(c,d) = (ac,bd)$ et l'addition par $(a,b)+(c,d) = (ad+bc,bd)$. On vérifie sans peine que cela fait de k un anneau avec l'élément neutre additif $(0,1)$ et l'élément neutre multiplicatif $(1,1)$. Si $(a,b) \neq (0,1)$, alors $a \neq 0$ et donc l'élément (b,a) est dans k et $(a,b)(b,a) = (1,1)$; inversement, si $(a,b)(c,d) = (1,1)$, alors $ac = bd \neq 0$, d'où $a \neq 0$ et $(b,a) \in k$, et par suite k est un corps. Nous immergeons R dans k en envoyant a sur $(a,1)$.

Une caractérisation intrinsèque d'un anneau intègre arbitraire est donnée dans l'exercice 7. Pour démontrer que cette caractérisation est correcte, construisez le corps de fractions comme dans le cas discret.

Si k est un corps, alors le sous-corps de k formé par tous les éléments de la forme $(n\cdot 1)/(m\cdot 1)$ où m et n sont des entiers et $m\cdot 1 \neq 0$, est le plus petit sous-corps de k, et il est appelé le **sous-corps premier** [2] de k. Ce corps est le corps de fractions du sous-anneau $\{\,n\cdot 1 : n \in \mathbb{Z}\,\}$ de k. Si $a_1,\ldots,a_n \in k$ et si k_0 est le sous-corps premier de k, nous disons que k est **engendré par** $a_1,\ldots,a_n$ si $k_0(a_1,\ldots,a_n) = k$. Un **corps premier** est un corps égal à son sous-corps premier.

Une fonction f d'un anneau R vers un anneau S est un **homomorphisme d'anneaux** si c'est un homomorphisme des groupes additifs et un homomorphisme des monoïdes multiplicatifs. La fonction de l'anneau des entiers $\mathbb{Z}$ vers S qui envoie n sur $n\cdot 1$ est un homomorphisme d'anneaux. Un sous-groupe additif I d'un anneau R est un **idéal** si pour tous $x \in I$ et $r \in R$ les éléments rx et xr sont dans I. On voit facilement que si f est un homomorphisme d'anneaux, alors $\ker f = f^{-1}(0)$ est un idéal. Un idéal I est **propre** si $1 \notin I$. Un **idéal à gauche** (resp. **idéal à droite**) I d'un anneau R est un sous-groupe additif de R tel que pour tous $r \in R$ et $x \in I$ l'élément rx (resp. xr) appartient à I. Un idéal à gauche I d'un anneau est **non nul** si I contient un élément non nul. Pour éviter la confusion entre idéaux à gauche, idéaux à droite et idéaux, un idéal est souvent appelé un **idéal bilatère**. Si I est un idéal bilatère de l'anneau R, alors la multiplication est une loi de composition sur le groupe quotient R/I, de sorte que R/I est un anneau.

Soient X et Y des sous-ensembles de l'anneau R. On définit XY comme le sous-groupe additif de R engendré par $\{\,xy : x \in X \text{ et } y \in Y\,\}$. Si X, Y et Z sont des sous-ensembles de R, alors $(XY)Z = X(YZ)$. Un sous-ensemble non

1. **NdT.** To embed. Nous utilisons dans la traduction de cet ouvrage la terminologie peu habituelle « immerger A dans B » pour dire qu'on donne un isomorphisme de l'objet A sur un sous-objet de B. Nous disons aussi parfois « plonger A dans B », et nous utilisons les termes de « plongement » ou « immersion ».

2. **NdT.** Prime field of k.

vide I est un idéal si, et seulement si, $RIR = I$, tandis que I est un idéal à gauche (resp. à droite) si $RI = I$ (resp. $IR = I$).

Si S est un sous-ensemble d'un anneau R, alors $(S) := RSR$ est le plus petit idéal de R contenant S, et on l'appelle l'**idéal engendré par** S. Si S est la famille finie $\{s_1, \ldots, s_n\}$, alors l'idéal engendré par S est noté $(s_1, \ldots, s_n)$. L'**idéal à gauche engendré par** S est RS, tandis que l'**idéal à droite engendré par** S est SR ; si S est un ensemble à un élément $\{s\}$, alors l'idéal à gauche ou à droite correspondant est appelé **principal**, et on le note Rs ou sR.

Si I et J sont des idéaux, alors IJ et $I \cap J$ sont des idéaux. L'ensemble $I \cup J$ n'est pas nécessairement un idéal ; l'idéal engendré par $I \cup J$ est l'ensemble $\{\, i + j : i \in I \text{ et } j \in J \,\}$ et on le note $I + J$. Plus généralement, si $\{I_i\}$ est une famille d'idéaux, alors l'idéal engendré par $\bigcup_i I_i$ est noté $\sum_i I_i$.

Le **transporteur**[1] **d'un ensemble** S **dans un idéal à gauche** I est l'idéal à gauche

$$I : S = \{\, x \in R : xS \subseteq I \,\}.$$

Le **radical** d'un idéal I dans un anneau commutatif est l'idéal $\sqrt{I} = \{\, x \in R : x^n \in I \text{ pour un } n \,\}$.

Le théorème fondamental des homomorphismes d'anneaux résulte immédiatement du théorème correspondant pour les groupes.

Théorème 2.1. *Soit I un idéal de l'anneau R. Si f est un homomorphisme de R vers un anneau S avec $f(I) = 0$, alors f est un homomorphisme de R/I vers S. Si f est surjectif et si le noyau de f est l'idéal I, alors f est un isomorphisme de R/I sur S.*

Soit I un idéal de l'anneau R. Un idéal (à gauche) de R/I est un idéal (à gauche) J de R contenant I. Si J est un idéal de R contenant I, alors $R/J \simeq (R/I)/(J/I)$.

Théorème 2.2. *Soient R un anneau, S un sous-anneau et I un idéal de R. Alors $S + I$ est un sous-anneau de R contenant I en tant qu'idéal, $S \cap I$ est un idéal de S, et $(S + I)/I \simeq S/(S \cap I)$.*

Démonstration. Clairement $S + I$ est un sous-anneau et I est un idéal de $S + I$. Définissons une fonction f de $S/(S \cap I)$ vers $(S + I)/I$ en posant $f(s) = s$. Notez que f est bien une fonction parce que si $s_1 = s_2$ dans $S/(S \cap I)$, alors $s_1 - s_2 \in I$ et donc $s_1 = s_2$ dans $(S+I)/I$. Clairement f est un homomorphisme. Maintenant définissons une fonction g de $(S + I)/I$ vers $S/(S \cap I)$ en posant $g(s + i) = s$. Pour voir que g est une fonction nous remarquons que si $s_1 + i_1 = s_2 + i_2$ dans $(S + I)/I$, alors $s_1 - s_2 \in I$, et donc $s_1 = s_2$ dans $S/(S \cap I)$. Il s'ensuit que f est un isomorphisme. □

1. **NdT.** Quotient of a left ideal I by a set S

Si P est un idéal d'un anneau commutatif R, alors nous disons que P est un **idéal premier** [1] si chaque fois que $xy \in P$, alors $x \in P$ ou $y \in P$. Si P est un idéal détachable propre de R, alors on voit facilement que P est premier si, et seulement si, R/P est un anneau intègre. Si p est un nombre premier, alors l'idéal (p) de $\mathbb{Z}$ est un idéal premier détachable propre, et il en va de même pour l'idéal 0.

Théorème 2.3. [2] *Soient $P_1, \ldots, P_n$ des idéaux détachables d'un anneau commutatif R tels que P_i est premier pour $i \leqslant n-2$. Si I est un idéal de type fini de R, alors, ou bien $I \subseteq P_i$ pour un i, ou bien il existe un $z \in I \setminus \bigcup_i P_i$.*

Démonstration. Soit $\{x_1, \ldots, x_m\}$ un système générateur de I et soit F l'ensemble des sous-ensembles finis S de $\{1, 2, \ldots, n\}$ tels que $\{x_1, \ldots, x_m\} \subseteq \bigcup_{j\in S} P_j$. Nous raisonnons par récurrence [3] sur $\#F$, le nombre des éléments de F. Si $\#F = 0$, alors $x_j \in I \setminus \bigcup_i P_i$ pour un j. Sinon prenons un $S \in F$ qui minimise $\#S$. Si $\#S \leqslant 1$, alors $I \subseteq P_i$ pour un i. Sinon $\#S \geqslant 2$ et pour chaque $i \in S$, il existe $a_i \in \{x_1, \ldots, x_m\}$ tel que $a_i \in P_i \setminus \bigcup_{S\setminus\{i\}} P_j$. Si $\#S = 2$, alors posons $x_{m+1} = \sum_{i\in S} a_i \in I \setminus \bigcup_{i\in S} P_i$. Si $\#S > 2$, alors P_i est premier pour un $i \in S$, de sorte que $x_{m+1} = a_i + \prod_{j\in S\setminus\{i\}} a_j \in I \setminus \bigcup_{i\in S} P_i$. Dans chaque cas nous pouvons agrandir $\{x_1, \ldots, x_m\}$, sans agrandir I, d'où $S \notin F$, et nous terminons par récurrence sur $\#F$. □

Théorème 2.4. *Soient $I_1, \ldots, I_n$ des idéaux de type fini dans un anneau commutatif R et soit P un idéal premier de R tel que le produit $I_1 \cdots I_n$ est contenu dans P. Alors $I_i \subseteq P$ pour un i.*

Démonstration. Par récurrence sur n il suffit de considérer le cas où $n = 2$. Soient $I_1 = (a_1, \ldots, a_s)$ et $I_2 = (b_1, \ldots, b_t)$. Puisque $a_i b_j \in P$, on a pour chaque i ou bien $a_i \in P$, ou bien $b_j \in P$ pour tous les j. □

Un **corps par négation** est un anneau commutatif qui est un corps pour la non-égalité et tel que 0 est un idéal premier. Un corps discret est un corps par négation. Un **idéal maximal** dans un anneau commutatif R est un idéal M tel que R/M est un corps par négation ; ainsi, un idéal M de R est maximal si, et seulement si, d'une part M est un idéal premier, et d'autre part « $x \in R \setminus M$ » équivaut à « $\exists r \in R,\ rx - 1 \in M$ ». Un idéal maximal détachable M est un idéal tel que R/M est un corps discret.

1. **NdT.** En mathématiques classiques, les idéaux premiers sont définis comme des idéaux propres, i.e. avec $1 \notin P$. Certaines démonstrations en mathématiques constructives préfèrent ne pas utiliser cette propriété, notamment lorsque l'idéal n'est pas à priori détachable.

2. **NdT.** Cette forme constructive du lemme d'évitement des idéaux premiers sera très utile dans les chapitres VIII et X.

3. **NdT.** Plutôt qu'une démonstration par récurrence coutumière, les auteurs donnent ici une démonstration de terminaison d'un algorithme.

La **caractéristique** d'un anneau k est l'ordre de l'élément 1 dans le groupe additif de k. Une convention standard est de dire que k est de **caractéristique 0** si l'ordre de 1 est infini. Ainsi la caractéristique d'un anneau discret k est le plus petit entier strictement positif n tel que $n \cdot 1 = 0$, si un tel entier existe, et est égale à 0 sinon. Le corps des nombres rationnels est de caractéristique 0, et le corps $\mathbb{F}_p = \mathbb{Z}/(p)$ est de caractéristique p. La caractéristique d'un corps discret n'est pas nécessairement un élément de $\mathbb{N}$ comme le montre l'exemple brouwerien suivant.

Une suite binaire qui contient au plus un élément 1 est appelée une **suite binaire fugitive**.

Exemple 2.5. Soit a une suite binaire fugitive. Définissons p_n par

$$p_n = \begin{cases} 0 & \text{si } a_n = 0 \\ \text{le } n\text{-ième nombre premier} & \text{si } a_n = 1. \end{cases}$$

Soit P l'idéal de $\mathbb{Z}$ engendré par les nombres p_n, et soit $R = \mathbb{Z}/P$. Alors R est un anneau intègre discret ; soit k son corps de fractions. La caractéristique de k n'est pas un élément de $\mathbb{N}$. □

Exercices

1. Montrer les identités suivantes dans un anneau arbitraire.
   (i) $a0 = 0a = 0$,
   (ii) $a(-b) = (-a)(b) = -ab$.
2. Utiliser les anneaux $\mathbb{Z}$ et $\mathbb{Q}$ pour construire un exemple brouwerien d'un anneau intègre discret dont les unités ne sont pas détachables.
3. Montrer qu'un anneau discret est un anneau à division si, et seulement si, les éléments non nuls forment un groupe multiplicatif.
4. *Les quaternions rationnels.* On écrit les éléments (a, b, c, d) de $R = \mathbb{Q}^4$ comme des sommes formelles $a + bi + cj + dk$, où les éléments de $\mathbb{Q}$ commutent avec i, j, et k, et où on pose $i^2 = j^2 = -1$ et $k = ij = -ji$. Notez que
$$(a + bi + cj + dk)(a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2$$
et montrez que R est un anneau à division non commutatif discret.
5. Montrer que dans un corps avec une inégalité cotransitive les opérations d'addition, de soustraction, de multiplication et de division (restreinte aux unités) sont fortement extensionnelles (voir l'exercice 1.5).
6. Soit R un sous-anneau d'un corps K. Montrer que
$$k = \{\, ab^{-1} : a, b \in R \text{ et } b \neq 0 \,\}$$

est un corps qui contient R. Montrer que si R est un sous-anneau d'un autre corps K', et si les inégalités sur K et K' coïncident sur R, alors k est isomorphe à k'. Montrer que l'inégalité sur R est consistante, cotransitive, étroite ou discrète si, et seulement si, l'inégalité sur k possède la même propriété.

7. Montrer qu'un anneau commutatif est un anneau intègre si, et seulement si, les conditions suivantes sont satisfaites :
   (i) $1 \neq 0$,
   (ii) $a \neq b$ si, et seulement si, $a - b \neq 0$,
   (iii) si $a \neq 0$ et $ab = 0$, alors $b = 0$,
   (iv) $a \neq 0$ et $b \neq 0$ si, et seulement si, $ab \neq 0$,

   Montrer qu'une condition nécessaire et suffisante pour qu'un anneau commutatif avec la non-égalité soit un anneau intègre est que l'on a $a \neq 0$ si, et seulement si, a est **simplifiable** [1] ($ab = 0$ implique $b = 0$).
8. Montrer les propriétés suivantes pour les idéaux dans un anneau commutatif.
   (i) $IJ \subseteq I \cap J$
   (ii) $IJ \subseteq K$ si, et seulement si, $I \subseteq K : J$
   (iii) Si $I \subseteq J$ alors $K : J \subseteq K : I$
   (iv) $(\bigcap_i I_i) : J = \bigcap_i (I_i : J)$
   (v) $I : \sum_i J_i = \bigcap_i (I : J_i)$
   (vi) $I : JK = (I : J) : K$
9. Montrer les propriétés suivantes pour les idéaux dans un anneau commutatif.
   (i) $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.
   (ii) Si $I^n \subseteq J$ pour un n, alors $\sqrt{I} \subseteq \sqrt{J}$.
   (iii) $\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$.
   (iv) $\sqrt{\sqrt{I}} = \sqrt{I}$.
10. Soit $\varphi\colon R \to R'$ un homomorphisme d'anneaux commutatifs, et soient I et J des idéaux de R'. Montrer que $\varphi^{-1}(I) \cap \varphi^{-1}(J) = \varphi^{-1}(I \cap J)$, que $\varphi^{-1}(I)\varphi^{-1}(J) \subseteq \varphi^{-1}(IJ)$, et que $\sqrt{\varphi^{-1}(I)} = \varphi^{-1}(\sqrt{I})$. Montrer que si φ est surjective, alors $\varphi^{-1}(I : J) = \varphi^{-1}I : \varphi^{-1}J$.
11. Montrer que $(12) \cup (45)$ n'est pas un idéal de l'anneau des entiers $\mathbb{Z}$. Montrer que $(12) + (45)$ et $(12) : (45)$ sont des idéaux principaux.

1. **NdT.** On dit aussi **régulier**.

12. Dans le théorème 2.3 il n'est pas nécessaire de savoir *lesquels* des $n-2$ idéaux sont premiers. Démontrer le théorème 2.3 sous l'hypothèse plus faible selon laquelle si $a_i b_i \in P_i$ pour $i = 1, \ldots, n$, alors pour au moins $n-2$ indices i, ou bien $a_i \in P_i$ ou bien $b_i \in P_i$.
13. Modifier le théorème 2.3 de manière qu'aucun des idéaux P_i ne soit supposé être premier, et la conclusion est alors que $I \subseteq P_i$ pour un certain i, ou alors il existe trois indices j distincts tels que P_j n'est pas premier (en un sens fort, convenable). Pouvez-vous démontrer que les trois idéaux P_j sont distincts (et pas seulement leurs indices) ?
14. Soient B et C deux sous-groupes détachables d'un groupe G. Montrer que si A est un sous-groupe de type fini de G, ou bien $A \subseteq B$, ou bien $A \subseteq C$, ou bien il existe un x dans $A \setminus (B \cup C)$. Donner un contre-exemple (non brouwerien) pour montrer que le résultat est faux pour trois sous-groupes.
15. Montrer qu'un anneau discret non trivial R est un anneau à division si, et seulement si, tout idéal de type fini est égal à R ou à 0. Donner un exemple brouwerien pour un idéal de $\mathbb{Q}$ qui n'est égal ni à $\mathbb{Q}$ ni à 0.
16. Montrer qu'un idéal d'un anneau commutatif R est un idéal premier propre si, et seulement si, c'est le noyau d'un homomorphisme de R dans un corps par négation.
17. Montrer qu'un anneau intègre fini est un corps. Montrer qu'un idéal détachable I de $\mathbb{Z}$ est maximal si, et seulement si, $I = (p)$ pour un nombre premier p.

3 Les nombres réels

Le prototype d'un corps de Heyting est le corps des nombres réels $\mathbb{R}$. L'ensemble $\mathbb{Q}^{\mathbb{N}}$ des suites de nombres rationnels forme un anneau commutatif pour l'addition et la multiplication coordonnée par coordonnée. Une suite de nombres rationnels $\{q_n\}$ est une **suite de Cauchy** si pour tout $\varepsilon \in \mathbb{Q}^{*+}$ il existe un $N \in \mathbb{N}$ tel que

$$|q_n - q_m| \leqslant \varepsilon \text{ pour tous } m, n \geqslant N.$$

On voit immédiatement que l'ensemble C des suites de Cauchy de nombres rationnels forme un sous-anneau de $\mathbb{Q}^{\mathbb{N}}$.

Une suite de nombres rationnels $\{q_n\}$ **converge vers 0** si pour tout $\varepsilon \in \mathbb{Q}^{*+}$, il existe un $N \in \mathbb{N}$ tel que $|q_n| \leqslant \varepsilon$ pour tout $n \geqslant N$. On vérifie facilement que l'ensemble I des suites de nombres rationnels qui convergent vers zéro forme un idéal de l'anneau C des suites de Cauchy. L'ensemble $\mathbb{R}$ des **nombres réels** est l'anneau quotient C/I. À chaque élément $q \in \mathbb{Q}$ nous pouvons faire correspondre la suite dont tous les éléments sont égaux à q, et nous immergeons ainsi de manière naturelle $\mathbb{Q}$ dans $\mathbb{R}$.

L'ensemble des nombres réels $\mathbb{R}$ possède un ordre naturel. On définit le fait que $a \in \mathbb{R}$ est **strictement positif** en demandant qu'il existe un $\varepsilon \in \mathbb{Q}^{*+}$ et un $N \in \mathbb{N}$ tels que $a_n \geqslant \varepsilon$ pour tout $n \geqslant N$. On vérifie facilement que cette définition respecte l'égalité de $\mathbb{R} = C/I$, et que l'ensemble des nombres réels strictement positifs est stable pour l'addition et la multiplication. Nous écrivons $a < b$, ou $b > a$, si $b - a$ est strictement positif ; en particulier, $a > 0$ signifie que a est strictement positif.

Théorème 3.1. *Les conditions suivantes pour un nombre réel a sont équivalentes.*

(i) *Il existe un $\varepsilon \in \mathbb{Q}^{*+}$ et un $N \in \mathbb{N}$ tels que $|a_n| \geqslant \varepsilon$ pour tout $n \geqslant N$.*

(ii) *$a < 0$ ou $a > 0$.*

(iii) *a est inversible.*

Démonstration. Supposons (i). Nous pouvons supposer que $|a_N - a_n| < \varepsilon/2$ pour tout $n \geqslant N$. Si $a_N \geqslant \varepsilon$, alors $a_n > \varepsilon/2$ pour tout $n \geqslant N$, donc $a > 0$. De même, si $a_N \leqslant -\varepsilon$, $a < 0$.

Supposons (ii), par exemple $a > 0$. Il existe un $\varepsilon \in \mathbb{Q}^{*+}$ et un $N \in \mathbb{N}$ tels que $a_n > \varepsilon$ pour tout $n \geqslant N$. Nous pouvons supposer que $a_n > \varepsilon$ pour *tout* $n \in \mathbb{N}$. Alors la suite $\{1/a_n\}$ est une suite de Cauchy et elle est l'inverse de a dans $\mathbb{R}$.

Finalement supposons (iii). Il existe une suite de Cauchy $\{b_n\}$ telle que $a_n b_n - 1$ converge vers 0. Considérons un $\varepsilon \in \mathbb{Q}^{*+}$ tel que $|b_n| < 1/\varepsilon$ pour tout n. Alors $|a_n|$ est plus grand que ε pour n assez grand. □

Nous définissons une inégalité sur $\mathbb{R}$ en disant que $a \neq b$ signifie que $b - a$ est inversible, de sorte que le théorème 3.1 nous dit que $a \neq b$ si, et seulement si, $a < b$ ou $b < a$. La cotransitivité de $a < b$ est le substitut constructif de la loi de trichotomie classique.

Théorème 3.2 (cotransitivité)**.** *Soient a, b et c des nombres réels. Si $a < c$, alors $a < b$ ou $b < c$.*

Démonstration. Considérons $m \in \mathbb{N}$ et $\varepsilon > 0$ tels que $a_m < c_m - 6\varepsilon$ et, pour tout $n \geqslant m$,

$$|a_n - a_m| < \varepsilon,$$
$$|c_n - c_m| < \varepsilon \text{ et}$$
$$|b_n - b_m| < \varepsilon.$$

Ou bien $b_m < c_m - 3\varepsilon$, auquel cas $b_n < c_n - \varepsilon$ pour tout $n \geqslant m$, et donc $b < c$, ou bien $b_m > a_m + 3\varepsilon$, auquel cas $b_n > a_n + \varepsilon$ pour tout $n \geqslant m$, et donc $b > a$. □

Nous écrivons $a \leqslant b$ lorsque $a < b + \varepsilon$ pour tout $\varepsilon > 0$. Cette relation est clairement transitive et réflexive. Pour démontrer que c'est une relation d'ordre, nous avons besoin du résultat suivant.

Théorème 3.3. *Si $a \leqslant b$ et $b \leqslant a$, alors $a = b$.*

Démonstration. Soit un $\varepsilon \in \mathbb{Q}^{*+}$. Comme $a \leqslant b$, nous avons un $N \in \mathbb{N}$ tel que $a_n - b_n < \varepsilon$ pour tout $n \geqslant N$. Comme $b \leqslant a$, nous avons un tel N qui vérifie en outre que $b_n - a_n < \varepsilon$ pour tout $n \geqslant N$. Cela dit que $|a_n - b_n| < \varepsilon$ pour tout $n \geqslant N$, et nous avons donc montré que $a_n - b_n$ converge vers 0, ce qui signifie que $a = b$. □

Corolaire 3.4. $\mathbb{R}$ *est un corps de Heyting.*

Démonstration. Si $a + b \neq 0$, ou bien $a + b > 0$, ou bien $a + b < 0$, et nous pouvons supposer que $a + b > 0$. Alors ou bien $a > 0$, ou bien $a < a + b$, en vertu du théorème 3.2 ; dans le premier cas on a $a \neq 0$, dans le second on a $0 < b$ et donc $b \neq 0$. Ainsi l'inégalité sur $\mathbb{R}$ est cotransitive.

Pour montrer que l'inégalité est étroite, supposons que $a \neq 0$ soit impossible. Pour chaque $\varepsilon > 0$, ou bien $a > 0$, ou bien $a < \varepsilon$ en vertu du théorème 3.2 ; le premier cas est impossible, donc $a < \varepsilon$. Par suite $a \leqslant 0$. De manière analogue $a \geqslant 0$, de sorte que $a = 0$ par le théorème 3.3. □

L'ensemble $\mathbb{R}$ n'est pas seulement un ensemble ordonné, c'est un treillis. Si a et b sont des nombres réels, alors la suite $c_n = \max(a_n, b_n)$ définit un nombre réel c qui est le supremum de a et b, ce que l'on écrit $c = \sup(a, b)$. L'infimum de a et b est $\inf(a, b) = -\sup(-a, -b)$. On peut définir la valeur absolue du nombre réel a comme $|a| = \sup(a, -a)$.

Le corps $\mathbb{C}$ des **nombres complexes** est obtenu à partir de l'espace vectoriel $\mathbb{R}^2$ en définissant la multiplication $(a, b)(c, d) = (ac - bd,\ ad + bd)$. On vérifie facilement que $\mathbb{C}$ est un corps de Heyting avec le neutre multiplicatif $(1, 0)$. Nous posons $i = (0, 1)$ et nous voyons que $i^2 = -1$ et que $\mathbb{C} = \mathbb{R} + \mathbb{R}i$.

Un **espace métrique** est un ensemble S donné avec une fonction d, appelée la **métrique**, ou encore la **distance**, de $S \times S$ vers $\mathbb{R}$ telle que

(i) $d(x, y) = d(y, x) \geqslant 0$,

(ii) $d(x, y) = 0$ si, et seulement si, $x = y$,

(iii) $d(x, z) \leqslant d(x, y) + d(y, z)$.

Les nombres réels forment un espace métrique pour la distance $d(x, y) = |x - y|$. Une **suite de Cauchy** dans un espace métrique S est une suite $\{x_n\}$ dans S telle que pour tout $\varepsilon \in \mathbb{Q}^{*+}$ il existe un $N \in \mathbb{N}$ tel que

$$d(x_n, x_m) \leqslant \varepsilon \text{ pour tous } m, n \geqslant N.$$

Une suite $\{x_n\}$ dans S **converge** vers $y \in S$ si pour tout $\varepsilon \in \mathbb{Q}^{*+}$ il existe un $N \in \mathbb{N}$ tel que $d(x_n, y) \leqslant \varepsilon$ pour tout $n \geqslant N$. Si $\{x_n\}$ converge vers y, nous disons que y est la **limite** de la suite $\{x_n\}$. On vérifie facilement que toute suite convergente est une suite de Cauchy. Si, inversement, toute suite de Cauchy converge vers un élément de S, nous disons que l'espace métrique S est **complet**. L'espace $\mathbb{R}$ est complet.

En imitant la construction de $\mathbb{R}$ à partir de $\mathbb{Q}$, nous pouvons immerger n'importe quel espace métrique S dans sa **complétion** $\hat{S}$, dont les éléments sont les suites de Cauchy dans S, avec $d(a, b)$ égal à la limite de $d(a_n, b_n)$, et en définissant $a = b$ par $d(a, b) = 0$. L'espace S est **dense** dans $\hat{S}$, i.e. pour tout ε strictement positif et tout $s \in \hat{S}$, on a un $a \in S$ tel que $d(a, s) < \varepsilon$. L'espace $\hat{S}$ est complet.

Exercices

1. Montrer que $a > b$ est impossible si, et seulement si, $a \leqslant b$.
2. Montrer que les propriétés suivantes sont équivalentes.
   (i) Pour tout $a \in \mathbb{R}$, ou bien $a > 0$ ou bien $a \leqslant 0$.
   (ii) LPO.
3. Montrer que $\mathbb{R}$ est un treillis distributif pour la relation d'ordre $\leqslant$.
4. Montrer que $|a| \geqslant 0$, et que $|a|$ est > 0 si, et seulement si, $a \neq 0$. Montrer que $|a + b| \leqslant |a| + |b|$.
5. Montrer que les propriétés suivantes sont équivalentes.
   (i) LLPO.
   (ii) Pour tout $a \in \mathbb{R}$, ou bien $a \leqslant 0$ ou bien $a \geqslant 0$.
   (iii) Pour tous $a, b \in \mathbb{R}$, si $ab = 0$, alors $a = 0$ ou $b = 0$.
   (iv) Si $a, b \in \mathbb{R}$, alors on a un $c \in \mathbb{R}$ tel que $a = cb$ ou $b = ca$.
   (v) Pour tous $a, b \in \mathbb{R}$, si $\sup(a, b) = 1$, alors $a = 1$ ou $b = 1$.
6. Montrer que le principe de Markov équivaut à ce que $\mathbb{R}$ soit un corps par négation.
7. *Le corps des nombres p-adiques.* Si p est un nombre premier, la **métrique p-adique sur** $\mathbb{Q}$ est définie pour $x_1 \neq x_2$ en posant $d(x_1, x_2) = p^n$ lorsque $p^n(x_1 - x_2)$ peut être écrit avec un numérateur et un dénominateur non divisibles par p. Montrer que d est une métrique, et que la complétion de $\mathbb{Q}$ pour cette métrique est un corps de Heyting.
8. Montrer que tout espace métrique est dense dans sa complétion, et que sa complétion est un espace métrique complet.

4 Modules

Si R est un anneau, un **R-module à gauche** est un groupe abélien additif M donné avec une fonction μ de $R \times M$ vers M, écrite $\mu(r,a) = ra$, appelée **multiplication scalaire**, telle que

(i) $r(a+b) = ra + rb$

(ii) $(r+s)a = ra + sa$

(iii) $(rs)a = r(sa)$

(iv) $1 \cdot a = a$

pour tous r, $s \in R$ et a, $b \in M$. Les **R-modules à droite** sont définis de la même manière, à ceci près que la multiplication scalaire est à droite : la seule réelle différence se trouve dans (iii) que l'on doit lire $a(rs) = (ar)s$, de sorte que pour les modules à droite, multiplier par rs est la même chose que d'abord multiplier par r et ensuite multiplier par s, tandis que pour les modules à gauche, multiplier par rs est la même chose que multiplier d'abord par s puis par r.

Tout groupe abélien est un $\mathbb{Z}$-module. L'ensemble R^n des n-uplets d'éléments de R est un R-module pour l'addition et la multiplication scalaire coordonnée par coordonnée. Si R est un anneau à division, un R-module est appelé un **espace vectoriel** sur R.

Soient M et N des R-modules à gauche. Un homomorphisme de groupes f de M vers N est un **homomorphisme de R-modules**, ou **une application R-linéaire**, si $f(ra) = rf(a)$ pour tous $r \in R$ et $a \in M$. Le **noyau** de f est $\ker f = \{\, a \in M : f(a) = 0 \,\}$, et l'**image** de f est $\operatorname{im} f = \{\, f(a) : a \in M \,\}$. On vérifie facilement que la catégorie des R-modules est une catégorie pré-additive.

L'ensemble $\mathrm{E}(M)$ des endomorphismes d'un groupe abélien M forme un anneau, où la multiplication est la composition des fonctions. Si R est un anneau et f est un homomorphisme d'anneaux de R vers $\mathrm{E}(M)$, alors M peut être muni d'une structure de R-module en posant $rm = f(r)m$ pour $r \in R$ et $m \in M$. Inversement, si M est un R-module, alors on peut définir un homomorphisme d'anneaux φ de R vers $\mathrm{E}(M)$ en posant $\varphi(r)(m) = rm$. L'homomorphisme φ est appelé une **représentation** de R comme anneau d'endomorphismes de M. Les représentations et les modules sont deux manières de regarder la même chose. Si le noyau de la représentation est nul, la représentation est dite **fidèle**. Un R-module M est **fidèle** si $r = 0$ chaque fois que $rm = 0$ pour tout $m \in M$.

Un sous-groupe N d'un R-module M est un **R-sous-module** si $ra \in N$ pour tous $a \in N$ et $r \in R$. Le sous-module de M engendré par un sous-ensemble X est le sous-groupe additif engendré par l'ensemble $\{\, rx : r \in R \text{ et } x \in X \,\}$. Le groupe quotient M/N est un R-module parce que la multiplication scalaire opère sur lui. Les théorèmes 1.1 et 1.2 s'appliquent pour les R-modules si nous remplaçons partout « groupe » par « module », et si nous considérons que tous les sous-modules sont normaux (ce qu'ils sont en tant que sous-groupes).

Si R et S sont des sous-anneaux d'un anneau A, alors A est, entre autres choses, un R-module à gauche et un S-module à droite. Ce genre de situation se produit suffisamment souvent pour mériter un nom. Soient R et S des anneaux et soit M un R-module à gauche qui est aussi un S-module à droite. Alors on dit que M est un **R-S-bimodule** si $(ra)s = r(as)$ pour tous $r \in R$, $a \in M$ et $s \in S$. Ainsi l'anneau R est un R-R-bimodule, et tout R-module est un R-$\mathbb{Z}$-bimodule. Si R est un anneau commutatif, il n'y a aucune différence entre R-modules à droite et à gauche, et chacun est un R-R-bimodule.

Les idéaux de R peuvent être décrits en termes des structures de modules sur R : un idéal à gauche est un sous-module du module à gauche R, un idéal à droite est un sous-module du module à droite R, et un idéal bilatère est un sous-module du R-R-bimodule R.

Soient M un R-module et $\{A_i\}_{i\in I}$ une famille de sous-modules de M. Le sous-module de M engendré par $\bigcup_{i\in I} A_i$ est noté $\sum_{i\in I} A_i$. Les A_i sont dits **indépendants** si lorsque $i_1, \ldots, i_n, j \in I$ et $x \in A_j \cap (A_{i_1} + \cdots + A_{i_n})$, alors ou bien $x = 0$ ou bien $i_m = j$ pour un m. Nous disons que M est la **somme directe** (**interne**) des sous-modules A_i, et nous écrivons $M = \bigoplus_{i\in I} A_i$, si $M = \sum_{i\in I} A_i$ avec les A_i indépendants. Si $I = \{1, \ldots, n\}$, nous écrivons $M = A_1 \oplus \cdots \oplus A_n$. Lorsque $I = \{1, 2\}$, on a $M = A_1 \oplus A_2$ si, et seulement si, $M = A_1 + A_2$ et $A_1 \cap A_2 = 0$. Par exemple, $M = \mathbb{Z}/(6)$, $A_1 = \{0, 2, 4\}$, et $A_2 = \{0, 3\}$.

Le produit d'une famille de R-modules $\{A_i\}_{i\in I}$ possède une structure naturelle de R-module pour laquelle il est le produit catégorique, ou **produit direct**, des modules A_i. Si f et g sont des fonctions dans ce produit, on définit $f + g$ par $(f + g)(i) = f(i) + g(i)$, et rf par $(rf)(i) = rf(i)$. Le produit direct est noté $\prod_{i\in I} A_i$.

Soient I un ensemble discret et $\{A_i\}_{i\in I}$ une famille de R-modules. Nous pouvons construire le coproduit catégorique (somme directe externe) de la manière suivante. Un élément $f \in \prod_{i\in I} A_i$ a un **support fini** s'il existe un sous-ensemble fini J de I tel que $f(i) = 0$ pour $i \in I \setminus J$. Pour un ensemble discret I, la somme directe externe de la famille $\{A_i\}_{i\in I}$ est l'ensemble des éléments du produit direct qui ont un support fini. On voit facilement que si f et g ont des supports finis, alors il en va de même pour $f + g$ et rf, de sorte que la somme directe externe est un sous-module du produit direct. Notez que si I est fini, alors le produit direct et la somme directe externe sont le même module. Si nous identifions le module A_i avec le sous-module $\{ f : f(j) = 0 \text{ pour } j \neq i \}$, nous voyons que la somme directe externe est une somme directe.

La construction précédente pose un problème si l'ensemble d'indices I n'est pas discret, parce que si A_i est discret et si $\{ f : f(j) = 0 \text{ pour } j \neq i \}$ contient un élément non nul, alors $\{i\}$ est une partie détachable de I. Pour construire une **somme directe externe** lorsque l'ensemble d'indices I n'est pas nécessairement discret, on considère l'ensemble F des suites finies d'éléments de la réunion disjointe des A_i. Soit alors l'égalité sur F engendrée par

(i) $(a_1, \ldots, a_n) = (a_{\sigma(1)}, \ldots, a_{\sigma(n)})$ si σ est une permutation de $\{1, \ldots, n\}$.

(ii) $(a_1, \ldots, a_{n-1}, a_n) = (a_1, \ldots, a_{n-1})$ si $a_n = 0$.

(iii) $(a_1, \ldots, a_{n-1}, a_n) = (a_1, \ldots, a_{n-1} + a_n)$ si a_{n-1} et a_n sont des éléments d'un même A_i.

Plus précisément, disons que deux suites de F sont **adjacentes** lorsqu'une permutation de l'une est obtenue en appliquant (ii) ou (iii) à une permutation de l'autre. Alors σ et τ sont **égales** dans F si l'on a une chaine de suites de F

$$\sigma = s_1, s_2, \ldots, s_m = \tau$$

telle que s_i est adjacente à s_{i+1} pour $i = 1, \ldots, m-1$.

Nous désirons identifier $\{\, (a) \in F : a \in A_i \,\}$ avec A_i. Pour ce faire nous devons montrer que si $(a) = (b)$, alors $a = b$. Cela est une conséquence de la propriété de Church-Rosser pour F.

Lemme 4.1 (propriété de Church-Rosser)**.** *Supposons que les suites σ et τ sont égales dans F, et notons $\ell(s)$ la longueur de la suite s. Alors il existe une chaine $\sigma = s_1, s_2, \ldots, s_m = \tau$ de suites de F telle que s_i est adjacente à s_{i+1} pour $i = 1, \ldots, m-1$, et pour $i = 2, \ldots, m-1$, si $\ell(s_{i-1}) < \ell(s_i)$, alors $\ell(s_i) < \ell(s_{i+1})$.*

Démonstration. Soit $\sigma = s_1, s_2, \ldots, s_m = \tau$ une chaine de suites de F telle que s_i est adjacente à s_{i+1} pour $i = 1, \ldots, m-1$. Nous procédons par récurrence sur $N = \sum_i \ell(s_i)$, en montrant que si $\ell(s_{i-1}) < \ell(s_i)$ et $\ell(s_i) > \ell(s_{i+1})$ pour un i, alors nous pouvons diminuer N.

Supposons que nous allions de s_i à s_{i+1} en supprimant un zéro z. Si z apparait dans s_{i-1}, nous pouvons remplacer s_i par s_{i-1} dans laquelle nous supprimons z. Sinon s_{i-1} provient de s_i en supprimant z, auquel cas nous pouvons omettre s_i. Le même argument s'applique si nous allons de s_i à s_{i-1} en supprimant un zéro.

Supposons que nous allions de s_i à s_{i+1}, et de s_i à s_{i-1}, en appliquant (iii). Dépendant du nombre de positions distinctes de s_i qui sont concernées, nous pouvons décrire les différents cas comme suit

s_{i-1}	s_i	s_{i+1}
$(a+b)$	(a,b)	$(a+b)$
$(a+b,c)$	(a,b,c)	$(a,b+c)$
$(a+b,c,d)$	(a,b,c,d)	$(a,b,c+d)$

Dans le premier cas nous pouvons omettre s_i et s_{i+1}. Dans le second cas, nous pouvons remplacer s_i par $(a+b+c)$, et dans le troisième nous pouvons remplacer s_i par $(a+b, c+d)$. □

Deux suites de F sont additionnées en les concaténant, la multiplication scalaire est faite coordonnée par coordonnée, et la suite vide sert d'élément neutre.

Vu la relation d'égalité nous pouvons de manière sûre et sans ambigüité écrire un élément $(a_1, a_2, \ldots, a_n)$ de F comme une somme formelle $a_1 + a_2 + \cdots + a_n$.

En identifiant le module A_i avec $\{(a) : a \in A_i\}$, nous voyons que F est somme directe interne des A_i ; la vérification de cette affirmation téméraire est laissée en exercice 5.

Si I est discret et si $(a_1, \ldots, a_n) \in F$, nous pouvons supposer que $a_m \in A_{i_m}$ avec $i_m \neq i_{m'}$ si $m \neq m'$, et nous pouvons identifier F avec l'ensemble des éléments de $\prod_{i\in I} A_i$ qui ont un support fini, comme précédemment.

Si chaque A_i est un même module M et si I est un ensemble d'indices arbitraire, nous notons la somme directe externe par $M^{(I)}$.

Le théorème suivant dit qu'une somme directe interne (et donc aussi la somme directe externe que nous avons identifiée à une somme directe interne) est un coproduit catégorique.

Théorème 4.2. *Si $M = \bigoplus_{i\in I} A_i$ et si $f_i \colon A_i \to N$ est une famille d'applications R-linéaires, alors il y a une unique application R-linéaire f de M vers N telle que $f = f_i$ sur A_i pour tout $i \in I$.*

Démonstration. Si $x \in M = \sum_{i\in I} A_i$, alors $x = \sum_{m=1}^{n} a_{i_m}$, avec $a_{i_m} \in A_{i_m}$. Par suite $f(x)$ doit être égal à $\sum_{m=1}^{n} f_{i_m}(a_{i_m})$, et donc f est unique. Si nous définissons $f(x)$ comme égal à $\sum_{m=1}^{n} f_{i_m}(a_{i_m})$, nous devons montrer que $f(x)$ est bien défini ; il suffit de montrer que si $x = 0$, alors $f(x) = 0$. Supposons que $x = \sum_{m=1}^{n} a_{i_m} = 0$. Comme les A_i sont indépendants, ou bien $a_{i_m} = 0$ pour chaque m, ou bien il y a un $m \neq m'$ tel que $i_m = i_{m'}$. Dans le dernier cas, nous pouvons additionner a_{i_m} et $a_{i_{m'}}$ dans A_{i_m}, et par suite $f(x) = 0$ pas récurrence sur n. On vérifie facilement que f est une application R-linéaire. □

Un R-module F est **libre** sur une famille d'éléments $\{x_i\}_{i\in I}$ de F si pour chaque fonction f qui envoie I dans le R-module M, il y a une unique application R-linéaire f^* de F vers M telle que $f^*(x_i) = f(i)$. Nous disons que $\{x_i\}_{i\in I}$ est une **base** pour F. L'unicité de f^* implique que des modules libres sur $\{x_i\}_{i\in I}$ et sur $\{y_i\}_{i\in I}$ sont isomorphes pour un isomorphisme qui envoie x_i sur y_i, de sorte que des modules libres dont les bases ont le même ensemble d'indices sont essentiellement les mêmes. Si $F = \bigoplus_{i\in I} Rx_i$ et si la fonction de R vers Rx_i qui envoie r sur rx_i est un isomorphisme pour chaque $i \in I$, le théorème 4.2 montre que F est libre sur $\{x_i\}_{i\in I}$. Si R est un anneau non trivial, alors $x_i \neq 0$ pour chaque $i \in I$, de sorte que si $x_i = x_j$, alors $i = j$; ainsi les éléments x_i de la base sont en correspondance bijective avec les éléments i de I. Ainsi lorsque nous nous restreignons aux anneaux non triviaux, nous pourrons définir une base comme un *ensemble* plutôt que comme une famille. Si R est un anneau trivial, alors toute famille d'éléments de n'importe quel R-module M est une base pour M.

Soit I un ensemble discret, et pour chaque $i \in I$ soit $\delta_i \in R^{(I)}$ tel que $\delta_i(i) = 1$ et $\delta_i(j) = 0$ pour $j \neq i$. Alors $R^{(I)}$ est libre sur $\{\delta_i\}_{i\in I}$. Pareillement, supposons

que I est un ensemble d'indices arbitraire, et que $\{R_i\}_{i\in I}$ est une famille telle que chaque R_i est une copie de R. Si pour chaque $i \in I$ nous définissons x_i comme la suite de longueur 1 dont l'élément est le neutre multiplicatif de R_i, alors $R^{(I)}$ est libre sur $\{x_i\}_{i\in I}$. Par abus de langage nous dirons que $R^{(I)}$ est **le module libre sur** I.

Si $I = \{1, \ldots, n\}$, alors nous écrivons R^n au lieu de $R^{(I)}$. Un module M possède une base de n éléments si, et seulement si, il est isomorphe à R^n, auquel cas nous disons que M est un **module libre de rang** n. Dans la section 6 nous verrons que pour un anneau commutatif non trivial R, le rang de M est un invariant. L'exercice 3 donne un exemple d'un anneau non commutatif non trivial R tel que les R-modules à gauche R et R^2 sont isomorphes.

Un R-module M est **de type fini** s'il existe une application R-linéaire surjective de R^n sur M pour un n strictement positif ; c'est-à-dire s'il existe des éléments $x_1, \ldots, x_n$ de M tels que tout élément de M peut s'écrire sous la forme $\sum_{i=1}^n r_i x_i$. Un R-module M est **cyclique** s'il existe une application R-linéaire surjective de R sur M ; c'est-à-dire s'il existe un $x \in M$ tel que tout élément de M est un multiple scalaire de x.

Théorème 4.3. *Soit R un sous-anneau d'un anneau E. Si M est un E-module de type fini (libre de rang n) et si E est un R-module de type fini (libre de rang m), alors M est un R-module de type fini (libre de rang mn).*

Démonstration. Soient $\varphi\colon R^m \to E$ un épimorphisme (isomorphisme) de R-modules et $\psi\colon E^n \to M$ un épimorphisme (isomorphisme) de E-modules. Alors $\varphi^n\colon R^{mn} \to E^n$ est un épimorphisme (isomorphisme) de R-modules, et $\psi\varphi^n\colon R^{mn} \to M$ est un épimorphisme (isomorphisme) de R-modules. □

Un R-module P est dit **projectif** si pour toute application R-linéaire g d'un R-module A sur un R-module B, et toute application R-linéaire f de P vers B, il existe une application R-linéaire $h\colon P \to A$ telle que $gh = f$. Les modules libres de rang fini sont projectifs : si $x_1, \ldots, x_n$ est une base de P, alors il existe $a_1, \ldots, a_n \in A$ tels que $g(a_i) = f(x_i)$ pour chaque i, et on a une application R-linéaire h telle que $h(x_i) = a_i$ pour chaque i ; les applications R-linéaires gh et f sont égales parce qu'elles coïncident sur la base.

Soit M un R-module de type fini. Si π est un épimorphisme d'un R-module libre de rang fini F sur M, de noyau K, alors M est isomorphe à F/K. Le théorème suivant montre ce qu'il advient lorsque nous obtenons la même chose pour d'autres couples (F, π) ; le résultat ressemble à la règle pour déterminer quand deux fractions sont égales.

Théorème 4.4 (l'astuce de Schanuel)**.** *Soient M un R-module, P_1 et P_2 des R-modules projectifs, et π_i une application R-linéaire de P_i sur M ($i = 1, 2$). Si K_i est le noyau de π_i, alors $K_1 \oplus P_2$ est isomorphe à $K_2 \oplus P_1$.*

Démonstration. Comme les modules P_i sont projectifs, nous avons des applications R-linéaires $\varphi_1 \colon P_2 \to P_1$ et $\varphi_2 \colon P_1 \to P_2$ qui vérifient $\pi_1\varphi_1 = \pi_2$ et $\pi_2\varphi_2 = \pi_1$. Considérons l'application R-linéaire de $K_1 \oplus P_2$ vers $K_2 \oplus P_1$ qui envoie (k_1, p_2) sur (k_2, p_1) où

$$k_2 = p_2 - \varphi_2(k_1 + \varphi_1 p_2), \quad p_1 = k_1 + \varphi_1 p_2$$

et l'application R-linéaire de $K_2 \oplus P_1$ vers $K_1 \oplus P_2$ qui envoie (k_2, p_1) sur (k_1, p_2) où

$$k_1 = p_1 - \varphi_1(k_2 + \varphi_2 p_1), \quad p_2 = k_1 + \varphi_2 p_1$$

On vérifie facilement que ces applications R-linéaires sont inverses l'un de l'autre. □

Un élément e d'un anneau est **idempotent** si $e^2 = e$. Un sous-module A de M est un **facteur direct** de M s'il existe un sous-module B de M, appelé un **supplémentaire** de A dans M, tel que $M = A \oplus B$. Les sous-modules 0 et M de M sont toujours facteurs directs supplémentaires l'un de l'autre.

Théorème 4.5. *Soit A un sous-module d'un R-module M. Alors A est un facteur direct de M si, et seulement si, il y a un endomorphisme idempotent e de M tel que $A = eM$. Dans ce cas le sous-module $(1-e)M$ et un supplémentaire de A.*

Démonstration. Supposons que $M = A \oplus B$. Si $x \in M$, nous pouvons écrire x de manière unique sous la forme $a + b$ pour un $a \in A$ et un $b \in B$. On définit un endomorphisme e de M en posant $e(x) = a$. On voit facilement que e est idempotent et que $eM = A$.

Inversement, supposons que e est un endomorphisme idempotent de M et que $A = eM$. Posons $B = (1-e)M$. Comme $x = ex + (1-e)x$, nous avons $A + B = M$. Si $x \in A \cap B$, alors $x = (1-e)y$ et $x = ez$. Donc $ex = e(1-e)y = (e - e^2)y = 0$ et $ex = e^2 z = ez = x$, de sorte que $x = 0$. Ainsi $A \cap B = 0$. □

L'idempotent e dans le théorème 4.5 est appelé la **projection** de M sur A (parallèlement à B).

Exercices

1. L'**anneau opposé** R^{op} d'un anneau R est formé avec le groupe additif R et la multiplication $ab \in R^{op}$ définie comme le produit ba de R. Montrer que tout R-module à gauche est un R^{op}-module à droite de manière naturelle. Si R est un anneau commutatif, l'anneau opposé est isomorphe à R, donc tout R-module à gauche est aussi un R-module à droite, et il n'est pas nécessaire de distinguer entre R-modules à gauche et à droite.

2. Soit R un anneau et soit M un R-module. Montrer qu'il existe un homomorphisme surjectif d'un R-module libre sur M.

3. Soient A et B des espaces vectoriels sur un corps discret k, chacun avec une base dénombrable infinie. Soit $V = A \oplus B$ et soit R l'anneau des endomorphismes de V. Construire un $x \in R$ tel que $xA = 0$ et $x\colon B \to V$ est un isomorphisme, et un $y \in R$ tel que $yB = 0$ et $y\colon A \to V$ est un isomorphisme. Montrer que $Rx \simeq Ry \simeq R$ comme R-modules, et que $R = Rx \oplus Ry$. Que nous dit cet exercice ?

4. Soient M un R-module et $\{A_i\}_{i\in I}$ une famille de R-modules. Soit $\{f_i\}_{i\in I}$ une famille d'homomorphismes de R-modules telle que f_i envoie M dans A_i. Soit π_i la projection de $\prod_{i\in I} A_i$ vers A_i. Montrer qu'il existe une unique application R-linéaire f de M vers $\prod_{i\in I} A_i$ telle que $\pi_i f = f_i$ pour chaque $i \in I$.

5. Soit F la somme directe externe de la famille $\{A_i\}_{i\in I}$, pour un ensemble d'indices arbitraire I. Montrer que l'homomorphisme de A_i vers F défini en envoyant $a \in A_i$ sur la suite (a) définie avant le lemme 4.1 est un monomorphisme. Montrer que si nous identifions A_i avec son image par ce monomorphisme, alors $F = \bigoplus_{i\in I} A_i$.

6. *Un facteur n'est pas nécessairement facteur direct.* Soit a une suite binaire fugitive, et soit $S = \{0, s, 2s, t, 2t\}$ avec
   — $s = t$ et $2s = 2t$ si $a_n = 1$ pour un entier pair n,
   — $s = 2t$ et $2s = t$ si $a_n = 1$ pour un entier impair n.
   Soit $I = \{x, y\}$ avec $x = y$ si $a_n = 1$ pour un n. Enfin soient $A_x = \{0, s, 2s\}$ et $A_y = \{0, t, 2t\}$ avec leurs structures évidentes de groupes à trois éléments. Montrer que l'on obtient ainsi un exemple brouwerien (LLPO) avec A_x qui n'est pas facteur direct dans $\bigoplus_{i\in I} A_i$.

7. Soient $\{A_i\}_{i\in I}$ une famille de modules et $f_i\colon A_i \to A$ une famille d'isomorphismes. Montrer que le noyau de l'homomorphisme $f\colon \bigoplus_{i\in I} A_i \to A$ induit par les isomorphismes f_i est un supplémentaire de chaque sous-module A_i.

8. Montrer que $A \oplus B$ est projectif si, et seulement si, A et B sont projectifs. Construire un module projectif à deux éléments sur l'anneau $\mathbb{Z}/(6)$.

9. Montrer qu'un module libre sur un ensemble projectif (voir l'exercice I.3.4) est projectif. Quel est le module libre sur un ensemble vide ?

10. *Les modules libres ne sont pas nécessairement projectifs.* Construire un exemple brouwerien pour une application R-linéaire α depuis un module F_1 libre de rang 2 sur un module libre F_2 tel qu'il n'y a pas d'application R-linéaire φ de F_2 vers F_1 avec $\alpha\varphi$ égal à l'application identique sur F_1. Suggestion : soient F_2 et F_1 des k-modules libres sur les ensembles A et B de l'exemple 3.1, où k est l'anneau des entiers modulo 2.

11. Montrer que si les modules libres sur des bases discrètes sont projectifs, alors l'axiome du choix le plus simple du monde est valide.
12. Soient I un ensemble discret et φ un homomorphisme non trivial de $\mathbb{Z}$-modules, de $\mathbb{Z}^{(I)}$ vers $\mathbb{Z}$. Montrer que $\ker\varphi$ est un facteur direct de $\mathbb{Z}^{(I)}$ si, et seulement si, $\operatorname{im}\varphi$ est cyclique. Construire un exemple brouwerien d'un homomorphisme φ (pas nécessairement non trivial) tel que $\ker\varphi$ est facteur direct mais $\operatorname{im}\varphi$ n'est pas cyclique.

5 Anneaux de polynômes

Si M est un monoïde et R un anneau, notons $R^{(M)}$ le R-module libre sur l'ensemble M. Nous pouvons voir les éléments de $R^{(M)}$ comme des sommes formelles finies $r_1m_1 + \cdots + r_nm_n$ avec les $m_i \in M$ et les $r_i \in R$. Définissons le produit de deux éléments de $R^{(M)}$ par

$$\Big(\sum\nolimits_{i=1}^{n} r_i m_i\Big)\Big(\sum\nolimits_{j=1}^{n'} r'_j m'_j\Big) = \sum\nolimits_{i=1}^{n}\sum\nolimits_{j=1}^{n'}(r_ir'_j)(m_im'_j).$$

Le produit $m_im'_j$ est le produit dans le monoïde M, tandis que $r_ir'_j$ est le produit dans l'anneau R. Cela fait de $R^{(M)}$ un anneau, que l'on appelle **la R-algèbre du monoïde** M [1], avec pour élément neutre multiplicatif $1 = 1_R1_M$. Si M est un groupe, alors $R^{(M)}$ est **la R-algèbre du groupe** M [2]. La fonction qui envoie r sur $r1$ est un isomorphisme de R sur un sous-anneau de $R^{(M)}$, et nous pouvons voir R comme un sous-ensemble de $R^{(M)}$ défini par cette immersion, autrement dit, l'élément $r1$ sera noté r et 1 sera identifié à 1_R.

Soit M le monoïde libre sur l'ensemble à un élément $\{X\}$. Alors

$$R^{(M)} = \{\, r_0 + r_1X + \cdots + r_nX^n : r_i \in R \text{ et } n \in \omega \,\}.$$

L'élément X est appelé une **indéterminée** et les éléments de $R^{(M)}$ sont appelés des **polynômes**. L'algèbre $R^{(M)}$ est notée $R[X]$ et on l'appelle l'**anneau de polynômes** [3] en (l'indéterminée) X (sur R).

L'anneau des polynômes en n indéterminées, $R[X_1, \ldots, X_n]$ est défini de manière inductive comme $R[X_1, \ldots, X_{n-1}][X_n]$. Un élément de $R[X_1, \ldots, X_n]$ écrit sous la forme $X_1^{e_1} \cdots X_n^{e_n}$ est appelé un **monôme** de **degré** $\sum_{i=1}^{n} e_i$. Si l'anneau R est discret, alors le **degré (total)** d'un polynôme non nul $f \in R[X_1, \ldots, X_n]$ est le maximum des degrés des monômes qui apparaissent dans f avec un coefficient non nul. L'anneau $R[X_1, \ldots, X_n]$ est le R-module libre sur l'ensemble des monômes ; en fait, les monômes forment un monoïde commutatif, et $R[X_1, \ldots, X_n]$ est la R-algèbre de ce monoïde.

1. **NdT.** Monoid ring.
2. **NdT.** Group ring.
3. **NdT.** Polynomial ring.

Si R est un sous-anneau d'un anneau commutatif S, un polynôme $f \in R[X_1, \dots, X_n]$ définit une fonction de S^n vers S : si $a_1, \dots, a_n$ sont des éléments de S, nous définissons $f(a_1, \dots, a_n)$ comme le résultat de la substitution des a_i aux X_i dans l'expression formelle de f, et en interprétant les opérations formelles dans $R[X_1, \dots, X_n]$ comme des opérations dans S. Nous demandons la commutativité parce que les indéterminées commutent les unes avec les autres ainsi qu'avec les éléments de R. Comme les a_i commutent entre eux, ainsi qu'avec les éléments de R, la fonction qui envoie f sur $f(a_1, \dots, a_n)$ est un homomorphisme d'anneaux.

Pour $n \in \mathbb{N}$, un polynôme $f \in R[X]$ qui peut être écrit sous la forme $\sum_{i=0}^{n-1} r_i X^i$ est dit être de **degré au plus** $n-1$, ce que l'on écrit $\deg f \leqslant n-1$, ou $\deg f < n$. Un polynôme est nul si, et seulement si, il a un degré au plus -1. Si $\deg f \leqslant d$ et si $r_d = 1$, nous disons que f est **unitaire**. Notez que ces définitions ne font pas référence à une inégalité sur R. Si $r_i \neq 0$ pour un $i \geqslant d$, nous disons que f est de **degré au moins** d, ce que l'on écrit $\deg f \geqslant d$. Si $\deg f \leqslant d$ et $\deg f \geqslant d$, nous disons que f est de **degré** d, et l'on écrit $\deg f = d$; dans ce cas nous disons que r_d est le **coefficient dominant** de f. Si R n'est pas discret, alors f n'a pas nécessairement un degré, même s'il a un coefficient non nul.

Si f et g sont des polynômes, nous écrivons $\deg f \leqslant \deg g$ si $\deg g < n$ implique $\deg f < n$ pour tout $n \in \mathbb{N}$; et nous écrivons $\deg f < \deg g$ si $\deg g < n+1$ implique $\deg f < n$ pour tout $n \in \mathbb{N}$. Notez que si $g = X^n + r_{n-1}X^{n-1} + \cdots + r_0$, alors $\deg f \leqslant \deg g$ si, et seulement si, $\deg f \leqslant n$, y compris si l'anneau est trivial.

Théorème 5.1. *Soient k un corps et $f, g \in k[X]$. Si $\deg f = m$ et $\deg g = n$, alors $\deg fg = m+n$.*

Démonstration. Soient a le coefficient dominant de f et b le coefficient dominant de g. Alors ab est le coefficient dominant de fg, et $\deg fg = \deg f + \deg g$. □

Théorème 5.2 (algorithme de division)**.** *Soit R un anneau commutatif et soient $f, g \in R[X]$ des polynômes tels que $\deg f \leqslant m$ et $\deg g \leqslant n \leqslant m+1$. Soit a le coefficient de X^n dans g. Il existe des polynômes $q, r \in R[X]$ tels que $a^{m-n+1} f = qg + r$ et $\deg r \leqslant n-1$.*

Démonstration. Nous procédons par récurrence sur $m-n$. Si $m-n = -1$, on prend $q = 0$ et $r = f$. Si $m-n \geqslant 0$ et $f = b_0 + b_1 X + \cdots + b_m X^m$, posons $f_1 = af - b_m X^{m-n} g$. Alors $\deg f_1 \leqslant m-1$, donc par récurrence $a^{m-n} f_1 = q_1 g + r$ pour un couple (q_1, r) de $R[X]$ avec $\deg r \leqslant n-1$. Ainsi $a^{m-n+1} f = (q_1 + a^{m-n} b_m X^{m-n})g + r$. □

Si le diviseur g est unitaire, ce que l'on peut supposer lorsque R est un corps discret, l'algorithme de division a une forme beaucoup plus agréable.

Corolaire 5.3. *Soient $f, g \in R[X]$ des polynômes sur un anneau commutatif R avec g unitaire. Alors il y a un unique couple (q, r) de $R[X]$ tel que $f = qg + r$ et $\deg r < \deg g$.*

Démonstration. Par le théorème 5.2 on a q et $r \in R[X]$, avec $\deg r < \deg g$, tel que $f = qg + r$. Pour démontrer l'unicité, on suppose que $f = q_1 g + r_1$ avec $\deg r_1 < \deg g$. Alors $(q - q_1)g = r_1 - r$ et $\deg(r_1 - r) < \deg g$, donc $q - q_1 = 0$ parce que g est unitaire (par récurrence sur l'entier n tel que $\deg(q - q_1) \leqslant n$), et ainsi $r_1 - r = 0$. □

Corolaire 5.4 (théorème du reste[1])**.** *Soient $f \in R[X]$ un polynôme sur un anneau commutatif R, et a un élément de R. Alors il existe un unique $q \in R[X]$ tel que $f(X) = q(X)(X - a) + f(a)$.*

Démonstration. Par le théorème 5.2 il existe $q \in R[X]$ et $r \in R$ uniques tels que $f(X) = q(X)(X - a) + r$. Mais alors $f(a) = q(a)(a - a) + r = r$. □

Sur un corps donné, nous pouvons construire un polynôme de degré au plus n qui prend des valeurs prescrites en $n + 1$ points distincts. Le théorème du reste montre que ce polynôme est unique, de sorte qu'un polynôme de degré au plus n ne peut pas avoir $n + 1$ racines distinctes. Ceci est l'un des quelques résultats dans la théorie générale des corps (comme opposés aux corps discrets ou aux corps de Heyting).

Théorème 5.5 (interpolation unique)**.** *Soient $a_0, \ldots, a_n$ des éléments deux à deux distincts dans un corps k, et soient $n + 1$ éléments $v_0, \ldots, v_n$ de k. Alors il existe un unique polynôme $f \in k[X]$ de degré au plus n tel que $f(a_i) = v_i$ pour chaque i.*

Démonstration. Nous démontrons l'existence par récurrence sur n. Si $n = 0$, prenons $f = v_0$. Si $n > 0$, alors par hypothèse de récurrence, on a un polynôme g de degré au plus $n - 1$ tel que $g(a_i) = (v_i - v_0)/(a_i - a_0)$ pour $1 \leqslant i \leqslant n$. Prenons $f(X) = (X - a_0)g(X) + v_0$.

Pour démontrer l'unicité, il suffit de montrer que si f est un polynôme de degré au plus n et si $f(a_i) = 0$ pour chaque i, alors $f = 0$. Nous procédons par récurrence sur n. Si $n = 0$, alors f est une constante, donc $f = 0$ parce que $f(a_0) = 0$. Supposons $n > 1$. Par le théorème du reste, nous pouvons écrire $f(X) = (X - a_n)g(X)$, où $\deg g \leqslant n - 1$. Comme $a_j \neq a_n$ pour $j < n$ et comme k est un corps, nous obtenons que $g(a_j) = 0$ pour $j < n$, donc $g = 0$ par récurrence. Par suite $f = 0$. □

1. **NdT.** Remainder theorem.

La démonstration du théorème 5.5 donne une construction par récurrence des coefficients λ_i de la **formule d'interpolation de Newton**

$$f = \lambda_0 + \lambda_1(X - a_0) + \lambda_2(X - a_0)(X - a_1) + \\ \cdots + \lambda_n(X - a_0)(X - a_1)\cdots(X - a_{n-1}).$$

Pour la **formule d'interpolation de Lagrange**, voir l'exercice 5.

Nous établissons l'algorithme d'Euclide pour les anneaux commutatifs discrets avec unités détachables, plutôt que seulement pour les corps discrets. L'algorithme construit le facteur commun recherché ou une non-unité non nulle. Une application typique est avec l'anneau $k[X]/(f)$, où k est un corps discret : la construction d'une non-unité non nulle donne une factorisation de f.

Théorème 5.6 (algorithme d'Euclide [1])**.** *Soient R un anneau commutatif discret avec unités détachables et I un idéal de type fini de $R[X]$. Ou bien l'idéal I est principal, ou bien il existe un élément de R non inversible et non nul.*

Démonstration. Ou bien $I = 0$, et alors I est principal, ou bien il y a un $n \in \mathbb{N}$ et un polynôme non nul $f \in I$ de degré $\deg f = n$. Nous pouvons supposer que f est unitaire (sinon nous avons une non-unité non nulle) et nous procédons par récurrence sur n. Si $n = 0$, alors $f = 1$, et donc $I = k[X] = (f)$. Si $n > 0$, alors chaque générateur g de I peut s'écrire comme $g = qf + r$ avec $\deg r < n$. Notons que $r \in I$. Ou bien chaque r est nul, ou bien l'un des r est $\neq 0$. Si chaque r est nul, alors $I = (f)$. Si un r est $\neq 0$, alors nous avons un polynôme non nul dans I de degré $< n$, et nous terminons par récurrence. □

Si $c = ab$ dans un anneau commutatif, alors nous disons que a **divise** c ; si a divise c nous disons que a est un **diviseur**, ou un **facteur**, de c.

Corolaire 5.7. *Soient k un corps discret et $a, b \in k[X]$. Alors il existe $s, t \in k[X]$ tels que $sa + tb$ divise a et b. Par suite $sa + tb$ est le plus grand commun diviseur de a et b au sens où tout diviseur commun de a et b divise $sa + tb$.*

Démonstration. Soit I l'idéal de $k[X]$ engendré par a et b. Comme k est un corps discret, le théorème 5.6 dit que I est principal ; autrement dit il existe s et t tels que $sa + tb$ divise a et b. □

Nous disons que deux éléments a et b dans un anneau commutatif sont **étrangers** [2] ou **fortement premiers entre eux** s'il existe des éléments s et t tels que $sa + tb = 1$. Ainsi le corolaire 5.7 implique que si deux polynômes sur un corps discret n'ont pas de facteur commun de degré strictement positif, ils sont étrangers. On voit facilement que si a et b sont étrangers et si a et c sont étrangers, alors a et bc sont étrangers (multiplier les deux équations).

1. **NdT.** L'algorithme d'Euclide est presque toujours utilisé sous la forme du corollaire 5.7, pour le cas où R est un corps discret. Voir cependant la démonstration du lemme IX.3.5.
2. **NdT.** Strongly relatively prime.

Exercices

1. Soient R et S des anneaux commutatifs, φ un homomorphisme d'anneaux de R vers S, et $s_1, \ldots, s_n$ des éléments de S. Montrer que φ admet une unique extension en un homomorphisme de $R[X_1, \ldots, X_n]$ vers S qui envoie X_i sur s_i.
2. Un **anneau intègre avec relation de séparation (étroite)** est un anneau intègre dont l'inégalité est une relation de séparation (étroite). Montrer que le corps de fractions d'un anneau intègre avec relation de séparation étroite est un corps de Heyting. Soient f et g des polynômes sur un anneau intègre avec relation de séparation R. Montrer que si $\deg f \geqslant i$ et $\deg g \geqslant j$, alors $\deg fg \geqslant i + j$. Utiliser ce résultat pour montrer que si R est un anneau intègre avec relation de séparation (étroite), alors il en va de même pour $R[X]$.
3. Soit R un anneau. L'**anneau des séries formelles** [1] $R[[X]]$ est défini comme l'ensemble des suites $\{a_n\}$ dans R, écrites sous la forme
$$a_0 + a_1 X + a_2 X^2 + \cdots ,$$
avec l'addition et la multiplication suggérées par la notation. Montrer que si R est un anneau intègre avec relation de séparation, il en va de même pour $R[[X]]$.
Idée. Supposez que R est un anneau intègre avec relation de séparation et que $fg = h \in R[[X]]$ avec
$$\begin{aligned} f &= f_0 + f_1 X + \cdots , \\ g &= g_0 + g_1 X + \cdots , \\ h &= h_0 + h_1 X + \cdots . \end{aligned}$$
Supposez que $f_i \neq 0$ et $g_j \neq 0$ pour un i, j ; montrez que $h_k \neq 0$ pour un $k \leqslant i + j$.
4. *Interpolation de Lagrange.* Montrer que le polynôme suivant satisfait le théorème 5.5.
$$f(X) = \sum\nolimits_{i=0}^{n} v_i \prod\nolimits_{j \neq i} \frac{X - \alpha_j}{\alpha_i - \alpha_j}.$$
5. Soit k un corps de Heyting et soit $f \in k[X]$ un polynôme non nul de degré au plus m. Montrer que si $a_0, a_1, \ldots, a_m$ sont des éléments distincts de k, alors il existe un i tel que $f(a_i) \neq 0$.
6. Soit k un corps de Heyting et soit $f \in k[X_1, \ldots, X_n]$ un polynôme non nul de degré au plus m en chaque variable séparément. Montrer que si k contient $m + 1$ éléments distincts, alors $f(a_1, \ldots, a_n) \neq 0$ pour des $a_i \in R$.

1. **NdT.** Formal power series ring.

7. Soit k un corps discret. Montrer que tout idéal premier propre non nul de $k[X]$ est maximal.
8. Soit f un polynôme non nul sur un corps discret k et soit $a \in k$. Montrer qu'il existe un unique entier naturel n et un unique polynôme $u \in k[X]$ tels que $f(X) = (X-a)^n u(X)$ et $u(a) \neq 0$. Si $n = 1$, a est appelé une **racine simple** de f ; si $n > 1$, a est appelé une **racine de multiplicité** n.
9. Donner un polynôme de degré 2 sur l'anneau des entiers modulo 6 avec 3 racines distinctes. Faire la même chose pour les quaternions rationnels.
10. Donner un contre-exemple brouwerien pour l'affirmation selon laquelle $\deg f \leqslant \deg g$ ou $\deg g \leqslant \deg f$ pour tous les polynômes f et g sur un anneau commutatif.

6 Matrices et espaces vectoriels

Soit α une application R-linéaire depuis un R-module à droite libre N vers un R-module à droite libre M. Si $e_1, \ldots, e_n$ est une base pour N et $f_1, \ldots, f_m$ est une base pour M, alors α détermine, et est déterminé par, la matrice $A = \{a_{ij}\}$ de format $m \times n$ telle que

$$\alpha(e_j) = \sum\nolimits_{i=1}^{m} f_i a_{ij}.$$

Si β est un homomorphisme d'un R-module libre L de base $d_1, \ldots, d_\ell$ vers N, alors nous obtenons une matrice $B = \{b_{jk}\}$ de format $n \times \ell$ telle que

$$\beta(d_k) = \sum\nolimits_{j=1}^{n} e_j b_{jk}.$$

Ainsi

$$\alpha\beta(d_k) = \alpha \sum\nolimits_{j=1}^{n} e_j b_{jk} = \sum\nolimits_{j=1}^{n} \alpha(e_j) b_{jk} = \sum\nolimits_{j=1}^{n} \sum\nolimits_{i=1}^{m} f_i a_{ij} b_{jk},$$

de sorte que la matrice qui correspond à $\alpha\beta$ est la **matrice produit** AB, qui est une matrice de format $m \times \ell$ dont l'entrée ik est $\sum_{j=1}^{n} a_{ij} b_{jk}$. Si nous considérons les applications R-linéaires de N vers N, nous obtenons un isomorphisme entre l'anneau $E_R(N)$ des endomorphismes du R-module à droite libre N et l'anneau $\mathrm{Mat}_n(R)$ des matrices de format $n \times n$ sur l'anneau R. La matrice qui correspond à l'endomorphisme identité est appelée une **matrice identité** et on la note I.

Si $e'_1, \ldots, e'_n$ est une autre base pour N, et $f'_1, \ldots, f'_m$ est une autre base pour M, notons σ et τ les automorphismes de N et M définis par $\sigma(e_j) = e'_j$, et $\tau(f_i) = f'_i$, et soient S et T les matrices de σ et τ par rapport aux anciennes bases. Alors la matrice de α par rapport aux nouvelles bases est donnée par

$$\alpha(e'_j) = \alpha(\sigma e_j) = \alpha\Big(\sum\nolimits_i e_i s_{ij}\Big) = \sum\nolimits_{i,k} f_k a_{ki} s_{ij} = \sum\nolimits_{i,k} \tau^{-1}(f'_k) a_{ki} s_{ij}$$

Ainsi $\tau\alpha(e'_j) = \sum_{ik} f'_k a_{ki} s_{ij}$, et donc la nouvelle matrice de $\tau\alpha$ est AS, et la nouvelle matrice de α est $T^{-1}AS$, où T^{-1} est la matrice de τ^{-1}.

La i-ième **ligne** $(a_{i1}, \ldots, a_{in})$ de A peut être considérée comme un élément du R-module à gauche R^n. L'**espace des lignes** de A est le sous-module de R^n engendré par les lignes de A. Une **manipulation élémentaire de lignes** [1] sur A consiste à

(i) échanger deux lignes, ou

(ii) multiplier une ligne par une unité de R, ou

(iii) ajouter un multiple d'une ligne à une autre ligne.

La matrice qui est obtenue à partir d'une manipulation élémentaire de lignes de A est la matrice de α par rapport à une autre base de M. Celle obtenue en échangeant les lignes s et t de A est la matrice de α si nous échangeons les éléments de base f_s et f_t. Celle obtenue en multipliant la ligne s de A par l'unité u est la matrice de α si nous remplaçons l'élément de base f_s par $f_s u^{-1}$. Celle obtenue en ajoutant r fois la ligne s à la ligne t est la matrice de α si nous remplaçons l'élément de base f_s par $f_s - f_t r$. L'espace des lignes de A est inchangé par les manipulations élémentaires de lignes.

La j-ième colonne $(a_{1j}, \ldots, a_{mj})$ de A peut être considérée comme un élément du R-module à droite R^m. Une **manipulation élémentaire de colonnes** [2] sur A consiste à

(i) échanger deux colonnes, ou

(ii) multiplier une colonne par une unité de R, ou

(iii) ajouter un multiple d'une colonne à une autre colonne.

La matrice qui est obtenue à partir d'une manipulation élémentaire de colonnes de A est la matrice de α par rapport à une autre base de M. Celle obtenue en échangeant les colonnes s et t de A est la matrice de α si nous échangeons les éléments de base e_s et e_t. La matrice obtenue en multipliant (à droite) la colonne s de A par l'unité u est la matrice de α si nous remplaçons l'élément de base e_s par $e_s u$. Celle obtenue en ajoutant r fois la colonne s à la colonne t est la matrice de α si nous remplaçons l'élément de base e_t par $e_t + e_s r$.

Une **matrice élémentaire** est une matrice obtenue en appliquant une manipulation élémentaire de lignes à une matrice identité. Si E est la matrice obtenue en appliquant la manipulation élémentaire de lignes ρ à la matrice identité, alors E peut être obtenue en appliquant une manipulation élémentaire de colonnes ρ' à la matrice identité. De plus, si A et B sont des matrices de formats convenables, alors EA est obtenue en appliquant la manipulation ρ à A, et BE est obtenue en appliquant la manipulation ρ' à B.

1. **NdT.** Elementary row operation.
2. **NdT.** Elementary column operation.

Une matrice avec exactement un 1 dans chaque ligne et chaque colonne et tous les autres coefficients nuls est appelée une **matrice de permutation**, et c'est un produit de matrices élémentaires.

On voit facilement qu'une matrice élémentaire a une inverse (à droite et à gauche) qui est aussi élémentaire.

Si k est un anneau à division, alors un k-module est appelé un **espace vectoriel** sur k. En mathématiques classiques tout espace vectoriel sur un anneau à division est libre. Ce n'est plus le cas constructivement, même pour les espaces vectoriels de type fini sur les corps discrets, comme le montre l'exemple brouwerien suivant.

Exemple 6.1. Soit a une suite binaire, soit $i^2 = -1$ et considérons la suite des sous-corps

$$k_n = \{\, s + ta_n i : s, t \in \mathbb{Q} \,\}.$$

du corps des nombres de Gauss $\mathbb{Q}(i)$. Posons $k = \bigcup k_n$. Alors k est un corps discret, et $\mathbb{Q}(i)$ est un k-module discret engendré par les deux éléments 1 et i. Mais nous ne pouvons pas construire une base de $\mathbb{Q}(i)$ sur k. □

Si l'espace vectoriel V est un k-module libre de rang n, alors n est appelé la **dimension** de V et on écrit $n = \dim_k V$, ou simplement $\dim V$; l'espace V est alors appelé un **espace vectoriel de dimension finie** sur k. Le théorème suivant montre, entre autres choses, que $\dim V$ est bien définie si k est discret.

Théorème 6.2. *Soient V et W des espaces vectoriels sur un anneau à division discret k, de dimensions respectives n et m, et soit T une application linéaire de V vers W. Alors il existe des bases $e_1, \ldots, e_n$ de V et $f_1, \ldots, f_m$ de W, et un indice $\ell \leqslant n$, tels que $T(e_i) = f_i$ pour $i \leqslant \ell$, et $T(e_i) = 0$ pour $i > \ell$.*

Démonstration. Soit $A = \{a_{ij}\}$ la matrice de T par rapport aux bases données pour V et W. Par des manipulations élémentaires de lignes et de colonnes nous pouvons faire que $a_{ij} = 0$ pour $i \neq j$, que $a_{ii} \in \{0, 1\}$, et que $a_{ii} \geqslant a_{jj}$ si $i \leqslant j$. Et ceci revient à construire les nouvelles bases voulues pour V et W. □

En prenant pour f l'application identique dans le théorème 6.2, nous voyons que la dimension d'un espace vectoriel de dimension finie est bien définie. Le théorème 6.2 implique de manière immédiate que $\ker T$ et $\operatorname{im} T$ sont des facteurs directs de dimension finie, et que $\dim \ker T + \dim \operatorname{im} T = \dim V$.

La difficulté dans l'exemple 6.1 est que le k-sous-espace engendré par 1 n'est pas détachable : nous ne pouvons pas dire si i est ou n'est pas dans ce sous-espace. Un *facteur direct* A d'un espace vectoriel discret est détachable parce que $x \in A$ si, et seulement si, la projection de x dans A est égale à x. Par suite le corolaire suivant implique que les sous-espaces vectoriels de type fini d'un espace vectoriel de dimension finie sont détachables.

Corolaire 6.3. *Soit V un espace vectoriel de dimension finie sur un anneau à division discret k. Soit W un sous-espace de type fini de V. Alors W est un facteur direct de dimension finie de V.*

Démonstration. Puisque W est de type fini, il existe un espace vectoriel de dimension finie F sur k et une application linéaire T de F sur W. Le théorème 6.2 montre que W est un facteur direct de dimension finie. □

Corolaire 6.4. *Soit V un espace vectoriel de dimension finie sur un anneau à division discret k. Alors l'intersection de deux sous-espaces de type fini de V est un facteur direct de dimension finie.*

Démonstration. Soient A et B des sous-espaces de type fini de V. Par le corolaire 6.3 nous pouvons trouver un sous-espace C supplémentaire de B dans V. La projection sur C, restreinte à A, est une application linéaire de A vers C dont le noyau est $A \cap B$. Par suite $A \cap B$ est un facteur direct de dimension finie de V. □

Soit V un espace vectoriel sur un anneau à division k. Nous disons que $v_1, \ldots, v_n \in V$ sont **(linéairement) dépendants** si l'on a des $a_i \in k$ tels que $\sum_i a_i v_i = 0$ avec $a_i \neq 0$ pour un i. Lorsque k et V sont discrets, nous disons que $v_1, \ldots, v_n$ sont **(linéairement) indépendants** s'ils ne sont pas dépendants ; on voit alors facilement que $v_1, \ldots, v_n$ forment une base de V si, et seulement si, ils sont indépendants et engendrent V (k et V supposés discrets).

Corolaire 6.5. *Soit V un espace vectoriel de dimension finie sur un anneau à division discret k. Si $v_1, \ldots, v_n$ sont des éléments de V, alors ou bien $v_1, \ldots, v_n$ sont dépendants, ou bien ils sont indépendants.*

Démonstration. Considérons l'application linéaire T de k^n vers V qui envoie la base naturelle sur $v_1, \ldots, v_n$. Le noyau de T est de dimension finie d'après le théorème 6.2, et $v_1, \ldots, v_n$ sont dépendants si, et seulement si, le noyau de T est non nul. □

Théorème 6.6. *Soient $k \subseteq K$ des anneaux à division discrets tels que K soit un espace vectoriel de dimension finie sur k, et soit V un espace vectoriel sur K. Alors V est de dimension finie sur K si, et seulement si, V est de dimension finie sur k, et dans ce cas on a $\dim_k V = \dim_k K \dim_K E$.*

Démonstration. Si V est de dimension finie sur K, alors, d'après le théorème 4.3, V est de dimension finie sur k, et la formule du produit pour les dimensions s'applique. Inversement, supposons que V soit de dimension finie sur k et que nous ayons construit un système $x_1, \ldots, x_m \in V$ qui est K-indépendant. Alors $Kx_1 + \cdots + Kx_m$ est un facteur direct de V en tant qu'espace vectoriel sur k, ceci d'après le corolaire 6.3. Si $Kx_1 + \cdots + Kx_m = V$, nous avons terminé ;

sinon un élément de V qui n'appartient pas à $Kx_1 + \cdots + Kx_m$ étend le système K-indépendant $x_1, \ldots, x_m$ et nous terminons par récurrence sur la dimension (sur k) d'un supplémentaire de $Kx_1 + \cdots + Kx_m$. □

Dans le théorème 6.6 il est également vrai que si V est de dimension finie sur k et sur K, et non nul, alors K est de dimension finie sur k. Nous n'aurons pas besoin de ce résultat qui est une conséquence immédiate du théorème d'Azumaya du chapitre suivant.

Exercices

1. Donner un exemple brouwerien pour un espace vectoriel V sur $\mathbb{Q}$ qui contient deux sous-espaces de dimension finie dont l'intersection n'est pas de dimension finie. (Suggestion : considérer l'espace vectoriel $V = \mathbb{Q}^2/S$ avec un sous-espace convenable S de $\mathbb{Q}^2$). Vous pouvez arranger les choses pour que votre exemple soit discret.
2. Généraliser les corolaires 6.3 et 6.4 au cas où V est un module libre sur un anneau à division discret k.
3. Montrer qu'une manipulation élémentaire de lignes de type (i) peut être réalisée au moyen de manipulations élémentaires de lignes de types (ii) et (iii).
4. Un anneau R est **von-Neumann-régulier** si pour chaque $a \in R$ on a un $x \in R$ tel que $axa = a$. Montrer que l'anneau des matrices $n \times n$ sur un anneau à division discret est von-Neumann-régulier. Montrer qu'un anneau est von-Neumann-régulier si, et seulement si, tout idéal principal à gauche est engendré par un idempotent.

7 Déterminants

Soit un anneau commutatif R et soit $A = \{a_{ij}\}$ un élément de $\mathrm{Mat}_n(R)$. Le **déterminant** de A est défini comme

$$\det A = \sum\nolimits_{\sigma} \mathrm{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)},$$

où σ parcourt le groupe S_n des permutations de $\{1, 2, \ldots, n\}$.

Théorème 7.1. *Soient A et B des matrices $n \times n$ sur un anneau commutatif.*

(i) $\det A = \det A^t$.

(ii) $\det A$ *est une fonction linéaire de chaque ligne de* A.

(iii) *Si deux lignes sont égales,* $\det A = 0$.

(iv) $\det AB = \det A \det B$.

Démonstration. Pour vérifier le point (i) notez que si $\tau = \sigma^{-1}$, alors

$$\text{dét } A = \sum\nolimits_{\sigma} \text{sgn}(\sigma) a_{\tau(1)1} \cdots a_{\tau(n)n} = \text{dét } A^t$$

car $\text{sgn}(\sigma) = \text{sgn}(\tau)$. Le point (ii) est clair d'après la définition de dét A car chaque terme dans la somme qui définit le déterminant contient exactement un élément de la ligne i. Concernant le point (iii), si les lignes i et j de A sont égales et si $i \neq j$, alors les permutations peuvent être rangées par paires $\{\sigma, \sigma \cdot (i,j)\}$. Les termes correspondant aux éléments de chaque paire dans la définition du déterminant sont égaux au signe près, de sorte que leur somme est nulle, ce qui établit le point (iii). Enfin considérons dét A dét $B =$

$$\Big(\sum\nolimits_{\sigma} \text{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)}\Big) \cdot \Big(\sum\nolimits_{\tau} \text{sgn}(\tau) b_{1\tau(1)} \cdots b_{n\tau(n)}\Big) =$$

$$\sum\nolimits_{\sigma,\tau} \text{sgn}(\sigma\tau) a_{1\sigma(1)} \cdots a_{n\sigma(n)} b_{1\tau(1)} \cdots b_{n\tau(n)} =$$

$$\sum\nolimits_{\sigma,\tau} \text{sgn}(\sigma\tau) a_{1\sigma(1)} b_{\sigma(1)\tau\sigma(1)} \cdots a_{n\sigma(n)} b_{\sigma(n)\tau\sigma(n)} =$$

$$\sum\nolimits_{\sigma} \sum\nolimits_{\pi} \text{sgn}(\pi) a_{1\sigma(1)} b_{\sigma(1)\pi(1)} \cdots a_{n\sigma(n)} b_{\sigma(n)\pi(n)}. \tag{7.2}$$

Si σ est une fonction de $\{1, 2, \ldots, n\}$ vers $\{1, 2, \ldots, n\}$ plutôt qu'une permutation, et si $\sigma(i) = \sigma(j)$ pour $i \neq j$, alors

$$\sum\nolimits_{\pi} \text{sgn}(\pi) a_{1\sigma(1)} b_{\sigma(1)\pi(1)} \cdots a_{n\sigma(n)} b_{\sigma(n)\pi(n)} = 0$$

parce que pour chaque permutation π les termes dans la somme indexés par π et par $\pi \cdot (i,j)$ ont pour somme 0. Par suite nous pouvons considérer que σ parcourt toutes les fonctions de $\{1, 2, \ldots, n\}$ vers $\{1, 2, \ldots, n\}$ dans (7.2), et ainsi

$$\text{dét } A \ \text{ dét } B = \sum\nolimits_{\pi} \text{sgn}(\pi) \prod\nolimits_{i} \sum\nolimits_{j} a_{ij} b_{j\pi(i)} = \text{dét } AB. \qquad \square$$

Le **cofacteur** A_{ij} de l'élément a_{ij} dans la matrice A est $(-1)^{i+j}$ fois le déterminant de la matrice de $\text{Mat}_{n-1}(R)$ obtenue en supprimant la ligne i et la colonne j de A. On voit facilement d'après la définition de dét A que, pour chaque i,

$$a_{i1}A_{i1} + a_{i2}A_{i2} + \cdots + a_{in}A_{in} = \text{dét } A,$$

ce qui explique le nom de *cofacteur*. D'après le théorème 7.1(iii), nous avons aussi l'égalité

$$a_{i1}A_{j1} + a_{i2}A_{j2} + \cdots + a_{in}A_{jn} = 0$$

lorsque $i \neq j$. Si nous définissons la **matrice adjointe** de A comme la matrice B dont l'entrée ij est A_{ji}, alors

$$AB = (\text{dét } A)\text{I} = (\text{dét } A^t)\text{I} = (A^t B^t)^t = BA. \tag{7.3}$$

Ainsi nous pouvons construire une inverse de la matrice A si nous pouvons construire un inverse du déterminant dét A.

Théorème 7.4. *Soient R un anneau commutatif et $A \in \mathrm{Mat}_n(R)$. Alors A est une unité de $\mathrm{Mat}_n(R)$ si, et seulement si,* dét A *est une unité de R* [1].

Démonstration. Si $AB = \mathrm{I}$, alors $(\text{dét}\, A)(\text{dét}\, B) = \text{dét}\, \mathrm{I} = 1$, et dét A est une unité de R. Inversement, si dét A est une unité de R, alors (7.3) montre que A est une unité de $\mathrm{Mat}_n(R)$. □

Nous pouvons maintenant montrer que le rang d'un module libre de rang fini sur un anneau commutatif non trivial est un invariant. En fait, nous démontrons un peu mieux.

Théorème 7.5. *Soit R un anneau commutatif. Soient $m < n$ des entiers strictement positifs et $\varphi\colon R^m \to R^n$ un épimorphisme de R-modules. Alors $R = 0$.*

Démonstration. On a une application R-linéaire $\psi\colon R^n \to R^m$ telle que $\varphi\psi = 1$. On étend φ en une application linéaire depuis $R^n = R^m \oplus R^{n-m}$ en posant $\varphi(R^{n-m}) = 0$ et l'on regarde ψ comme une application linéaire vers R^n. Comme $(\text{dét}\, \varphi)(\text{dét}\, \psi) = 1$ et dét $\varphi = 0$, on a $1 = 0$ dans R. □

Lemme 7.6. *Soient R un anneau commutatif, M un R-module, et une matrice $A \in \mathrm{Mat}_n(R)$. Si U est une matrice de format $n \times 1$ à coefficients dans M et si $AU = 0$, alors* $(\text{dét}\, A)U = 0$.

Démonstration. Soit B la matrice adjointe de A. Alors $BAU = 0$, et donc $(\text{dét}\, A)U = 0$. □

Si $A \in \mathrm{Mat}_n(R)$ avec R un anneau commutatif, $X\mathrm{I} - A$ est une matrice à coefficients dans $R[X]$. Le déterminant de $X\mathrm{I} - A$ est appelé le **polynôme caractéristique** de A. Le **polynôme caractéristique** d'un endomorphisme α d'un R-module libre F de rang n est le polynôme caractéristique de la matrice de α par rapport à une base de F. Le polynôme caractéristique de α est unitaire de degré n. Si B est la matrice de α par rapport à une autre base de F, alors $B = S^{-1}AS$ pour une matrice inversible $S \in \mathrm{Mat}_n(R)$. Par suite, le polynôme caractéristique de B est le déterminant de $X\mathrm{I} - S^{-1}AS = S^{-1}(X\mathrm{I} - A)S$, qui est égal au déterminant de $X\mathrm{I} - A$, de sorte que le polynôme caractéristique de α ne dépend pas de la base choisie de F. Le théorème de Cayley-Hamilton dit que α annule son polynôme caractéristique.

1. **NdT.** En fait, la démonstration dit aussi que si la matrice est inversible à gauche, ou à droite, elle est inversible.

Théorème 7.7 (Cayley-Hamilton)**.** *Soient R un anneau commutatif et $f(X)$ le polynôme caractéristique d'un endomorphisme α d'un R-module F libre de rang fini. Alors $f(\alpha) = 0$.*

Démonstration. Soit S le sous-anneau (commutatif) de l'anneau des endomorphismes de F engendré par α et R. Alors F est un S-module *via* la multiplication dans F. Soit $A = \{a_{ij}\}$ la matrice de α par rapport à une base $u_1, \ldots, u_n$ de F, de sorte que

$$\alpha u_j = \sum\nolimits_i a_{ij} u_i.$$

Soit $U = (u_1, \ldots, u_n)^t$ et soit $C = \alpha \mathrm{I} - A$, qui est une matrice $\in \mathrm{Mat}_n(S)$. Alors $C^t U = 0$ et donc $(\det C^t)U = 0$ par le lemme 7.6. Par suite $\det C^t = 0$. Or $\det C^t = \det C = f(\alpha)$. □

Exercices

1. Soit R un anneau commutatif et soit une application $f\colon \mathrm{Mat}_n(R) \to R$ telle que

   (i) $f(A)$ est une fonction linéaire de chaque ligne de A ;

   (ii) $f(A) = 0$ si deux lignes de A sont égales.

   Montrer qu'il existe un $r \in R$ tel que $f(A) = r \det A$. Utiliser ce résultat pour montrer que $\det AB = \det A \det B$.

2. Soit M un module libre de rang n sur un anneau commutatif R et soit α un endomorphisme de M. Si A et $B \in \mathrm{Mat}_n(R)$ sont des matrices de α par rapport à des bases de M, montrer que $\det A = \det B$.

3. Une autre démonstration du théorème de Cayley-Hamilton.

   (i) Montrer que $\mathrm{Mat}_n(R[X])$ est isomorphe à $\mathrm{Mat}_n(R)[X]$ pour tout anneau R.

   (ii) Soient S un anneau non nécessairement commutatif, $a \in S$, et $f, g \in S[X]$. Montrer que si $f(X) = g(X)(X - a)$, alors $f(a) = 0$. (Attention, il n'est pas vrai que si $f(X) = (X - a)g(X)$, alors $f(a) = 0$.)

   (iii) Démontrer le théorème 7.7 en posant $S = \mathrm{Mat}_n(R)$ et en utilisant (7.3) pour factoriser le polynôme caractéristique $f(X)$ sous la forme $g(X)(X - a)$, vu comme un élément de $S[X]$. Enfin appliquer (ii).

4. On considère le déterminant $\det M$ de la **matrice de Vandermonde**

$$M = \begin{bmatrix} 1 & X_1 & X_1^2 & \cdots & X_1^{m-1} \\ 1 & X_2 & X_2^2 & \cdots & X_2^{m-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & X_m & X_m^2 & \cdots & X_m^{m-1} \end{bmatrix}$$

à coefficients dans l'anneau commutatif $k[X_1, \ldots, X_m]$. Montrer que

$$\text{dét } M = \prod_{i<j}(X_j - X_i).$$

Utiliser cette formule pour démontrer que si $f = f_0 + f_1X + \cdots + f_{m-1}X^{m-1} \neq 0$ est un polynôme sur un corps de Heyting k, et si $a_1, \ldots, a_m$ sont des éléments deux à deux distincts de k, alors $f(a_i) \neq 0$ pour un i.

8 Polynômes symétriques

Soient R un anneau commutatif et $f \in R[X_1, \ldots, X_n]$ un polynôme à coefficients dans R. Nous disons que f est **invariant** par une permutation π de l'ensemble des indéterminées $\{X_1, \ldots, X_n\}$ si

$$f(X_1, \ldots, X_n) = f(\pi(X_1), \ldots, \pi(X_n)).$$

Si f est invariant par toute permutation de ses indéterminées, nous disons que f est un **polynôme symétrique**. Si nous considérons

$$f = (Y + X_1)(Y + X_2) \cdots (Y + X_n)$$

comme un polynôme en les indéterminées $Y, X_1, \ldots, X_n$ à coefficients dans R, il est clair que f est invariant par toute permutation des indéterminées $X_1, \ldots, X_n$. Donc si nous écrivons f comme un polynôme

$$Y^n + \sigma_1 Y^{n-1} + \cdots + \sigma_n$$

en Y à coefficients dans $R[X_1, \ldots, X_n]$, les coefficients σ_i sont des polynômes symétriques de $R[X_1, \ldots, X_n]$. En développant f comme une somme de monômes, nous trouvons

$$\sigma_1 = \sum_i X_i,\ \sigma_2 = \sum_{i<j} X_iX_j,\ \sigma_3 = \sum_{i<j<k} X_iX_jX_k,\ \ldots,\ \sigma_n = X_1X_2 \cdots X_n.$$

Les polynômes $\sigma_1, \ldots, \sigma_n$ sont appelés les **polynômes symétriques élémentaires** en n indéterminées.

Clairement tout polynôme dans le sous-anneau $R[\sigma_1, \ldots, \sigma_n]$ de $R[X_1, \ldots, X_n]$ est symétrique ; le fait que chaque polynôme symétrique a une représentation unique en tant qu'élément de $R[\sigma_1, \ldots, \sigma_n]$ est le théorème fondamental des polynômes symétriques.

Théorème 8.1. *Soit f un polynôme symétrique de $R[X_1, \ldots, X_n]$. Alors il existe un unique polynôme $h \in R[Y_1, \ldots, Y_n]$ tel que $f = h(\sigma_1, \ldots, \sigma_n)$.*

Démonstration. Nous construisons h par récurrence sur n. En remplaçant R par $\mathbb{Z}[r_1, \ldots, r_m]$, où les r_i sont les indéterminées qui correspondent aux coefficients des monômes dans l'expression de f, nous pouvons supposer, afin de construire h, que R est discret ; cette convention technique nous permet de parler de degrés. Si $n = 1$, alors $\sigma_1 = X_1$ et tout polynôme est symétrique, de sorte que nous pouvons choisir $h = f(Y_1)$. Si $n > 1$, considérons les polynômes symétriques élémentaires $\tau_1, \ldots, \tau_{n-1}$ en les indéterminées $X_1, \ldots, X_{n-1}$. Notons que $\tau_i = \sigma_i(X_1, \ldots, X_{n-1}, 0)$. Par récurrence nous pouvons construire $g \in R[Y_1, \ldots, Y_{n-1}]$ tel que

$$f(X_1, \ldots, X_{n-1}, 0) = g(\tau_1, \ldots, \tau_{n-1}).$$

Nous pouvons supposer que g ne contient aucun monôme $Y_1^{e_1} \cdots Y_{n-1}^{e_{n-1}}$ tel que $\sum_{i=1}^{n-1} ie_i$ soit supérieur au degré total de $f(X_1, \ldots, X_{n-1}, 0)$. Alors le polynôme

$$f_1 = f - g(\sigma_1, \ldots, \sigma_{n-1})$$

est symétrique et $f_1(X_1, \ldots, X_{n-1}, 0) = 0$. Donc f_1 est divisible par X_n, et par symétrie il est divisible par X_i pour chaque i. Ceci implique que f_1 est divisible par $\sigma_n = X_1 X_2 \cdots X_n$, et nous pouvons écrire $f_1 = \sigma_n f_2$ où f_2 est symétrique et de plus petit degré que f_1 et f. Par récurrence sur le degré de f nous savons construire $p \in R[Y_1, \ldots, Y_n]$ tel que $f_2 = p(\sigma_1, \ldots, \sigma_n)$, et nous posons $h = Y_n p + g$.

Pour montrer que h est unique, il suffit de montrer que si $g(\sigma_1, \ldots, \sigma_n) = 0$ pour un $g \in R[Y_1, \ldots, Y_n]$, alors $g = 0$. Nous procédons par récurrence sur n. Le cas $n = 1$ est trivial, aussi nous pouvons supposer que $n > 1$ et écrire $g = g_m Y_n^m + g_{m-1} Y_n^{m-1} + \cdots + g_0$ comme un polynôme en Y_n ayant ses coefficients g_i dans $R[Y_1, \ldots, Y_{n-1}]$. En substituant σ_i à Y_i et en posant ensuite $X_n = 0$ nous obtenons $g_0(\tau_1, \ldots, \tau_{n-1}) = 0$, où les τ_i sont des polynômes symétriques élémentaires en $X_1, \ldots, X_{n-1}$. Par récurrence sur n nous concluons que $g_0 = 0$. Alors $g = Y_n p$ pour un $p \in R[Y_1, \ldots, Y_n]$. Puis, comme $0 = g(\sigma_1, \ldots, \sigma_n) = \sigma_n p(\sigma_1, \ldots, \sigma_n)$, nous en déduisons que $p(\sigma_1, \ldots, \sigma_n) = 0$, et par récurrence sur m que $p = 0$, et donc que $g = 0$. □

Corolaire 8.2. *Les polynômes symétriques élémentaires $\sigma_1, \ldots, \sigma_n$ sont algébriquement indépendants sur R ; c'est-à-dire, si $g(\sigma_1, \ldots, \sigma_n) = 0$, alors $g = 0$.* □

L'anneau de polynômes $R[X_1, \ldots, X_n]$ est un module sur le sous-anneau $R[\sigma_1, \ldots, \sigma_n]$ des polynômes symétriques. Nous montrons que c'est un module libre de rang fini.

Lemme 8.3. *Le sous-anneau $R[\sigma_1, \ldots, \sigma_n, X_j, \ldots, X_n]$ de $R[X_1, \ldots, X_n]$ est formé des polynômes qui sont invariants par toute permutation de $X_1, \ldots, X_{j-1}$.*

Démonstration. Soit $S = R[X_j, \dots, X_n]$, et soient $\tau_1, \dots, \tau_{j-1}$ les polynômes symétriques élémentaires en $X_1, \dots, X_{j-1}$. Les polynômes de $R[X_1, \dots, X_n] = S[X_1, \dots, X_{j-1}]$ qui sont invariants par toute permutation de $X_1, \dots, X_{j-1}$ constituent le sous-anneau $S[\tau_1, \dots, \tau_{j-1}]$ d'après le théorème 8.1. On doit donc montrer que $S[\sigma_1, \dots, \sigma_n] = S[\tau_1, \dots, \tau_{j-1}]$. Comme chaque σ_i est invariant par les permutations de $X_1, \dots, X_{j-1}$, on a $S[\sigma_1, \dots, \sigma_n] \subset S[\tau_1, \dots, \tau_{j-1}]$. Posons

$$f(Y) = (Y + X_1)(Y + X_2) \cdots (Y + X_n) \text{ et}$$
$$g(Y) = (Y + X_j)(Y + X_{j+1}) \cdots (Y + X_n).$$

Les polynômes unitaires f et g sont des éléments de $S[\sigma_1, \dots, \sigma_n][Y]$ et l'on a

$$f = gq \text{ où } q = (Y + X_1) \cdots (Y + X_{j-1}) = Y^{j-1} + \tau_1 Y^{j-2} + \cdots + \tau_{j-1}.$$

Par ailleurs, la division de f par g dans $S[\sigma_1, \dots, \sigma_n][Y]$ donne $f = gq_1 + r_1$ avec $\deg(r_1) < \deg(g)$.
Donc on a $\deg_Y(g(q_1 - q)) < \deg_Y(g)$ dans $R[X_1, \dots, X_n][Y]$, ce qui implique $q_1 = q$.
Ainsi $q \in S[\sigma_1, \dots, \sigma_n][Y]$ et donc $S[\tau_1, \dots, \tau_{j-1}] \subset S[\sigma_1, \dots, \sigma_n]$. □

Théorème 8.4. *Les monômes $X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}$ avec $i_k \leqslant k - 1$ forment un système libre de $n!$ générateurs de $R[X_1, \dots, X_n]$ lorsque l'on voit cet anneau comme un module sur $R[\sigma_1, \dots, \sigma_n]$.*

Démonstration. Soit $R_j = R[\sigma_1, \dots, \sigma_n, X_j, \dots, X_n]$. Nous allons montrer que les éléments $1, X_j, X_j^2 \dots, X_j^{j-1}$ forment une famille libre de générateurs de R_j sur R_{j+1}. D'après le lemme 8.3, le polynôme $f_j(Y) = (Y - X_1)(Y - X_2) \cdots (Y - X_j)$ a ses coefficients dans R_{j+1}. Le polynôme f_j est unitaire de degré j, et $f_j(X_j) = 0$. Donc $1, X_j, X_j^2 \dots, X_j^{j-1}$ engendrent $R_j = R_{j+1}[X_j]$ sur R_{j+1}. Il reste à voir que $1, X_j, X_j^2 \dots, X_j^{j-1}$ sont indépendants sur R_{j+1}. Supposons que $g(X_j) = 0$ pour un $g \in R_{j+1}[Y]$ tel que $\deg g < j - 1$. Comme g est invariant par les permutations de $X_1, \dots X_j$, nous avons $g(X_i) = 0$ si $1 \leqslant i \leqslant j$, de sorte que g a j racines distinctes ; donc $g = 0$ car $X_i - X_j$ est simplifiable d'après l'unicité dans le théorème du reste. □

Exercices

1. Soit K un corps discret et soient $\sigma_1, \dots, \sigma_n$ les polynômes symétriques élémentaires de $K[X_1, \dots, X_n]$. Montrer que l'ensemble des $n!$ monômes $X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}$ avec $i_k \leqslant k - 1$ forment une base du corps de fractions de $K[X_1, \dots, X_n]$ en tant qu'espace vectoriel sur le corps de fractions de $K[\sigma_1, \dots, \sigma_n]$.

2. Montrer que l'algorithme suivant réécrit un polynôme symétrique donné f comme un polynôme en les polynômes symétriques élémentaires. On ordonne les monômes $X_1^{i_1}X_2^{i_2}\cdots X_n^{i_n}$ lexicographiquement en posant

$$X_1^{i_1}X_2^{i_1}\cdots X_n^{i_n} \leqslant X_1^{j_1}X_2^{j_2}\cdots X_n^{j_n}$$

si pour chaque k ou bien $i_k \leqslant j_k$ ou bien il y a un $m < k$ tel que $i_m < j_m$. Soit $aX_1^{i_1}X_2^{i_2}\cdots X_n^{i_n}$ le terme dominant de f par rapport à cet ordre lexicographique. Montrer que $i_k \geqslant i_{k+1}$ pour $k = 1, \ldots, n-1$. Retrancher

$$a\sigma_1^{i_1-i_2}\sigma_2^{i_2-i_3}\cdots\sigma_n^{i_n}$$

de f. Montrer que la différence a un degré plus petit pour cet ordre lexicographique. Remplacer f par la différence et recommencer.

3. Exprimer $\sum_{i=1}^n X_i^3$ en termes des polynômes symétriques élémentaires $\sigma_1, \ldots, \sigma_n$.
4. Soient R un anneau commutatif et $E = \prod_{i<j}(X_i - X_j) \in R[X_1, \ldots, X_n]$.
   (a) Montrer que le polynôme E est **alternant**, c'est-à-dire

$$E(\pi X_1, \ldots, \pi X_n) = \operatorname{sgn}(\pi)E(X_1, \ldots, X_n)$$

   pour chaque permutation π, et que E^2 est symétrique. Montrer que si 2 est une unité de R, alors tout polynôme alternant est de la forme fE où f est un polynôme symétrique.

   (b) Montrer qu'il existe un polynôme $d \in \mathbb{Z}[Y_1, \ldots, Y_n]$ tel que si $\prod_{i=1}^n (X - r_i) = X^n + a_1X^{n-1} + \cdots + a_n$, où les r_i et a_j sont dans un corps K, alors les r_i sont distincts si, et seulement si, $d(a_1, \ldots, a_n) \neq 0$ dans K.

   (c) Montrer que E est invariant par les permutations paires des X_i. Montrer que si 2 est une unité de R, alors $R[E, \sigma_1, \ldots, \sigma_n]$ est l'anneau de tous les polynômes invariants par les permutations paires des X_i.

9 Notes

Nous laissons ouverte la question de savoir ce que devrait être une inégalité raisonnable sur un anneau à division. Pour qu'un anneau à division soit un anneau à division au sens classique, l'inégalité doit être standard ; mais cette requête est trop faible pour fournir des conséquences utiles. Beaucoup de corps non discrets, comme les nombres réels ou les nombres complexes, sont des corps de Heyting. Quoique les corps discrets soient aussi des corps de Heyting, la tentation d'identifier la notion de corps avec celle de corps de Heyting est amoindrie par l'existence de corps par négation naturels (les corps résiduels de

valeurs absolues non archimédiennes) qui ont une inégalité ni cotransitive ni étroite.

Lorsqu'un idéal P dans un anneau commutatif n'est pas détachable ce n'est pas clair de déterminer ce que ce devrait être pour cet idéal d'être premier. Dans l'anneau des nombres réels, l'idéal 0 n'est pas premier selon notre définition, parce qu'il est possible de construire deux nombres réels dont le produit est nul et pour lesquels nous ne pouvons pas dire lequel est nul. En effet, LLPO est équivalent à l'affirmation à propos de nombres réels que si $ab = 0$, alors $a = 0$ ou $b = 0$ (exercice 3.5). Dans les anneaux avec une notion d'inégalité positive, comme les nombres réels, il est naturel de définir un idéal premier comme un idéal tel que chaque fois que $a, b \notin P$, alors $ab \notin P$. Notre définition d'un idéal premier a le mérite de ne pas se référer à l'inégalité.

Comme P est un idéal premier si, et seulement si, P est le noyau d'un homomorphisme dans un corps par négation, il est naturel de définir un idéal maximal comme le noyau d'un homomorphisme *sur* un corps par négation. Il peut y avoir une meilleure définition mais nous ne le saurons pas tant que nous n'aurons pas trouvé une théorie intéressante concernant les idéaux maximaux non détachables.

Les modules libres sur des ensembles non discrets ne sont pas juste des curiosités. Ils sont utilisés par exemple pour construire les groupes d'homologie singulière et pour construire les produits tensoriels de modules arbitraires.

III. Anneaux et modules

Sommaire

1 Idéaux quasi-réguliers et radical de Jacobson

Un élément r d'un anneau R est appelé **quasi-régulier à droite** si $1-r$ a un inverse à droite, **quasi-régulier à gauche** s'il a un inverse à gauche. Si r est à la fois quasi-régulier à droite et à gauche, nous disons que r est **quasi-régulier**. Un élément $r \in R$ est **nilpotent** si $r^n = 0$ pour un entier strictement positif n ; nous disons que R est **sans élément nilpotent** ou **réduit** si tout élément nilpotent est nul. Notez que si $r^n = 0$ et si $s = 1 + r + r^2 + \cdots + r^{n-1}$, alors $(1-r)s = s(1-r) = 1$, donc tout élément nilpotent est quasi-régulier. Un idéal à gauche L de R est appelé **quasi-régulier** si tout élément de L est quasi-régulier à gauche.

Théorème 1.1. *Soit L un idéal quasi-régulier à gauche. Alors tout élément de L est quasi-régulier.*

Démonstration. Si $r \in L$, alors $s(1-r) = 1$ pour un $s \in R$. Comme $-sr \in L$, l'élément $s = 1 + sr$ a un inverse à gauche t. Donc $1 - r = ts(1-r) = t$, et $(1-r)s = ts = 1$. □

Lemme 1.2. *Si ab est quasi-régulier à gauche (à droite), alors il en va de même pour ba.*

Démonstration. Si $c(1-ab)=1$, alors $(1+bca)(1-ba)=1-ba+bc(1-ab)a=1$. Si $(1-ab)c=1$, alors $(1-ba)(1+bca)=1$. □

Théorème 1.3. *L'ensemble des éléments r tels que Rr est un idéal à gauche quasi-régulier est un idéal bilatère.*

Démonstration. Vu le lemme 1.2, il suffit de montrer que si Ra et Rb sont quasi-réguliers, alors il en va de même pour $a+b$. Prendre un s tel que $s(1-a)=1$ et un t tel que $t(1-sb)=1$. Alors $ts(1-(a+b))=1$. □

L'idéal du théorème 1.3 est appelé le **radical de Jacobson** de R.

Lemme 1.4 (Nakayama)**.** *Soient M un R-module à gauche de type fini et L un idéal à gauche quasi-régulier de R. Si $LM=M$, alors $M=0$.*

Démonstration. Soit $x_1,\dots,x_n$ un système générateur de M. Alors $x_1\in LM$, et nous pouvons écrire $x_1=a_1x_1+\cdots+a_nx_n$ avec chaque a_i dans L. Mais $1-a_1$ est inversible à gauche. Ainsi $x_1=(1-a_1)^{-1}(a_2x_2+\cdots+a_nx_n)$, et donc M est engendré par $x_2,\dots,x_n$. Nous terminons par récurrence sur n. □

Exercices

1. Utilisez l'identité dans la démonstration du lemme 1.2, avec $a=1$, pour montrer que si un élément d'un anneau possède un unique inverse à gauche alors il possède un inverse à droite [Rudin 1985].
2. Montrer que les anneaux suivants ont leur radical de Jacobson réduit à 0.
   (i) L'anneau des entiers $\mathbb{Z}$.
   (ii) Tout anneau à division discret.
   (iii) L'anneau de polynômes $R[X]$ pour un anneau intègre discret R.
   (iv) Un anneau von-Neumann-régulier (voir l'exercice II.6.4).
3. Déterminer le radical de Jacobson du sous-anneau de $\mathbb{Q}$ formé par les nombres rationnels qui peuvent être écrits avec un dénominateur impair. Construire un exemple brouwerien pour un anneau intègre discret dénombrable dont le radical de Jacobson n'est pas détachable.
4. Un élément x d'un R-module M est appelé un **non-générateur** si pour tout sous-module A de M tel que $Rx+A=M$, alors $A=M$. Montrer qu'un élément x de R est dans le radical de Jacobson de R si, et seulement si, x est un non-générateur du R-module à gauche R.
5. Un **idéal à gauche maximal détachable** d'un anneau R est un idéal à gauche propre L tel que si $x\in R$, alors $x\in L$ ou $Rx+L=R$. Montrer que tout idéal à gauche maximal détachable contient le radical de Jacobson. Montrer que si tout élément de R qui n'est contenu dans aucun idéal à

gauche maximal détachable a un inverse à gauche (le lemme de Zorn démontre cela en mathématiques classiques), alors le radical de Jacobson est égal à l'intersection les idéaux à gauche maximaux détachables.

6. Soit A une matrice carrée dont les entrées sont dans le radical de Jacobson d'un anneau. Montrer que $I-A$ est inversible, où I est la matrice identité correspondante.
7. Si J est le radical de Jacobson de R, montrer que le radical de Jacobson de R/J est nul.
8. Utiliser le lemme II.7.6 pour montrer que si M est un module de type fini sur un anneau commutatif R et si I est un idéal de R, alors $IM = M$ si, et seulement si, $(1-r)M = 0$ pour un $r \in R$. Utiliser cela pour démontrer le lemme de Nakayama pour les anneaux commutatifs.
9. Utilisez l'exercice 8 pour montrer que tout module de type fini M sur un anneau commutatif R est **hopfien** : tout épimorphisme de M sur M est un automorphisme (si f est un endomorphisme de M, considérer M en tant que $R[f]$-module).

2 Modules cohérents, noethériens

Soient R un anneau et M un R-module. Alors M est dit **noethérien** si l'ensemble des sous-modules de type fini de M, ordonné par l'inclusion, vérifie la condition de chaine ascendante. Un anneau R est **noethérien à gauche** si R est noethérien en tant que module à gauche sur lui-même. Ainsi R est noethérien à gauche si, et seulement si, pour toute suite $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ d'idéaux à gauche de type fini de R il existe un n tel que $I_n = I_{n+1}$.

On voit facilement que l'anneau des entiers est noethérien, comme l'est $k[X]$ si k est un corps discret. Les modules finis sont noethériens, et si R contient un corps discret k, alors les R-modules qui sont des k-espaces vectoriels de dimension finie sont noethériens – plus généralement, si S est un sous-anneau de R et si M est un R-module qui est noethérien comme S-module, alors M est noethérien comme R-module. Le théorème de la base de Hilbert (voir le chapitre VIII) implique que les anneaux de polynômes en plusieurs variables sur les entiers, ou sur un corps discret, sont noethériens.

Théorème 2.1. *Soit N un sous-module d'un module M. Alors M est noethérien si, et seulement si, N et M/N sont noethériens.*

Démonstration. Notons π l'application linéaire naturelle de M vers M/N.

Supposons M noethérien. Tout d'abord N est clairement noethérien. Considérons ensuite une chaine croissante de sous-modules de type fini de M/N : $J_1 \subseteq J_2 \subseteq \cdots$. Nous pouvons construire une chaine $I_1 \subseteq I_2 \subseteq \cdots$ de sous-modules de type fini de M telle que $\pi I_m = J_m$. Il existe un n tel que $I_{n+1} = I_n$, donc $J_{n+1} = J_n$, et par suite M/N est noethérien.

Inversement, supposons que N et M/N sont noethériens, et soit $I_1 \subseteq I_2 \subseteq \cdots$ une chaine de sous-modules de type fini de M. Alors $\pi I_1 \subseteq \pi I_2 \subseteq \cdots$ est une chaine de sous-modules de type fini du module noethérien M/N, donc il existe un n tel que $\pi I_n = \pi I_{n+1}$. Ainsi $I_{n+1} = I_n + K$ pour un certain sous-module de type fini K de N. En itérant cette construction, nous obtenons une suite d'entiers positifs $n_1 < n_2 < \cdots$ et une chaine croissante de sous-modules de type fini K_i de N, telles que $I_{n_i+1} = I_{n_i} + K_i$. Comme N est noethérien, on a un i tel que $K_i = K_{i-1} \subseteq I_{n_i}$, et ainsi $I_{n_i+1} = I_{n_i}$. □

Un R-module M est **de présentation finie** lorsqu'il existe une application linéaire depuis un R-module libre de rang fini sur M avec un noyau de type fini. Le théorème suivant montre que si M est de présentation finie, alors *toute* application linéaire depuis un R-module de type fini sur M a un noyau de type fini.

Théorème 2.2. *Si f est une application linéaire depuis un R-module de type fini M_1 sur un R-module de présentation finie M_2, alors le noyau de f est de type fini.*

Démonstration. Soit F_i un R-module libre de rang fini, et soit π_i une application linéaire de F_i sur M_i telle que $\ker \pi_2$ soit de type fini. Par l'astuce de Schanuel (théorème II.4.4), nous avons

$$\ker f\pi_1 \oplus F_2 \simeq \ker \pi_2 \oplus F_1.$$

Par suite $\ker f\pi_1$ est de type fini. Comme π_1 est surjectif, le module $\ker f = \pi_1(\ker f\pi_1)$ est aussi de type fini. □

Théorème 2.3. *Soit N un sous-module du R-module M. Alors*

(i) *si M est de présentation finie et si N est de type fini, M/N est de présentation finie,*

(ii) *si N et M/N sont de présentation finie, M est de présentation finie.*

Démonstration. Notons π l'application linéaire naturelle de M sur M/N.

Pour démontrer (i) considérons une application linéaire φ depuis un module libre de rang fini F sur M avec un noyau K de type fini, et soit $N' \subset F$ de type fini avec $\varphi(N') = N$. Alors $K + N' = \ker \pi\varphi$ est de type fini, et M/N est de présentation finie.

Pour démontrer (ii) considérons des applications linéaires φ_1 et φ_2 depuis des modules libres de rang fini F_1 et F_2 sur N et M/N avec des noyaux de type fini K_1 et K_2 respectivement. Soit $\varphi\colon F_1 \oplus F_2 \to M$ une application linéaire telle que $\varphi(x_1) = \varphi_1(x_1)$ et $\pi\varphi(x_2) = \varphi_2(x_2)$. Alors φ envoie $F_1 \oplus F_2$ sur M. Si $K = \ker \varphi$ et si π_2 est la projection de $F_1 \oplus F_2$ sur F_2, on a la suite exacte $0 \to F_1 \cap K \to K \to \pi_2(K) \to 0$. Mais $\pi_2(K) = K_2$ et $K \cap F_1 = K_1$, donc K est de type fini. □

Un R-module est dit **cohérent**[1] si tout sous-module de type fini est de présentation finie. Un anneau R est **cohérent à gauche** s'il est cohérent en tant que R-module à gauche. En mathématiques classiques tout anneau noethérien à gauche est cohérent à gauche.

Dans la suite, si nous ne précisons pas, noethérien signifie noethérien à gauche et cohérent signifie cohérent à gauche.

Théorème 2.4. *Un R-module M est cohérent si, et seulement si, les propriétés suivantes sont satisfaites.*

(i) *L'intersection de deux sous-modules de présentation finie de M est de type fini.*

(ii) *Si $x \in M$, alors $\{\, r \in R : rx = 0 \,\}$ est un idéal à gauche de type fini de R.*

Démonstration. Supposons que M est cohérent et que N_1 et N_2 sont des sous-modules de type fini de M. Soit un $x \in M$. Soit φ_i $(i = 1, 2)$ une application linéaire depuis un R-module libre de rang fini F_i sur N_i, et soit K le noyau (de type fini) de l'application linéaire correspondante de $F_1 \oplus F_2$ vers M. Notons π_1 la projection de $F_1 \oplus F_2$ sur F_1. Le module $N_1 \cap N_2 = \varphi_1(\pi_1 K)$ est de type fini, cela montre (i). Le sous-module cyclique Rx de M est de présentation finie, donc le noyau de l'application linéaire qui envoie R sur Rx est de type fini, cela montre (ii).

Inversement, supposons (i) et (ii), et soit A un sous-module de type fini de M. Si A est cyclique, alors A est de présentation finie par (ii). Sinon $A = N_1 + N_2$ avec chaque N_i engendré par moins d'éléments que A. Par récurrence, chaque N_i est de présentation finie, et par (i) l'intersection $N_1 \cap N_2$ est de type fini. Par le théorème 2.3(ii) la somme directe $N_1 \oplus N_2$ est de présentation finie. Mais $N_1 \oplus N_2$ s'envoie sur $A = N_1 + N_2$ avec un noyau isomorphe à $N_1 \cap N_2$, donc A est de présentation finie par le théorème 2.3(i). □

Théorème 2.5. *Soit N un sous-module de type fini d'un module M. Alors M est cohérent si, et seulement si, N et M/N sont cohérents.*

Démonstration. Soit π l'application linéaire naturelle de M sur M/N. Si M est cohérent, alors N est clairement cohérent. Si B est un sous-module de type fini de M/N, alors $B = \pi(A)$ pour un sous-module de type fini A de M. Mais

1. **NdT.** Bourbaki (Algèbre, chapitre X, ou Algèbre commutative, chapitre I) appelle module *pseudo-cohérent* ce que [CCA] appelle module cohérent (conformément à l'usage le plus répandu, notamment dans la littérature anglaise), et *module cohérent* ce que [CCA] appelle module cohérent de présentation finie. Ceci est naturellement à relier aux « faisceaux algébriques cohérents » de J.-P. Serre (précurseurs des faisceaux de modules sur un schéma de Grothendieck) qui sont localement donnés par des modules de présentation finie cohérents. Signalons aussi que le Stacks Project (ouvrage collectif, `http://stacks.math.columbia.edu`) adopte la définition de Bourbaki pour les modules cohérents.

$A \cap N$ est de type fini d'après le théorème 2.4, donc B est de présentation finie d'après le théorème 2.3(i).

Inversement, supposons que N et M/N sont cohérents, et soit A un sous-module de type fini de M. Alors $A \cap N$ est de type fini d'après le théorème 2.2, et par suite il est de présentation finie parce que N est cohérent. Par ailleurs πA est de présentation finie parce que M/N est cohérent. Donc A est de présentation finie d'après le théorème 2.3(ii). □

Corolaire 2.6. *Un module de présentation finie sur un anneau cohérent est cohérent.*

Démonstration. En utilisant de manière répétée le théorème 2.5, on montre que les modules libres de rang fini sont cohérents. En appliquant une autre fois le théorème 2.5, dans l'autre direction, on montre que les modules de présentation finie sont cohérents. □

Un module est **fortement discret** [1] si tout sous-module de type fini est détachable. Un anneau R est **fortement discret à gauche** si R est fortement discret en tant que module à gauche sur lui-même. Notez que R est fortement discret à gauche si, et seulement si, R/I est discret pour tout idéal à gauche de type fini I de R.

Les anneaux de polynômes sur les corps discrets sont des exemples d'anneaux cohérents noethériens fortement discrets. En mathématiques classiques, *tout* anneau noethérien est cohérent fortement discret (mais voir les exercices 3 et 4).

Théorème 2.7. *Soit N un sous-module de type fini d'un module cohérent M. Alors M est fortement discret si, et seulement si, N et M/N sont fortement discrets.*

Démonstration. Si M est fortement discret, alors clairement N et M/N sont fortement discrets. Inversement, supposons que N et M/N sont fortement discrets, et soit π l'application linéaire naturelle de M sur M/N. Pour montrer que M est fortement discret, considérons un sous-module de type fini P de M et un $x \in M$. Si $\pi x \notin \pi P$, alors $x \notin P$. Si $\pi x = \pi p$ pour un $p \in P$, alors $x \in P$ si, et seulement si, $x - p \in P \cap N$, qui est un sous-module de type fini de N parce que M est cohérent. □

Corolaire 2.8. *Si M est un module de présentation finie sur un anneau noethérien cohérent à gauche R, alors M est un module cohérent noethérien. Si en outre R est fortement discret, alors M est fortement discret.*

1. **NdT.** Strongly discrete. Dans le livre [CCA] la terminologie était initialement : le module « a des sous-modules détachables », i.e. « has detachable submodules ».

Démonstration. Soit $\mathcal{C}$ la classe des R-modules cohérents noethériens (fortement discrets). Comme $R \in \mathcal{C}$, par récurrence sur n et en utilisant les théorèmes 2.1 et 2.5 (et 2.7), on obtient que $R^n \in \mathcal{C}$. Comme M est de présentation finie, $M \in \mathcal{C}$ d'après les théorèmes 2.1 et 2.5 (et 2.7). □

Exercices

1. Montrer qu'un anneau commutatif R est fortement discret si, et seulement si, R/I est discret pour tout idéal de type fini I de R.
2. Montrer que tout idéal non nul de type fini de l'anneau $\mathbb{Z}$ des entiers a une profondeur finie dans l'ensemble ordonné des idéaux de type fini de $\mathbb{Z}$. Montrer que tout idéal non nul de type fini de l'anneau $k[X]$, où k est un corps discret, a une profondeur bornée.
3. Soit a une suite binaire. Soit k le corps à deux éléments et soit R le sous-anneau de l'anneau fini $k[X,Y]/(X,Y)^2$ engendré par 1, X, et $\{a_nY\}$. Montrer que R est un exemple brouwerien pour un anneau noethérien fortement discret mais pas cohérent. Faire la même chose pour l'anneau $\mathbb{Z}/I$ où I est engendré par les éléments $a_n n!$.
4. Construire un exemple brouwerien d'un anneau discret cohérent noethérien R, et d'un idéal de type fini I de R, tels que I n'est pas détachable dans R. (Suggestion : définir R situé quelque part entre $\mathbb{Z}$ et $\mathbb{Q}$.)
5. Soit I un idéal de type fini d'un anneau commutatif cohérent noethérien fortement discret R. Montrer que le radical de I est détachable. (Suggestion : soit $x \in R$; considérer la chaine croissante des idéaux $I : x^m$.)
6. Montrer que les modules de type fini cohérents sur les anneaux fortement discrets sont discrets.
7. Montrer que si S est un sous-anneau de R et si M est un R-module qui est noethérien comme S-module, alors M est noethérien comme R-module.
8. Montrer que si un module est borné en nombre, alors il est noethérien.
9. Montrer que tout corps discret est cohérent. Montrer que l'anneau $\mathbb{Z}$ est cohérent.
10. Un sous-module A d'un R-module B est appelé **pur** si chaque fois qu'un système fini d'équations

$$\sum r_{ij}x_j = a_i,$$

avec les coefficients r_{ij} dans R et les a_i dans A, a une solution dans B, alors il a une solution dans A. Montrer que $A \subseteq B$ est pur si, et seulement si, toute application linéaire depuis un module de présentation finie vers B/A se relève en une application linéaire vers B. Montrer que tout sous-groupe pur non nul du groupe abélien cyclique $\mathbb{Z}$ est égal à $\mathbb{Z}$.

11. Montrer que tout module noethérien M est hopfien (exercice 1.9). (Si $f(z) = 0$, construire une suite telle que $x_0 = z$ et $f(x_i) = x_{i-1}$.)

3 Localisation

Soit R un anneau commutatif. Nous construisons des anneaux de fractions sur R essentiellement de la même manière que nous avons construit les nombres rationnels à partir des nombres entiers. D'abord nous décidons d'un sous-ensemble S de R dont nous acceptons les éléments comme dénominateurs ; dans la construction des nombres rationnels cet ensemble est l'ensemble des entiers strictement positifs. En général nous demandons que l'ensemble S soit un **sous-monoïde multiplicatif** de R, autrement dit que $1 \in S$ et que si s_1 et $s_2 \in S$, alors $s_1 s_2 \in S$.

Les éléments de l'**anneau de fractions** $S^{-1}R$ sont les couples r/s avec $r \in R$ et $s \in S$. L'addition et la multiplication sont définies par les formules habituelles :

$$r_1/s_1 + r_2/s_2 = (r_1 s_2 + r_2 s_1)/(s_1 s_2),$$
$$(r_1/s_1)(r_2/s_2) = (r_1 r_2)/(s_1 s_2),$$

mais nous devons faire assez attention pour définir l'égalité des fractions parce que tout élément s de S est inversible dans $S^{-1}R$, et par suite un élément r de R tel que $sr = 0$ doit être nul dans $S^{-1}R$. En gardant à l'esprit cette précaution, nous disons que deux fractions r_1/s_1 et r_2/s_2 sont **égales** s'il existe un élément $s \in S$ tel que $s(r_1 s_2 - r_2 s_1) = 0$. On a un morphisme naturel $R \to S^{-1}R$ défini en envoyant l'élément r sur l'élément $r/1$. Nous laissons au lecteur le soin de vérifier que $S^{-1}R$ est un anneau. On dit aussi que $S^{-1}R$ est le **localisé de** R **en** S.

Plus généralement, si M est un R-module, nous pouvons construire le **module de fractions** $S^{-1}M$ dont les éléments sont les fractions m/s avec $m \in M$ et $s \in S$. L'égalité et l'addition sont définies comme pour $S^{-1}R$, tandis que la multiplication par les éléments de R, ou de $S^{-1}R$, est définie de la manière évidente. Ainsi $S^{-1}M$ est un $S^{-1}R$-module. Si N est un sous-module de M, alors $S^{-1}N$ est un sous-module de $S^{-1}M$. On dit aussi que $S^{-1}M$ est le **localisé de** M **en** S.

Si P est un idéal premier propre de R, $S = R \setminus P$ est un sous-monoïde multiplicatif de R. Dans ce cas nous notons M_P le module $S^{-1}M$. Si P est détachable, l'anneau R_P est **local** en ce sens que pour tout $x \in R$, x ou $1 - x$ est inversible ; en effet, un élément r/s de R_P est inversible si $r \notin P$, tandis que si $r \in P$, $s - r \notin P$, et donc $1 - r/s = (s - r)/s$ est inversible. Lorsque R est un anneau intègre discret, $P = 0$ est un idéal premier propre détachable et l'anneau R_P est le corps de fractions de R.

Soit r un élément d'un anneau commutatif R, et soit S le sous-monoïde multiplicatif de R engendré par r. D'après les définitions, l'élément r est nil-

potent si, et seulement si, $S^{-1}R = 0$. Nous utiliserons cette propriété dans les démonstrations du théorème 3.1, du lemme 3.2 et du corolaire 3.4 ci-après.

Notre premier résultat généralise le théorème II.7.5 qui démontrait en utilisant les déterminants que le rang d'un module libre de rang fini sur un anneau commutatif non trivial est un invariant.

Théorème 3.1. *Soit R un anneau commutatif. S'il y a un monomorphisme de R^m vers R^n avec $m > n$, alors R est trivial.*

Démonstration. Soit A la matrice de format $m \times n$ qui représente une application linéaire injective φ de R^m vers R^n. Nous démontrons d'abord que les éléments de la première colonne de la matrice sont nilpotents. Si r est un élément de la première colonne, alors notons $S = \{1, r, r^2, \ldots\}$ et passons à l'anneau $T = S^{-1}R$. On vérifie facilement que A est la matrice d'un application linéaire injective de T^m vers T^n. En utilisant des manipulations élémentaires de lignes et de colonnes sur A, ce qui revient à changer les bases de T^n et T^m, nous obtenons que la première colonne et la première ligne de A sont nulles sauf pour un 1 dans le coin nord-ouest. Soit $e_1, \ldots, e_m$ la nouvelle base de T^m. Si $n = 1$ alors $\varphi(e_m) = 0$, et donc $0 = 1$ dans T parce que φ est injectif. Si $n > 1$, alors $0 = 1$ dans T par récurrence, avec la matrice obtenue à partir de A en supprimant la première ligne et la première colonne. Ainsi r est nilpotent dans R.

Soit I l'idéal de R engendré par les éléments de la première colonne de A et soit $e_1, \ldots, e_m$ la base naturelle de R^m. Alors $I^k = 0$ pour un certain $k \geqslant 0$. Mais si $I^k e_1 = 0$ pour un $k \geqslant 1$, alors $\varphi(I^{k-1}e_1) = 0$, et donc $I^{k-1}e_1 = 0$ car φ est injective. Ainsi $e_1 = 0$ et R est trivial. □

Le théorème 3.1 généralise le théorème II.7.5 parce que si R^n s'envoie sur R^m avec $m > n$, alors, comme R^m est projectif, R^m s'envoie injectivement dans R^n. Le théorème suivant sera utilisé dans le chapitre VIII.

Lemme 3.2. *Soient $R \subseteq T$ des anneaux commutatifs et A une matrice sur R. Supposons que*

(i) *si $(c, 0, \ldots, 0)$ est dans l'espace des lignes de A sur R, alors $c = 0$,*

(ii) *$(1, 0, \ldots, 0)$ est dans l'espace de lignes de A sur T.*

Alors $R = 0$.

Démonstration. Nous remarquons que si (R, T, A) satisfait les hypothèses et si S est un monoïde de R, alors $(S^{-1}R, S^{-1}T, A)$ satisfait aussi les hypothèses.

Nous remarquons aussi que si nous faisons subir à A des manipulations élémentaires de lignes à coefficients dans R et si A' est la nouvelle matrice, alors (R, T, A') satisfait aussi les hypothèses.

Nous allons montrer le résultat par récurrence sur le nombre de lignes de A.

Tout d'abord si A a une seule ligne $(a_1, \ldots, a_n)$, il existe un $b \in T$ tel que $ba_1 = 1$ et $ba_i = 0$ pour $i > 1$, d'où $a_i = ba_1a_i = a_1ba_i = 0$. Donc $A = (a_1, 0, \ldots, 0)$ et d'après (i), $a_1 = 0$, donc $1 = ba_1 = 0$ dans T, mais aussi dans R.

Supposons maintenant que A a au moins $m + 1$ lignes ($m \geqslant 1$).

Considérons un coefficient $a = a_{ij}$ de A, où $j > 1$, et le monoïde $S = \{1, a, a^2, \ldots\}$. On a $(S^{-1}R, S^{-1}T, A)$ qui satisfait les hypothèses, et par manipulations élémentaires de lignes sur $S^{-1}R$ on remplace a par 1 et les autres coefficients de sa colonne par 0. On vérifie alors que si l'on supprime la ligne et la colonne du 1 en question, les hypothèses sont toujours satisfaites. Par hypothèse de récurrence, nous concluons que $a = a_{ij}$ est nilpotent. Nous venons d'établir que tous les coefficients de A en dehors de la première colonne sont nilpotents.

Considérons ensuite un coefficient $a = a_{i1}$ de la première colonne et le monoïde $S = \{1, a, a^2, \ldots\}$. On a $(S^{-1}R, S^{-1}T, A)$ qui satisfait les hypothèses, et en multipliant la ligne ρ_i par $1/a$, on remplace a par 1 et ses autres coefficients restent nilpotents. Soit I l'idéal engendré par ces coefficients. On a un k tel que $I^k = 0$. Pour un r arbitraire dans I^{k-1}, la ligne $r\rho_i$ a ses coefficients nuls sauf le premier, qui est r, ainsi $r = 0$ d'après l'hypothèse (i). Par suite $I = 0$, et donc $\rho_i = (1, 0, \ldots, 0)$, d'où $1 = 0$ d'après l'hypothèse (i), i.e. $S^{-1}R = 0$, et $a = a_{i1}$ est nilpotent.

Ainsi les a_{i1} sont nilpotents. Donc 1 est nilpotent dans T, i.e. $1 = 0$ dans T et R. □

Théorème 3.3. *Soient $R \subseteq T$ des anneaux commutatifs, et I un idéal de $R[X]$ tel que $I \cap R = 0$ et $1 \in TI$. Alors $R = 0$.*

Démonstration. Tout élément de TI peut être écrit sous la forme $t_1p_1 + \cdots + t_mp_m$, avec $p_i \in I$ et $t_i \in T$. Écrivons 1 de cette manière, et appliquons le lemme 3.2 à la matrice des coefficients des p_i. □

Corolaire 3.4. *Soient $R \subseteq T$ des anneaux commutatifs, et I un idéal de $R[X]$ tel que $1 \in TI$. Alors l'annulateur de $R \cap I$ est formé d'éléments nilpotents.*

Démonstration. Supposons que $r(R \cap I) = 0$. Soit S le sous-monoïde multiplicatif de R engendré par r, et passons à $S^{-1}R$. Le théorème 3.3 s'applique et nous dit que $S^{-1}R = 0$, donc r est nilpotent. □

Exercices

1. Soit R un anneau commutatif cohérent fortement discret et soit P un idéal premier propre de type fini de R. Montrer que R_P est discret.

2. Soient S un sous-monoïde multiplicatif d'un anneau commutatif R, M un R-module, et N_1 et N_2 des sous-modules de M. Montrer que
$$S^{-1}(N_1 \cap N_2) = S^{-1}N_1 \cap S^{-1}N_2$$
et que
$$S^{-1}(N_1 + N_2) = S^{-1}N_1 + S^{-1}N_2.$$
3. Soit S un sous-monoïde multiplicatif d'un anneau commutatif R, et soit $\varphi\colon R \to S^{-1}R$ le morphisme naturel. Montrer que $S^{-1}R$ est discret si, et seulement si, $\ker\varphi$ est détachable dans R. Montrer que si R est un anneau discret réduit et si S est de type fini, alors $S^{-1}R$ est discret.
4. Soit S un sous-monoïde multiplicatif d'un anneau commutatif R. Montrer que si M est un R-module cohérent, $S^{-1}M$ est un $S^{-1}R$-module cohérent.
5. Soit P un idéal premier propre détachable d'un anneau commutatif R. Montrer que le radical de Jacobson de R_P est détachable, et que son complément est formé par les unités de R_P.
6. Soient k un corps discret et a, b, c, s des indéterminées. Soit $R = k[a, b, c]/(ca, cb, c^2)$ et soit $S = R[s]/(sa + (1-s)b)$. Soit I l'idéal de $R[X]$ engendré par $1 + aX$ et $1 + bX$. Montrer que $I \cap R$ est engendré par c et $b - a$, et que $1 \in SI$. Ainsi, nous ne pouvons pas renforcer le théorème 3.3 en ajoutant à la conclusion que l'annulateur de $I \cap R$ est nul.
7. Montrer qu'une matrice A de format $m \times n$ sur un anneau commutatif R a une inverse à gauche si, et seulement si, les déterminants des matrices carrées $n \times n$ extraites de A engendrent R en tant qu'idéal.

4 Produits tensoriels

Soient A un anneau, R un sous-anneau et B un R-module à gauche. Il y a une façon naturelle de construire un A-module à gauche à partir de B. Nous considérons les sommes formelles $\sum a_i b_i$, et nous disons que deux telles sommes formelles sont égales lorsque nous pouvons obtenir l'une à partir de l'autre en appliquant les lois de distributivité à droite et à gauche, la loi d'associativité $(ar)b = a(rb)$, et les calculs qui se déroulent entièrement à l'intérieur de A ou de B. La structure d'anneau de A est utilisée uniquement pour obtenir la structure de A-module sur les sommes formelles ; en général, en utilisant pour A uniquement sa structure de R-module à droite, le résultat est un groupe abélien. Nous donnons maintenant la spécification précise de cette construction.

Définition 4.1. Soient R un anneau, A un R-module à droite, et B un R-module à gauche. Le **produit tensoriel** $A \otimes B$ est défini comme le quotient du groupe abélien libre $F(A \times B)$ sur $A \times B$ par le sous-groupe $K(A \times B)$ de $F(A \times B)$ engendré par les éléments de la forme

(i) $(a_1 + a_2, b) - (a_1, b) - (a_2, b)$
(ii) $(a, b_1 + b_2) - (a, b_1) - (a, b_2)$
(iii) $(ar, b) - (a, rb)$.

Nous notons l'image de l'élément (a, b) de $A \times B$ dans $A \otimes B$ par $a \otimes b$. Une fonction f de $A \times B$ vers un groupe abélien G est dite **bilinéaire** si

(i) $f(a_1 + a_2,\, b) = f(a_1, b) + f(a_2, b)$
(ii) $f(a, b_1 + b_2) = f(a, b_1) + f(a, b_2)$
(iii) $f(ar, b) = f(a, rb)$,

autrement dit, si la fonction induite de $F(A \times B)$ vers G envoie $K(A \times B)$ sur zéro. Par suite, tout application bilinéaire f de $A \times B$ vers G induit un unique homomorphisme de groupes abéliens de $A \otimes B$ vers G qui envoie $a \otimes b$ sur $f(a, b)$. En conséquence, nous pouvons définir un homomorphisme φ de $A \otimes B$ vers G en spécifiant les valeurs qu'il prend pour les éléments $a \otimes b$, et en vérifiant que la fonction

$$A \times B \to G, \quad (a, b) \to \varphi(a \otimes b)$$

est bilinéaire.

Le produit tensoriel $A \otimes B$ dépend de l'anneau R; si nous voulons une notation pour indiquer cet anneau, nous écrivons $A \otimes_R B$. Si A est un S-R-bimodule, et B est un R-module à gauche, alors le groupe abélien $A \otimes_R B$ a une structure naturelle de S-module à gauche obtenue en posant $s(a \otimes b) = sa \otimes b$. En particulier, si R est commutatif, alors $A \otimes B$ est un R-module.

Le produit tensoriel de deux modules cycliques a une description simple.

Théorème 4.2. *Soient R un anneau, I un idéal à droite, J un idéal à gauche, et B un R-module à gauche. Alors*

(i) $(R/I) \otimes B \simeq B/IB$
(ii) $(R/I) \otimes (R/J) \simeq R/(I + J)$.

Si I est un idéal, alors ce sont des isomorphismes de R-modules à gauche.

Démonstration. Dans le point (i), les deux membres ont seulement une structure de groupes abéliens, i.e. de $\mathbb{Z}$-modules. Pour démontrer (i) nous définissons une application $\mathbb{Z}$-linéaire φ de $(R/I) \otimes B$ vers B/IB en posant $\varphi(r \otimes b) = rb$, et une application $\mathbb{Z}$-linéaire ψ de B/IB vers $(R/I) \otimes B$ en posant $\psi(b) = 1 \otimes b$. Nous notons que si $r - r' \in I$, alors $rb - r'b \in IB$, donc φ est bien définie. Par ailleurs, si $b - b' \in IB$, alors $1 \otimes b - 1 \otimes b' = 1 \otimes (b - b') = 0$ dans $(R/I) \otimes B$, donc ψ est bien définie. Comme $r \otimes b = 1 \otimes rb$, les deux applications $\mathbb{Z}$-linéaires φ et ψ sont inverses l'une de l'autre.

Le point (ii) résulte du point (i) parce que $I(R/J) = (I + J)/J$.

Si I est un idéal (bilatère), alors R/I et B/IB sont des R-modules à gauche et la structure de R-module sur $(R/I) \otimes B$ est donnée par $r(1 \otimes b) = r \otimes b$, donc φ et ψ sont des applications R-linéaires. □

En particulier en prenant $I = 0$ dans le théorème 4.2(i), si B est un R-module à gauche, alors $R \otimes_R B \simeq B$.

Théorème 4.3. *Soient R un anneau, $\{A_i\}_{i\in I}$ une famille de R-modules à droite, et $\{B_j\}_{j\in J}$ une famille de R-modules à gauche. Alors on a un isomorphisme naturel*

$$\bigoplus\nolimits_{i\in I} A_i \otimes \bigoplus\nolimits_{j\in J} B_j \;\simeq\; \bigoplus\nolimits_{i,j\in I\times J} (A_i \otimes B_j).$$

Démonstration. Exercice 1. □

Corolaire 4.4. *Le produit tensoriel de deux modules libres sur un anneau commutatif R est un module libre. En particulier, $R^m \otimes R^n \simeq R^{mn}$.*

Démonstration. Cela résulte des théorèmes 4.2 et 4.3. □

Le produit tensoriel est un **bifoncteur** en ce sens qu'étant données des applications R-linéaires $f\colon A \to A'$ et $g\colon B \to B'$, il y a un homomorphisme naturel de groupes abéliens $f \otimes g\colon A \otimes B \to A' \otimes B'$ défini par $(f \otimes g)(a \otimes b) = f(a) \otimes g(b)$. Si R est commutatif, alors $f \otimes g$ est une application R-linéaire.

Une suite de deux applications R-linéaires $A \to B \to C$ est **exacte en** B si l'image de $A \to B$ est égale au noyau de $B \to C$. Une suite d'applications R-linéaires $A_1 \to A_2 \to \cdots \to A_n$ est **exacte** si elle est exacte en A_i pour $i = 2, \ldots, n-1$. La suite $0 \to A \to B$ est exacte si, et seulement si, $A \to B$ est injective ; la suite $A \to B \to 0$ est exacte si, et seulement si, $A \to B$ est surjective.

Théorème 4.5. *Soit R un anneau, et soient*

$$A \to B \to C \to 0 \;\; \textit{et} \;\; A' \to B' \to C' \to 0$$

des suites exactes de R-modules à droite et à gauche respectivement. Alors la suite

$$(A \otimes B') \oplus (B \otimes A') \to B \otimes B' \to C \otimes C' \to 0$$

est exacte.

Démonstration. Soit K l'image de $(A \otimes B') \oplus (B \otimes A')$ dans $B \otimes B'$. L'homomorphisme de $B \otimes B'$ vers $C \otimes C'$ envoie K sur 0, donc il induit

$$\varphi\colon (B \otimes B')/K \to C \otimes C'.$$

Nous allons montrer que φ est un isomorphisme en construisant son inverse. Nous définissons un homomorphisme $\psi\colon C \otimes C' \to (B \otimes B')/K$ de la manière suivante. Étant donné $c \otimes c' \in C \otimes C'$, nous choisissons un $b \in B$ qui a pour image c, et un $b' \in B'$ qui a pour image c'. Nous définissons $\psi(c \otimes c')$ comme

l'image de $b \otimes b'$ dans $(B \otimes B')/K$; si b_1 et b_2 ont pour image c et si b'_1 et b'_2 ont pour image c', alors

$$b_1 \otimes b'_1 - b_2 \otimes b'_2 = (b_1 - b_2) \otimes b'_1 + b_2 \otimes (b'_1 - b'_2)$$

est un élément de K, donc ψ est bien défini. On voit facilement que la bilinéarité requise est satisfaite, ce qui fait que nous avons bien défini un homomorphisme (de groupes abéliens) de source $C \otimes C'$. Clairement, φ et ψ sont inverses l'un de l'autre. □

Corolaire 4.6. *Soit M un module à gauche sur un anneau R, et soit $A \to B \to C \to 0$ une suite exacte de R-modules à droite. Alors la suite $A \otimes M \to B \otimes M \to C \otimes M \to 0$ est exacte.*

Démonstration. Prendre $A' = 0$ et $B' = C' = M$ dans le théorème 4.5. □

Corolaire 4.7. *Si C et C' sont des modules de présentation finie sur un anneau commutatif R, alors il en va de même pour $C \otimes C'$.*

Démonstration. Nous pouvons prendre pour A', B', A et B des R-modules de type fini dans l'hypothèse du théorème 4.5. □

La relation d'égalité sur $A \otimes B$ admet la description suivante.

Théorème 4.8. *Soient R un anneau, A un R-module à droite engendré par des éléments $a_1, \dots, a_m$, et B un R-module à gauche. L'élément $\sum_{i=1}^m a_i \otimes b_i$ est nul dans $A \otimes B$ si, et seulement si, il existe des éléments $r_{ij} \in R$ et $c_j \in B$ tels que*

(i) $b_i = \sum_j r_{ij} c_j$,

(ii) $\sum_i a_i r_{ij} = 0$.

Démonstration. Clairement la condition implique l'égalité $\sum a_i \otimes b_i = 0$. Inversement, soit F un R-module à droite libre de rang m, et envoyons F sur A avec un noyau K en envoyant une base $e_1, \dots, e_m$ de F sur les éléments $a_1, \dots, a_m$. Cela donne la suite exacte

$$K \otimes B \to F \otimes B \to A \otimes B \to 0$$

L'élément $\sum_{i=1}^m e_i \otimes b_i$ de $F \otimes B$ a pour image 0 dans $A \otimes B$, donc il est l'image d'un élément de $K \otimes B$ que nous pouvons écrire sous la forme $\sum_j k_j \otimes c_j$ avec les $k_j \in K$ et les $c_j \in B$, ce qui donne

$$\sum\nolimits_{i=1}^m e_i \otimes b_i = \sum\nolimits_j \Big(\sum\nolimits_i e_i r_{ij} \Big) \otimes c_j = \sum\nolimits_i e_i \otimes \Big(\sum\nolimits_j r_{ij} c_j \Big).$$

Comme les e_i sont une base de F, nous avons $b_i = \sum r_{ij} c_j$. Comme $\sum_i e_i r_{ij} \in K$, nous avons $\sum_i a_i r_{ij} = 0$. □

Exercices

1. Soient $\{B_i\}_{i\in I}$ une famille de R-modules à gauche et A un R-module à droite. Montrer que l'on a un isomorphisme naturel
$$A \otimes \bigoplus\nolimits_{i\in I} B_i \simeq \bigoplus\nolimits_{i\in I}(A \otimes B_i).$$
2. Si S est un sous-monoïde multiplicatif d'un anneau commutatif R et si M est un R-module, montrer que $S^{-1}M \simeq (S^{-1}R) \otimes M$ comme $S^{-1}R$-modules.
3. Soient a une suite binaire, A le groupe des entiers modulo 5, C le groupe des entiers modulo 25, et soit B le sous-groupe de C engendré par 5 et l'ensemble $\{\, a_n : n = 1, 2, \ldots\}$. Montrer que A et B sont des groupes abéliens discrets, et que $A \otimes B$ est discret si, et seulement si, $a_n = 1$ pour un n, ou $a_n = 0$ pour tout n.
4. Soit a une suite binaire. Soit F l'anneau des entiers modulo 2, et soit R le sous-anneau de $F[x, y, s, t]/(sx + ty - 1)$ engendré par x, y et l'ensemble $\{\, a_n s, a_n t : n = 1, 2, \ldots\}$. Soit $A = R/(x)$ et $B = R/(y)$. Montrer que A et B sont des R-modules de présentation finie discrets, et que $A \otimes B$ est discret si, et seulement si, $a_n = 1$ pour un n, ou $a_n = 0$ pour tout n.
5. Montrer que le sous-module $A \subseteq B$ est pur si, et seulement si, l'homomorphisme naturel $M \otimes A \to M \otimes B$ est injectif pour tout module à droite de présentation finie M. Montrer que l'expression « de présentation finie » peut être supprimée dans l'affirmation précédente.

5 Modules plats

Soit R un anneau et soit M un R-module à gauche. Nous disons que M est **plat** si pour tous $x_1, \ldots, x_m \in M$ et tous $r_1, \ldots, r_m \in R$ tels que $\sum r_i x_i = 0$, il existe des $y_1, \ldots, y_n \in M$ et des $a_{ij} \in R$ tels que $x_i = \sum_j a_{ij} y_j$ et $\sum_i r_i a_{ij} = 0$. La platitude est clairement une propriété locale en ce sens qu'un R-module est plat si, et seulement si, tout sous-module de type fini est contenu dans un sous-module plat.

Théorème 5.1. *Si $\{M_i\}_{i\in I}$ est une famille de R-modules, alors $\bigoplus_{i\in I} M_i$ est plat si, et seulement si, chaque M_i est plat.*

Démonstration. Comme la platitude est une propriété locale, nous pouvons supposer que I est finiment énumérable, disons $I = \{s_1, \ldots, s_n\}$. Notons $M = \bigoplus_{i\in I} M_i$.
Supposons tout d'abord que les M_i sont plats. Considérons une égalité dans M
$$0 = \sum\nolimits_{1\leqslant \ell \leqslant m} r_\ell x_\ell = \bigoplus\nolimits_{1\leqslant k\leqslant n} y_k$$

avec $y_k = \sum_{1\leqslant\ell\leqslant m} r_\ell x_{k,\ell}$ et les $x_{k,\ell} \in M_{i_k}$.
Par définition de l'égalité dans M, puisque $\bigoplus_{1\leqslant k\leqslant n} y_k = 0$, on est dans (au moins) l'un des deux cas suivants :

— tous les y_k sont nuls,
— deux indices sont égaux dans I : $i_k =_I i_h$ pour h et k distincts dans $\{1,\dots,n\}$.

Le premier cas se traite en considérant les relations données par la platitude dans chaque M_{i_k}. Le deuxième cas se ramène au premier par récurrence sur n.
Supposons maintenant que M est plat et considérons par exemple l'indice $i_1 \in I$ et une égalité $\sum_{1\leqslant\ell\leqslant m} r_\ell x_\ell = 0$ dans M_{i_1}. Puisque M est plat, on écrit

$$x_\ell =_M \sum\nolimits_{1\leqslant j\leqslant p} g_{\ell,j} z_j \text{ avec } \sum\nolimits_{1\leqslant\ell\leqslant m} r_\ell g_{\ell,j} =_R 0 \text{ pour chaque } j.$$

On écrit $z_j = \bigoplus_{1\leqslant k\leqslant n} y_{j,k}$ avec $y_{j,k} \in M_{i_k}$, ce qui donne

$$x_\ell =_M \bigoplus\nolimits_{1\leqslant k\leqslant n} \sum\nolimits_{1\leqslant j\leqslant p} g_{\ell,j} y_{j,k}$$

Par définition de l'égalité dans M, on est dans (au moins) l'un des deux cas suivants :

— pour chaque ℓ, on a $x_\ell = \sum_{1\leqslant j\leqslant p} g_{\ell,j} y_{j,1}$ dans M_{i_1},
— on a dans I : $i_1 =_I i_h$ pour un $h \neq 1$ dans $\{1,\dots,n\}$.

Dans le premier cas, on a dans M_{i_1} les égalités qui nous conviennent.
Le deuxième cas se ramène au premier par récurrence sur n. □

La partie « seulement si » du théorème 5.1 nous donne une information plus précise que seulement « un facteur direct d'un module plat est plat », parce que les M_i ne sont pas nécessairement des facteurs directs de la somme directe.

Corolaire 5.2. *Les modules libres et les modules projectifs sont plats.*

Démonstration. Le fait que le R-module à gauche R est plat est obtenu en prenant $n = 1$ et $y_1 = 1$ dans la définition de la platitude. Ensuite le théorème 5.1 montre que les modules libres sont plats. Si P est projectif, alors l'application naturelle du module libre $R^{(P)}$ sur P a une inverse à droite, donc P est un facteur direct de $R^{(P)}$, et donc P est plat. □

Un diagramme de modules et applications linéaires, comme par exemple le carré

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ {\scriptstyle\beta}\downarrow & & \downarrow{\scriptstyle\gamma} \\ C & \xrightarrow[\delta]{} & D\,, \end{array}$$

est dit **commutatif** si toutes les composées de flèches dans le diagramme qui commencent au même endroit et se terminent au même endroit sont égales. Par exemple le carré est commutatif si, et seulement si, $\gamma\alpha = \delta\beta$.

Théorème 5.3. *Soit M un R-module à gauche. Les conditions suivantes sont équivalentes.*

(i) *M est plat.*

(ii) *Pour tout idéal à droite I de R, l'homomorphisme $I \otimes M \to M$ est injectif.*

(iii) *Pour tout R-module à droite libre de rang fini B et tout sous-module $A \subseteq B$, l'homomorphisme $A \otimes M \to B \otimes M$ est injectif.*

(iv) *Pour tout R-module à droite B et tout sous-module $A \subseteq B$, l'homomorphisme $A \otimes M \to B \otimes M$ est injectif.*

Démonstration. Supposons (i) et considérons une somme $\sum r_i \otimes x_i \in I \otimes M$ qui devient nulle dans M. Alors $\sum r_i x_i = 0$, et il existe des $y_j \in M$ et des $a_{ij} \in R$ tels que $x_i = \sum_j a_{ij} y_j$ et $\sum_i r_i a_{ij} = 0$. Ainsi

$$\sum\nolimits_i r_i \otimes x_i = \sum\nolimits_i \sum\nolimits_j r_i \otimes a_{ij} y_j = \sum\nolimits_j \sum\nolimits_i r_i a_{ij} \otimes y_j = 0$$

et (ii) est satisfaite.

Supposons maintenant (ii). Nous allons montrer (iii) par récurrence sur le rang de B. Si B est de rang 1, alors B est isomorphe à R et (ii) s'applique. Soit $B = B_1 \oplus B_2$ avec les B_i libres de rangs plus petits que celui de B. Soit $A_1 = A \cap B_1$ et soit A_2 la projection de A dans B_2. Nous considérons le diagramme commutatif suivant.

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & A_1 \otimes M & \longrightarrow & A \otimes M & \longrightarrow & A_2 \otimes M \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & B_1 \otimes M & \longrightarrow & B \otimes M & \longrightarrow & B_2 \otimes M
\end{array}$$

La première ligne est exacte d'après le corolaire 4.6, et $B_1 \otimes M$ est un facteur direct de $B \otimes M$ parce que B_1 est un facteur direct de B. Les première et troisième colonnes du diagramme sont exactes par récurrence. Une chasse facile dans le diagramme montre que la seconde colonne est également exacte, donc (iii) est satisfaite.

Supposons (iii). Pour démontrer (iv) il nous suffit de traiter le cas où B est un R-module à droite de type fini, parce que si un élément est nul dans $B \otimes M$, alors il est déjà nul dans $B \otimes N$ pour un sous-module de type fini N de M. Envoyons un R-module à droite libre de type fini F sur B avec un noyau K, et soit F' l'image réciproque de A dans F. Considérons le diagramme commutatif

suivant.

$$\begin{array}{ccccccccc} & & & & 0 & & & & \\ & & & & \downarrow & & & & \\ 0 & \longrightarrow & K\otimes M & \longrightarrow & F'\otimes M & \longrightarrow & A\otimes M & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & K\otimes M & \longrightarrow & F\otimes M & \longrightarrow & B\otimes M & \longrightarrow & 0 \end{array}$$

D'après l'hypothèse (iii), les lignes et les colonnes sont exactes. Une chasse facile dans le diagramme montre que l'homomorphisme $A\otimes M\to B\otimes M$ est aussi injectif.

Enfin supposons (iv), avec une somme $\sum_i r_i x_i = 0$. Soit I l'idéal à droite de R engendré par les r_i et considérons l'homomorphisme de $I\otimes M$ vers $R\otimes M$. L'élément $\sum_i r_i\otimes x_i$ a pour image zéro, et l'hypothèse (iv) nous dit que nous avons $\sum_i r_i\otimes x_i = 0$. Maintenant nous voyons que (i) est satisfaite en vertu du théorème 4.8. □

Corolaire 5.4. *Soient M un R-module à gauche, B un R-module à droite, et A un sous-module de B. Si B/A est plat, alors l'homomorphisme de $A\otimes M$ vers $B\otimes M$ est injectif.*

Démonstration. Envoyons un module libre F sur M avec K pour noyau, et considérons le diagramme commutatif suivant dans lequel $C = B/A$.

$$\begin{array}{ccccccccc} & & & & 0 & & & & \\ & & & & \downarrow & & & & \\ & & A\otimes K & \longrightarrow & A\otimes F & \longrightarrow & A\otimes M & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & B\otimes K & \longrightarrow & B\otimes F & \longrightarrow & B\otimes M & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & C\otimes K & \longrightarrow & C\otimes F & \longrightarrow & C\otimes M & & \end{array}$$

La colonne du milieu est exacte parce que F est libre ; la dernière ligne est exacte parce que C est plat. Soit $x\in A\otimes M$ nul dans $B\otimes M$. Alors x provient d'un $y\in A\otimes F$, qui s'envoie sur un $z\in B\otimes F$, qui provient d'un $w\in B\otimes K$. Maintenant w a une image nulle dans $C\otimes F$, et donc aussi dans $C\otimes K$. Par suite w provient d'un $u\in A\otimes K$, qui s'envoie sur y dans $A\otimes F$ parce qu'il s'envoie sur z dans $B\otimes F$. Ainsi $x = 0$. □

Exercices

1. Soit S un sous-monoïde multiplicatif d'un anneau commutatif R. Montrer que $S^{-1}R$ est un R-module plat.

2. Soit A un module à droite plat (sur un anneau R) tel que AI est une partie détachable de A pour tout idéal à droite de type fini I de R. Soit B un R-module à gauche cohérent de type fini. Montrer que $A \otimes B$ est discret.

3. Montrer que les propriétés suivantes sur un anneau R sont équivalentes.

   (i) $\prod_{i\in\mathbb{N}} M_i$ est un R-module à gauche plat si tous les M_i sont plats.

   (ii) $R^{\mathbb{N}}$ est un R-module à gauche plat.

   (iii) Si $\varphi\colon R^n \to R$ est une application linéaire de R-modules à droite, alors tout ensemble dénombrable d'éléments de $\ker\varphi$ est contenu dans un sous-module de type fini de $\ker\varphi$.

   Lorsque R est dénombrable et discret, montrer que (iii) est équivalent au fait que R est cohérent à droite.

4. *Les modules plats de présentation finie sont projectifs.* Soit F un R-module à gauche libre de rang fini, et K un sous-module de type fini de F. Pour $x \in F$ notons I_x l'idéal à droite de R engendré par les coordonnées de x dans F. Montrer que les conditions suivantes sont équivalentes.

   (i) F/K est plat [1].

   (ii) $x \in I_x K$ pour chaque $x \in K$.

   (iii) Pour tout $x \in K$ il existe une application linéaire $f\colon F \to K$ telle que $x = f(x)$.

   (iv) K est un facteur direct de F.

   Utilisez votre démonstration pour montrer que si R est commutatif et si F est fortement discret, alors on peut décider si F/K est ou n'est pas projectif.

5. Montrer que tout module sur un anneau à division discret est plat. Montrer que si $k \subseteq K$ sont des corps discrets, et si V est un espace vectoriel sur k, alors $v_1, \ldots, v_n \in V$ sont linéairement dépendants sur k si, et seulement si, ils sont linéairement dépendants sur K dans $K \otimes_k V$.

6. Utiliser le théorème 5.3(ii) pour montrer que si $A \subseteq B$ et si A et B/A sont plats, alors B est plat. En déduire que si tout R-module cyclique est plat alors tout R-module est plat. Montrer qu'un anneau R est von-Neumann-régulier (voir l'exercice II.6.4) si, et seulement si, tout R-module est plat. Montrer que si R est von-Neumann-régulier, alors tout idéal à gauche de type fini de R est un facteur direct, et donc R est cohérent.

1. **NdT.** Notez que F/K est un module de présentation finie arbitraire et que la condition (iv) implique que F/K est un module projectif.

6 Anneaux locaux

Un anneau R est dit **local** si pour tout $r \in R$, r ou $1 - r$ est inversible. Une condition équivalente est que si $r_1 + r_2$ est inversible, alors r_1 ou r_2 est inversible. Un corps de Heyting est un anneau local, et beaucoup de résultats dans cette section et la suivante présentent un intérêt par ce qu'ils disent au sujet des corps de Heyting. En fait, un corps de Heyting peut être caractérisé comme un anneau commutatif local dans lequel 1 ne peut pas être nul et dans lequel tout élément qui ne peut pas être une unité est nul. Un avantage de travailler avec les anneaux locaux plutôt qu'avec les corps de Heyting, outre la plus grande généralité, est que nous n'employons pas de notions négatives comme celles utilisées dans la phrase précédente.

Un endomorphisme f d'un anneau R en tant que R-module à gauche est donné par $f(x) = xf(1)$, de sorte que la fonction $f \mapsto f(1)$ est un isomorphisme de l'anneau $E_R(R)$ des endomorphismes de R en tant que R-module à gauche vers l'anneau opposé à R. Comme l'anneau opposé à un anneau local est local, si R est local, alors le module à gauche R a pour anneau d'endomorphismes un anneau local.

Soit e un idempotent dans un anneau local. Si e est une unité, alors $e = 1$; si $1 - e$ est unité, alors $e = 0$ (éventuellement les deux). Donc si l'anneau d'endomorphismes d'un module M est local, tout facteur direct de M est égal à 0 ou à M, c'est-à-dire, M est **indécomposable**. Les théorèmes suivants qui traitent de décompositions directes de modules qui ont un anneau d'endomorphismes local sont appelés des **théorèmes d'Azumaya**. Gardez présent à l'esprit que si R est un corps de Heyting, ou même simplement un anneau local, alors R^n est une somme directe de R-modules qui ont un anneau d'endomorphismes local.

Lemme 6.1. *Soit $B \oplus C = A_1 \oplus \cdots \oplus A_n$ un module. Si l'anneau d'endomorphismes de C est local, alors $B \oplus C = B \oplus D$, avec $D \subseteq A_i$ pour un i.*

Démonstration. Soient π_i, π_B, et π_C les projections sur A_i, B et C respectivement. Alors $\pi_C(\pi_1 + \cdots + \pi_n)$ est l'application identique de C, donc l'un des $\pi_C\pi_i$ est un automorphisme de C. Posons $D = \pi_i C$. Alors π_C envoie D isomorphiquement sur C, et donc $B \oplus C = B \oplus D$. □

Le premier théorème d'Azumaya montre que les facteurs directs de modules qui ont des anneaux d'endomorphismes locaux sont de nouveau des sommes directes de modules qui ont des anneaux d'endomorphismes locaux.

Théorème 6.2. *Soient $A \oplus B = C_1 \oplus \cdots \oplus C_n$ des modules tels que l'anneau d'endomorphismes de chaque C_i est local. Alors il existe des modules D_j tels que*

$$A = D_1 \oplus \cdots \oplus D_m \text{ et } B = D_{m+1} \oplus \cdots \oplus D_n,$$

et une permutation σ telle que $C_i \simeq D_{\sigma(i)}$ pour chaque i.

Démonstration. Par le lemme 6.1 nous trouvons D_1, contenu dans A ou dans B, tel que $D_1 \oplus C_2 \oplus \cdots \oplus C_n = C_1 \oplus C_2 \oplus \cdots \oplus C_n$. Nous pouvons supposer que $D_1 \subseteq B$. Alors $B = B' \oplus D_1$ et $A \oplus B' \simeq C_2 \oplus \cdots \oplus C_n$, et nous terminons par récurrence sur n. □

Le théorème 6.2 implique qu'un facteur direct d'un module libre de rang fini sur un anneau local est un module libre de rang fini. Le théorème d'Azumaya qui suit montre qu'un module dont l'anneau d'endomorphismes est local a la propriété de **simplification** dans une somme directe.

Théorème 6.3. *Étant donné un isomorphisme de modules $A \oplus C \simeq B \oplus C$, si l'anneau d'endomorphismes de C est local, alors $A \simeq B$.*

Démonstration. Nous pouvons supposer que $A \oplus C' = B \oplus C = E$ avec $C' \simeq C$. D'après le lemme 6.1, nous pouvons supposer que $C' \subseteq B$ ou que $C' \subseteq C$. Dans le deuxième cas C' est un facteur direct de C, donc $C' = C$ ou $C' = 0$, et par suite $A \simeq E/C \simeq B$. Si $C' \subseteq B$, nous écrivons $B = B' \oplus C'$, donc $A \oplus C' = B' \oplus C' \oplus C$, et $A \simeq E/C' \simeq B' \oplus C \simeq B$. □

Le théorème 6.3 nous montre que si R est un anneau local et si $R^m \simeq R^n$, alors $m = n$ ou R est trivial. Rappelons que ceci est également vrai pour les anneaux commutatifs (théorème II.7.5), mais pas pour les anneaux en général (exercice II.4.3).

On définit une **inégalité** sur un anneau local en posant $r_1 \neq r_2$ si $r_1 - r_2$ est inversible. En utilisant cette inégalité non standard nous pouvons développer de manière naturelle une grande partie de la théorie des espaces vectoriels de dimension finie sur les corps de Heyting dans la situation plus générale des modules libres de rang fini sur un anneau local. Cette inégalité est symétrique et invariante par translation pour n'importe quel anneau et, pour un anneau local, elle est aussi cotransitive. Si elle est consistante, l'anneau est non trivial. L'exercice II.1.5 montre que l'addition et la soustraction sont fortement extensionnelles. Pour démontrer que la multiplication est fortement extensionnelle, nous avons besoin du lemme suivant.

Lemme 6.4. *Si a et b sont des éléments d'un anneau local R, et si ab est inversible, alors a et b sont inversibles.*

Démonstration. Nous pouvons supposer que $ab = 1$. Il suffit de démontrer que $-a$ ou b est inversible, et nous pouvons donc supposer que $1 + a$ et $1 - b$ sont inversibles. Alors $a - b = (1 + a)(1 - b)$ est inversible, et donc a ou $-b$ est inversible. □

Si a, b, c et d sont des éléments d'un anneau local R, et si $ab \neq cd$, alors $ab \neq ad$ ou $ad \neq cd$ par cotransitivité ; donc $b \neq d$ ou $a \neq c$ d'après le lemme 6.4.

Ainsi la multiplication est fortement extensionnelle. Par suite, si $f(X_1, \ldots, X_n)$ est une fonction construite à partir d'éléments de R et des variables $X_1, \ldots, X_n$ en utilisant seulement la multiplication et l'addition, et si $f(0, \ldots, 0) = 0$, alors $f(r_1, \ldots, r_n) \neq 0$ implique que $r_i \neq 0$ pour un i.

Une caractérisation standard des anneaux locaux en mathématiques classiques est que les éléments non inversibles forment un idéal. L'exercice 4 explique pourquoi nous n'utilisons pas cette caractérisation, mais les anneaux locaux non triviaux ont effectivement cette propriété.

Théorème 6.5. *Soit R un anneau local. Alors l'ensemble*

$$M = \{\, r \in R : \text{ si } r \text{ est inversible, alors } R \text{ est trivial} \,\}$$

est le radical de Jacobson de R.

Démonstration. Soit Rr un idéal à gauche quasi-régulier. Si r est inversible, alors $1 \in Rr$, donc 0 est inversible, et par suite R est trivial ; ainsi $r \in M$. Inversement, supposons que $m \in M$ et $r \in R$. L'un des deux éléments rm ou $1 - rm$ est inversible. Si rm est inversible alors m est inversible d'après le lemme 6.4, donc R est trivial et $1 - rm$ est également inversible. Par suite Rm est un idéal à gauche quasi-régulier. □

Soit M un module sur un anneau local R. L'**inégalité forte** sur M est définie en posant $x \neq y$ s'il existe une application linéaire $f : M \to R$ telle que $f(x) \neq f(y)$. L'inégalité forte sur M est la plus petite inégalité qui rend les applications linéaires de M vers R fortement extensionnelles. Sur le module R^n, l'inégalité forte est celle qu'il est naturel d'imposer ; elle peut être décrite en termes des coordonnées comme suit.

Théorème 6.6. *Soient R un anneau local et x, y des éléments de R^n. Alors $u \neq v$ pour l'inégalité forte sur R^n si, et seulement si, $x - y$ a une coordonnée inversible dans R.*

Démonstration. Soit $e_1, \ldots, e_n$ la base naturelle de R^n et soit $x - y = \sum_i a_i e_i$. Si a_i est inversible, alors $f(x) \neq f(y)$ où f est la projection de R^n sur son i-ième facteur. Inversement, supposons que $f(x) \neq f(y)$ pour une application R-linéaire $f : R^n \to R$. Alors $\sum_i \varphi(a_i e_i) \neq 0$, et donc $a_i \varphi(e_i) = \varphi(a_i e_i) \neq 0$ pour un i. Par suite $a_i \neq 0$. □

Nous disons que les éléments $u_1, \ldots, u_m$ de R^n sont **linéairement indépendants** sur l'anneau local R si $\sum_{i=1}^m r_i u_i \neq 0$ dès que l'un des $r_i \in R$ est $\neq 0$. Clairement toute base est linéairement indépendante. Nous allons montrer dans le théorème 6.10 qu'inversement, si $u_1, \ldots, u_m$ engendrent R^n et sont linéairement indépendants, alors ils forment une base. Nous montrerons aussi que tout ensemble linéairement indépendant de R^n peut être étendu en une base de R^n.

Le lemme 6.4, selon lequel $ab = 1$ implique que a et b sont inversibles, s'étend des anneaux locaux aux matrices sur les anneaux locaux. En outre les matrices inversibles sont toutes des produits de matrices élémentaires.

Théorème 6.7. *Soit A une matrice $n \times n$ sur un anneau local R. Si A est inversible à droite ou à gauche, alors A est un produit de matrices élémentaires, et donc A a un inverse (à droite et à gauche).*

Démonstration. En considérant les matrices transposées, il suffit de traiter le cas où la matrice A possède une inverse à gauche B. Alors $\sum_{j=1}^{n} b_{1j}a_{j1} = 1$, et il existe un j tel que $b_{1j}a_{j1}$ est inversible. Le lemme 6.4 implique alors que a_{j1} est inversible. Donc nous pouvons trouver un produit E de matrices élémentaires tel que la première colonne de EA est nulle sauf pour un 1 en première position. Comme $(BE^{-1})(EA) = I$, et comme E a un inverse, nous pouvons supposer que $a_{11} = 1$ et $a_{i1} = 0$ pour $i \neq 1$; notons que cela implique que $b_{11} = 1$ et $b_{i1} = 0$ pour $i \neq 1$. Notons M^* la matrice M privée de sa première ligne et de sa première colonne, alors $B^*A^* = I^*$, donc par récurrence sur n nous trouvons un produit E de matrices élémentaires tel que EA est la matrice identité sauf pour $a_{12}, \ldots, a_{1n}$. Et ses entrées restantes sont facilement annulées au moyen de manipulations élémentaires. □

Une conséquence du théorème précédent est que lorsque A est une matrice inversible, $C \neq 0$ si, et seulement si, $CA \neq 0$, car l'équivalence est claire pour une matrice élémentaire. Le même résultat vaut pour la multiplication à droite.

Les deux lemmes suivants concernent l'indépendance linéaire d'éléments dans des modules de type fini.

Lemme 6.8. *Soit R un anneau local et M une matrice $m \times n$ sur R. Soit A une matrice inversible $m \times m$, et soit B une matrice inversible $n \times n$. Alors les lignes de M sont linéairement indépendantes si, et seulement si, les lignes de AMB sont linéairement indépendantes.*

Démonstration. Comme A et B sont inversibles, il suffit de montrer que si les lignes de M sont linéairement indépendantes, alors il en va de même pour les lignes de AMB. Les lignes de M sont linéairement indépendantes si, et seulement si, pour toute matrice X de format $1 \times m$ avec $X \neq 0$, on a $XM \neq 0$. Si $X \neq 0$, alors $XA \neq 0$ et nous avons $XAM \neq 0$ parce que les lignes de M sont linéairement indépendantes, et donc $XAMB \neq 0$. □

Lemme 6.9. *Soit R un anneau local et M une matrice $m \times n$ sur R. Si les lignes de M sont linéairement indépendantes, alors ou bien R est trivial, ou bien il existe une matrice carrée inversible A et une matrice de permutation B telles que les m premières colonnes de AMB forment la matrice identité de format $m \times m$.*

Démonstration. La matrice A est construite par des manipulations élémentaires de lignes (en partant de la matrice identité) et la matrice B en permutant les colonnes (de la matrice identité). Comme la première ligne de M est non nulle, nous pouvons en permutant les colonnes et en multipliant par une unité obtenir un 1 en position nord-ouest. Nous pouvons alors annuler les autres coefficients de la première colonne par des manipulations élémentaires de lignes. Les lignes de la matrice qui en résulte sont linéairement indépendantes en vertu du lemme 6.8. Si $m > n = 1$, alors R est trivial ; sinon par récurrence sur le nombre de lignes, ou bien R est trivial ou bien nous pouvons exécuter des manipulations élémentaires sur les lignes 2 à m, et permuter les colonnes entre 2 et n, de manière à obtenir la matrice identité de format $(m-1)\times(m-1)$ sur les lignes 2 à m et les colonnes 2 à m. Enfin par des manipulations élémentaires de lignes nous transformons les m premières colonnes en la matrice identité. □

Nous pouvons maintenant démontrer que tout ensemble linéairement indépendant dans un module libre de rang fini sur un anneau local peut être étendu en une base.

Théorème 6.10. *Soit R un anneau local et soient $v_1,\dots,v_m$ des éléments d'un R-module libre de rang fini F. Soit $e_1,\dots,e_n$ une base de F.*

- *Si $m < n$, il existe j tel que $v_1,\dots,v_m,e_j$ sont linéairement indépendants,*
- *si $m = n$, $v_1,\dots,v_m$ est une base de F,*
- *si $m > n$, R est trivial.*

Démonstration. Nous pouvons supposer que F est l'ensemble des matrices de format $1\times n$ sur R, que v_i est la i-ième ligne d'une matrice M de format $m\times n$, et que e_j est la matrice de format $1\times n$ avec un 1 dans la j-ième colonne et 0 ailleurs.

Si $m \leqslant n$, alors par le lemme 6.9 nous pouvons trouver une matrice carrée inversible A et une matrice de permutation B telles que les m premières colonnes de AMB forment la matrice identité de format $m\times m$. Si $m = n$, alors M est inversible, donc ses lignes sont une base de F. Si $m < n$, alors, comme B est une matrice de permutation, il existe j tel que $e_jB = e_{m+1}$. Les lignes de AMB, avec la ligne e_{m+1}, sont linéairement indépendantes. Donc les lignes de AM, avec la ligne e_j, sont linéairement indépendantes. Comme A est inversible, les lignes de M, avec la ligne e_j, sont linéairement indépendantes d'après le lemme 6.8.

Si $m > n$, alors $v_1,\dots,v_n$ forment une base de F, donc v_{n+1} peut être écrit comme une combinaison linéaire de $v_1,\dots,v_n$. Mais $v_1,\dots,v_{n+1}$ sont linéairement indépendants, donc $0 \neq 0$ dans R, et R est trivial. □

Exercices

1. Montrer que si $C_1 \oplus \cdots \oplus C_n \simeq D_1 \oplus \cdots \oplus D_n$ et si les anneaux d'endomorphismes des modules C_i et D_i sont locaux, alors il existe une permutation σ de $\{1, \ldots, n\}$ telle que $C_i \simeq D_{\sigma(i)}$ pour chaque i.
2. Utiliser les théorèmes d'Azumaya pour montrer que si A et B sont des matrices carrées sur un anneau local avec $AB = I$, alors A et B sont inversibles.
3. Montrer que l'inégalité définie sur un anneau local est symétrique et cotransitive.
4. Montrer que les propriétés suivantes sont équivalentes.
   (i) Le principe de Markov.
   (ii) Pour tout anneau commutatif dénombrable discret, si les éléments non inversibles de R forment un idéal, alors l'anneau est local.

   Idée : pour montrer que (ii) implique (i), considérer une suite binaire a, le monoïde

   $$S = \{\, m \in \mathbb{Z} : m = 1, \text{ ou } m \neq 0 \text{ et } a_n = 1 \text{ pour un } n \,\}$$

   et l'anneau $R = S^{-1}\mathbb{Z}$.
5. Donner un exemple d'éléments a et b dans un anneau avec $ab = 1$, alors que ni a ni b n'est inversible.
6. Montrer que si R est local, alors le module R^n est hopfien (exercice 1.9).
7. Soit R un anneau local et M un R-module muni d'une inégalité forte. Montrer que l'addition et la multiplication scalaire dans M sont fortement extensionnelles.
8. Généraliser le théorème II.6.6 au cas d'anneaux locaux $k \subseteq K$, en supposant que le K-module V est donné avec une inégalité telle que la multiplication scalaire soit fortement extensionnelle et que chacune des trois occurrences de l'expression « de dimension finie » implique un isomorphisme avec R^n préservant l'inégalité.
9. Soit k le corps des entiers modulo 2. Montrer que $K = k[X]/(X^2)$ est un anneau local isomorphe à k^2, mais que l'inégalité sur K en tant qu'anneau local diffère de l'inégalité sur K en tant que k-module. Pour l'anneau $V = k[X, Y]/(X, Y)^2$ montrer que l'exercice 8 est en échec parce que V n'est pas un module libre sur K.
10. Montrer que si R est un anneau local et si $u_1, \ldots, u_m$ est une base de R^n, alors $m = n$ ou $R = 0$.
11. Montrer que si R est un anneau local, si $e_1, \ldots, e_n$ est une base d'un R-module libre F, et si $v_1, \ldots, v_m$ engendrent F, alors il existe un i tel que $v_i, e_2, \ldots, e_n$ est une base de F.

7 Anneaux commutatifs locaux

Si R est un anneau commutatif local, nous définissons $R(X)$, en analogie avec le corps des fractions rationnelles sur un corps, en inversant tous les éléments de $R[X]$ qui ont un coefficient inversible.

Lemme 7.1. *Soient R un anneau commutatif local et X une indéterminée. Soit S l'ensemble des polynômes dans $R[X]$ qui ont un coefficient inversible. Alors :*

(i) *S est un monoïde multiplicatif,*

(ii) *si $fg = 0$ pour $f \in S$ et $g \in R[X]$, alors $g = 0$,*

(iii) *si $fg \in S$, alors $f \in S$, et si $f + g \in S$, alors $f \in S$ ou $g \in S$.*

Démonstration. Soient $f = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_0$ et $g = b_m X^m + b_{m-1}X^{m-1} + \cdots + b_0$. Soit $fg = c_{m+n}X^{m+n} + \cdots + c_0$. Supposons que a_i et b_j sont inversibles. Alors $a_i b_j$ est inversible, donc c_{i+j} ou $c_{i+j} - a_i b_j$ est inversible. Dans le premier cas nous avons montré (i) ; dans le second cas, l'élément $\sum a_p b_q$, avec la somme portant sur les indices p, q tels que $p + q = i + j$ et $p \neq i$, est inversible. Comme R est local, il existe un $p < i$ ou un $q < j$ tel que $a_p b_q$ est inversible, donc $a_p b_j$ ou $a_i b_q$ est inversible, et nous avons démontré (i) par récurrence sur $i + j$.

Pour démontrer (ii) supposons que a_i est inversible et que $fg = 0$. Nous pouvons supposer que $a_i = 1$. Alors la matrice $(m+1) \times (m+1)$

$$\begin{pmatrix} 1 & a_{i-1} & a_{i-2} & \cdots & a_{i-m} \\ a_{i+1} & 1 & a_{i-1} & \cdots & a_{i-m+1} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{i+m} & a_{i+m-1} & a_{i+m-2} & \cdots & 1 \end{pmatrix}$$

avec $a_j = 0$ si $j < 0$ ou $j > n$, annule le vecteur $(b_0, \ldots, b_m)^t$. Notons d le déterminant de la matrice, nous avons $db_j = 0$ pour tous les j (lemme II.7.6). Si d est inversible, nous avons terminé. Si $d-1$ est inversible, alors a_j est inversible pour un $j < i$ (en considérant la formule de définition du déterminant), et nous terminons par récurrence sur i.

Pour démontrer (iii) supposons d'abord que $fg \in S$; dans ce cas c_k est inversible pour un k. Comme R est local, $a_i b_j$ est inversible pour un couple (i, j) tel que $i + j = k$. Ainsi a_i est inversible, et $f \in S$. Supposons ensuite que $f + g \in S$. Alors $a_i + b_i$ est inversible pour un i, et donc a_i ou b_i est inversible. □

Théorème 7.2. *Soient R un anneau commutatif local et X une indéterminée. Soit $R(X)$ l'anneau $S^{-1}R[X]$ où S est l'ensemble des éléments de $R[X]$ qui ont un coefficient inversible. Alors $R(X)$ est un anneau local contenant $R[X]$. Si R est un corps de Heyting, il en va de même pour $R(X)$.*

Démonstration. Si $a/s + a'/s' = (as' + a's)/ss'$ est inversible dans $R(X)$, alors $t(as' + a's) \in S$ pour un $t \in R[X]$, et donc a ou a' est un élément de S d'après le lemme 7.1(iii) ; par suite $R(X)$ est local. Le lemme 7.1(ii) nous dit que l'application R-linéaire naturelle de $R[X]$ vers $R(X)$ est injective.

Supposons que l'inégalité sur R est étroite. S'il est impossible que a/s soit inversible dans $R(X)$, a ne peut pas être un élément de S, donc aucun coefficient de a ne peut être inversible, ce qui montre que tous les coefficients de a sont nuls. Donc l'inégalité sur $R(X)$ est étroite.

Si l'inégalité sur R est consistante, i.e. 1 ne peut être égal à 0 dans R, comme l'application R-linéaire naturelle de R vers $R(X)$ (*via* $R[X]$) est injective, l'inégalité sur $R(X)$ est consistante. □

Théorème 7.3. *Soit R un anneau commutatif local et e un endomorphisme idempotent d'un R-module libre de rang fini F. Alors le noyau de e est un R-module libre de rang fini.*

Démonstration. L'anneau des endomorphismes du R-module R est isomorphe à l'anneau R, donc le théorème d'Azumaya 6.2 s'applique. □

Si e est un idempotent dans un anneau local, alors e est inversible, auquel cas $e = 1$, ou $1 - e$ est inversible, auquel cas $e = 0$. Nous appelons **anneau impotent** un anneau commutatif réduit dans lequel tout idempotent est égal à 0 ou à 1. Un anneau commutatif local réduit est impotent.

Théorème 7.4. *Soient R un anneau impotent et g un diviseur d'un polynôme unitaire de $R[X]$. Il existe une unité λ de R telle que $\lambda^{-1}g$ est unitaire.*

Démonstration. Soit $gh = X^m + c_{m-1}X^{m-1} + \cdots + c_0$, avec

$$g = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0 \quad \text{et} \quad h = b_nX^n + b_{n-1}X^{n-1} + \cdots + b_0.$$

Nous montrons d'abord que $a_ib_j = 0$ si $i + j > m$. Nous procédons par récurrence descendante sur $i + j$ en notant que a_ib_j est trivialement nul si $i+j > 2n$. Supposons que pour un $k > m$, $a_ib_j = 0$ chaque fois que $i+j \geqslant k+1$. Le coefficient de degré k de gh est

$$a_0b_k + a_1b_{k-1} + \cdots + a_kb_0 = 0.$$

En multipliant cette égalité par a_ib_{k-i} nous obtenons $(a_ib_{k-i})^2 = 0$, et donc $a_ib_{k-i} = 0$ puisque R est réduit. Cela complète la récurrence.

Maintenant considérons l'égalité

$$a_0b_m + a_1b_{m-1} + \cdots + a_mb_0 = 1.$$

En multipliant par a_ib_{m-i} nous voyons que a_ib_{m-i} est idempotent, et donc égal à 0 ou 1 parce que R est impotent. S'ils sont tous nuls, R est trivial et

le théorème est trivialement vrai. Sinon, il existe des indices i et j tels que $i+j=m$ et $a_ib_j=1$. Si $k>i$, alors $a_kb_j=0$, donc $a_k=0$. Ainsi nous pouvons prendre $\lambda=a_i$. □

Corolaire 7.5. *Si g et h sont des polynômes à coefficients dans un anneau impotent et si $gh=X^d$, il existe une unité λ et un entier naturel $r\leqslant d$ tels que $g=\lambda X^r$.*

Démonstration. D'après le théorème 7.4, quitte à multiplier g et h par des unités, nous pouvons les supposer unitaires, disons de degrés r et $s=d-r$. Posons $g_1=X^rg(1/X)$ et $h_1=X^sh(1/X)$. On a $g_1h_1=1$, donc le théorème 7.4 implique que g_1 et h_1 sont de degrés $\leqslant 0$. Donc $g_1=1$, puis $g=1$. □

Lemme 7.6. *Soit α un endomorphisme d'un module libre de rang fini sur un anneau impotent. Si α est nilpotent, le polynôme caractéristique de α est égal à une puissance de X.*

Démonstration. Supposons que $\alpha^m=0$. Soit A une matrice $n\times n$ pour α, et soit I la matrice identité de format $n\times n$. Alors

$$X^m\mathrm{I}=(X\mathrm{I}-A)(X^{m-1}\mathrm{I}+X^{m-2}A+\cdots+XA^{m-2}+A^{m-1}).$$

En prenant les déterminants des deux membres nous obtenons

$$X^{mn}=f(X)g(X)$$

où f est le polynôme caractéristique de α. Alors f est égal à une puissance de X d'après le corolaire 7.5. □

Théorème 7.7. *Soit α un endomorphisme d'un module libre de rang fini V sur un anneau commutatif local réduit. Soit $f(X)$ son polynôme caractéristique, et supposons que $f(X)=(X-\lambda)^ng(X)$ où $g(\lambda)$ est une unité. Alors $V=H\oplus K$ où H est un module libre de rang n, $\alpha-\lambda$ est un automorphisme sur K, et $(\alpha-\lambda)^nH=0$.*

Démonstration. Le théorème du reste montre que les polynômes $X-\lambda$ et $g(X)$ sont étrangers, donc $(X-\lambda)^n$ et $g(X)$ sont étrangers, et par suite il existe des polynômes $s(X)$ et $t(X)$ tels que

$$s(X)(X-\lambda)^n+t(X)g(X)=1.$$

Soit $e=s(\alpha)(\alpha-\lambda)^n$. Alors $e^2=e(1-t(\alpha)g(\alpha))=e$ parce que $f(\alpha)=0$. Soient H le noyau de e et K le noyau de $1-e$; comme $\alpha e=e\alpha$, on a $\alpha H\subseteq H$ et $\alpha K\subseteq K$. Comme $e=s(\alpha)(\alpha-\lambda)^n=(\alpha-\lambda)s(\alpha)(\alpha-\lambda)^{n-1}$ est l'application identique sur K et $\alpha K\subseteq K$, nous obtenons que $\alpha-\lambda$ est un automorphisme de K.

Si le module libre de rang fini K est nul, alors $e = 0$ et $H = V$, donc $g(\alpha)$ est injectif parce que $t(\alpha)g(\alpha) = 1$. Dans ce cas $(\alpha - \lambda)^n = 0$ parce que $0 = f(\alpha) = g(\alpha)(\alpha - \lambda)^n$. D'après le lemme 7.6, nous savons que $f(X)$ est une puissance de $X - \lambda$, donc $g = 1$ et le théorème est vérifié.

Si le rang de K est > 0, nous pouvons écrire $f = f_H f_K$, où f_H et f_K sont les polynômes caractéristiques de α restreint à H et K respectivement. Comme $f_K(\lambda)$ est le déterminant de $\alpha - \lambda$ agissant sur K, nous obtenons que $f_K(\lambda)$ est une unité. Ainsi $f_H = (X - \lambda)^n g^*(X)$ où $g^*(\lambda)$ est une unité. Par récurrence sur la dimension de V, le module H est libre de rang n et $(\alpha - \lambda)^n H = 0$. □

Exercices

1. Montrer que si a, b et c sont des polynômes sur un corps de Heyting, et si $\deg a \leqslant \deg b$, alors $\deg ac \leqslant \deg bc$.
2. *Unités de $R[X]$.* Soit R un anneau commutatif. Montrer que si le terme constant de g est inversible et si tous les autres coefficients de g sont nilpotents, alors g est une unité de $R[X]$. Inversement, si g est une unité de $R[X]$, montrer que le terme constant de g est inversible dans R, et que tous les autres coefficients de g sont nilpotents. (Considérer $S = \{1, a, a^2, \ldots\}$ où a est le coefficient de plus haut degré de g que l'on ne sait pas être nilpotent, et montrer que $S^{-1}R$ est trivial.)
3. Montrer que le théorème 7.4 caractérise les anneaux impotents (il suffit de considérer les polynômes de la forme $aX + b$).
4. Donner un exemple d'un anneau commutatif local où le lemme 7.6 est en défaut.
5. Donner un exemple brouwerien d'un endomorphisme α de $\mathbb{R}^2$, où $\mathbb{R}$ est le corps des nombres réels, tel que le polynôme caractéristique f de α annule λ, mais ne peut pas être écrit sous la forme donnée dans le théorème 7.7.
6. *La forme canonique de Jordan, I.* Soit α un endomorphisme d'un module libre de rang fini V sur un anneau commutatif local réduit R. On suppose que le polynôme caractéristique de α est un produit de polynômes de la forme $(X - \lambda)^m$ avec des λ distincts (pour l'inégalité sur R). Montrer que V est une somme directe de sous-modules V_λ tels que $\alpha V_\lambda \subseteq V_\lambda$, avec le polynôme caractéristique de la restriction de α à V_λ égal à $(X - \lambda)^m$.
7. *La forme canonique de Jordan, II.* Soit R un anneau commutatif local et soit α un endomorphisme de R^n tel que $\alpha^m = 0$ et $\operatorname{im} \alpha^i$ est de dimension finie pour $i = 1, \ldots, m$.
   (i) Montrer que $H_i = (\ker \alpha) \cap (\operatorname{im} \alpha^i)$ est de dimension finie, et par suite est un facteur direct de R^n.

(ii) Montrer que $\ker \alpha = V_0 \oplus \cdots \oplus V_{m-1}$ où $H_i = V_i \oplus H_{i+1}$

(iii) Considérer une base e_{ij} pour chaque V_i, donc pour $\ker \alpha$. Poser $e_{ij} = \alpha^i x_{ij}$ et montrer que $\{\, \alpha^k x_{ij} : k \leqslant i \,\}$ est une base de R^n.

8. Donner un exemple brouwerien d'un endomorphisme nilpotent α de $\mathbb{R}^2$ tel que $\operatorname{im} \alpha$ n'est pas de dimension finie.

8 Notes

Notre théorie des anneaux et modules noethériens fait un usage extensif de l'axiome du choix dépendant. Élaborer une théorie qui n'utilise pas l'axiome du choix dépendant semble trop ambitieux pour le but de ce livre, et il semble probable que la théorie classique serait, au mieux, significativement déformée.

En mathématiques classiques, la condition de chaine ascendante sur les sous-modules est équivalente à la condition de chaine ascendante sur les sous-modules de type fini, et la seconde condition admet des exemples constructifs intéressants (contrairement à la première). D'autre part, la condition de chaine descendante ne semble pas admettre elle-même un traitement constructif. Un cas d'école serait de formuler une condition de chaine descendante qui serait satisfaite par le groupe abélien $\mathbb{Z}(p^\infty)$, la composante p-primaire de $\mathbb{Q}/\mathbb{Z}$.

La définition d'un module *cohérent* provient de [Bourbaki 1961, §2, exercice 11] sous le nom de module *pseudo-cohérent*, le terme *cohérent* étant réservé pour les modules pseudo-cohérents de type fini.

Le théorème classique selon lequel un anneau est cohérent à droite si, et seulement si, les produits de modules à gauche plats sont plats nécessite l'axiome du choix sous sa forme forte. L'exercice 5.3 donne la version dénombrable de ce théorème.

La démonstration que les modules de présentation finie plats sont projectifs dans l'exercice 5.4 provient de [Bourbaki 1961, §2, Exercice 23(a)]. La conséquence qu'on en tire pour décider si un module de présentation finie est projectif se trouve dans [Baumslag, Cannonito & Miller 1981, Lemma 5.1], où l'hypothèse de commutativité n'est pas faite mais semble être utilisée ; le problème est que $I_x K$ n'est pas nécessairement un sous-module. L'article de Baumslag est écrit dans le contexte de la théorie des fonctions récursives et il utilise le principe de Markov. Pour la relation entre l'algèbre constructive et l'algèbre récursive, voir [Bridges-Richman 1987].

Dans l'article [Julian, Mines et Richman, 1978], un corps est défini comme un anneau commutatif local réduit dans lequel 0 ne peut pas être égal à 1.

IV. Divisibilité dans les anneaux intègres

Sommaire

1 Divisibilité dans les monoïdes réguliers

Un monoïde commutatif est appelé un **monoïde régulier** [1] si $ab = ac$ implique $b = c$. Si R est un anneau intègre discret, l'ensemble des éléments non nuls R forme un monoïde régulier discret. Cet exemple motive notre étude des monoïdes réguliers généraux. La terminologie introduite pour les monoïdes réguliers se transfère aux anneaux intègres discrets en considérant le monoïde des éléments non nuls.

Si a et b sont des éléments d'un monoïde régulier M, alors nous disons que a **divise** b et nous écrivons $a|b$ s'il existe un $c \in M$ tel que $b = ca$. Les diviseurs de 1 sont les unités de M et forment un sous-monoïde U de M qui est un groupe. Si U est détachable, nous disons que M est un monoïde **avec unités détachables** [2]. Deux éléments a et b de M sont dits **associés**, ce que l'on écrit $a \sim b$, si chacun divise l'autre. Comme M est régulier, on obtient que $a \sim b$ si, et seulement si, il existe une unité u telle que $b = ua$. À partir de M, on construit le monoïde M/U en déclarant que deux éléments sont égaux s'ils sont associés. Nous travaillons dans M/U quand nous nous intéressons aux éléments

1. **NdT.** Cancellation monoid.
2. **NdT.** M has recognizable units.

« à une unité très » : en particulier, la relation $a|b$ peut être vue dans M/U où elle est une relation d'ordre.

Nous disons que d est un **plus grand commun diviseur**, ou un **pgcd**, de a et b, si $d|a$ et $d|b$ et si pour tout c tel que $c|a$ et $c|b$, on a $c|d$. Remarquez que les pgcds sont uniques dans M/U, et que le pgcd de a et b est la borne inférieure de a et b dans l'ensemble ordonné M/U. Si d est un pgcd de a et b, alors nous le notons $\mathrm{pgcd}(a,b)$, vu comme un élément de M/U.

Deux éléments a et b sont dits **premiers entre eux** si $\mathrm{pgcd}(a,b) = 1$. Un **monoïde à pgcd** [1] est un monoïde régulier dans lequel toute paire d'éléments possède un plus grand commun diviseur. Un **anneau intègre à pgcd** [2] est un anneau intègre discret dont les éléments non nuls forment un monoïde à pgcd.

Théorème 1.1. *Soient a, b et c des éléments d'un monoïde à pgcd M. Alors :*

(i) $\mathrm{pgcd}(\mathrm{pgcd}(a,b),c) = \mathrm{pgcd}(a,\mathrm{pgcd}(b,c))$,

(ii) $c \cdot \mathrm{pgcd}(a,b) = \mathrm{pgcd}(ca,cb)$,

(iii) *si* $x = \mathrm{pgcd}(a,b)$, *alors* $\mathrm{pgcd}(a,bc) = \mathrm{pgcd}(a,xc)$,

(iv) *si* $a|bc$ *et* $\mathrm{pgcd}(a,b) = 1$, *alors* $a|c$ [3].

Démonstration. Le point (i) est facilement vérifié.

Pour le point (ii), posons $d = \mathrm{pgcd}(a,b)$ et $e = \mathrm{pgcd}(ca,cb)$. Alors $cd|e$, donc $e = cdx$. Il reste à voir que x est une unité. On a $ca = ea' = cdxa'$, donc $a = dxa'$. On obtient de la même manière $b = dxb'$. Ainsi $dx|d$, et x est une unité.

Pour le point (iii) nous avons

$$\begin{aligned}\mathrm{pgcd}(a,bc) &= \mathrm{pgcd}(\mathrm{pgcd}(a,ac),bc) = \mathrm{pgcd}(a,\mathrm{pgcd}(ac,bc))\\ &= \mathrm{pgcd}(a,c\cdot\mathrm{pgcd}(a,b)) = \mathrm{pgcd}(a,xc).\end{aligned}$$

Enfin le point (iv) est une conséquence immédiate du point (iii) en prenant $x = 1$. □

Un élément non inversible p d'un monoïde régulier est dit **irréductible** si chaque fois que $p = ab$, alors a ou b est inversible. Nous disons qu'un élément non inversible p est **premier** si chaque fois que $p|ab$, alors $p|a$ ou $p|b$. Il est clair que tout élément premier est irréductible.

Lemme 1.2. *Dans un monoïde à pgcd tout élément irréductible est premier* [4].

1. **NdT.** GCD-monoid.
2. **NdT.** GCD-domain.
3. **NdT.** Cela est souvent appelé « lemme de Gauss » dans la littérature française.
4. **NdT.** Cela est souvent appelé « lemme d'Euclide » dans la littérature française.

Démonstration. Soit p un élément irréductible et supposons que $p|ab$. Nous devons montrer que $p|a$ ou $p|b$. Soit $d = \mathrm{pgcd}(p, a)$, et donc $p = cd$ pour un certain c. Comme p est irréductible, c ou d est inversible. Si c est inversible, alors p divise d, donc p divise a. Si d est inversible, alors $\mathrm{pgcd}(p, a) = 1$, donc p divise b d'après le théorème 1.1(iv). □

Lemme 1.3. *Un monoïde à pgcd M a ses unités détachables si, et seulement si, la divisibilité est décidable dans M.*

Démonstration. Si la divisibilité est décidable dans M, alors nous pouvons décider si $u|1$, donc les unités sont détachables. Inversement, supposons que les unités de M sont détachables. Soient a et b des éléments de M, et soit $d = \mathrm{pgcd}(a, b)$. On a un élément s tel que $a = sd$. Alors $a|b$ si, et seulement si, $a|d$ si, et seulement si, s est une unité. □

Définition 1.4. Soit M un monoïde régulier. Un élément $a \in M$ est dit **borné par l'entier naturel** n si chaque fois que $a = a_0 \cdots a_n$ avec des $a_i \in M$, alors l'un des a_i est inversible. Un élément de M est **borné** s'il est borné par un entier naturel ; le monoïde M est **à décomposition bornée** [1] si tous ses éléments sont bornés. Un anneau intègre discret est **à factorisation bornée** [2] si ses éléments non nuls forment un monoïde à décomposition bornée.

Les unités de M sont exactement les éléments qui sont bornés par 0. Un élément de M est irréductible si, et seulement si, il est borné par 1 mais pas par 0.

Un **idéal principal** d'un monoïde commutatif M est un sous-ensemble I de M tel que $I = Ma = \{\, ma : m \in M \,\}$ pour un $a \in M$. Nous disons que le monoïde M **satisfait la condition de chaine des diviseurs** si pour chaque chaine ascendante $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ d'idéaux principaux, il y a un n tel que $I_n = I_{n+1}$. On dit qu'un anneau intègre discret satisfait la condition de chaine des diviseurs si le monoïde des éléments non nuls la satisfait.

Un monoïde régulier M est à décomposition bornée si, et seulement si, pour chaque $a \in M$ il existe un n tel que pour toute chaine $I_0 \subseteq I_1 \subseteq \cdots \subseteq I_n$ d'idéaux principaux, avec $I_0 = Ma$, il existe $j < n$ tel que $I_j = I_{j+1}$; ainsi un monoïde à décomposition bornée satisfait la condition de chaine des diviseurs. L'anneau des entiers est à factorisation bornée parce que tout entier non nul n est borné par $|n|$. L'anneau de polynômes $F[X]$ sur un corps discret F est à factorisation bornée car tout polynôme non nul f est borné par $\deg f$. Un anneau intègre à pgcd qui satisfait la condition de chaine des diviseurs est appelé un **quasi-AFU** [3], où AFU est un acronyme pour « anneau à factorisation unique (en facteurs premiers) ».

1. **NdT.** Bounded monoid.
2. **NdT.** Bounded discrete domain.
3. **NdT.** Quasi-UFD. Nous ne traduisons pas par « anneau quasi-factoriel », parce que [CCA] utilise « factoriel » en un sens plus fort que le sens usuel en français.

Exemple 1.5. Soit a une suite binaire. Soit $R = \bigcup_n \mathbb{Z}[a_n/2]$. Alors R est un exemple brouwerien d'un quasi-AFU sans unités détachables, car nous ne pouvons pas décider si 2 est inversible. Clairement, nous ne pouvons pas écrire les éléments 6 et 10 de R comme produits de facteurs irréductibles. Cependant, nous allons voir qu'étant donné un ensemble fini S d'éléments non nuls d'un quasi-AFU, nous pouvons trouver un ensemble P d'éléments deux à deux premiers entre eux tel que tout élément de S est associé à un produit d'éléments de P (théorème 1.8). □

Lemme 1.6. *Soit M un monoïde à pgcd qui satisfait la condition de chaine des diviseurs, et soient $p_1, \dots, p_m$ des éléments deux à deux premiers entre eux de M. Pour tout $a \in M$, nous pouvons construire des éléments $a_0, a_1, \dots, a_m \in M$ tels que*

(i) $a = a_0 a_1 \cdots a_m$,

(ii) *il existe un e tel que $a_j | p_j^e$ pour $j = 1, \dots, m$,*

(iii) *a_0 et p_j sont premiers entre eux pour $j = 1, \dots, m$.*

Démonstration. Pour $j = 1, \dots, m$ considérons la suite $x_n = a/\operatorname{pgcd}(a, p_j^n)$. D'après la condition de chaine des diviseurs, il existe un entier n tel que $x_n | x_{n+1}$; posons $n_j = n$ et $a_j = a/x_n = \operatorname{pgcd}(a, p_j^n) = \operatorname{pgcd}(a, p_j^{n+1})$. Comme les p_j sont deux à deux premiers entre eux, il en va de même pour les a_j. En utilisant plusieurs fois le théorème 1.1(iv) nous obtenons un élément a_0 tel que $a = a_0 a_1 \cdots a_m$. Il nous reste avoir que $\operatorname{pgcd}(a_0, p_j) = 1$ pour tout j. L'élément

$$a_j = \operatorname{pgcd}(a, p_j^{n_j+1}) = \operatorname{pgcd}(a_0 a_j, p_j p_j^{n_j})$$

est divisible par $\operatorname{pgcd}(a_0, p_j) \operatorname{pgcd}(a_j, p_j^{n_j})$ qui est égal à $\operatorname{pgcd}(a_0, p_j) a_j$, donc $\operatorname{pgcd}(a_0, p_j) = 1$. □

Lemme 1.7. *Soit M un monoïde à pgcd qui satisfait la condition de chaine des diviseurs, et soient $a, b \in M$. Alors il existe des éléments $a^+, a^-, c, b^+, b^- \in M$ tels que*

(i) *$a = a^+ c b^-$ et $b = a^- c b^+$,*

(ii) *$a^- | a^+$ et $b^- | b^+$,*

(iii) *a^+, c et b^+ sont deux à deux premiers entre eux.*

Démonstration. Soient $x = a/d$ et $y = b/d$ où $d = \operatorname{pgcd}(a, b)$. Alors x et y sont premiers entre eux, donc d'après le lemme 1.6 nous pouvons écrire $d = a^- c b^-$ avec $a^- | x^n$, $b^- | y^m$, et c étranger à la fois à x et y. Posons $a^+ = x a^-$ et $b^+ = y b^-$, donc $a = dx = a^+ c b^-$ et $b = dy = b^+ c a^-$. Comme x^{n+1}, y^{m+1} et c sont deux à deux premiers entre eux, il en va de même pour a^+, b^+ et c. □

Comme exemple de la décomposition obtenue dans le lemme 1.7, considérons le monoïde $\mathbb{N}^*$ des entiers strictement positifs. Si a et b sont des éléments de $\mathbb{N}^*$, alors a^+ et a^- sont les facteurs de a et b formés des nombres premiers qui ont un plus grand exposant dans a que dans b. De la même manière b^+ et b^- sont les facteurs de b et a formés des nombres premiers qui ont un plus grand exposant dans b que dans a, tandis que c est le facteur de a (ou de b) formé des nombres premiers qui ont le même exposant dans b et dans a. Si $a = 840 = 2^3 \cdot 3 \cdot 5 \cdot 7$ et $b = 300 = 2^2 \cdot 3 \cdot 5^2$, alors $a^+ = 56$, $a^- = 4$, $c = 3$, $b^+ = 25$, et $b^- = 5$. Notez que $\operatorname{pgcd}(a, b) = a^- c b^-$.

Théorème 1.8 (factorisation partielle)**.** *Soient $x_1, \ldots, x_k$ des éléments d'un monoïde à pgcd M qui satisfait la condition de chaine des diviseurs. Alors on peut construire une famille P d'éléments de M deux à deux premiers entre eux telle que chaque x_i est associé à un produit d'éléments de P.*

Démonstration. Voyons d'abord le cas $k = 2$. Nous construisons des suites $r_n = a_1(n) \cdots a_{m(n)}(n)$ et $s_n = b_1(n) \cdots b_{m(n)}(n)$ de la manière suivante. On pose $m(0) = 1$, $r_0 = a_1(0) = x_1$ et $s_0 = b_1(0) = x_2$. Pour simplifier la notation nous omettons la dépendance en n de m et des a_i et b_i. Supposons que nous avons construit $r_n = a_1 \cdots a_m$ et $s_n = b_1 \cdots b_m$ avec $\operatorname{pgcd}(a_i, a_j) = \operatorname{pgcd}(b_i, b_j) = \operatorname{pgcd}(a_i, b_j) = 1$ si $i \neq j$. Alors nous construisons r_{n+1} et s_{n+1} comme suit. Pour chaque i nous écrivons $a_i = a_i^+ c_i b_i^-$ et $b_i = a_i^- c_i b_i^+$ comme dans le lemme 1.7. Ensuite nous posons

$$r_{n+1} = (a_1^+/a_1^-) \cdots (a_m^+/a_m^-) b_1^- \cdots b_m^-$$

$$s_{n+1} = a_1^- \cdots a_m^- (b_1^+/b_1^-) \cdots (b_m^+/b_m^-).$$

Nous voyons facilement que, sauf pour les couples $(a_i^+/a_i^-, a_i^-)$ et $(b_i^+/b_i^-, b_i^-)$, les $2m$ facteurs de r_{n+1} et de s_{n+1} sont deux à deux premiers entre eux. Les idéaux principaux Mr_0s_0, Mr_1s_1, $Mr_2s_2, \ldots$ forment une chaine ascendante. D'après la condition de chaine des diviseurs, on a un n tel que $r_n s_n \sim r_{n+1} s_{n+1} = a_1^+ \cdots a_m^+ b_1^+ \cdots b_m^+$, donc les éléments a_i^-, c_i et b_i^- sont tous inversibles. Ainsi les éléments $a_1, \ldots, a_m, b_1, \ldots, b_m$ sont conjugués de $a_1^+, \ldots, a_m^+, b_1^+, \ldots, b_m^+$ et sont donc deux à deux étrangers. Il nous suffit maintenant de montrer que si nous pouvons écrire les éléments de la famille

$$E = \{\, a_i^-,\ (a_i^+/a_i^-),\ b_i^-,\ (b_i^+/b_i^-) : i = 1, \ldots, m \,\}$$

comme produits d'éléments deux à deux premiers entre eux, alors nous pouvons faire la même chose pour $a_1, \ldots, a_m, b_1, \ldots, b_m$. Supposons que Q est une famille finie d'éléments deux à deux premiers entre eux et que chaque élément de E est associé à un produit d'éléments de Q. Nous pouvons supposer que chaque élément de Q divise un élément de E. Alors d'après le lemme 1.7 chacun des

$a_1, \ldots, a_m, b_1, \ldots, b_m$ est associé à un produit d'éléments de $Q \cup \{c_1, \ldots, c_m\}$, et les éléments de cette dernière famille sont deux à deux premiers entre eux.

Pour $k > 2$ nous procédons par récurrence sur k. Soit $P = \{p_1, \ldots, p_m\}$ une famille d'éléments deux à deux premiers entre eux telle que chacun des éléments $x_1, \ldots, x_{k-1}$ est associé à un produit d'éléments de P. D'après le lemme 1.6, nous pouvons écrire $x_n = a_0 a_1 \cdots a_m$ où a_i divise une puissance de p_i et $\operatorname{pgcd}(a_0, p_i) = 1$ pour $i = 1, \ldots, m$. D'après le cas $k = 2$, nous pouvons construire pour chaque i une famille finie S_i d'éléments deux à deux premiers entre eux telle que a_i et p_i sont associés à des produits d'éléments de S_i, et chaque élément de S_i divise une puissance de p_i. Alors $\{a_0\} \cup S_1 \cup \cdots \cup S_m$ forme une famille d'éléments deux à deux premiers entre eux qui convient pour $x_1, \ldots, x_m$. □

Exercices

1. Montrer que l'ensemble des entiers pairs strictement positifs, avec 1, forme un monoïde (multiplicatif) régulier discret M. Trouver des éléments a et b de M qui n'ont pas de pgcd.
2. Construire des éléments a, b et c dans un monoïde régulier discret tels que $a|bc$, et $\operatorname{pgcd}(a, b) = 1$, mais a ne divise pas c.
3. Montrer que l'ensemble des entiers strictement positifs égaux à 1 modulo 3 est un monoïde (multiplicatif) régulier discret M. Est-ce que M est un monoïde à pgcd ?
4. Le **plus petit commun multiple**, noté $\operatorname{ppcm}(a, b)$, de deux éléments a et b dans un monoïde régulier M est un élément $m \in M$ multiple de a et b qui divise tout multiple commun à a et b. Montrer que si $\operatorname{ppcm}(a, b)$ existe, alors $\operatorname{pgcd}(a, b)$ existe et est égal à $ab/\operatorname{ppcm}(a, b)$. Montrer que si M est un monoïde à pgcd, alors $\operatorname{ppcm}(a, b)$ existe toujours. Construire des éléments a et b d'un monoïde régulier discret M tels que $\operatorname{pgcd}(a, b)$ existe, mais $\operatorname{ppcm}(a, b)$ n'existe pas.
5. Soit M un monoïde régulier. Définir ce que signifie le fait d'être un plus grand commun diviseur, noté $\operatorname{pgcd}(a_1, \ldots, a_n)$, ou un plus petit commun multiple, noté $\operatorname{ppcm}(a_1, \ldots, a_n)$, d'une famille finie $a_1, \ldots, a_n$ d'éléments de M. Montrer que si M est un monoïde à pgcd, alors ils existent toujours.
6. Soit R un monoïde à pgcd. Montrer que si $\operatorname{pgcd}(a, b) = 1$, alors $\operatorname{pgcd}(a, b^n c) = \operatorname{pgcd}(a, c)$ pour tout n.
7. Soit $M_1 = \{\, 2^n : n \in \mathbb{N} \,\}$, et soit $M_2 = M_1 \setminus \{2\}$. Utiliser ces monoïdes pour construire un exemple brouwerien d'un monoïde régulier discret avec unités détachables dans lequel la divisibilité n'est pas décidable (vous ne pouvez pas décider si $4|8$).

8. Soit M un sous-monoïde d'un groupe abélien multiplicatif G. Pour x et $y \in G$, nous disons que x **divise** y (relativement à M), si $yx^{-1} \in M$. Définir le pgcd dans G pour cette notion de divisibilité. Montrer que si M engendre G comme groupe et si M est un monoïde à pgcd, alors $\text{pgcd}(a, b)$ existe pour tous $a, b \in G$, et que le théorème 1.1 s'applique. Montrer que tout monoïde régulier peut être immergé comme sous-monoïde d'un groupe abélien (essentiellement) unique qu'il engendre comme groupe.
9. Soit P l'ensemble des idéaux principaux d'un anneau intègre à pgcd R, ordonné par inclusion. Montrer que P est un treillis distributif.
10. Soient a, b et c des éléments d'un monoïde régulier. Montrer que si $\text{pgcd}(ca, cb)$ existe, alors $\text{pgcd}(a, b)$ existe et $\text{pgcd}(ca, cb) = c \cdot \text{pgcd}(a, b)$.
11. Soit $R = \mathbb{Z}[Y, X_1, X_2, \ldots]/I$, où I est l'idéal engendré par $\{ X_{i+1}Y - X_i : i \geqslant 1 \}$. Montrer que R est un anneau intègre à pgcd qui ne satisfait pas la condition de chaine des diviseurs. Montrer qu'il n'existe aucune famille finie Q d'éléments deux à deux premiers entre eux telle que Y et X_1 sont associés à des produits d'éléments de Q.
12. Montrer que les éléments a^+, a^-, c, b^+, et b^- du lemme 1.7 sont uniques à des unités près.

2 Anneaux à factorisation unique et domaines de Bézout

Les questions reliées à la factorisation sont plus délicates en algèbre constructive qu'en algèbre classique parce qu'il est possible que nous ne sachions pas dire si un élément a ou n'a pas une factorisation non triviale.

Définition 2.1. Un anneau intègre discret R est appelé un **anneau à factorisation unique** [1], ou un **AFU**, si tout élément r non nul de l'anneau est inversible ou admet une factorisation essentiellement unique en produit d'éléments irréductibles, i.e. si $r = p_1 \cdots p_m$ et $r = q_1 \cdots q_n$ sont deux factorisations de r en produit d'éléments irréductibles, alors $m = n$ et on peut réindexer les facteurs de façon à ce que $p_i \sim q_i$ pour chaque i. Nous disons que R est **factoriel** si $R[X]$ est un anneau à factorisation unique.

Notez qu'un anneau à factorisation unique a ses unités détachables, i.e. la relation $u|1$ est décidable. Les corps discrets sont des exemples triviaux d'anneaux à factorisation unique. Il est bien connu que l'anneau $\mathbb{Z}$ est un anneau à factorisation unique. Notre définition un peu spéciale des anneaux *factoriels* est en accord avec notre utilisation du terme lorsqu'on l'applique aux corps discrets, et elle nous permet de montrer que $R[X]$ est factoriel

1. **NdT.** Unique factorization domain, ou UFD.

si R est factoriel. Voici un contre-exemple brouwerien pour le théorème de mathématiques classiques qui affirme que si R et un anneau à factorisation unique alors il en va de même pour $R[X]$.

Exemple 2.2. Soient a une suite binaire, $\mathbb{Q}$ le corps des nombres rationnels, $i^2 = -1$, et $k = \bigcup_n \mathbb{Q}(ia_n)$. Alors k est un corps discret, donc un anneau à factorisation unique. Cependant, nous ne pouvons pas factoriser $X^2 + 1$ en produit d'éléments irréductibles dans $k[X]$. □

Les notions de quasi-AFU, anneau à pgcd à factorisation bornée, anneau à factorisation unique, et anneau factoriel sont équivalentes en mathématiques classiques, mais l'anneau $k[X]$ de l'exemple 2.2 est un exemple brouwerien d'un anneau à pgcd à factorisation bornée qui n'est pas un anneau à factorisation unique, tandis que le corps k de l'exemple 2.2 est un exemple brouwerien d'un anneau à factorisation unique qui n'est pas un anneau factoriel. Dans le théorème 3.5 nous donnons un exemple brouwerien d'un quasi-AFU qui n'est pas un anneau à pgcd à factorisation bornée. On vérifie par contre facilement que les autres implications sont valables.

Théorème 2.3. *Soit R un anneau intègre discret. Alors*

(i) *si R est factoriel, c'est un anneau à factorisation unique,*

(ii) *si R est un anneau à factorisation unique, alors c'est un anneau à pgcd à factorisation bornée,*

(iii) *si R est un anneau à pgcd à factorisation bornée, alors c'est un quasi-AFU.* □

Un sous-monoïde multiplicatif S d'un anneau commutatif R est dit **saturé** si $xy \in S$ implique $x \in S$.

Théorème 2.4. *Soit R un anneau intègre discret et soit S un sous-monoïde multiplicatif de R qui ne contient pas* 0*. Alors*

(i) *si R est un anneau à pgcd, il en va de même pour $S^{-1}R$,*

(ii) *si S est saturé et détachable, $S^{-1}R$ a ses unités détachables.*

Démonstration. Pour démontrer (i) nous observons que $\operatorname{pgcd}(a/s, b/t) = \operatorname{pgcd}(a, b)/1$. Pour démontrer (ii) nous allons voir que a/s est inversible si, et seulement si, $a \in S$. Si a/s est inversible, alors $ab/st = 1/1$ pour un $b/t \in S^{-1}R$, donc $ab = st \in S$, et $a \in S$. Inversement, si $a \in S$, alors $a(1/a) = 1/1$. □

Théorème 2.5. *Soit R un anneau à factorisation unique et soit S un sous-monoïde multiplicatif saturé détachable de R qui ne contient pas* 0*. Alors $S^{-1}R$ est aussi un anneau à factorisation unique.*

Démonstration. Si $r/s \in S^{-1}R$, alors nous écrivons r et s comme produits d'éléments irréductibles de R. D'après le théorème 2.4, nous savons décider pour chaque facteur irréductible de r s'il est inversible dans $S^{-1}R$ ou pas. Les facteurs irréductibles de r qui ne sont pas inversibles constituent une décomposition en facteurs irréductibles de $r/s \in S^{-1}R$. □

Corolaire 2.6. *Si R est factoriel et si S est un sous-monoïde multiplicatif saturé détachable de R qui ne contient pas 0, alors $S^{-1}R$ est aussi factoriel.* □

Dans le théorème 2.5 l'hypothèse que S est saturé est essentielle. Voici un exemple brouwerien. Soit a une suite binaire fugitive. Soit $R = S^{-1}\mathbb{Z}$ avec

$$S = \{\, q : q = 1 \text{ ou } q = 2^{mn} \text{ pour des entiers } m, n \text{ tels que } a_n = 1 \,\}.$$

Alors S est sous-monoïde multiplicatif détachable de $\mathbb{Z}$ qui ne contient pas 0. Mais nous ne sommes pas capables de dire si 2 est ou n'est pas une unité dans R.

Définition 2.7. Un **anneau de Bézout intègre**, ou **domaine de Bézout** est un anneau intègre discret tel que pour tous éléments a, b on a deux éléments s, t tels que $sa + tb$ divise a et b. Un **anneau principal** [1] est un domaine de Bézout qui satisfait la condition de chaine des diviseurs.

Notez que si $sa + tb$ divise a et b, alors $sa + tb = \mathrm{pgcd}(a, b)$. Un anneau principal est **noethérien**, i.e. pour toute suite $I_1 \subseteq I_2 \subseteq \cdots$ d'idéaux de type fini, il existe un n tel que $I_n = I_{n+1}$.

Théorème 2.8. *Pour un anneau intègre discret R, les propriétés suivantes sont équivalentes.*

(i) *L'anneau R est un domaine de Bézout.*

(ii) *Tout idéal de type fini de R est principal.*

(iii) *Tout idéal de type fini de R est principal, et R est un anneau à pgcd.* □

Corolaire 2.9. *Si K est un corps discret, alors $K[X]$ est un anneau principal à factorisation bornée.*

Démonstration. Combiner le théorème 2.8 et le corolaire II.5.7. □

Un exemple d'un domaine de Bézout qui n'est pas un anneau principal est obtenu de la manière suivante. Soit k un corps discret, et soit M le monoïde additif des nombres rationnels $\geqslant 0$. Soit R l'anneau $k^{(M)}$; les éléments de R peuvent être vus comme des polynômes en X à coefficients dans k avec des exposants dans M. Si $m_1, m_2, \ldots$ est une suite strictement décroissante de nombres rationnels positifs, alors $(X^{m_1}), (X^{m_2}), \ldots$ est une suite strictement croissante d'idéaux de type fini de R. Par ailleurs, étant donné un nombre fini

1. **NdT.** Principal ideal domain, ou PID.

d'éléments de R, ils sont tous contenus dans un $k[X^m]$ pour un $m \in M$, donc R est un domaine de Bézout.

Si k est un corps discret, alors $k[X]$ est un anneau principal, mais $k[X]$ n'est pas nécessairement un anneau à factorisation unique – voir l'exemple 2.2. Un exemple brouwerien d'un anneau principal qui n'est pas un anneau à factorisation unique est construit comme suit. Soit a une suite binaire, et soit $R = \bigcup_n \mathbb{Z}[ia_n]$. Alors R est un anneau principal, mais nous ne pouvons pas factoriser l'élément 2 en produit de facteurs irréductibles. Notez que R est un anneau à pgcd à factorisation bornée. De manière générale un anneau principal est un quasi-AFU.

Dans la section 4 nous montrons que $\mathbb{Q}[X]$ est un anneau à factorisation unique, i.e. $\mathbb{Q}$ est factoriel. Dans le chapitre VI nous verrons qu'un corps discret k est factoriel si, et seulement si, il a un test pour l'existence d'un zéro, i.e. tout polynôme de $k[X]$ a ou n'a pas un zéro dans k. Cela nous donnera de nouveaux exemples de corps discrets factoriels.

Exercices

1. Soit R un anneau intègre discret. Montrer que les propriétés suivantes sont équivalentes.
   (i) R est un anneau à factorisation unique.
   (ii) Tout élément non nul de R est inversible ou est un produit d'éléments premiers.
   (iii) R est un anneau à pgcd à factorisation bornée, et tout élément non nul est inversible, ou est irréductible, ou possède un diviseur propre.
   (iv) R est un quasi-AFU, et tout élément non nul est inversible, ou est irréductible, ou possède un diviseur propre.

   Remarque : la démonstration que (iv) implique (i) utilise l'axiome du choix dépendant.
2. *Critère d'Eisenstein.* Soit R un anneau intègre discret, et soit $f = a_0 + \cdots + a_n X^n \in R[X]$ tel que tout diviseur commun des a_i est inversible. Soit $p \in R$ un élément premier tel que p ne divise pas a_n, et p^2 ne divise pas a_0, mais p divise a_i pour $i < n$. Montrer que f est irréductible dans $R[X]$.
3. Soit R un anneau principal, et soit S un sous-monoïde multiplicatif de R qui ne contient pas 0. Montrer que $S^{-1}R$ est un anneau principal.
4. Montrer qu'un domaine de Bézout est cohérent. Montrer que si un domaine de Bézout a ses unités détachables, il est fortement discret.
5. Montrer que si R est un domaine de Bézout, tout sous-module de type fini de R^n est libre de rang au plus n.

3 Anneaux de Dedekind-Hasse et anneaux euclidiens

Il est fréquent qu'un anneau intègre discret admette une fonction vers les entiers naturels qui peut être utilisée pour étudier les questions de divisibilité : par exemple la fonction valeur absolue sur $\mathbb{Z}$, la fonction degré pour les polynômes sur un corps discret, ou la norme pour les anneaux d'entiers algébriques. Si la fonction se comporte bien pour un algorithme de division, ou si elle satisfait la condition de Dedekind-Hasse, alors l'anneau intègre considéré est un anneau principal.

Définition 3.1. Soit ν une fonction depuis l'ensemble des éléments non nuls d'un anneau intègre discret R vers les entiers naturels. Alors on dit que ν est une

(i) **pseudonorme** si pour tous a, b non nuls dans R avec $b|a$, ou bien $a \sim b$, ou bien il existe un $b' \sim b$ tel que $\nu(b') < \nu(a)$.

(ii) **fonction de Dedekind-Hasse** si pour tous a, b non nuls dans R, ou bien $a|b$, ou bien il existe un r non nul dans (a, b) tel que $\nu(r) < \nu(a)$.

(iii) **fonction euclidienne**si pour tous a, b non nuls dans R, ou bien $a|b$, ou bien il existe un r non nul dans R tel que $a|(b - r)$ et $\nu(r) < \nu(a)$.

Un **anneau de Dedekind-Hasse** est un anneau intègre donné avec une fonction de Dedekind-Hasse. Un **anneau euclidien** est un anneau intègre donné avec une fonction de euclidienne.
Nous disons que la fonction ν est **multiplicative** si $\nu(ab) = \nu(a)\nu(b) > 0$ pour tous a, b non nuls dans R. Une pseudonorme multiplicative est appelée une **norme multiplicative**.

La notion de pseudonorme est purement technique. Une notion constructivement satisfaisante de norme devrait probablement se situer quelque part entre pseudonorme et norme multiplicative, peut-être à l'une de ces deux extrémités.

Théorème 3.2. *Toute fonction euclidienne est une fonction de Dedekind-Hasse. Toute fonction de Dedekind-Hasse est une pseudonorme. Si ν est une pseudonorme, tout élément non nul a est borné par $\nu(a)$. Si ν est une norme multiplicative, alors a est inversible si, et seulement si, $\nu(a) = 1$.*

Démonstration. La première affirmation est évidente. Démontrons la seconde. Soit ν une fonction de Dedekind-Hasse et soit b qui divise a. Nous procédons par récurrence sur $\nu(a)$. Ou bien $a|b$, et donc $a \sim b$, ou bien il existe un élément non nul $r \in (a, b) = (b)$ tel que $\nu(r) < \nu(a)$. Dans ce dernier cas par récurrence, ou bien $r \sim b$, et nous pouvons prendre $b' = r$, ou bien il existe $b' \sim b$ tel que $\nu(b') < \nu(r) < \nu(a)$.

Pour démontrer la troisième affirmation, supposons que ν est une pseudo-norme et soit a un élément non nul. Nous démontrons que a est borné par $n = \nu(a)$ par récurrence sur n. Supposons que $a = a_0 b$ avec $b = a_1 \cdots a_n$ si $n > 0$, et $b = 1$ si $n = 0$. Si $a|b$ alors a_0 est inversible. S'il existe $b' \sim b$ tel que $\nu(b') < \nu(a)$, alors par récurrence b', et donc aussi b, est borné par $n-1$, donc l'un des a_i est inversible.

Finalement supposons que ν est une norme multiplicative. Comme $\nu(1) = \nu(1)\nu(1) > 0$, nous avons $\nu(1) = 1$. Si a est inversible, alors $ac = 1$ pour un c, donc $\nu(a)\nu(c) = 1$ et $\nu(a) = 1$. Inversement, supposons que $\nu(a) = 1$. Comme $1|a$ et que ν est une pseudonorme, ou bien $a \sim 1$, donc a est inversible, ou bien il existe b' tel que $\nu(b') < \nu(a) = 1$, ce qui est impossible. □

La condition de Dedekind-Hasse fournit un critère pour qu'un anneau soit un anneau principal à factorisation bornée.

Théorème 3.3. *Un anneau intègre discret R qui a une fonction de Dedekind-Hasse est un anneau principal à factorisation bornée.*

Démonstration. Soit ν une fonction de Dedekind-Hasse pour l'anneau R. Comme R est à factorisation bornée d'après le théorème 3.2, il suffit de démontrer que R est un domaine de Bézout. Étant donnés des éléments non nuls a et b de R et un élément non nul c dans l'idéal (a, b), nous montrons par récurrence sur $\nu(c)$ qu'il y a un diviseur commun de a et b dans l'idéal (a, b). Comme ν est une fonction de Dedekind-Hasse, ou bien $c|a$, ou bien il existe un élément non nul r dans (c, a) tel que $\nu(r) < \nu(c)$. De la même manière, ou bien $c|b$, ou bien il existe un élément non nul r dans (c, b) tel que $\nu(r) < \nu(c)$. Ainsi, ou bien c est un diviseur commun de a et b, ou bien il existe un élément non nul r dans (a, b) tel que $\nu(r) < \nu(c)$, et nous terminons par récurrence. □

Exemple 3.4 (*une norme multiplicative qui est une fonction de Dedekind-Hasse mais qui n'est pas euclidienne*)**.** Soit $\rho_0 = (1 + \sqrt{-19})/2$ et soit $R = \mathbb{Z}[\rho_0]$. On vérifie facilement que R est un $\mathbb{Z}$-module libre de base $\{1, \rho_0\}$. La divisibilité dans R est explicite : on calcule la fraction dans $\mathbb{Q}(\sqrt{-19})$ et on l'exprime sur la base précédente. La fonction

$$N(a + b\sqrt{-19}) = (a + b\sqrt{-19})(a - b\sqrt{-19}) = a^2 + 19b^2$$

est une fonction multiplicative sur $\mathbb{Q}(\sqrt{-19})$ qui se restreint en une norme sur R. On a aussi

$$N(c + d\rho_0) = c^2 + cd + 5d^2 = (c + d\rho_0)(c - d\rho_0).$$

Pour $\rho = c + d\rho_0 \in R$, $N(c + d\rho_0) \simeq c^2 + d^2 + cd \simeq 0$ ou 1 ou 3 mod 4. Donc 2 divise ρ dans R si, et seulement si, $N(\rho)$ est pair (en fait multiple de 4), si, et seulement si, c et d sont pairs. Donc 2 est premier dans R.

Nous voulons montrer que pour tous α, β non nuls dans R, ou bien $\alpha|\beta$, ou bien il existe un r non nul dans (α, β) tel que $N(r) < N(\alpha)$. Nous supposons que α ne divise pas β et nous pouvons aussi supposer que 2 ne divise pas à la fois α et β, car le rapport β/α est seul pertinent.
Notons que $4 < \sqrt{19} < 4 + \frac{3}{8}$. Sous les hypothèses précédentes, nous allons voir comment construire un élément θ de R tel que

$$0 < N(\beta/\alpha - \theta) < 1 \text{ ou } 0 < N(2\beta/\alpha - \theta) < 1 \text{ ou } 2|\alpha.$$

Dans le dernier cas $\alpha = 2\alpha_1$, $(2, \beta) = (1)$ (car $N(\beta)$ impair $\in (\beta)$) donc $\alpha_1 \in (\alpha, \beta)$ avec $N(\alpha_1) < N(\alpha)$. Cela démontrera donc que N est une norme de Dedekind-Hasse sur R.
En écrivant

$$\beta/\alpha - \theta = a + b\sqrt{-19}$$

nous pouvons trouver facilement un $\theta \in R$ tel que $|b| \leqslant 1/4$ et $|a| \leqslant 1/2$. Si $|b| \leqslant 3/16$, alors $N(\beta/\alpha - \theta) \leqslant 235/256 < 1$, et nous avons terminé. Sinon $|b| > 3/16$, et nous pouvons trouver un $\theta' \in R$ tel que

$$2\beta/\alpha - \theta' = a' + b'\sqrt{-19}$$

avec $|b'| \leqslant 1/8$ et $|a'| \leqslant 1/2$, donc $N(2\beta/\alpha - \theta') < 1$. Le seul problème est que α pourrait diviser 2β. Mais si $\alpha\delta = 2\beta$, ou bien $2|\delta$, auquel cas $\alpha|\beta$ contrairement à l'hypothèse, ou bien $2|\alpha$.

Par ailleurs N n'est pas une norme euclidienne parce qu'il n'y a pas d'élément θ de R tel que $N(\beta/\alpha - \theta) < 1$ si $\beta = \rho_0$ et $\alpha = 2$. En fait, R n'admet pas de fonction euclidienne (voir l'exercice 11). □

En mathématiques classiques, tout anneau intègre à factorisation bornée R possède une pseudonorme : on prend pour $\nu(x)$ le plus petit n tel que x est borné par n. Et si R est un anneau principal, alors ν est une norme multiplicative et une fonction de Dedekind-Hasse. Constructivement, nous devons réclamer plus. Le théorème suivant donne la construction d'une telle norme si l'anneau principal est aussi un anneau à factorisation unique.

Théorème 3.5.
— *Tout anneau à factorisation unique admet une norme multiplicative.*
— *Toute pseudonorme sur un domaine de Bézout est une fonction de Dedekind-Hasse.*

Démonstration. Soit R un anneau à factorisation unique. Pour un élément non nul $a \in R$, on définit $\nu(a) = 2^n$, où n est le nombre d'éléments premiers, en comptant les multiplicités, dans une décomposition en facteurs premiers de a. Clairement ν est une norme multiplicative.

Soient R un domaine de Bézout, a, b non nuls dans R et ν une pseudonorme sur R. On a un d non nul dans R tel que $(a, b) = (d)$. Comme d divise a et que ν

est une pseudonorme, ou bien $a \sim d$, et alors a divise b, ou bien il existe $d' \sim d$ tel que $\nu(d') < \nu(a)$. Par suite ν est une fonction de Dedekind-Hasse. □

La valeur absolue est une norme multiplicative euclidienne sur l'anneau des entiers. Si F est un corps discret, alors le degré est une fonction euclidienne sur l'anneau $F[X]$. Notez que cette fonction n'est pas multiplicative, mais que la norme euclidienne $2^{\deg(f)}$ est bien multiplicative.

Une norme euclidienne multiplicative sur l'anneau $\mathbb{Z}[\sqrt{2}]$ est donnée par

$$\nu(a + b\sqrt{2}) = |a^2 - 2b^2| = |(a + b\sqrt{2})(a - b\sqrt{2})|.$$

On voit facilement que ν est multiplicative. Pour montrer que ν est euclidienne, considérons des éléments $a + b\sqrt{2}$ et $c + d\sqrt{2} \neq 0$ de $\mathbb{Z}[\sqrt{2}]$. Nous pouvons trouver les nombres rationnels p et q tels que $(a + b\sqrt{2})/(c + d\sqrt{2}) = p + q\sqrt{2}$, puis des entiers m et n tels que $|p - m| \leqslant 1/2$ et $|q - n| \leqslant 1/2$. Alors

$$(p + q\sqrt{2})(c + d\sqrt{2}) = (a + b\sqrt{2}) = (m + n\sqrt{2})(c + d\sqrt{2}) + (s + t\sqrt{2}),$$

donc $\nu(s + t\sqrt{2}) = |(p - m)^2 - 2(q - n)^2|\nu(c + d\sqrt{2}) \leqslant \nu(c + d\sqrt{2})/2$. Ainsi ν est euclidienne. □

Exemple 3.6 (*un anneau principal qui n'est pas à factorisation bornée*)**.** Soit a une suite binaire fugitive, et soit

$$R = \mathbb{Q}[X, a_1Y_1, a_2Y_2, \ldots]/(a_1(X - Y_1), a_2(X - Y_2^2), \ldots).$$

Alors R est un anneau principal, mais nous ne pouvons pas trouver de borne pour X. □

Théorème 3.7. *Soit R un anneau intègre discret et soit ν une fonction de Dedekind-Hasse sur R telle que $\nu(a) = \nu(b)$ si $a \sim b$. Soit S un sous-ensemble multiplicatif de R qui ne contient pas 0. Alors ν se prolonge en une fonction de Dedekind-Hasse sur $S^{-1}R$ qui est euclidienne si ν est euclidienne.*

Démonstration. Posons $\nu(r/s) = \nu(r/\operatorname{pgcd}(r, s))$. Cette fonction est bien définie parce que $\nu(a) = \nu(b)$ si $a \sim b$. On vérifie sans problème que ν a les propriétés voulues. □ □

Exemple 3.8 (*un anneau intègre avec une fonction euclidienne, mais qui n'a pas ses unités détachables*)**.** Soit R l'anneau des entiers, et soit S le sous-ensemble multiplicatif $\{\, 2a_n : n \in \mathbb{N} \,\}$ pour une suite binaire a. Étendez la fonction valeur absolue sur R en une fonction euclidienne sur $S^{-1}R$ (utilisez le théorème 3.7). □

Exercices

1. Un anneau intègre discret à factorisation bornée R sera appelé un **DH-anneau** si pour tous a et b non nuls dans R, avec a borné par n, ou bien $a|b$, ou bien il existe $c \in (a,b)$ qui est borné par $n-1$. Montrer qu'un DH-anneau est un anneau principal.
2. Disons qu'un anneau intègre à factorisation bornée R est **strictement borné** si chaque fois que a divise un élément b qui est borné par n, alors ou bien b divise a, ou bien a est borné par $n-1$. Montrer qu'un anneau intègre à factorisation bornée avec unités détachables est strictement borné. Montrer qu'un DH-anneau (voir l'exercice 1) est strictement borné. Montrer qu'un anneau principal strictement borné est un DH-anneau.
3. Soient a une suite binaire et $R = \mathbb{Q}[Y^2, a_1Y, a_1/(Y^2-1),\ a_2Y,\ a_2/(Y^2-1), \ldots]$. Montrer que R est un exemple brouwerien d'un anneau principal à factorisation bornée qui n'est pas strictement borné (voir l'exercice 2) en considérant les éléments $a = Y^2$ et $b = Y^2(Y^2-1)$. Montrer que R admet une fonction euclidienne, mais pas une fonction euclidienne multiplicative.
4. Montrer que l'anneau de l'exemple 3.6 est un anneau principal.
5. Soit R un anneau euclidien. Montrer que pour chaque $x \neq 0$ il existe une unité u telle que $\nu(x) \geqslant \nu(u)$.
6. Montrer que l'anneau $\mathbb{Z}[i]$ des entiers de Gauss admet une norme euclidienne multiplicative.
7. Montrer que toute pseudonorme sur un anneau principal est une fonction de Dedekind-Hasse.
8. *Un étrange principe d'omniscience.* On considère les sous-ensembles C_n de l'ensemble $2^{\mathbb{N}}$ des suites binaires définis par récurrence comme suit.

$$\begin{aligned} C_0 &= \{0\}. \\ C_{n+1} &= \{\, a : \text{si } a_i = 1, \text{ alors ou bien } a_j = 1 \text{ pour un } j > i, \\ &\qquad\qquad \text{ou bien } a_{i+1}, a_{i+2}, \ldots \text{ est dans } C_n \,\}. \end{aligned}$$

   Montrer que $a \in C_1$ si $\{\, m : a_m = 1 \,\}$ est fini ou infini. Montrer que $a \in C_n$ si $\{\, m : a_m = 1 \,\}$ est borné par n. Montrer que LPO est équivalent à $2^{\mathbb{N}} = C_1$. Que faites-vous du principe d'omniscience $2^{\mathbb{N}} = \bigcup_n C_n$?
9. *Un anneau principal à factorisation bornée qui n'admet pas de pseudonorme.* Soient k le corps à deux éléments et a une suite binaire ; on définit $\varphi_n \colon k(X_n) \to k(X_{n+1})$ par

$$\varphi_n(X_n) = a_n(X_{n+1}^2 + n) + X_{n+1}.$$

Soit R_n le sous-anneau de $k(X_n)$ défini par $R_1 = k[X_1]$, $R_{n+1} = \varphi_n(R_n)$ si $a_n = 0$, et sinon $R_{n+1} = S_n^{-1}\varphi_n(R_n)$, où S_n est le sous-ensemble multiplicatif engendré par $X_{n+1}^2 + X_{n+1} + 1$. Montrer que la limite directe R des anneaux R_n est un anneau principal à factorisation bornée. Montrer que le principe d'omniscience de l'exercice 8 serait vérifié si R admettait une pseudonorme.

10. Montrer que $\mathbb{Z}[(1+\sqrt{-19})/2]$ est la clôture intégrale de $\mathbb{Z}$ dans $\mathbb{Q}[\sqrt{-19}]$.
11. Montrer que les unités de l'anneau R de l'exemple 3.4 sont ± 1. Soient $\alpha = 2$ et $\beta = (1 + \sqrt{-19})/2$. En utilisant la fonction N, montrer que α, $\alpha + 1$, $\alpha - 1$, β, $\beta + 1$, et $\beta - 1$ sont deux à deux premiers entre eux. Supposons que R admette une fonction euclidienne ν, et soit γ un élément non inversible dans R. En divisant γ par α et β, montrer qu'il y a un élément non inversible γ' de R tel que $\nu(\gamma') < \nu(\gamma)$.
12. Construire un exemple brouwerien d'un anneau principal muni d'une fonction de Dedekind-Hasse mais sans unités détachables ni fonction euclidienne. (Regardez $\mathbb{Z}[(1 + \sqrt{-19})/2] \subseteq \mathbb{Q}[\sqrt{-19}]$.)

4 Anneaux de polynômes

Dans cette section nous étudions les propriétés d'un anneau intègre discret R qui sont héritées dans l'anneau des polynômes $R[X]$.

Définition 4.1. Soit R un anneau intègre à pgcd, et soit $f \in R[X]$. Le pgcd des coefficients de f est appelé le **contenu** de f et noté par $\mathrm{cont}(f)$. Si $\mathrm{cont}(f) = 1$, alors f est dit **primitif**.

Lemme 4.2. *Soient R un anneau intègre à pgcd et K son corps de fractions. Soit $f \in K[X]$, nous pouvons trouver un $c \in K$ et un polynôme primitif $g \in R[X]$ tels que $f = cg$. Si en outre $f = c'g'$ pour un $c' \in K$ et un polynôme primitif $g' \in R[X]$, alors $c = uc'$ avec u inversible dans R.*

Démonstration. On écrit $f = c_0 g_0$ avec $c_0 \in K$ et $g_0 \in R[X]$. Soient $g = g_0/\mathrm{cont}(g_0)$ et $c = c_0 \cdot \mathrm{cont}(g_0)$, alors $f = cg$ et g est un polynôme primitif. Si maintenant $f = c'g'$ avec $c' \in K$ et g' un polynôme primitif dans $R[X]$, considérons un élément non nul $d \in R$ tel que dc et dc' sont dans R. Alors dc et dc' sont tous deux égaux au contenu de df, donc $dc = udc'$ avec u inversible dans R. Ainsi $c = uc'$. □

Lemme 4.3 (lemme de Gauss)**.** *Soient R un anneau intègre à pgcd et $f, g \in R[X]$. Alors* $\mathrm{cont}(fg) = \mathrm{cont}(f)\mathrm{cont}(g)$.

Démonstration. Soient $m = \deg f$ et $n = \deg g$. Nous procédons par récurrence sur $m + n$. Comme $\mathrm{cont}(ah) = a \cdot \mathrm{cont}(h)$ pour une constante a et un polynôme

h, nous pouvons diviser f et g par leur contenu et il suffit de démontrer le lemme lorsque f et g sont des polynômes primitifs. Soient $c = \mathrm{cont}(fg)$ et $d = \mathrm{pgcd}(c, f_m)$, où f_m est le coefficient dominant de f. Alors $d|(f - f_m X^m)g$. Si $f = f_m X^m$ le lemme est clair. Sinon, par récurrence, $d|\mathrm{cont}(f - f_m X^m)\mathrm{cont}(g)$. Comme g est primitif, nous avons $d|(f - f_m X^m)$, donc $d|f$. Comme f est primitif, nous avons $d = \mathrm{pgcd}(c, f_m) = 1$. De la même manière nous démontrons que $\mathrm{pgcd}(c, g_n) = 1$. Donc, par le théorème 1.1(iii), nous avons $c = \mathrm{pgcd}(c, f_m g_n) = 1$, et fg est un polynôme primitif. □

Corolaire 4.4. *Soient R un anneau intègre à pgcd, k son corps de fractions et f et g des polynômes de $R[X]$. Alors f divise g dans $R[X]$ si, et seulement si, f divise g dans $k[X]$ et* cont(f) *divise* cont(g).

Démonstration. L'implication «seulement si» est immédiate d'après le lemme de Gauss. Pour démontrer «si» nous pouvons supposer que le polynôme f est primitif. D'après le lemme 4.2, nous pouvons écrire $g = ahf$ avec h un polynôme primitif de $R[X]$ et $a \in k$. D'après le lemme de Gauss, le polynôme fh est primitif, donc $a = \mathrm{cont}(g) \in R$ d'après le lemme 4.2. Ainsi f divise g dans $R[X]$. □

Théorème 4.5. *Soient R un anneau intègre à pgcd et k son corps de fractions. Soient f et g des polynômes de $k[X]$, chacun avec un coefficient inversible dans R. Si fg est un polynôme primitif de $R[X]$, alors f et g sont dans $R[X]$.*

Démonstration. On a des constantes $a, b \in k$ et des polynômes primitifs $f_1, g_1 \in R[X]$ tels que $f = af_1$ et $g = bg_1$. Comme f et g ont des unités de R parmi leurs coefficients, a^{-1} et b^{-1} sont dans R. D'après le lemme de Gauss, le polynôme $f_1 g_1 = a^{-1}b^{-1}fg$ est primitif. Donc $a^{-1}b^{-1}$ est une unité de R, par suite a et $b \in R$ et donc f et $g \in R[X]$. □

Théorème 4.6. *Soient R un anneau intègre à pgcd et k son corps de fractions. Soient f et g des polynômes de $k[X]$ tels que $fg \in R[X]$. Alors il existe un $b \in k$ tel que bf et $g/b \in R[X]$.*

Démonstration. On a des constantes $a, b \in k$ et des polynômes primitifs $f_1, g_1 \in R[X]$ tels que $f = af_1$ et $g = bg_1$. D'après le lemme de Gauss, le polynôme $f_1 g_1$ est primitif, donc $ab = \mathrm{cont}(fg) \in R$ d'après le lemme 4.2. Par suite $bf = abf_1$ et $g/b = g_1 \in R[X]$. □

Théorème 4.7. *Soit R un anneau intègre discret.*

(i) *Si R est un anneau à pgcd, alors il en va de même pour $R[X]$.*

(ii) *Si R est à factorisation bornée, alors il en va de même pour $R[X]$.*

(iii) *Si R a ses unités détachables, alors il en va de même pour $R[X]$.*

(iv) *Si la divisibilité est décidable dans R, alors il en va de même pour $R[X]$.*

(v) *Si R satisfait la condition de chaine des diviseurs, alors il en va de même pour $R[X]$.*

(vi) *Si R est un quasi-AFU, alors il en va de même pour $R[X]$.*

Démonstration. Soit k le corps de fractions de R.

Pour démontrer (i) on considère f et g dans $R[X]$. Soit h un polynôme primitif de $R[X]$ tel que h est un pgcd de f et g dans $k[X]$. Soit $d = \operatorname{pgcd}(\operatorname{cont}(f), \operatorname{cont}(g))$. On va montrer que $dh = \operatorname{pgcd}(f, g)$. D'après le corolaire 4.4, dh divise f et $g \in R[X]$. Inversement, supposons que q divise f et $g \in R[X]$. Alors q divise h dans $k[X]$, et $\operatorname{cont}(q)$ divise $\operatorname{cont}(f)$ et $\operatorname{cont}(g)$, donc il divise d. Ainsi q divise dh d'après le corolaire 4.4. Nous avons montré que dh est un pgcd de f et g.

Pour démontrer (ii) soit $f \in R[X]$ de degré n, et soit a son coefficient dominant. Si a est borné par m, alors f est borné par $m + n$.

L'assertion (iii) est triviale, car l'anneau $R[X]$ a les mêmes unités que R.

Pour démontrer (iv) nous montrons par récurrence sur $n = \deg g$ que nous pouvons décider si f divise g. Soient a le coefficient dominant de f, et b le coefficient dominant de g. Nous pouvons supposer que $\deg f \leqslant \deg g$. Si a ne divise pas b, alors f ne divise pas g. Si $a|b$, alors il existe des polynômes q et h tels que $g = qf + h$ et $\deg h \leqslant n - 1$. Alors $f|g$ si, et seulement si, $f|h$. Par récurrence nous pouvons décider si f divise h, et donc nous pouvons décider si f divise g.

Supposons que R satisfait la condition de chaine des diviseurs. Soit $(f_1) \subseteq (f_2) \subseteq \cdots$ une chaine ascendante d'idéaux principaux de $R[X]$. Nous construisons un p tel que $(f_p) = (f_{p+1})$ par récurrence sur $\deg f_1$. Soit a_i le coefficient dominant de f_i. Alors $a_{i+1}|a_i$ pour chaque $i > 1$, donc il existe un m tel que $a_m|a_{m+1}$. Si $\deg f_m = \deg f_{m+1}$, alors $f_m|f_{m+1}$ et nous avons terminé. Sinon $\deg f_{m+1} < \deg f_m \leqslant \deg f_1$, et nous considérons la suite des f qui commence à f_{m+1}. Par récurrence nous trouvons l'entier n tel que $(f_n) = (f_{n+1})$.

L'assertion (vi) résulte de (v) et (i). □

Théorème 4.8 (Kronecker 1)**.** *Si R est un anneau à factorisation unique infini avec un nombre fini d'unités, alors il en va de même pour $R[X]$. Donc R est factoriel.*

Démonstration. Soit k le corps de fractions de R. Soit $f \in R[X]$ un polynôme de degré n. Il suffit de construire un ensemble fini de polynômes qui contient tous les diviseurs de f dont le degré est au plus $n/2$. Soient $a_0, \ldots, a_m$ des éléments distincts de R, avec $n \leqslant 2m$. Comme R est un anneau à factorisation unique avec un nombre fini d'unités, tout $f(a_i)$ non nul a un ensemble fini de diviseurs. Si un $f(a_i) = 0$, alors $f = (X - a_i)g$ et nous terminons par récurrence sur n. Nous pouvons donc supposer que $f(a_i) \neq 0$ pour tout i. Notez que si $g|f$, alors $g(a_i)|f(a_i)$ pour tout i. Il y a seulement un nombre fini de suites $b_0, \ldots, b_m$

telles que b_i divise $f(a_i)$ pour tout i. Par le théorème d'interpolation unique (théorème II.5.5) nous avons pour chaque suite $b_0, \ldots, b_m$ un unique polynôme $g \in k[X]$ de degré au plus m tel que $g(a_i) = b_i$ pour tout i. L'ensemble de ces polynômes g est un ensemble fini de polynômes de $k[X]$ qui contient tous les diviseurs de f dans $R[X]$ de degré au plus $n/2$. Enfin un polynôme g de degré au plus $n/2$ est un diviseur de f si, et seulement si, $g \in R[X]$ et $f/g \in R[X]$, et cela est décidable car $R[X]$ est une partie détachable de $k[X]$. □

Le théorème « Kronecker 1 » montre que $\mathbb{Z}[X_1, \ldots, X_n]$ est factoriel pour tout n. Avec le corolaire 2.6 nous voyons que $\mathbb{Q}[X_1, \ldots, X_n]$ est aussi factoriel. Si k est un corps fini, alors $k[X_1, \ldots, X_n]$ est factoriel, car un $f \in k[X_1, \ldots, X_n]$ n'a qu'un nombre fini de diviseurs. Cependant, les anneaux à factorisation unique ne sont pas tous factoriels, comme le montre l'exemple 2.2.

Le théorème « Kronecker 1 » a pour hypothèse le fait que l'anneau R est infini. Mais les anneaux à factorisation unique finis sont certainement factoriels. Dans le théorème VI.6.8 nous allons éliminer l'hypothèse que l'anneau est fini ou infini.

La clôture algébrique k de $\mathbb{Q}$ – voir le corolaire VI.2.5 – ainsi que l'anneau des polynômes $k[X]$ est un anneau à factorisation unique, donc k est factoriel. Mais « Kronecker 1 » ne suffit pas pour démontrer que $k[X]$ est factoriel comme c'était le cas pour $k = \mathbb{Q}$. Une autre astuce de Kronecker montre que $R[X, Y]$ est un anneau à factorisation unique si $R[X]$ en est un.

Théorème 4.9 (Kronecker 2)**.** *Si R est un anneau factoriel, alors il en va de même pour $R[X]$.*

Démonstration. Pour $m > 0$, soit $\varphi_m \colon R[X, Y] \to R[X]$ l'homomorphisme d'anneaux qui est l'identité sur $R[X]$ et qui envoie Y sur X^m. Soit $\psi \colon R[X] \to R[X, Y]$ l'application R-linéaire qui envoie X^n sur $Y^q X^r$ où $n = qm + r$ et $0 \leqslant r < m$. Soit $R[X, Y]_m$ l'ensemble des polynômes de $R[X]$ dont le degré en X est strictement plus petit que m. Alors :

$$\begin{gathered}\varphi_m\psi \text{ est l'identité sur } R[X],\\ \psi\varphi_m \text{ est l'identité sur } R[X, Y]_m,\\ \text{si } a, b \in R[X, Y] \text{ et } ab \in R[X, Y]_m, \text{ alors } a, b \in R[X, Y]_m.\end{gathered}$$

Pour factoriser un polynôme $f \in R[X, Y]$ de degré en X inférieur à m, consultez le nombre fini de factorisations (à des unités près) $\varphi_m(f) = ab$. Faites un test pour voir si $\psi(a)\psi(b) = f$. Toute factorisation de f doit avoir cette forme. □

Exercices

1. Montrer que X^4+1 est irréductible sur $\mathbb{Q}[X]$ en utilisant les techniques de « Kronecker 1 » et du corolaire 2.6. Utiliser « Kronecker 1 » pour factoriser $X^4 + 4$.

2. Décomposer $X^4 + 4Y^4$ en facteurs premiers sur l'anneau $\mathbb{Z}[X, Y]$.
3. Utiliser « Kronecker 2 » avec le polynôme $X^2 + Y$ pour voir que même si l'image $\varphi_m(f)$ se factorise dans $k[X]$, le polynôme de départ ne se factorise pas nécessairement.

5 Notes

La condition de chaine des diviseurs est définie en termes de chaine ascendante d'idéaux principaux $I_1 \subseteq I_2 \subseteq \cdots$ plutôt que de chaine (descendante) d'éléments $a_1, a_2, \ldots$ vérifiant $a_{i+1}|a_i$ pour tout i. Les deux versions sont équivalentes en présence de l'axiome du choix dépendant. La version avec les idéaux nous permet de démontrer – dans ce chapitre et le chapitre VI – les propriétés de base des anneaux principaux sans utiliser l'axiome du choix dépendant.

Dans les quasi-AFU, les anneaux principaux et les anneaux euclidiens, nous ne savons pas nécessairement factoriser les éléments non nuls. Par contre nous pouvons utiliser le théorème de factorisation partielle pour écrire des éléments non nuls $a_1, \ldots, a_n$ dans un quasi-AFU comme produits d'éléments deux à deux premiers entre eux $p_1, \ldots, p_m$.

Les théorèmes Kronecker 1 et 2 sont dans [Kronecker 1882]. Il fournissent les algorithmes pour décomposer des polynômes sur les entiers (en plusieurs indéterminées) en produits de polynômes premiers. Nous ne sommes pas concernés ici par l'efficacité de ces algorithmes.

V. Anneaux principaux

Sommaire

1 Diagonalisation des matrices

La théorie des modules sur un anneau principal est étroitement reliée à la théorie des espaces vectoriels sur un corps et elle est presque identique à la théorie des groupes abéliens, qui sont les modules sur l'anneau des entiers. L'analogue d'un espace vectoriel de dimension finie est un module de présentation finie sur un anneau principal. Un module de présentation finie est donné par une matrice. Dans cette section, nous démontrons quelques faits de base concernant les matrices sur un anneau principal.

Une matrice $A = (a_{ij})$ de format $m \times n$ est dite **diagonale** si $a_{ij} = 0$ lorsque $i \neq j$. Deux matrices A et B de format $m \times n$ sont **équivalentes** s'il y a une matrice inversible C de format $m \times m$ et une matrice inversible D de format $n \times n$ telles que $A = CBD$.

Lemme 1.1. *Toute matrice sur un anneau principal est équivalente à une matrice diagonale.*

Démonstration. La clé du problème est donnée par la construction de certaines matrices inversibles de format 2×2. Si $sa + tb = d \neq 0$ est le pgcd de a et b, alors pour tous u, v il existe w, x tels que

$$\begin{pmatrix} a & b \\ u & v \end{pmatrix} \cdot \begin{pmatrix} s & -b/d \\ t & a/d \end{pmatrix} = \begin{pmatrix} d & 0 \\ w & x \end{pmatrix}.$$

En outre le facteur de droite est inversible puisque son déterminant est égal à 1. De la même manière, si a et b sont dans une même colonne, nous multiplions à gauche comme suit.

$$\begin{pmatrix} s & t \\ -b/d & a/d \end{pmatrix} \cdot \begin{pmatrix} a & u \\ b & v \end{pmatrix} = \begin{pmatrix} d & w \\ 0 & x \end{pmatrix}.$$

Donc si a et b sont des entrées dans une même ligne (ou colonne) d'une matrice B, nous pouvons multiplier la matrice B à droite (ou à gauche) par une matrice inversible et obtenir ainsi aux positions occupées par a et b respectivement le pgcd d et 0, ceci sans changer les entrées hors des lignes (colonnes) de a et b.

Étant donnée une matrice A nous allons la multiplier à gauche et à droite par des matrices inversibles et obtenir une matrice diagonale. Si $A = 0$ c'est terminé. Sinon par des échanges de lignes et de colonnes, nous pouvons amener un élément non nul a_1 dans le coin nord-ouest. En multipliant à droite par des matrices inversibles nous remplaçons a_1 par a_2, le pgcd de tous les éléments de la première ligne et nous annulons le reste de première ligne. De la même manière par des multiplications à gauche nous pouvons remplacer a_2 par a_3, le pgcd de tous les éléments qui se trouvent maintenant dans la première colonne, et nous annulons le reste de première colonne. On continue en remplaçant a_3 par a_4, le pgcd de tous les éléments qui se trouvent maintenant dans la première ligne, et ainsi de suite. De cette manière, nous produisons une suite $(a_1), (a_2), \ldots$ d'idéaux principaux telle que $a_{i+1}|a_i$ pour chaque i. Donc, pour un certain n, nous obtenons $a_n|a_{n+1}$. Cela signifie que a_n est un pgcd des éléments de la première ligne (ou colonne), tandis que les éléments restants sur la première colonne (ou ligne) sont nuls. Maintenant, revenant à l'étape n, par des manipulations élémentaires de colonnes (lignes), nous pouvons annuler tous les éléments de la première ligne (colonne) sans changer le première colonne (ligne). Ainsi, excepté le coin nord-ouest, les premières ligne et colonne sont nulles. Enfin, par récurrence sur la taille la matrice nous obtenons une matrice diagonale. □

Une matrice $A = (a_{ij})$ est en **forme normale de Smith** si elle est diagonale et si $a_{ii}|a_{i+1,i+1}$ pour tout i.

Théorème 1.2. *Toute matrice sur un anneau principal est équivalente à une matrice en forme normale de Smith.*

Démonstration. D'après le lemme 1.1, il suffit de traiter le cas d'une matrice diagonale. Soient a, b des éléments diagonaux non nuls et $d = sa + tb$ le pgcd de a et b. Alors

$$\begin{pmatrix} s & t \\ -b/d & a/d \end{pmatrix} \cdot \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \cdot \begin{pmatrix} 1 & -tb/d \\ 1 & sa/d \end{pmatrix} = \begin{pmatrix} d & 0 \\ 0 & ab/d \end{pmatrix}.$$

En utilisant de manière répétée cette observation nous pouvons ramener la matrice à une forme diagonale dans laquelle le coefficient nord-ouest divise tous les autres. On termine par récurrence sur la taille de la matrice. □

Nous voulons montrer maintenant que toute matrice est équivalente à une matrice en forme normale de Smith de manière essentiellement unique.

Étant donnée une matrice A, nous notons $\Delta_i(A)$ l'idéal engendré par les déterminants de toutes les sous-matrices carrées de taille i extraites de A.

Lemme 1.3. *Soient A et B des matrices $m \times n$ équivalentes sur un anneau intègre à pgcd R. Alors $\Delta_i(A) = \Delta_i(B)$ pour tout i.*

Démonstration. Il suffit de montrer que si C est une matrice inversible de format $m \times m$, alors $\Delta_i(CA) = \Delta_i(A)$. Les lignes de CA sont des combinaisons linéaires des lignes de A. Donc les déterminants des sous-matrices $i \times i$ de CA sont des combinaisons linéaires des déterminants des sous-matrices $i \times i$ de A. Donc $\Delta_i(A) \supseteq \Delta_i(CA)$. Comme C est inversible, nous avons aussi $\Delta_i(CA) \supseteq \Delta_i(C^{-1}CA) = \Delta_i(A)$. Et donc $\Delta_i(CA) = \Delta_i(A)$. □

Théorème 1.4. *Deux matrices en forme normale de Smith sur un anneau intègre à pgcd sont équivalentes si, et seulement si, les éléments diagonaux correspondants sont associés.*

Démonstration. Soit $D = (d_{ij})$ une matrice en forme normale de Smith. On vérifie facilement que $\Delta_1(D) = (d_{11})$ et que $\Delta_i(D) \cdot (d_{i+1,i+1}) = \Delta_{i+1}(D)$ pour chaque $i \leqslant m-1$. Ainsi les éléments diagonaux de D sont déterminés, à une unité près, par les idéaux $\Delta_i(D)$. Le lemme 1.3 nous dit que cela implique que si deux matrices en forme normale de Smith sont équivalentes alors leurs éléments diagonaux sont associés. □

Exercices

1. Trouver une matrice en forme normale de Smith sur $\mathbb{Z}$ qui est équivalente à la matrice
$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}.$$

2. Un **anneau de valuation** [1] est un anneau commutatif tel que pour tous éléments a et b, on a $(a) \subseteq (b)$ ou $(b) \subseteq (a)$. Montrer que toute matrice sur un anneau de valuation est équivalente à une matrice en forme normale de Smith.

1. **NdT.** Valuation ring. Il s'agit ici des anneaux de valuation au sens de Kaplansky ; Bourbaki réclame qu'un anneau de valuation soit intègre.

3. Montrer qu'une matrice carrée sur $\mathbb{Z}$ est inversible si, et seulement si, elle est un produit de matrices élémentaires.
4. Montrer qu'une matrice carrée sur $\mathbb{Z}$ a son déterminant égal à 1 si, et seulement si, elle est un produit de matrices élémentaires correspondant aux manipulations élémentaires de type (iii). Idée :

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}.$$

2 Modules de présentation finie

Soit M un module sur un anneau commutatif R. Une **présentation finie** de M est un triplet $(M, (x_1, \ldots, x_n), A)$, où $x_1, \ldots, x_n$ est un système générateur fini de M et A est une matrice $m \times n$ d'éléments de R dont les lignes engendrent le module des relations entre les x_i. Ainsi pour chaque élément $(\alpha_1, \ldots, \alpha_n) \in R^n$ nous avons $\alpha_1 x_1 + \cdots + \alpha_n x_n = 0$ si, et seulement si, $(\alpha_1, \ldots, \alpha_n) = vA$ pour un $v \in R^m$. Nous pouvons identifier un module de présentation finie avec sa présentation finie.

La matrice A contient toute l'information sur la structure du module M. Étant donné le module M, la matrice A dépend du choix des générateurs $x_1, \ldots, x_n$ de M et du choix des générateurs du module des relations. Si $M \simeq R/(r_1) \oplus \cdots \oplus R/(r_n)$, nous obtenons une matrice diagonale A pour M ; inversement, si nous pouvons obtenir une matrice diagonale A pour M, alors nous avons montré que M est une somme directe de modules cycliques. Il nous importe donc d'examiner comment on peut passer d'une matrice de présentation pour M à une autre.

Soit $(M, (x_1, \ldots, x_n), A)$ un R-module de présentation finie. Alors $(M, (x_1, \ldots, x_n), B)$ est un R-module de présentation finie si, et seulement si, les lignes de B engendrent le même sous-module de R^n que les lignes de A ; cela se produit si $B = FA$ pour une matrice F inversible de taille m. Que se passe-t-il pour la matrice des relations A d'un module de présentation finie $(M, (x_1, \ldots, x_n), A)$ quand nous changeons le système générateur $(x_1, \ldots, x_n)$?

Théorème 2.1. *Soit $(M, (x_1, \ldots, x_n), A)$ un module de présentation finie sur un anneau commutatif R et soit E une matrice inversible de taille n sur R. Alors $(M, (x_1, \ldots, x_n), A) = (M, (x_1, \ldots, x_n)E^t, AE^{-1})$.*

Démonstration. Notons $(y_1, \ldots, y_n)^t = E(x_1, \ldots, x_n)^t$. Clairement $y_1, \ldots, y_n$ engendrent M. En outre les propriétés suivantes sont équivalentes.

$$(r_1, \ldots, r_n)E^{-1}(y_1, \ldots, y_n)^t = (r_1, \ldots, r_n)(x_1, \ldots, x_n)^t = 0,$$
$$(r_1, \ldots, r_n) = (s_1, \ldots, s_m)A \text{ pour un } (s_1, \ldots, s_m),$$
$$(r_1, \ldots, r_n)E^{-1} = (s_1, \ldots, s_m)(AE^{-1}).$$

Donc le module des relations entre les y_i est engendré par les lignes de AE^{-1}. □

Corolaire 2.2. *Soient A une matrice $m \times n$ sur un anneau commutatif R et $(M, (x_1, \ldots, x_n), A)$ un R-module de présentation finie. Soient E une matrice inversible $n \times n$ sur R et F une matrice inversible $m \times m$ sur R. Alors $(M, (x_1, \ldots, x_n), A) = (M, (x_1, \ldots, x_n)E^t, FAE^{-1})$.*

Démonstration. Comme les lignes de FAE^{-1} engendrent le même module que celles de AE^{-1}, le corolaire est une conséquence immédiate du théorème 2.1. □

Théorème 2.3 (théorème de structure)**.** *Soit M un module de présentation finie sur un anneau principal R. Alors il existe des idéaux principaux $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_n$ tels que M est isomorphe à la somme directe $R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_n$.*

Démonstration. Soit $(M, (x_1, \ldots, x_n), A)$ une présentation finie de M. D'après le théorème 1.4, on a des matrices inversibles E et F telles que la matrice $D = FAE^{-1}$ est en forme normale de Smith. D'après le corolaire 2.2, nous avons

$$(M,\ (x_1, \ldots, x_n),\ A) = (M,\ (x_1, \ldots, x_n)E^t,\ D).$$

Si $(y_1, \ldots, y_n) = (x_1, \ldots, x_n)E^t$, alors $M = Ry_1 \oplus \cdots \oplus Ry_n$ et $Ry_i \simeq R/I_i$ avec $I_i = (d_{ii})$. □

La décomposition obtenue dans le théorème 2.3 est essentiellement unique sur n'importe quel anneau commutatif.

Théorème 2.4. *Soient R un anneau commutatif, $m \leqslant n$ des entiers strictement positifs, et $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_m$ et $J_1 \supseteq J_2 \supseteq \cdots \supseteq J_n$ des idéaux de R. Supposons qu'un R-module M soit isomorphe à $\bigoplus_{i=1}^{m} R/I_i$ et à $\bigoplus_{j=1}^{n} R/J_j$. Alors*

(a) $J_1 = J_2 = \cdots = J_{n-m} = R$.

(b) $I_i = J_{n-m+i}$ *pour* $i = 1, \ldots, m$.

Démonstration. Pour démontrer (a) il suffit de voir que si $m < n$, alors $J_1 = R$. Soit $S = R/J_1$. Alors

$$S^n = \bigoplus\nolimits_{j=1}^{n} R/(J_j + J_1) \simeq M/(J_1M) \simeq \bigoplus\nolimits_{i=1}^{m} R/(I_i + J_1)$$

comme S-modules. Nous avons une application linéaire surjective de S^m sur $\bigoplus_{i=1}^{m} R/(I_i + J_1)$, donc de S^m sur S^n, donc $S = 0$ d'après le théorème II.7.5.

Puisque (a) est valide, nous pouvons supposer que $m = n$. Pour démontrer (b) il suffit, par symétrie, de voir que $I_k \subseteq J_k$ pour $k = 1, \ldots, n$. Soit $x \in I_k$. Alors

$$\bigoplus\nolimits_{j=1}^{n} R/(J_j : x) \simeq xM \simeq \bigoplus\nolimits_{i=k+1}^{n} R/(I_i : x)$$

où $(K : x) = \{\, r \in R : rx \in K \,\}$. En appliquant (a) à xM nous obtenons $(J_1 : x) = (J_2 : x) = \cdots = (J_k : x) = R$. Donc $x \in J_k$. □

Exercices

1. Montrer qu'un groupe abélien de présentation finie est une somme directe d'un nombre fini de groupes cycliques finis ou infinis.
2. Donner un exemple brouwerien d'un groupe cyclique qui n'est ni fini ni infini.
3. Montrer que si une matrice $m \times n$ sur un anneau commutatif R a un inverse à gauche et si $m < n$, alors $R = 0$.
4. Soit H un sous-groupe détachable d'un groupe abélien libre (un $\mathbb{Z}$-module libre) sur un ensemble discret. Montrer que pour chaque $h \in H$ il existe un $x \in H$ tel que $h \in \langle x \rangle$ et $H/\langle x \rangle$ est un sous-groupe détachable d'un groupe abélien libre sur un ensemble discret.
5. Utilisez l'exercice 4 pour montrer qu'un sous-groupe détachable d'un groupe abélien libre sur un ensemble discret dénombrable est un groupe abélien libre sur un ensemble discret dénombrable. (Construire des générateurs x_i pour H par récurrence de façon à ce que $H/\langle x_1, \ldots, x_{n-1} \rangle$ soit un sous-groupe détachable d'un groupe abélien libre sur un ensemble discret dénombrable pour chaque $n \geqslant 1$.)

3 Modules de torsion, p-composantes, diviseurs élémentaires

Soit M un module sur un anneau intègre discret R. Le **sous-module de torsion** $\tau(M)$ de M est défini comme $\tau(M) = \{\, m \in M : am = 0 \text{ pour un } a \neq 0 \,\}$. On voit facilement que $\tau(M)$ est un sous-module de M. Si $\tau(M) = M$, alors nous disons que M est un module de **torsion**. Si d est un élément non nul de R et si $dM = 0$, alors nous disons que M est **annulé** par d.

Théorème 3.1. *Soit M un module de présentation finie sur un anneau principal R. Alors le sous-module de torsion $\tau(M)$ est un sous-module de présentation finie détachable de M, et $M \simeq \tau(M) \oplus R^n$ pour un n. De plus $\{\, d \in R : d\tau(M) = 0 \,\}$ est un idéal principal non nul.*

Démonstration. D'après le théorème 2.3, il existe des idéaux principaux $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_m$ tels que M est isomorphe à la somme directe $R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_m$. Si $I_k = 0$ pour chaque k, les conclusions sont claires. Sinon nous trouvons un k tel que $I_k \neq 0$ et $I_i = 0$ pour $i > k$. On a alors $\tau(M) \simeq R/I_1 \oplus \cdots \oplus R/I_k$ et $M \simeq \tau(M) \oplus R^{m-k}$. De plus $I_k = \{\, d \in R : d\tau(M) = 0 \,\}$. □

Soit M un module sur un anneau commutatif R, et soit $d \in R$. Alors la **d-composante** de M est définie par $M_d = \{\, m \in M : d^k m = 0 \text{ pour un } k \,\}$. Nous vérifions facilement que M_d est un sous-module de M. Observons que $M_a + M_b \subseteq M_{ab}$ pour tous $a, b \in R$ et que $M_{a^n} = M_a$ pour tout $n > 0$.

Lemme 3.2. *Soient M un module sur un anneau commutatif R, et a et b des éléments étrangers de R. Alors $M_{ab} = M_a \oplus M_b$, et si M est de type fini, la projection de M_{ab} sur M_a est réalisée par la multiplication par un élément de R. Le module M_{ab} est cyclique si, et seulement si, les sous-modules M_a et M_b sont cycliques.*

Démonstration. Pour montrer que $M_{ab} = M_a \oplus M_b$, il suffit de voir que $K = K_a \oplus K_b$ pour chaque sous-module de type fini de M_{ab}. Nous pouvons donc supposer que M est de type fini. Dans ce cas on a $a^k b^k M_{ab} = 0$ pour un entier strictement positif k.

Il existe s et $t \in R$ tels que $sa^k + tb^k = 1$. Soit $\pi_a = tb^k$ et $\pi_b = sa^k$. Alors

(i) $\pi_a M_{ab} \subseteq M_a$ et $\pi_b M_{ab} \subseteq M_b$,

(ii) $\pi_a M_b = 0$ et $\pi_b M_a = 0$,

(iii) $\pi_a x = x$ pour $x \in M_b$ et $\pi_b x = x$ pour $x \in M_a$,

donc $M_{ab} = M_a \oplus M_b$ et la multiplication par π_a donne la projection de M_{ab} sur M_a.

Si $M_{ab} = Rx$, alors M_a est engendré par $\pi_a x$ et M_b est engendré par $\pi_b x$. Inversement, supposons que $M_a = Ry$ et $M_b = Rz$, et posons $x = y + z$. Alors $y = \pi_a x \in Rx$ et $z = \pi_b x \in Rx$, donc $M_{ab} = Rx$. □

Théorème 3.3. *Soit M un module sur un anneau commutatif. Soit $a = {p_1}^{e_1} \cdots {p_m}^{e_m}$, où les p_i sont deux à deux étrangers. Alors $M_a = M_{p_1} \oplus \cdots \oplus M_{p_m}$, et si M est de type fini, la projection de M_a sur M_{p_i} est réalisée par la multiplication par un élément de l'anneau.*

Démonstration. Appliquer le lemme 3.2 de manière répétée. □

Si p est premier dans un anneau intègre discret R, alors un R-module M est dit **p-primaire** si $M_p = M$. Si $dM = 0$ pour un élément d non nul R qui est un produit de puissances d'éléments deux à deux étrangers, alors nous pouvons décomposer M en une somme directe de sous-modules primaires [1] d'après le théorème 3.3.

Théorème 3.4. *Soient R un anneau principal, p un élément premier dans R, et M un R-module p-primaire de présentation finie. Alors M est isomorphe à une somme directe finie de R-modules, tous de la forme $R/(p^n)$ pour un $n > 0$.*

Démonstration. D'après le théorème de structure (théorème 2.3), M est isomorphe à une somme directe finie de R-modules, tous de la forme R/I pour un idéal principal I. Comme M est p-primaire, chaque I contient une puissance strictement positive de p. Si $p^m \in I = (a)$, alors $p^m = ab$. Comme p est premier, nous pouvons écrire $a = up^n$ où u est inversible ; donc $I = (p^n)$. □

1. **NdT.** En fait, si la terminologie « p-primaire » renvoie bien au cas des éléments p premiers, le théorème 3.3 donne un résultat un peu moins fort : si $dM = 0$, alors M est la somme directe de ses p_i-composantes pour les p_i définis précédemment.

Les puissances de p dans le théorème 3.4 sont appelées les **diviseurs élémentaires** de M. Lorsque M peut être écrit comme une somme directe de sous-modules primaires, que l'on appelle ses **composantes primaires**, les diviseurs élémentaires de M sont les diviseurs élémentaires de ces sous-modules primaires de M.

Exercices

1. Donnez les composantes primaires du groupe abélien $\mathbb{Z}/12\mathbb{Z}$.
2. Soient R un domaine de Bézout et p premier dans R. Montrer que $R/(p^m)$ est un anneau de valuation. Démontrer le théorème 3.4 lorsque R est un domaine de Bézout.

4 Transformations linéaires

Soit V un espace vectoriel de dimension finie sur un corps discret k, et soit $T\colon V \to V$ une transformation linéaire [1]. Nous pouvons faire de l'espace vectoriel V un module sur $k[X]$ en définissant $Xv = T(v)$ pour $v \in V$. D'après le théorème de Cayley-Hamilton, le $k[X]$-module V est annulé par le polynôme caractéristique de T. Nous allons montrer que le $k[X]$-module V est de présentation finie.

Lemme 4.1. *Soient V un espace vectoriel sur un corps discret k de base $u_1, \dots, u_n$ et $T\colon V \to V$ une transformation linéaire telle que $T(u_i) = \sum a_{ji}u_j$. Soit $e_1, \dots, e_n$ une base pour $k[X]^n$, et définissons l'application $k[X]$-linéaire $\varphi\colon k[X]^n \to V$ qui envoie $\sum f_i(X)e_i$ sur $\sum f_i(T)u_i$. Définissons $d_i \in k[X]^n$ par*

$$d_i = Xe_i - \sum\nolimits_{j=1}^{n} a_{ji}e_j.$$

Alors $\ker\varphi$ est un $k[X]$-module libre de base $d_1, \dots, d_n$.

Démonstration. De manière évidente on a $d_1, \dots, d_n \in \ker\varphi$. Supposons que $g_1e_1 + \cdots + g_ne_n \in \ker\varphi$, avec les $g_i \in k[X]$. En utilisant les relations $Xe_i = d_i + \sum_{j=1}^{n} a_{ji}e_j$, nous pouvons écrire

$$g_1e_1 + \cdots + g_ne_n = h_1d_1 + \cdots + h_nd_n + b_1e_1 + \cdots + b_ne_n,$$

avec les $b_i \in k$. Donc $b_1e_1 + \cdots + b_ne_n \in \ker\varphi$, d'où $b_1u_1 + \cdots + b_nu_n = 0$. Comme $u_1, \dots, u_n$ est une base du k-espace vectoriel V, cela implique que chaque $b_i = 0$. Par suite $d_1, \dots, d_n$ engendrent $\ker\varphi$.

Si $h_1d_1 + \cdots + h_nd_n = 0$, alors $\sum_{i=1}^{n} h_iXe_i = \sum_{i=1}^{n}\sum_{j=1}^{n} h_ia_{ji}e_j$ et donc $h_jXe_j = \sum_{i=1}^{n} h_ia_{ji}e_j$ pour chaque j. Si un h_i est non nul, nous pouvons

1. **NdT.** Une application linéaire d'un espace vectoriel vers lui-même.

supposer que le degré de h_1 est maximal parmi les degrés de $h_1, \ldots, h_n$. Mais cela est impossible car $h_1 X = \sum_{i=1}^{n} h_i a_{1i}$. Donc $d_1, \ldots, d_n$ sont linéairement indépendants. □

D'après le théorème 2.3, le $k[X]$-module V peut être écrit sous la forme $V = C_1 \oplus \cdots \oplus C_s$, où les C_i sont des $k[X]$-modules cycliques, isomorphes à $k[X]/(f_i)$ pour des polynômes unitaires non nuls f_i, avec f_i qui divise f_{i+1} pour $i = 1, \ldots, s-1$. Le polynôme f_s engendre l'idéal $\{\, g \in k[X] : gV = 0 \,\} = \{\, g \in k[X] : g(T) = 0 \,\}$, et il est appelé le **polynôme minimal** de la transformation linéaire T. D'après le théorème de Cayley-Hamilton, le polynôme minimal de T divise le polynôme caractéristique de T ; les deux polynômes sont égaux si, et seulement si, V est un $k[X]$-module cyclique.

Si λ est un zéro du polynôme caractéristique de T, nous disons que λ est une **valeur propre** de T. Si λ est une valeur propre de T, il existe un élément non nul v de V, appelé un **vecteur propre** de T, avec $(T - \lambda)v = 0$, c'est-à-dire $Tv = \lambda v$. Ainsi $X - \lambda$ doit diviser le polynôme minimal de T, et donc λ est aussi une racine du polynôme minimal de T.

La décomposition de V en une somme directe de $k[X]$-modules cycliques fournit une base de V comme espace vectoriel sur k par rapport à laquelle la transformation linéaire T a une forme canonique. Soit c_i un générateur de C_i comme $k[X]$-module, et soit m le degré de f_i. Alors $c_i, Xc_i, \ldots, X^{m-1}c_i$ est une base de C_i comme espace vectoriel sur k. En notant $f_i = X^m - b_{i,1}X^{m-1} - \cdots - b_{i,m}$, la matrice de la restriction de T à C_i pour la base $c_i, Xc_i, \ldots, X^{m-1}c_i$ est

$$B_i = \begin{pmatrix} 0 & 0 & \cdots & 0 & b_{i,m} \\ 1 & 0 & \cdots & 0 & b_{i,m-1} \\ 0 & 1 & \cdots & 0 & b_{i,m-2} \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & b_{i,2} \\ 0 & 0 & \cdots & 1 & b_{i,1} \end{pmatrix}.$$

La matrice B_i est appelée la **matrice compagne** [1] de f_i. Notez que f_i est le polynôme caractéristique de B_i. En prenant une telle base pour chaque C_i, nous obtenons une base pour k par rapport à laquelle la matrice de T a la forme

$$\begin{pmatrix} B_1 & & & \\ & B_2 & & \\ & & \ddots & \\ & & & B_s \end{pmatrix}$$

où B_i est la matrice compagne de f_i. Cette matrice est appelée la **forme canonique rationnelle** [2] de T. On voit immédiatement que le polynôme caractéristique

1. **NdT.** Companion matrix.
2. **NdT.** On dit parfois : forme réduite de Frobenius.

de cette matrice est égal à $f_1 f_2 \cdots f_s$.

Théorème 4.2 (forme canonique de Jordan)**.** *Soit T une transformation linéaire d'un espace vectoriel de dimension finie V sur un corps discret k, telle que le polynôme caractéristique de T est un produit de facteurs linéaires. Alors nous pouvons trouver une base de V relativement à laquelle la matrice de T a la forme*

$$A = \begin{pmatrix} J_1 & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_r \end{pmatrix}$$

où chaque matrice J_i est une matrice $m \times m$ de la forme

$$J(m,\lambda) = \begin{pmatrix} \lambda & 0 & \cdots & 0 & 0 \\ 1 & \lambda & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & \lambda & 0 \\ 0 & 0 & \cdots & 1 & \lambda \end{pmatrix}.$$

pour certains m et certains λ. La diagonale de A, c'est-à-dire la matrice A dans laquelle on annule les coefficients hors de la diagonale, peut être écrite comme un polynôme en A.

Démonstration. D'après le théorème 3.3, nous pouvons écrire le $k[X]$-module V comme une somme directe de modules primaires $V_{X-\lambda}$, et le théorème 3.4 nous dit que $V_{X-\lambda}$ est une somme directe de modules, chacun isomorphe à un $k[X]/((X-\lambda)^m)$ pour un m. Ce dernier module a une base sur k de la forme $1, (X-\lambda), \ldots, (X-\lambda)^{m-1}$, et relativement à cette base la matrice de la restriction de T à $V_{X-\lambda}$ est de la forme $J(m,\lambda)$. En réalisant cette construction sur chaque $V_{X-\lambda}$, nous obtenons une base relativement à laquelle la matrice de T a la forme voulue A. La diagonale de A est un polynôme en A parce que, d'après le théorème 3.3, les projections de V sur les $V_{X-\lambda}$ sont données par des polynômes en A. □

Une matrice $J(m,\lambda)$ dans la décomposition de Jordan est appelée un **bloc de Jordan**.

Nous disons que la transformation linéaire $T : V \to V$ est **diagonalisable** si V admet une base de vecteurs propres de T. Ainsi T est diagonalisable si, et seulement si, il existe une base de V relativement à laquelle la matrice de T est diagonale. Nous pouvons exprimer le fait que T est diagonalisable en termes du polynôme minimal de T.

Théorème 4.3. *Soit T une transformation linéaire d'un espace vectoriel de dimension finie V sur un corps discret k. Alors T est diagonalisable si, et seulement si, le polynôme minimal de T est un produit de facteurs linéaires unitaires deux à deux distincts.*

Démonstration. Si $\lambda_1, \ldots, \lambda_m$ sont les coefficients diagonaux d'une matrice diagonale qui représente T, alors clairement le polynôme minimal de T est $(X-\lambda_1)(X-\lambda_2)\cdots(X-\lambda_m)$. Inversement, si le polynôme minimal de T est $(X-\lambda_1)(X-\lambda_2)\cdots(X-\lambda_m)$ avec les λ_i distincts, alors V admet une base de vecteurs propres de T d'après le théorème 3.3. □

Deux matrices diagonales commutent toujours, donc il n'y a pas d'espoir d'obtenir une base par rapport à laquelle deux transformations linéaires T_1 et T_2 ont chacune une matrice diagonale, à moins que T_1 et T_2 commutent. Cette condition s'avère être suffisante.

Théorème 4.4. *Soient T_1 et T_2 deux transformations linéaires d'un espace vectoriel de dimension finie V sur un corps discret k. Supposons que T_1 et T_2 commutent. Si V admet des bases de vecteurs propres pour T_1 et pour T_2, alors V admet une base dont les éléments sont des vecteurs propres communs à T_1 et T_2.*

Démonstration. Notons $V_\lambda^i = \ker(T_i - \lambda)$ le sous-espace de V dont les éléments non nuls sont les vecteurs propres de T_i avec la valeur propre λ. Alors pour $i = 1, 2$, l'espace vectoriel V est une somme directe de sous-espaces V_λ^i lorsque λ parcourt les valeurs propres de T_i. Comme T_2 commute avec $T_1 - \lambda$, le sous-espace V_λ^1 est invariant par T_2, donc aussi par la projection de V sur V_μ^2, car celle-ci est un polynôme en T_2. Par suite $V_\lambda^1 = \sum_\mu V_\lambda^1 \cap V_\mu^2$, donc $V = \sum_{\lambda,\mu} V_\lambda^1 \cap V_\mu^2$. □

Exercice

1. Montrer que la forme canonique de Jordan d'une transformation linéaire est unique en ce sens que pour chaque couple (m, λ), le nombre de blocs de Jordan $J(m, \lambda)$ qui apparaissent est invariant (indépendant de la base choisie).

5 Notes

La forme normale de Smith pour les matrices sur $\mathbb{Z}$ remonte à [Smith 1861]. Les éléments diagonaux sont appelés les **facteurs invariants** ; le théorème 1.4 donne la raison de cette terminologie.

La condition de chaine ascendante est utilisée dans le lemme 1.1 pour diagonaliser une matrice. La question de savoir si cette condition est réellement nécessaire, ou si au contraire toutes les matrices sur les domaines de Bézout sont

diagonalisables, a été un supplice de Tantale pour beaucoup de gens pendant de nombreuses années [1].

Les démonstrations usuelles de l'unicité de la décomposition d'un module sur un anneau principal en une somme directe de modules cycliques utilisent des décompositions en facteurs premiers, malgré le fait que Kaplansky a démontré le théorème 2.4 plus général en 1949 (en utilisant deux raisonnements par l'absurde). Comme nous ne savons pas nécessairement factoriser complètement les éléments d'un anneau principal, nous avons été conduit à redécouvrir le théorème meilleur (celui de Kaplansky). Le théorème de factorisation partielle (théorème IV.1.8) a été formulé pour donner une version constructive du théorème moins bon [2].

1. **NdT.** Le théorème a été étendu à de nombreuses classes de domaines de Bézout. La plus simple est celle des domaines de Bézout de dimension 1.

2. **NdT.** D'une part, on voit facilement que le théorème de factorisation partielle implique l'unicité dans le cas de l'existence d'une décomposition en facteurs premiers. D'autre part, dans la plupart des démonstrations en mathématiques classiques qui utilisent le fait qu'un anneau principal est un anneau à factorisation unique, on peut utiliser comme substitut constructif le théorème de factorisation partielle.

VI. Théorie des corps

Sommaire

1 Extensions entières et anneaux impotents

Soit R un sous-anneau d'un anneau commutatif E. Un élément de E est dit **entier** sur R s'il annule un polynôme unitaire de $R[X]$. La **clôture intégrale de R dans E** est l'ensemble des éléments de E qui sont entiers sur R. Si tout élément de E est entier sur R, nous disons que E est une **extension entière** de R ou simplement qu'il est **entier sur** R. Si R est égal à la clôture intégrale de R dans E, nous disons que R est **intégralement clos dans** E. Si R est un corps, le mot *entier* dans les définitions précédentes peut être remplacé par le mot **algébrique**. Nous allons montrer que la clôture intégrale de R dans E est un sous-anneau de E. Nous établissons tout d'abord un lemme.

Lemme 1.1. *Soient $R \subseteq E$ des anneaux commutatifs. Si $\alpha \in E$ annule un polynôme unitaire f de degré n sur R, alors l'anneau $R[\alpha]$ est engendré par $1, \alpha, \ldots, \alpha^{n-1}$ comme R-module.*

Démonstration. Si $\beta \in R[\alpha]$, on a $\beta = g(\alpha)$ pour un $g \in R[X]$. D'après l'algorithme de division (théorème II.5.2), on a des polynômes q et $r \in R[X]$ tels que $\deg r \leqslant n-1$ et $g = qf + r$. Alors $\beta = g(\alpha) = r(\alpha)$ est une combinaison R-linéaire de $1, \alpha, \ldots, \alpha^{n-1}$. □

Rappelons que l'on dit qu'un R-module M est **fidèle** lorsque $rM = 0$ implique $r = 0$.

Théorème 1.2. *Soient E un anneau commutatif, R un sous-anneau de E, $n \in \mathbb{N}^*$ et $\alpha \in E$. Les propriétés suivantes sont équivalentes.*

(i) *α annule un polynôme unitaire de degré n sur R.*

(ii) *$R[\alpha]$ est engendré par n éléments comme R-module.*

(iii) *Il existe un sous-R-module fidèle M de E, engendré par n éléments, tel que $\alpha M \subseteq M$.*

Démonstration. Supposons (i), alors $R[\alpha]$ est engendré par $1, \alpha, \ldots, \alpha^{n-1}$. Supposons (ii), alors $M = R[\alpha]$ vérifie (iii). Supposons que (iii) est vérifié et que $m_1, \ldots, m_n$ engendrent M. Écrivons $\alpha m_j = \sum r_{ij} m_i$ avec des $r_{ij} \in R$. Soit f le polynôme caractéristique de la matrice $\{r_{ij}\}$. Alors $f(\alpha) m_j = 0$ pour chaque j d'après le lemme II.7.6, donc $f(\alpha) = 0$ parce que M est fidèle. □

Corolaire 1.3. *Si β annule un polynôme unitaire de degré n sur R et si $\alpha \in R[\beta]$, alors α annule un polynôme unitaire de degré n sur R.*

Démonstration. Appliquer le théorème 1.2 avec $M = R[\beta]$. □

Corolaire 1.4. *Si α est entier sur R et si β est entier sur $R[\alpha]$, alors $R[\alpha, \beta]$ est entier sur R. Donc les éléments de E entiers sur R forment un sous-anneau de E.*

Démonstration. D'après le théorème 1.2, $R[\alpha]$ est un R-module de type fini, et $R[\alpha, \beta]$ est un $R[\alpha]$-module de type fini. D'après le théorème II.4.3, $R[\alpha, \beta]$ est un R-module (fidèle) de type fini, donc le théorème 1.2 dit que $R[\alpha, \beta]$ est entier sur R. □

Corolaire 1.5. *Soient $R \subseteq E \subseteq F$ des anneaux commutatifs avec E entier sur R. Alors tout élément de F entier sur E est entier sur R. Si E est une extension de type fini de R, alors E est un R-module de type fini.*

Démonstration. Démontrons d'abord le second point. Soit $E = R[a_1, \ldots, a_n]$. Alors $R[a_1]$ est un R-module de type fini d'après le lemme 1.1, et E est un $R[a_1]$-module de type fini par récurrence sur n. Donc E est un R-module de type fini d'après le théorème II.4.3. Pour démontrer le premier point, nous pouvons supposer que E est de type fini. Si $\alpha \in F$ est entier sur E, il y a un sous-E-module fidèle de type fini M de F tel que $\alpha M \subseteq M$. Mais M est un R-module de type fini d'après le théorème II.4.3, donc α est entier sur R. □

Le corolaire 1.5 montre que la clôture intégrale de R dans E est intégralement close dans E. Un anneau intègre discret est dit **intégralement clos** s'il est intégralement clos dans son corps de fractions.

Théorème 1.6. *Tout anneau intègre à pgcd est intégralement clos.*

Démonstration. Tout élément du corps de fractions de R peut être écrit sous la forme u/v avec u et v premiers entre eux dans R. Soit $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ un polynôme unitaire de $R[X]$ tel que $f(u/v) = 0$. Alors $v^n f(u/v) = 0$ donc $v|u^n$. Comme u et v sont premiers entre eux, v divise u, i.e. $u/v \in R$. □

Rappelons qu'un anneau commutatif E est impotent si

(i) $a^n = 0$ avec $n > 0$ implique $a = 0$, et

(ii) $a^2 = a$ implique $a = 0$ ou $a = 1$.

La condition (i), qui est équivalente à « $a^2 = 0$ implique $a = 0$ », dit que l'anneau E est réduit. La condition (ii) dit que les seuls éléments idempotents de E sont 0 et 1. Tout corps de Heyting est un anneau impotent. Nous allons montrer que si E est une extension impotente d'un corps discret k, alors les éléments de E algébriques sur k forment un corps discret. Comme les nombres complexes forment un corps de Heyting, cela implique que les nombres algébriques forment un corps discret.

Lemme 1.7. *Soient a et b des éléments d'un anneau impotent tels que $a+b = 1$ et $ab = 0$. Ou bien $a = 0$ et $b = 1$, ou bien $a = 1$ et $b = 0$.*

Démonstration. Multiplions l'équation $a+b = 1$ par b ; vu l'égalité $ab = 0$, nous avons $b^2 = b$. Comme l'anneau est impotent, cela donne $b = 0$ ou $b = 1$. □

Lemme 1.8. *Soient E un anneau impotent, k un sous-anneau de E et $\alpha \in E$. Si $f, g \in k[X]$ sont étrangers et si $f(\alpha)g(\alpha) = 0$, alors $f(\alpha)$ ou $g(\alpha)$ est inversible, donc ou bien $g(\alpha) = 0$ ou bien $f(\alpha) = 0$.*

Démonstration. Comme f et g sont étrangers, on a $s, t \in k[X]$ tels que $s(\alpha)f(\alpha) + t(\alpha)g(\alpha) = 1$. D'après le lemme 1.7 on a $s(\alpha)f(\alpha) = 1$ ou $t(\alpha)g(\alpha) = 1$. Par suite $f(\alpha)$ ou $g(\alpha)$ est inversible, et l'autre est nul. □

Théorème 1.9. *Soient E un anneau impotent et k un sous-corps discret de E. Si $\alpha \in E$ est algébrique sur k, $k[\alpha]$ est un corps discret. Par suite l'ensemble des éléments de E algébriques sur k est un corps discret.*

Démonstration. Soit $\gamma \in k[\alpha]$. Nous pouvons supposer que $k[\alpha] = E$, et nous allons montrer que γ est inversible ou nul. D'après le corolaire 1.4, γ est algébrique sur k. On a donc un polynôme unitaire $g \in k[X]$ tel que $g(\gamma) = 0$. Écrivons $g(X) = X^m h(X)$ avec $h(0) \neq 0$. D'après le lemme 1.8, ou bien γ^m est inversible, et donc γ est inversible, ou bien $\gamma^m = 0$, et $\gamma = 0$ parce que E est impotent. □

Corolaire 1.10. *Soient $k \subseteq K = k(x_1, \ldots, x_n)$ des corps discrets. Alors les propriétés suivantes sont équivalentes.*

(i) *K est algébrique sur k,*

(ii) *$x_1, \ldots, x_n$ sont algébriques sur k,*

(iii) *K est un espace vectoriel de type fini sur k.*

Dans ce cas on a

(iv) $K = k[x_1, \ldots, x_n]$.

Démonstration. Clairement (i) implique (ii).

Supposons (ii). Pour démontrer (iii), il suffit de démontrer que $k(x_1, \ldots, x_i)$ est un espace vectoriel de type fini sur $k(x_1, \ldots, x_{i-1})$ pour chaque i. Comme x_i est algébrique sur k, il est entier sur $k(x_1, \ldots, x_{i-1})$; le résultat découle alors du théorème 1.2.

Le théorème 1.2 montre que (i) découle de (iii). Enfin supposons (i). Alors $k[x_1, \ldots, x_n]$ est un corps d'après le théorème 1.9, donc (iv) est vérifié. □

En fait, lorsque la condition (iv) du corolaire 1.10 est vérifiée, il en va de même pour les autres conditions ; ce résultat est parfois appelé le **Nullstellensatz faible**. Nous démontrons un résultat un peu plus fort.

Théorème 1.11. *Soient $R \subseteq S = R[x_1, \ldots, x_n]$ des anneaux commutatifs discrets avec unités détachables. Alors S est entier sur R, ou S contient un élément non nul non inversible, ou R contient un élément non nul non inversible.*

Démonstration. Il suffit de démontrer que pour chaque i, x_i est entier sur R, ou S contient un élément non nul non inversible, ou R contient un élément non nul non inversible. Notons

$$R(x_i) = \{\, fg^{-1} : f, g \in R[x_i] \text{ et } g \text{ est inversible dans } S \,\}.$$

Alors l'anneau $R(x_i)$ a ses unités détachables, donc par récurrence sur n nous pouvons supposer que S est entier sur $R(x_i)$. En prenant une puissance du produit des dénominateurs qui apparaissent dans les coefficients des polynômes unitaires annulés par les x_j sur $R(x_i)$, nous construisons un polynôme $\beta \in R[X]$ tel que $\beta(x_i)$ est inversible dans S et $\beta(x_i)x_j$ est entier sur $R[x_i]$ pour chaque j. Nous pouvons supposer que β est unitaire, ou alors que son coefficient dominant est non nul non inversible dans R. Nous pouvons supposer que x_i est inversible dans S et, en multipliant par X si nécessaire, nous pouvons supposer que β est non constant. Tout élément de S peut être multiplié par une puissance de $\beta(x_i)$ pour en faire un élément entier sur $R[x_i]$. En particulier, ou bien $1 - \beta(x_i) = 0$, auquel cas x_i est entier sur R, ou bien $1 - \beta(x_i)$ est un élément non nul non inversible de S, ou bien il existe un m tel que l'élément $\alpha(x_i) = \beta(x_i)^m(1 - \beta(x_i))^{-1}$ est entier sur $R[x_i]$, et donc est une racine

d'un polynôme unitaire $f(X) \in R[x_i][X]$. En multipliant $f(\alpha(x_i)) = 0$ par $(1-\beta(x_i))^d$, où d est le degré de f, nous obtenons

$$\beta(x_i)^{md} = g(x_i)(1-\beta(x_i)).$$

Comme $\beta(X)^{md}$ et $1-\beta(X)$ sont étrangers dans $R[X]$, on a $(1-\beta(x_i))h(x_i) = 1$ pour un $h \in R[X]$, et donc x_i annule le polynôme $(1-\beta(X))h(X) - 1$. Ou bien le coefficient dominant de ce polynôme est un élément non nul non inversible de R, ou bien x_i est entier sur R. □

Voici maintenant la forme la plus familière du Nullstellensatz faible.

Corolaire 1.12. *Soient $k \subseteq K = k[x_1, \ldots, x_n]$ des corps discrets. Alors K est algébrique sur k.*

Démonstration. Les corps discrets K et k n'ont pas d'éléments non nuls non inversibles, donc K est algébrique sur k d'après le théorème 1.11. □

Si E est un anneau commutatif qui contient un corps discret k et qui est de dimension finie sur k, tout $\alpha \in E$ est entier sur k d'après le théorème 1.2. Donc $k[\alpha]$ est un espace vectoriel de type fini sur k parce qu'il est engendré par $1, \alpha, \ldots, \alpha^{n-1}$ pour un certain $n > 0$. Comme nous pouvons décider si les éléments $1, \alpha, \ldots, \alpha^m$ sont linéairement indépendants ou pas, nous pouvons construire un polynôme unitaire $f \in k[X]$ de degré minimum tel que $f(\alpha) = 0$. Si $g(\alpha) = 0$ pour un $g \in k[X]$, alors f divise g. En effet, le reste r de la division de g par f est nul parce qu'il vérifie $r(\alpha) = 0$ et $\deg(r) < \deg(f)$. Ainsi $k[\alpha] \simeq k[X]/(f(X))$. Le polynôme f est appelé le **polynôme minimal** de α sur k.

En particulier, lorsqu'un anneau $k[\alpha]$ est un espace vectoriel de dimension finie sur un corps discret k, l'élément α possède un polynôme minimal f et $k[\alpha] \simeq k[X]/(f(X))$.

Si E est impotent, le théorème 1.13 montre que f est irréductible.

Théorème 1.13. *Soient E un anneau commutatif, k un sous-corps discret de E et $\alpha \in E$. Si α annule un polynôme f irréductible sur k, alors $k[\alpha]$ est un k-espace vectoriel de dimension finie et f est le polynôme minimal de α sur k. Si E est impotent et si $k[\alpha]$ est contenu dans un sous-k-espace vectoriel de dimension finie de E, alors α annule un polynôme irréductible sur k.*

Démonstration. Si α annule un polynôme irréductible de degré n sur k, alors $1, \alpha, \ldots, \alpha^{n-1}$ est une base de $k[\alpha]$ sur k. Inversement, supposons que E est impotent et que V est un sous-k-espace vectoriel de dimension finie de E qui contient $k[\alpha]$. Alors le théorème 1.2 nous dit que α est entier sur k et et que $k[\alpha]$ est un k-espace vectoriel de type fini, donc $k[\alpha]$ est de dimension finie d'après le corolaire II.6.3. Soit alors f le polynôme minimal de α sur k. Montrons qu'il est irréductible. Notons que d'après le théorème 1.9, l'anneau $k[\alpha]$ est un corps discret. Donc, si $f = gh$, ou bien $g(\alpha) = 0$, ou bien $h(\alpha) = 0$. Mais $g(\alpha) = 0$ implique que g est un multiple de f. Ainsi f est irréductible. □

Exercices

1. Soient $R \subseteq E$ des anneaux commutatifs avec E entier sur R et soit I un idéal de R. Montrer que si $\alpha \in IE$, alors il existe des éléments $r_i \in I^i$ tels que $\alpha^n + r_1\alpha^{n-1} + \cdots + r_n = 0$. En déduire que $R \cap IE \subseteq \sqrt{I}$ [1].
2. Soit K une extension finie de $\mathbb{Q}$. Montrer qu'un élément de K est entier sur $\mathbb{Z}$ si, et seulement si, son polynôme minimal sur $\mathbb{Q}$ a tous ses coefficients dans $\mathbb{Z}$. Montrer que la clôture intégrale de $\mathbb{Z}$ dans $\mathbb{Q}(i)$ est $\mathbb{Z}[i]$ (l'anneau des entiers de Gauss est la clôture intégrale de $\mathbb{Z}$ dans le corps des nombres de Gauss).
3. Dans un anneau arbitraire, montrer que si $a = 0$ chaque fois que $a^2 = 0$, alors $a = 0$ chaque fois que $a^n = 0$ pour un $n > 0$.
4. Montrer que les corps de Heyting et les corps par négation sont des anneaux impotents.
5. Soient k l'anneau des entiers modulo 2, $E = k[X]/(X^2)$ et $F = k[X]/(X^2 - X)$. Montrer que E et F sont algébriques sur k, mais que ce ne sont pas des corps. Pourquoi le théorème 1.9 ne s'applique-t-il pas ?
6. Soit k un sous-corps discret d'un anneau commutatif E. Si $\alpha \in E$ annule un polynôme irréductible sur k de degré n, montrer que $1, \alpha, \ldots, \alpha^{n-1}$ est une base de $k[\alpha]$ sur k.
7. Notons $\mathbb{Z}_{(2)}$ l'anneau des entiers localisé en 2. Utiliser l'inclusion $\mathbb{Z}_{(2)} \subseteq \mathbb{Q} = \mathbb{Z}_{(2)}[1/2]$ pour montrer que la condition « ou bien R contient un élément non nul non inversible » ne peut pas être omise dans la conclusion du Nullstellensatz faible. Utiliser la même inclusion pour construire un exemple brouwerien où le Nullstellensatz faible est en défaut parce que R n'a pas ses unités détachables.

2 Indépendance algébrique et bases de transcendance

Soient $k \subseteq K$ des anneaux commutatifs. Les éléments $x_1, \ldots, x_n$ de K sont dits **algébriquement indépendants** sur k si pour tout $f \in k[X_1, \ldots, X_n]$, $f(x_1, \ldots, x_n) = 0$ implique $f = 0$. Si k est discret, les éléments $x_1, \ldots, x_n$ sont dits **algébriquement dépendants** sur k s'il existe un f non nul dans $k[X_1, \ldots, X_n]$ tel que $f(x_1, \ldots, x_n) = 0$; dans ce cas, $x_1, \ldots, x_n$ sont algébriquement indépendants si, et seulement si, ils ne sont pas algébriquement dépendants.

Si K est discret et si S est un sous-ensemble fini de K, alors nous disons que l'ensemble S est **algébriquement dépendant**, ou **algébriquement indépendant** si ses éléments (ordonnés d'une manière ou d'une autre) le sont.

1. **NdT.** Ce résultat est une version constructive du théorème « lying over » pour les extensions entières en mathématiques classiques.

Nous pouvons ramener la notion de dépendance algébrique à celle d'éléments algébriques de la manière suivante.

Théorème 2.1. *Si $k \subseteq K$ sont des corps discrets, alors $x_1, \dots, x_n \in K$ sont algébriquement dépendants sur k si, et seulement si, il existe un i tel que x_i est algébrique sur $k(x_1, \dots, x_{i-1})$.*

Démonstration. Supposons que x_i annule un polynôme non nul $f(X_i)$ à coefficients dans $k(x_1, \dots, x_{i-1})$. Alors on a des polynômes non nuls $g \in k[X_1, \dots, X_i]$ et $h \in k[X_1, \dots, X_{i-1}]$ tels que

$$f(X_i) = g(x_1, \dots, x_{i-1}, X_i)/h(x_1, \dots, x_{i-1}) \text{ et } g(x_1, \dots, x_i) = 0.$$

Donc $x_1, \dots, x_i$, et aussi $x_1, \dots, x_n$, sont algébriquement dépendants sur k.

Inversement, supposons que $x_1, \dots, x_n$ sont algébriquement dépendants sur k. Alors il existe un polynôme g non nul dans $k[X_1, \dots, X_n]$ tel que $g(x_1, \dots, x_n) = 0$. Alors $g(x_1, \dots, x_{n-1}, X_n)$ est un polynôme en X_n à coefficients dans $k[x_1, \dots, x_{n-1}]$ annulé par x_n. Si $g(x_1, \dots, x_{n-1}, X_n) = 0$, alors tout coefficient non nul de g, où g est vu comme un polynôme en X_n à coefficients dans $k[X_1, \dots, X_{n-1}]$, donne une relation de dépendance algébrique pour $x_1, \dots, x_{n-1}$, et nous terminons par récurrence sur n. Si $g(x_1, \dots, x_{n-1}, X_n) \neq 0$, alors x_n est algébrique sur $k(x_1, \dots, x_{n-1})$. □

Nous obtenons comme corolaire le **lemme d'échange** pour la dépendance algébrique.

Corolaire 2.2. *Soient $k \subseteq K$ des corps discrets et $x, y \in K$. Si x est algébrique sur $k(y)$, ou bien y est algébrique sur $k(x)$, ou bien x est algébrique sur k.*

Démonstration. D'après le théorème 2.1 nous savons que y, x sont algébriquement dépendants sur k, donc x, y sont algébriquement dépendants sur k. La conclusion résulte du théorème 2.1. □

Le corolaire 2.2 est l'analogue du lemme d'échange pour la dépendance linéaire des vecteurs : si x est une combinaison linéaire de $y_1, \dots, y_n$, alors ou bien x est une combinaison linéaire de $y_1, \dots, y_{n-1}$, ou bien y_n est une combinaison linéaire de $y_1, \dots, y_{n-1}$ et x (voir l'exercice 2).

Théorème 2.3. *Soient $k \subseteq K$ des corps discrets. Soient S et T des sous-ensembles finis de K tels que K est algébrique sur $k(S)$. Ou bien T est algébriquement dépendant sur k, ou bien nous pouvons trouver une partition de S en sous-ensembles finis S_0 et S_1 avec $\#S_0 = \#T$ et K algébrique sur $k(T \cup S_1)$.*

Démonstration. Nous procédons par récurrence sur $m = \#(T \backslash S)$. Si $m = 0$, nous pouvons prendre $S_0 = T$. Sinon considérons un $x \in T \backslash S$. Notons $S = \{s_1, \dots, s_k\}$ avec les éléments de $T \cap S$ en premier. Une application répétée du

corolaire 2.2 à x et $k(s_1, \ldots, s_j)$ pour $j = k, k-1, \ldots$ nous donne le résultat suivant : ou bien on voit que x est algébrique sur k, et alors T est algébriquement dépendant, ou bien on trouve un élément s_i algébrique sur $k(s_1, \ldots, s_{i-1}, x)$ avec x algébrique sur $k(s_1, \ldots, s_i)$. Si $s_i \in T$, T est algébriquement dépendant. Si $s_i \notin T$, on remplace s_i par x dans S et on termine par récurrence sur m. □

Soient $k \subseteq K$ des corps discrets, et soit B un sous-ensemble fini de K qui est algébriquement indépendant sur k. L'extension $k \subseteq k(B)$ est dite **purement transcendante**, et si K est algébrique sur $k(B)$, nous disons que B une **base de transcendance** de K sur k. Une conséquence immédiate du théorème 2.3 est la suivante.

Corolaire 2.4. *Deux bases de transcendance d'un corps discret K sur un corps discret k ont le même nombre d'éléments.*

Si B est une base de transcendance de K sur k, alors le nombre d'éléments de B est appelé le **degré de transcendance de K sur k**, et on le note $\mathrm{trdeg}_k K$. Le degré de transcendance d'une extension algébrique est 0, avec l'ensemble vide pour base de transcendance.

Une conséquence purement constructive du théorème 2.3 est que nous pouvons décider la dépendance algébrique lorsque nous avons une base de transcendance.

Corolaire 2.5. *Soit K un corps discret de degré de transcendance n sur un sous-corps k. Tout sous-ensemble fini de K est algébriquement dépendant, ou algébriquement indépendant, sur k.*

Démonstration. Soient S une base de transcendance de K de cardinalité n et T un sous-ensemble fini de K. D'après le théorème 2.3, ou bien T est algébriquement dépendant, ou bien nous pouvons agrandir T en un ensemble T' de cardinalité n tel que K est algébrique sur $k(T')$. Si T' était algébriquement dépendant, nous pourrions construire un ensemble T'' de cardinalité $n-1$ avec K algébrique sur $k(T'')$; mais cela contredirait le théorème 2.3 parce que S est algébriquement indépendant. □

Lemme 2.6. *Soit K un corps discret de degré de transcendance n sur un sous-corps k. Si K est algébrique sur $k(S)$ pour un sous-ensemble $S \subseteq K$, alors S contient une base de transcendance de K sur k. Si S est un sous-ensemble fini de K algébriquement indépendant sur k, alors S peut être étendu en une base de transcendance.*

Démonstration. Choisissons un sous-ensemble fini B de S tel que tout élément de la base de transcendance, et donc K lui-même, est algébrique sur $k(B)$. D'après le corolaire 2.5, nous pouvons décider si B est algébriquement dépendant ou pas. Si B est algébriquement indépendant, alors B est la base de

transcendance cherchée. Si B est algébriquement dépendant, alors on a un $b \in B$ tel que K est algébrique sur $k(B \setminus \{b\})$, auquel cas nous terminons par récurrence sur $\#B$.

Supposons maintenant que S est un ensemble fini algébriquement indépendant. D'après le théorème 2.3 nous pouvons agrandir S en un sous-ensemble fini S' de K de cardinalité n tel que K est algébrique sur $k(S')$. D'après la première partie de ce lemme, S' contient une base de transcendance ; donc S' est une base de transcendance d'après le corolaire 2.4. □

Théorème 2.7. *Soient $k \subseteq K \subseteq L$ des corps discrets. Si deux des trois extensions $k \subseteq L$, $K \subseteq L$ et $k \subseteq K$ ont des bases de transcendance finies, alors il en va de même pour la troisième, et l'on a*

$$\operatorname{trdeg}_k L = \operatorname{trdeg}_K L + \operatorname{trdeg}_k K.$$

Démonstration. Si B_0 est une base de transcendance de K sur k, et B_1 une base de transcendance de L sur K, on vérifie facilement que $B_0 \cup B_1$ est une base de transcendance de L sur k. Si B_0 est une base de transcendance de K sur k, et B_1 est une base de transcendance de L sur k, alors, d'après le théorème 2.3, nous pouvons supposer que $B_0 \subseteq B_1$, et donc $B_1 \setminus B_0$ est une base de transcendance de L sur K.

Finalement, supposons que B_0 est une base de transcendance de L sur K et que B_1 est une base de transcendance de L sur k. Nous pouvons trouver un sous-ensemble fini S de K tel que chaque élément de B_1, et par suite L, est algébrique sur $k(S \cup B_0)$. D'après le théorème 2.3, nous pouvons supposer que S est algébriquement indépendant sur k. Si $x \in K$, par une application répétée du corolaire 2.2 nous voyons que x est algébrique sur $k(S)$, parce que B_0 est algébriquement indépendant sur K. □

Soient k un corps discret et X une indéterminée. Le **théorème de Lüroth** dit que tout corps intermédiaire entre k et $k(X)$ est de la forme $k(z)$ pour un $z \in k(X)$. Nous ne pouvons pas espérer démontrer le théorème de Lüroth même pour les sous-corps détachables de $k(X)$. Mais le théorème de Lüroth est valide pour un sous-corps détachable de type fini, et un argument trivial en mathématiques classiques donne alors le théorème de Lüroth classique. Nous démontrons d'abord que si $t \in k(X) \setminus k$, alors $k(X)$ est de dimension finie sur $k(t)$.

Lemme 2.8. *Soient k un corps discret, X une indéterminée, et $t \in k(X) \setminus k$. Si $t = u(X)/v(X)$, avec u et v des polynômes premiers entre eux dans $k[X]$, alors $p(Y) = tv(Y) - u(Y)$ est un polynôme irréductible sur $k(t)$ annulé par X.*

Démonstration. Notez que $p(Y) \neq 0$ parce que $t \notin k$. Clairement $p(X) = 0$, donc $k(X)$ est algébrique sur $k(t)$. Ainsi t est transcendant (i.e. algébriquement indépendant) sur k.

D'après le lemme de Gauss, il suffit de démontrer que $p(Y)$ est irréductible dans $k[t][Y]$. Supposons que $p = gh$ avec g et $h \in k[t][Y]$. Comme le t-degré de p est 1, g ou h est de t-degré 0, disons g. Donc $g \in k[Y]$. Comme g divise $p(Y) = tv(Y) - u(Y)$, et comme u et v sont premiers entre eux, on a $g \in k$. Donc $p(Y)$ est irréductible sur $k(t)$. □

Si K est un sous-corps de $k(X)$ et si $t \in K \backslash k$, le lemme 2.8 dit que $k(X)$ est de dimension finie sur $k(t)$. Comme, en mathématiques classiques, cela implique immédiatement que K est de dimension finie sur $k(t)$, le théorème de Lüroth classique est une conséquence directe du lemme 2.8 et du théorème suivant.

Théorème 2.9. *Soient k un corps discret, X une indéterminée sur k, et $\alpha_1, \ldots, \alpha_n \in k(X)$. Alors $k(\alpha_1, \ldots, \alpha_n) = k(z)$ pour un $z \in k(X)$.*

Démonstration. Soit $K = k(\alpha_1, \ldots, \alpha_n)$. Nous pouvons supposer que $\alpha_1 \notin k$. D'après le lemme 2.8, le corps $k(X)$ est de dimension finie sur $k(\alpha_1)$, donc $k(X)$ est de dimension finie sur $K = k(\alpha_1)[\alpha_2, \ldots, \alpha_n]$. Ainsi X annule un polynôme irréductible $f \in K[Y]$. Comme X est transcendant sur k, un coefficient z de f n'est pas dans k. Nous allons montrer que $k(z) = K$.

Écrivons $z = u(X)/v(X)$ avec u et v des polynômes premiers entre eux dans $k[X]$, et posons $p(Y) = zv(Y) - u(Y)$. Le lemme 2.8 dit que $p(Y)$ est irréductible sur $k(z)$. Nous montrons maintenant que $\deg p = \deg f$, d'où il suit que $k(z) = K$, car $k(z) \subseteq K$.

Pour un polynôme arbitraire $q \in k(X)[Y]$, notons q^* un polynôme primitif de $k[X][Y]$ tel que $q/q^* \in k(X)$; en particulier on a $p^* = u(X)v(Y) - v(X)u(Y)$. Soit $m = \deg_X f^*$ le plus grand des X-degrés des coefficients de f^*. Comme f est un polynôme unitaire, $\deg_X p^* = \deg_Y p^* = \max(\deg u, \deg v) \leqslant m$. Du fait que $f(X) = 0$ et f est irréductible dans $K[Y]$, nous pouvons écrire $p = fg$ avec $g \in K[Y]$. Alors $p^*(Y) = df^*(Y)g^*(Y)$ pour un $d \in k$, donc $\deg_X p^* = m$ et $\deg_X g^* = 0$. Par suite $g^*(Y) \in k[Y]$; mais $g^*(Y)$ divise $p(Y)$, qui est irréductible sur $k(z)$, donc $g^*(Y) \in k$. Ainsi $\deg_Y p^* = \deg_Y f^*$, donc $\deg p = \deg f$. □

Nous terminons cette section avec la construction d'un exemple qui donnera un exemple brouwerien d'un corps séparablement factoriel mais pas factoriel, et qui montrera la nécessité des hypothèses de séparabilité dans les théorèmes VII.1.1 et VII.2.4.

Théorème 2.10. *Soit F un corps discret de caractéristique 2, et soit $K = F(b, s, t)$, où b, s et t sont des indéterminées. Soient $a = bs^2 + t^2$ et $k = F(a, b)$. Alors k est algébriquement clos dans K.*

Démonstration. Notez que K est de degré de transcendance 3 sur F, et que $t^2 \in F(a, b, s) = k(s)$, donc K est algébrique sur $k(s)$. Par suite a et b sont algébriquement indépendants sur F, et s est transcendant sur k. D'après les

théorèmes 1.6 et IV.4.7, l'anneau $F[a,b]$ est intégralement clos dans k, et par suite dans $k(s)$.

Maintenant soit $\theta \in K$ un élément algébrique sur k, et soit $f \in F[a,b,X]$ un polynôme non nul tel que $f(\theta) = 0$. Soient n le degré de f et $r \in F[a,b]$ le coefficient dominant de f. Le polynôme $r^{n-1} f\,(X/r)$ est unitaire à coefficients dans $F[a,b]$, donc $r\theta$ est entier sur $F[a,b]$. Par suite $w = (r\theta)^2 \in k(s)$ est aussi entier sur $F[a,b]$, donc $w \in F[a,b]$. Écrivons $r\theta = p/q + (u/v)t$ avec $p,q,u,v \in F[a,b,s]$. Alors $w = p^2/q^2 + (u^2/v^2)(a + bs^2)$, car notre corps est de caractéristique 2, ainsi

$$p^2v^2 + u^2q^2(a + bs^2) = wq^2v^2. \qquad (*)$$

Si $u = 0$, alors $r\theta = p/q$ est entier sur $F[a,b]$ et appartient à $k(s)$, donc $r\theta \in F[a,b]$, et par suite $\theta \in k$ comme voulu. Sinon, soit n le plus grand exposant d'une puissance de s qui divise u^2q^2. Le coefficient de s^n dans le côté gauche de l'équation $(*)$ contient seulement des puissances paires de b et il est non nul parce qu'il contient une puissance impaire de a. Par suite w (qui est dans $F[a,b]$) et donc aussi wq^2v^2, contient seulement des puissances paires de b. Mais le coefficient de s^{n+2} dans le côté gauche de $(*)$ contient une puissance impaire de b. Donc $u \neq 0$ est impossible. □

Exercices

1. Soient $k \subseteq E$ des corps discrets, S un sous-ensemble fini de E, et K un sous-corps de E algébrique sur k. Montrer que S est algébriquement dépendant sur K si, et seulement si, il est algébriquement dépendant sur k.

2. Une **génératrice** [1] sur un ensemble discret S est une fonction s depuis les sous-ensembles finis de S vers les sous-ensembles de S telle que

   (i) si $A \subseteq B$, alors $sA \subseteq sB$,

   (ii) $A \subseteq sA$,

   (iii) si B est un sous-ensemble fini de sA, alors $sB \subseteq sA$,

   (iv) si $x \in s(A \cup \{y\})$, alors $x \in sA$ ou $y \in s(A \cup \{x\})$.

   Soient $k \subseteq K$ des corps discrets, et pour un sous-ensemble fini A de K, définissons $sA = \{\, x \in K : x \text{ est algébrique sur } k(A) \,\}$. Soit V un espace vectoriel discret sur le corps discret k, et pour un sous-ensemble A de V, définissons sA comme le sous-espace de V engendré par A. Montrer que nous obtenons une génératrice dans chaque cas. Développer la théorie de la section précédente dans ce contexte plus général.

1. **NdT.** Span operation.

3. Donner un exemple brouwerien d'un corps discret K avec un sous-corps détachable k tel que $K = k(\theta)$ alors que K n'a pas de base de transcendance sur k.
4. Construire un exemple brouwerien d'un sous-corps détachable de $\mathbb{Q}(X)$ qui n'est pas de la forme $\mathbb{Q}(z)$.
5. Soient F un corps discret de caractéristique 2, b et t des indéterminées, et P une assertion. On définit

$$k = \{\, x \in F(b) : x \in F(b^2) \text{ ou } P \,\} \text{ et}$$
$$K = \{\, x \in k(t^2 + bt) : x \in k(t^4 + b^2t^2) \text{ ou } P \,\}.$$

Montrer que K est un sous-corps détachable de $k(t)$, qui contient proprement k, et que l'on a $K = k(z)$ pour un z si, et seulement si, P ou non P.

3 Corps de décomposition et clôtures algébriques

Soit f un polynôme non constant sur un corps discret k ; nous voulons construire un corps discret K qui contient k et tel que f a une racine dans K. Si nous nous contentons d'un *anneau* discret K nous prenons pour K le quotient $k[X]/(f)$: si α est l'image de X dans K on a $K = k[\alpha]$ et α est une racine de f. Cependant, K est un *corps* seulement dans le cas où f est irréductible.

Théorème 3.1. *Soit f un polynôme non constant sur un corps discret k. Soit $K = k[X]/(f)$, et notons α l'image de X dans K. Alors $K = k[\alpha]$ est un anneau commutatif discret qui contient k, et $f(\alpha) = 0$. En outre K est un corps discret si, et seulement si, f est irréductible.*

Démonstration. L'algorithme de division (théorème II.5.2) nous permet de décider si un polynôme de $k[X]$ est ou n'est pas divisible par f, donc K est discret. Comme f est non constant, k s'envoie sur une copie isomorphe de lui-même dans K, que nous pouvons identifier avec k. Alors clairement $K = k[\alpha]$ et $f(\alpha) = 0$.

Si K est un corps et si $f = gh$, alors $gh = 0$ dans K, donc $g = 0$ dans K ou $h = 0$ dans K. Donc $f|g$ ou $f|h$ et par suite f est irréductible. Inversement, si f est irréductible et si g est un élément arbitraire de K, alors, d'après le corolaire II.5.7, on a s et $t \in k[X]$ tels que $sf + tg$ divise à la fois f et g. Comme f est irréductible, nous pouvons supposer que $sf + tg$ est égal à f ou à 1. Si $sf + tg = f$ alors $f|g$, donc $g = 0$ dans K ; si $sf + tg = 1$, alors t est l'inverse de g dans K. □

Si f n'est pas irréductible, il est plus difficile de construire un corps extension de k dans lequel f a une racine : la technique classique et de travailler avec un facteur irréductible de f, mais il se peut que nous ne soyons pas capable d'en trouver un (voir l'exemple IV.2.2). En fait, nous ne pouvons pas toujours construire une telle extension (exercice 1). Cependant, si k est dénombrable, nous pouvons construire un tel corps en construisant un idéal maximal détachable M dans $k[X]$ qui contient f, sans construire pour autant un générateur de M.

Lemme 3.2. *Soit R un anneau commutatif dénombrable fortement discret. Si I est un idéal propre de type fini de R, il est contenu dans un idéal maximal détachable.*

Démonstration. Soit $r_1, r_2, \ldots$ une énumération de R. Nous allons construire une suite croissante d'idéaux de type fini I_j démarrant avec $I_1 = I$. Si I_j a été construit, nous construisons I_{j+1} comme suit : si $1 \in I_j + Rr_j$ nous posons $I_{j+1} = I_j$, sinon nous posons $I_{j+1} = I_j + Rr_j$. Soit M la réunion des idéaux I_j. Comme $r_j \in M$ si, et seulement si, $r_j \in I_{j+1}$, l'idéal M est détachable. Si $r_j \notin M$, alors $r_j \notin I_{j+1}$ donc $1 \in I_j + Rr_j \subseteq M + Rr_j$, donc M est maximal. □

Théorème 3.3. *Soient k un corps discret dénombrable et f un polynôme non constant de $k[X]$. Alors on peut construire un corps discret dénombrable E qui contient k et un $\alpha \in E$ tel que $f(\alpha) = 0$.*

Démonstration. Les idéaux de type fini de $k[X]$ sont principaux d'après l'algorithme d'Euclide, donc détachables d'après l'algorithme de division. Ainsi le lemme 3.2 s'applique et nous pouvons construire un idéal maximal détachable M de $k[X]$ qui contient f. La solution est donnée alors par $E = k[X]/M$ et α est l'image de X dans E. □

Soit f un polynôme unitaire sur un corps k. Un corps K extension de k est appelé un **corps de décomposition** pour f sur k si

$$f(X) = (X - \alpha_1) \cdots (X - \alpha_n)$$

et $K = k[\alpha_1, \ldots, \alpha_n]$. Notez que K est dénombrable si k est dénombrable.

Théorème 3.4. *Soit $f(X)$ un polynôme non nul sur un corps discret dénombrable k. Alors nous pouvons construire un corps de décomposition discret pour f sur k.*

Démonstration. Application répétée du théorème 3.3. □

Les corps de décomposition sur des corps dénombrables peuvent être utilisés quand on travaille avec un corps discret arbitraire k de la manière suivante. Si f est un polynôme de $k[X]$, on considère le sous-corps k_0 de k engendré par les coefficients de f. Comme k_0 est dénombrable, f possède un corps de

décomposition sur k_0. Nous utilisons alors les zéros de f dans ce corps de décomposition pour obtenir des informations sur f comme polynôme de $k[X]$.

En mathématiques classiques, le corps de décomposition pour un polynôme sur un corps k est unique en ce sens que deux corps de décomposition arbitraires sont isomorphes sur k. Constructivement, il se peut que nous ne soyons pas capables de construire un tel isomorphisme (voir l'exercice 2). Nous avons des problèmes même si f est irréductible parce que, après avoir ajouté un zéro α de f sur k, il se peut que nous ne soyons pas capables de trouver les facteurs irréductibles de f dans $k[\alpha][X]$ (voir l'exercice 3).

Un corps Ω est **algébriquement clos** si tout polynôme unitaire de degré au moins 1 dans $\Omega[X]$ a une racine dans Ω. Cela implique que tout polynôme unitaire de $\Omega[X]$ se décompose en un produit de facteurs linéaires sur Ω. Si un corps algébriquement clos Ω est algébrique sur un sous-corps k, alors Ω est appelé une **clôture algébrique** de k. D'un point de vue constructif, il se peut que nous ne soyons pas capables d'immerger un corps discret dans un corps algébriquement clos, ou que nous construisions deux clôtures algébriques sans être capables de construire un isomorphisme entre elles. Cependant, pour les corps discrets dénombrables nous pouvons construire une clôture algébrique.

Théorème 3.5. *Soit k un corps discret dénombrable. Alors il existe une clôture algébrique discrète de k.*

Démonstration. Soit $f_1, f_2, \ldots$ un énumération des polynômes non constants de $k[X]$. Soit k_1 un corps de décomposition discret pour f_1 sur k. Si nous avons construit $k_1 \subseteq k_2 \subseteq \cdots \subseteq k_j$ nous prenons pour k_{j+1} un corps de décomposition discret de f_{j+1} sur k_j. Finalement nous définissons $\Omega = \cup k_j$, i.e. la limite directe des corps k_j. Il nous faut montrer que Ω est algébriquement clos. Soit un $f \in \Omega[X]$. D'après le théorème 3.3, nous avons un corps discret E qui contient Ω et une racine α de f. Alors α est algébrique sur k d'après le corolaire 1.5, donc il y a un polynôme $f_j \in k[X]$ tel que $f_j(\alpha) = 0$. Comme f_j est un produit de facteurs linéaires sur k_{j+1}, on en déduit que α est un élément de $k_{j+1} \subseteq \Omega$. □

Exercices

1. Déduire l'axiome du choix le plus simple du monde comme conséquence de l'assertion que si k est un corps discret et f est un polynôme non constant sur k, alors il existe un corps extension de k dans lequel f a une racine. Idée : pour un ensemble à deux éléments S, soit k_S l'anneau engendré par S sur $\mathbb{Q}$ soumis aux relations $s^2 = -1$ pour $s \in S$ et $\sum_{s\in S} s = 0$. Si T est un ensemble d'ensembles à deux éléments avec au plus un élément, on définit $k = \bigcup_{S\in T} k_S$ et l'on considère $f(X) = X^2 + 1$.
2. Soit a une suite binaire fugitive, et soit $k = \bigcup_n \mathbb{Q}(ia_n)$. Énumérer l'anneau $k[X]$ de telle manière que si $a_{2n} = 1$, alors le polynôme $X - i$

précède $X+i$, tandis que si $a_{2n+1}=1$, alors $X+i$ précède $X-i$. Utiliser cette énumération pour construire un corps de décomposition E pour le polynôme X^2+1 sur k *via* le lemme 3.2 et le théorème 3.3. Montrer que E et $\mathbb{Q}(i)$ constituent un exemple brouwerien de deux corps de décomposition pour X^2+1 sur k qui ne sont pas isomorphes sur k.

3. Construire un exemple brouwerien d'un corps k, qui se situe entre $\mathbb{Q}$ et $\mathbb{Q}[i\sqrt{3}]$, tel que le polynôme X^3-2 n'a pas un corps de décomposition unique sur k, alors même qu'il est irréductible sur k.
4. *Corps de décomposition non isomorphes.* Soient a une suite binaire fugitive et e une suite dans $\{-1,1\}$. Soit P_e l'idéal de l'anneau de polynômes $\mathbb{Q}(i)[X]$ engendré par les éléments $(iX-ne_n)a_n$.
   (i) Montrer que P_e est un idéal premier détachable.
   (ii) Montrer que $P=P_e\cap\mathbb{Q}[X]$ est un idéal premier détachable de $\mathbb{Q}[X]$, et qu'il ne dépend pas de e.
   (iii) Soit k le corps de fractions de $\mathbb{Q}[X]/P$, et soit K_e le corps de fractions de $\mathbb{Q}(i)[X]/P_e$. Notons x_e l'image de X dans K_e. Montrer que K_e est un corps de décomposition pour le polynôme Y^2+1 sur $\mathbb{Q}(x_e)\simeq k$.
   (iv) Soient $e_n=1$ et $f_n=(-1)^n$ pour tout n. Soit $\varphi\colon K_e\to K_f$ un isomorphisme. Montrer que si $\varphi(ix_e)\neq ix_f$, alors $a_n=0$ pour chaque n pair, et que si $\varphi(ix_e)\neq -ix_f$, alors $a_n=0$ pour chaque n impair.

4 Séparabilité et diagonalisabilité

Si $f=a_0+a_1X+\cdots+a_{n-1}X^{n-1}+a_nX^n$ est un polynôme sur un anneau commutatif k, la **dérivée formelle** de f est définie par

$$f'=a_1+2a_2X+\cdots+(n-1)a_{n-1}X^{n-2}+na_nX^{n-1}.$$

Un polynôme $f\in k[X]$ est **séparable sur** k s'il est étranger à sa dérivée formelle, c'est-à-dire si l'idéal de $k[X]$ engendré par f et f' contient 1. Lorsque k est un corps discret, l'algorithme d'Euclide nous permet de décider si un polynôme f est ou n'est pas séparable.

Théorème 4.1. *Soient k un anneau commutatif et $f,g\in k[X]$. Alors :*

(i) $(f+g)'=f'+g'$,
(ii) $(fg)'=f'g+fg'$,
(iii) *fg est séparable si, et seulement si, f et g sont séparables et étrangers.*

Démonstration. Le point (i) est clair. Pour démontrer le point (ii) on considère $f=aX^m$ et $g=bX^n$. On obtient

$$(fg)'=(m+n)abX^{m+n-1}=mabX^{m+n-1}+nabX^{m+n-1}=f'g+fg',$$

et le résultat général découle du point (i). Pour le point (iii) on calcule $(fg)' = f'g + fg'$. Clairement l'idéal $(fg,\ f'g + fg')$ est contenu dans chacun des idéaux (f, f'), (g, g') et (f, g). Inversement,

$$(fg, f'g + fg') \supseteq (f, f'g + fg')(g, f'g + fg') = \\ (f, f'g)(g, fg') \supseteq (f, f')(g, g')(f, g)^2. \qquad \square$$

Si un polynôme f à coefficients dans un corps discret est séparable, nous pouvons trouver des polynômes s et t à coefficients dans le corps engendré par les coefficients de f tels que $sf + tf' = 1$; en effet, l'algorithme d'Euclide utilise uniquement ces coefficients. Ainsi la notion de séparabilité des polynômes sur un corps est absolue en ce sens qu'elle ne dépend pas du corps particulier dans lequel sont considérés habiter les coefficients du polynôme. Nous pouvons caractériser la séparabilité d'un polynôme sur un corps en termes de l'absence de racines multiples.

Théorème 4.2. *Soit f un polynôme sur un corps discret, et soit k le corps engendré par les coefficients de f. Si f est séparable, il n'a jamais de racine multiple dans un corps discret qui contient k. Si f n'est pas séparable, il a une racine multiple dans un corps discret qui contient k.*

Démonstration. Nous pouvons supposer le degré de f strictement positif. Si r est une racine de f dans un corps discret qui contient k et si $f(X) = (X - r)g(X)$, alors $f'(X) = g(X) + (X - r)g'(X)$, donc $f'(r) = g(r)$. Si f est séparable, alors $s(X)f(X) + t(X)f'(X) = 1$, donc $t(r)f'(r) = 1$, et donc $g(r)$ (égal à $f'(r)$) est non nul. Inversement, soit K un corps de décomposition pour f sur k, et écrivons $f(X) = a\prod_i (X - r_i)$ avec $a \neq 0$. Si f n'est pas séparable, alors f et f' ont un facteur commun non trivial, donc une racine commune r_j. Mais $f'(r_j) = a\prod_{i\neq j}(r_j - r_i)$, donc $r_j = r_i$ pour un $i \neq j$. $\square$

Soit k un sous-corps discret d'un anneau commutatif E. Un élément de E est **séparable sur** k s'il annule un polynôme séparable de $k[X]$; l'anneau E est une **extension séparable** de k si tout élément de E est séparable sur k, et k est **séparablement clos** dans E si tout élément de E séparable sur k est dans k.

Le **corps de définition** d'un ensemble fini de matrices sur un corps est par définition le corps (dénombrable) engendré par leurs coefficients. Si des matrices sont linéairement dépendantes sur un corps discret k, alors elles sont déjà linéairement dépendantes sur leur corps de définition : en effet, si nous traitons ces matrices comme si elles étaient des vecteurs lignes, alors les lemmes III.6.8 et III.6.9 montrent que si des lignes sont indépendantes sur leur corps de définition, alors elles sont indépendantes sur k ; et des lignes sont ou bien linéairement dépendantes, ou bien linéairement indépendantes (corolaire II.6.5). En particulier, les coefficients du polynôme minimal d'une matrice sont dans le corps de définition de cette matrice, donc le polynôme minimal d'une matrice ne

dépend pas du corps particulier dans lequel sont considérées habiter les entrées de la matrice. De la même manière, si une matrice A peut être écrite comme un polynôme en une matrice B, alors le polynôme peut être choisi avec ses coefficients dans le corps de définition de A et B. La relation fondamentale entre séparabilité et diagonalisabilité est la suivante.

Lemme 4.3. *Une matrice sur un corps discret est séparable si, et seulement si, elle est diagonalisable sur un certain corps discret.*

Démonstration. Si une matrice A est diagonalisable sur un corps F, alors le polynôme minimal de A est séparable d'après les théorèmes V.4.3 et 4.2. Inversement, si A est séparable, soit F un corps de décomposition pour le polynôme minimal de A sur le corps de définition de A. Alors A est diagonalisable sur F d'après les théorèmes V.4.3 et 4.2. □

Le lemme suivant nous permet de traduire les questions à propos d'éléments algébriques sur un corps discret en questions à propos de matrices.

Lemme 4.4. *Soient E un anneau commutatif qui contient un corps discret k, f et g des polynômes de $k[X]$, et α et β des éléments de E tels que $f(\alpha) = g(\beta) = 0$. Alors il existe des matrices carrées A et B de même taille à coefficients dans k telles que $AB = BA$ et $f(A) = g(B) = 0$, et un homomorphisme d'anneaux de $k[A, B]$ sur $k[\alpha, \beta]$ égal à l'identité sur k qui envoie A sur α et B sur β.*

Démonstration. L'anneau $k[X, Y]/(f(X), g(Y)) = k[x, y]$ est de dimension finie sur k et s'envoie naturellement sur $k[\alpha, \beta]$. Soient T_x et T_y les transformations linéaires sur $k[x, y]$ données par les multiplications par x et y, et soient A et B les matrices de T_x et T_y par rapport à une base de $k[x, y]$. Alors les isomorphismes naturels $k[A, B] \simeq k[T_x, T_y] \simeq k[x, y]$ et l'homomorphisme de $k[x, y]$ sur $k[\alpha, \beta]$ donnent les résultats souhaités. □

Théorème 4.5. *Soit E est un anneau commutatif qui contient un corps discret k. Les éléments de E séparables sur k forment un anneau.*

Démonstration. Il suffit de démontrer que si α et β sont séparables sur k, alors tout élément de $k[\alpha, \beta]$ est séparable sur k. Soient f et g des polynômes séparables annulés par α et β respectivement, et prenons A et B comme dans le lemme 4.4. Il suffit de démontrer que tout élément de $k[A, B]$ est séparable. Étant donnée une matrice C dans $k[A, B]$, nous pouvons construire un corps F qui contient le corps de définition de A, B et C, sur lequel les polynômes minimaux de A et B sont des produits de facteurs linéaires. D'après les théorèmes V.4.3 et V.4.4 nous pouvons diagonaliser simultanément les matrices A et B, et donc aussi la matrice C, sur le corps F. Donc la matrice C est séparable d'après les théorèmes V.4.3 et 4.2. □

Nous pouvons caractériser le fait qu'une extension E d'un corps discret k est séparable en termes de l'absence d'éléments nilpotents lorsque nous pouvons remplacer le corps de base k par une extension convenable. Cette caractérisation peut servir de définition de la séparabilité dans le cas d'une extension non nécessairement algébrique [1]. Nous allons établir cette caractérisation uniquement pour le cas où k est dénombrable, en laissant la formulation du cas général en exercice.

Théorème 4.6. *Soit k un sous-corps discret d'un anneau commutatif E. Considérons les deux conditions suivantes.*

(i) *E est séparable sur k.*

(ii) *Pour tout corps discret K extension de k, l'anneau $K \otimes_k E$ est sans éléments nilpotents.*

Alors (i) *implique* (ii) *; inversement, si k est dénombrable et si E est algébrique sur k,* (ii) *implique* (i).

Démonstration. Supposons (i). L'anneau $K \otimes_k E$ est engendré sur K par des éléments séparables sur k ; donc tout élément θ de $K \otimes_k E$ est séparable sur K d'après le théorème 4.5. Si $\theta^n = 0$, alors θ annule le polynôme X^n et un polynôme $f(X)$ séparable sur K. Le pgcd de $f(X)$ et X^n divise X^n et il est séparable, donc il est égal à X, et ainsi $\theta = 0$.

Inversement, supposons (ii) et k dénombrable. Considérons un $\theta \in E$ qui annule un polynôme non nul f sur k. Nous procédons par récurrence sur le degré n de f. Si f est séparable nous avons terminé. Sinon, d'après les théorèmes 3.4 et 4.2, nous pouvons construire un corps discret K extension de k tel que f a une racine multiple dans K. Nous écrivons $f(X) = (X - r)g(X)$ avec $g(r) = 0$, donc $f | g^2$. Alors $g(\theta) \in K \otimes_k E$ et $g(\theta)^2 = 0$, donc $g(\theta) = 0$. Cela signifie que les éléments $1, \theta, \ldots, \theta^{n-1}$ de $K \otimes_k E$ sont linéairement dépendants sur K, donc aussi sur k (exercice III.5.5). Ainsi nous pouvons trouver dans $k[X]$ un polynôme de degré plus petit que n annulé par θ. □

Exercices

1. Soient $k \subseteq E$ des anneaux commutatifs et f un polynôme séparable de $k[X]$. Montrer que tout facteur carré de f dans $E[X]$ est inversible dans E.
2. Soient k un anneau commutatif, $a \in k$ et $f \in k[X]$. Montrer que $X - a$ est étranger à f si, et seulement si, $f(a)$ est inversible dans k.
3. Soient $a_1, \ldots, a_n$ des éléments d'un anneau commutatif k. Montrer que le polynôme $(X - a_1)(X - a_2) \cdots (X - a_n)$ est séparable si, et seulement si, $a_i - a_j$ est inversible dans k pour tous $i \neq j$.

1. Voir par exemple la notion d'extension séparable de corps dans Bourbaki.

4. Soient a, b et c des éléments d'un anneau commutatif k. Montrer que $aX + b$ est séparable si, et seulement si, a et b sont étrangers. Montrer que si $b^2 - 4ac$ est inversible, alors $aX^2 + bX + c$ est séparable.
5. Soit E un anneau commutatif discret algébrique sur un sous-corps k. Montrer que E est séparable sur k si, et seulement si, pour tout sous-ensemble fini S de k et tout sous-ensemble fini T de E, il y a un sous-corps dénombrable k' de k qui contient S et tel que, pour chaque corps dénombrable K extension de k', l'anneau $K \otimes_{k'} k'[T]$ est sans éléments nilpotents.

5 Éléments primitifs

Soit E un anneau commutatif qui contient un corps discret k. Un élément θ de E est un **élément primitif** de E sur k si $E = k[\theta]$. Nous allons montrer que si E est de type fini et séparable, alors on peut construire un élément primitif si k est suffisamment grand, ou si E est un corps discret.

Nous regardons d'abord la situation où k est suffisamment grand. Le point clé consiste à montrer que $k[A, B] = k[C]$ lorsque A et B sont des matrices séparables qui commutent.

Théorème 5.1. *Soient A et B des matrices $n \times n$ qui commutent sur un corps discret k de cardinalité plus grande que $n(n-1)/2$. Si B est séparable, il existe un élément c de k tel que A et B peuvent être écrites comme des polynômes en $A + cB$, à coefficients dans k.*

Démonstration. Il suffit de traiter le cas où k est dénombrable, et on peut aussi supposer que k est un corps de décomposition pour les polynômes minimaux de A et B (théorème 3.4).

Nous regardons d'abord le cas où A est aussi séparable. D'après le lemme 4.3 et les théorèmes V.4.3 et V.4.4, nous pouvons supposer que A et B sont diagonales avec les éléments diagonaux $a_1, \dots, a_n$ et $b_1, \dots, b_n$. On prend un c distinct des $(a_j - a_i)/(b_i - b_j)$ pour chaque paire (i, j) telle que $b_i \neq b_j$. Alors $a_i + cb_i \neq a_j + cb_j$ si $a_i \neq a_j$ ou $b_i \neq b_j$. Le théorème d'interpolation II.5.5 nous dit que A et B peuvent être écrites comme des polynômes en $A + cB$ [1].

Pour le cas général, nous pouvons supposer que B est de la forme diagonale par blocs comme suit

$$\begin{pmatrix} B_1 & & & \\ & B_2 & & \\ & & \ddots & \\ & & & B_n \end{pmatrix}$$

1. **NdT.** Si m est le nombre de paires (a_i, b_i) distinctes, il existe deux polynômes d'interpolation $g(X)$ et $h(X) \in k[X]$ de degré au plus $m-1$ qui satisfont $g(a_i + cb_i) = a_i$ et $h(a_i + cb_i) = b_i$ pour tous les i : on a alors $g(A + cB) = A$ et $h(A + cB) = B$.

avec $B_i = \lambda_i I_{n_i}$ et les λ_i deux à deux distincts. Comme $AB = BA$, la matrice A a la même structure de blocs que B, mais avec des blocs A_i arbitraires. Nous pouvons mettre chaque bloc A_i en forme canonique de Jordan sans modifier B. On prend un $c \in k$ comme dans le cas particulier précédent, tel que B et la diagonale de A peuvent être écrites comme des polynômes en la diagonale de $A + cB$. Notez que $A + cB$ est en forme canonique de Jordan, donc sa diagonale peut être écrite comme un polynôme en $A + cB$. Comme $A + cB$ est égal à A en dehors de la diagonale, nous avons réussi. □

Corolaire 5.2. *Soit E un anneau commutatif qui contient un corps discret k et soient α et β des éléments de E avec α algébrique et β séparable sur k. Si k est suffisamment grand, il existe un $\theta \in E$ tel que $k[\alpha, \beta] = k[\theta]$.*

Démonstration. Soient f et g des polynômes sur k, avec g séparable, tels que $f(\alpha) = g(\beta) = 0$. Soient A et B des matrices comme dans le lemme 4.4. D'après le théorème 5.1, si k est suffisamment grand, il existe un $c \in k$ tel que A et B peuvent être écrites comme des polynômes en $A + cB$. On prend $\theta = \alpha + c\beta$. □

Si le corps k est trop petit, alors le corolaire 5.2 peut se trouver en défaut (exercice 2). Cependant, si E est un corps discret, le corolaire 5.2 est valable pour n'importe quel k. Classiquement, on traite séparément les deux cas où k est fini ou infini. Nous devons être un tout petit peu précautionneux car il se peut que nous ne sachions pas déterminer si k est fini ou infini. Le lemme suivant nous donne un élément primitif quand E est un corps fini.

Lemme 5.3. *Soit k un corps discret et soit G un sous-groupe fini du groupe multiplicatif des éléments non nuls de k. Alors G est cyclique.*

Démonstration. Soient x et y des éléments de G d'ordres m et n respectivement. Nous construisons un élément de G d'ordre $q = \text{ppcm}(m, n)$. On écrit $q = ab$ avec $(a, b) = 1$, $a|n$ et $b|m$. Nous montrons que $x^a y^b$ est d'ordre q. Clairement $(x^a y^b)^q = 1$; supposons que $(x^a y^b)^i = 1$. Alors $x^{ai} = y^{-bi}$, donc $(x^{ai})^a = 1$, d'où $m|a^2 i$ et donc $b|i$. De la même manière $a|i$, donc $q|i$.

Donc si g est un élément de G d'ordre maximal N, $x^N = 1$ pour tout $x \in G$. Comme le polynôme $X^N - 1$ a au plus N racines (théorème II.5.5), il y a au plus N éléments dans G, donc ils doivent tous être une puissance de g. □

L'astuce pour le cas général est de passer à un sous-corps qui, ou bien est fini, ou bien contient suffisamment d'éléments.

Théorème 5.4. *Soient k un corps discret de type fini et N un entier strictement positif. Ou bien k est fini, ou bien k contient plus que N éléments.*

Démonstration. Ou bien $0, 1, 2, \ldots, N$ sont des éléments distincts de k, ou bien k est de caractéristique finie au plus N, donc nous pouvons supposer être dans le

dernier cas. Soit k_0 le sous-corps premier (fini) de k, et considérons un système générateur $a_1, \ldots, a_n$ de k, i.e. $k = k_0(a_1, \ldots, a_n)$. Soit $S \subseteq k_0[X_1, \ldots, X_n]$ l'ensemble fini des polynômes dont le degré en chaque variable X_i est au plus N, et soit $\overline{S}$ l'image de S dans k lorsqu'on envoie X_i sur a_i. On a $\#\overline{S} \leqslant N$ ou $\#\overline{S} > N$, donc nous pouvons supposer $\#\overline{S} \leqslant N$. Nous allons montrer que k est fini.

Soit $p \in k_0[X_1, \ldots, X_n]$. Nous allons construire un polynôme $q \in S$ tel que $p(a_1, \ldots, a_n) = q(a_1, \ldots, a_n)$. Si $a_t = 0$, nous pouvons remplacer chaque puissance strictement positive de X_t dans p par X_t. Si $a_t \neq 0$, alors, comme la suite $1, a_t, \ldots, a_t^N$ d'éléments de $\overline{S}$ a $N+1$ termes, deux doivent être égaux, donc l'ordre multiplicatif de a_t est au plus N. Par suite pour tout entier $m > 0$, on a $a_t^m = a_t^j$ pour un unique $j < N$, donc nous pouvons remplacer chaque occurrence de X_t^m dans p par X_t^j, ce qui nous donne un élément q de S. Comme tout élément de k est un quotient de deux tels polynômes q, le corps k est fini. □

Corolaire 5.5. *Soient $k \subseteq E$ des corps discrets et $\alpha, \beta \in E$. Supposons que α est algébrique et β séparable sur k. Alors il existe un $\theta \in E$ tel que $k[\theta] = k[\alpha, \beta]$.*

Démonstration. Nous pouvons supposer que k est engendré par les coefficients de deux polynômes annulés par α et β. D'après le théorème 5.4, ou bien k est assez grand, donc $k[\alpha, \beta] = k[\theta]$ d'après le corolaire 5.2, ou bien k est fini, donc $k[\alpha, \beta]$ est fini et $k[\alpha, \beta] = k[\theta]$ d'après le lemme 5.3. □

Dans le corolaire 5.5 il suffit que β soit séparable sur $k[\alpha]$: voir le théorème 6.7.

Exercices

1. Montrer que les matrices 3×3 diagonales sur un corps k à deux éléments forment une extension finie séparable de k qui n'a pas d'élément primitif.
2. Soit E un anneau commutatif qui contient un corps discret k. Soient α et β des éléments de E tels que α est séparable sur k et β annule un polynôme séparable sur $k[\alpha]$. Montrer que β est séparable sur k.
3. Construire un exemple brouwerien d'un corps qui n'est ni fini ni infini.

6 Séparabilité et caractéristique p

Un cas extrême de polynôme non séparable est un polynôme non constant f tel que $f' = 0$. C'est possible même lorsque k est un corps discret, si k est de caractéristique finie p.

Théorème 6.1. *Soient p un nombre premier, R un anneau commutatif tel que $pR = 0$, et q une puissance*[1] *de p. Alors la fonction qui envoie $x \in R$ sur x^q est un homomorphisme d'anneaux, dont l'image $R^q = \{\, x^q : x \in R \,\}$ est un sous-anneau de R. Si R est réduit, cet homomorphisme est injectif et donne un isomorphisme de R sur R^q. Pour un $f \in R[X]$, on a $f' = 0$ si, et seulement si, $f(X) = f_0(X^p)$ pour un $f_0 \in R[X]$.*

Démonstration. Si $0 < i < p$, le coefficient binomial $\binom{p}{i}$ est divisible par p, donc $(a+b)^p = a^p + b^p$. Par récurrence, la fonction qui envoie x sur x^q est un homomorphisme d'anneaux ; l'image d'un homomorphisme d'anneaux est un sous-anneau. L'homomorphisme est injectif si son noyau est nul.

Si n n'est pas divisible par p, il est étranger à p, donc inversible dans R. Donc si $f' = 0$, le coefficient de X^n dans f, pour n non divisible par p, est 0 ; donc $f(X) = f_0(X^p)$ pour un $f_0 \in R[X]$. Inversement, la dérivée de $f_0(X^p)$ est clairement 0. □

Voici maintenant un critère de séparabilité pour un élément d'un corps discret de caractéristique p.

Théorème 6.2. *Soient k un corps discret de caractéristique p, q une puissance de p, et α un élément d'un anneau commutatif qui contient k. Alors α est séparable sur k si, et seulement si, $\alpha \in k[\alpha^q]$.*

Démonstration. Si $\alpha \in k[\alpha^q]$, alors en écrivant α comme une combinaison linéaire de puissances de α^q on obtient un polynôme $f \in k[X]$ tel que $f' = 1$ et $f(\alpha) = 0$, donc α est séparable sur k. Inversement, supposons que α annule un polynôme séparable f de $k[X]$. Il suffit de démontrer que l'image β de X dans $k[X]/(f(X))$ peut être écrite comme un polynôme en β^q. Soit T_β la transformation linéaire de $k[\beta]$ induite par la multiplication par β, et soit B une matrice pour T_β. Il suffit de démontrer que B peut être écrite comme un polynôme en B^q. Comme B est séparable, nous pouvons supposer que la matrice B est diagonale. D'après le théorème 6.1, la fonction qui envoie $x \in k$ sur x^q est injective, donc des éléments diagonaux de B^q sont égaux si, et seulement si, les éléments diagonaux correspondants de B sont égaux. Le théorème d'interpolation II.5.5 nous dit que la matrice B peut être écrite comme un polynôme en B^q. □

Le théorème suivant est utilisé dans les situations où nous aimerions factoriser des polynômes en produits d'irréductibles mais où nous ne pouvons pas le faire.

Théorème 6.3. *Soient k un anneau commutatif discret avec unités détachables, et S un ensemble fini de polynômes unitaires de $k[X]$. Alors, ou bien k contient*

1. **NdT.** Sauf précision contraire, lorsque nous parlons d'une puissance d'un nombre premier, il s'agit toujours d'une puissance p^m avec $m > 0$.

un élément non nul non inversible, ou bien nous pouvons construire un ensemble fini T de polynômes unitaires de $k[X]$ tel que :

(i) *tout élément de T est de la forme $f(X^q)$ avec f séparable et q égal à 1 ou à une puissance d'un nombre premier nul dans k,*

(ii) *les éléments de T sont deux à deux étrangers,*

(iii) *tout polynôme de S est un produit de polynômes de T.*

Démonstration. Nous procédons par récurrence sur la somme des carrés des degrés des polynômes dans S. Nous allons transformer l'ensemble S en l'ensemble voulu T ou alors trouver un élément non nul non inversible dans k. Étant donnés deux éléments $s_1, s_2 \in S$, l'algorithme d'Euclide construit ou bien un élément non nul non inversible de k, ou bien un polynôme unitaire h qui engendre l'idéal (s_1, s_2). Si $h \neq 1$, nous pouvons remplacer s_1 et s_2 par h, s_1/h et s_2/h, ce qui fait décroitre la somme des carrés des degrés. Nous pouvons donc supposer que les polynômes de S sont deux à deux étrangers.

Si g est unitaire de degré $n > 0$ et si $g' = 0$, alors $n = 0$ dans k, donc ou bien k contient un élément non nul non inversible, ou bien un nombre premier p est nul dans k. Dans le dernier cas nous pouvons écrire $g = f(X^p)$. En répétant cet argument nous voyons que pour tout $s \in S$ nous pouvons supposer que $s = f(X^q)$ avec q égal à 1 ou à une puissance d'un nombre premier nul dans k, et $f' \neq 0$. Nous pouvons supposer que l'algorithme d'Euclide construit un polynôme unitaire h qui engendre l'idéal (f, f'). Si $h \neq 1$ nous remplaçons s par $h(X^q)$ et $s/h(X^q)$, ce qui fait décroitre la somme des carrés des degrés. □

Corolaire 6.4. *Soient $k \subseteq E$ des corps discrets et $\alpha \in E$ entier sur k. Alors il existe q, égal à 1 ou à une puissance de la caractéristique finie de k, tel que α^q est séparable sur k.*

Démonstration. Soit g un polynôme non nul de $k[X]$ tel que $g(\alpha) = 0$. Alors, d'après le théorème 6.3, nous pouvons écrire g comme un produit $\prod_i f_i(X^q)^{n_i}$ où les f_i sont des polynômes séparables premiers entre eux. Clairement, l'un des $f_i(\alpha^q)$ est nul. □

Lemme 6.5. *Soient p un nombre premier et R un anneau commutatif tels que $pR = 0$. Soient q une puissance de p et $a \in R$. Si $X^q - a = f(X)g(X)$, avec f et g des polynômes étrangers unitaires sur R, alors f ou g est égal à 1.*

Démonstration. On a $f'g + fg' = 0$ et $uf + vg = 1$, d'où $g' = g(vg - uf')$ puis $g' = 0$. De même, on a $f' = 0$. Ainsi, il existe des polynômes f_1 et g_1 tels que $f(X) = f_1(X^p)$ et $g(X) = g_1(X^p)$. Si $q = p$, alors clairement f_1 ou g_1 est égal à 1. Sinon

$$X^{q/p} - a = f_1(X)g_1(X)$$

et nous terminons par récurrence sur q, car si

$$s(X)f_1(X^p) + t(X)g_1(X^p) = 1,$$

alors en notant $s_1(X^p)$ et $t_1(X^p)$ les sommes des monômes dans s et t de degrés divisibles par p, nous avons

$$s_1(X^p)f_1(X^p) + t_1(X^p)g_1(X^p) = 1,$$

donc

$$s_1(X)f_1(X) + t_1(X)g_1(X) = 1,$$

et f_1 et g_1 sont étrangers. □

Théorème 6.6. *Soient k un corps discret de caractéristique finie p, $a \in k$, et q une puissance de p. Si $X^q - a$ est réductible dans $k[X]$, alors $a \in k^q$.*

Démonstration. D'après le lemme 6.5 le polynôme $X^q - a$ n'a pas deux diviseurs étrangers dans $k[X]$. Donc, d'après le théorème 6.3, nous pouvons écrire $X^q - a$ sous la forme $h(X)^m$ pour un certain polynôme unitaire $h \in k[X]$ et un $m > 1$. Notez que m est une puissance de p car m divise q. Comme $h(0)^m = -a$, nous pouvons poser $b = -h(0)^{m/p}$, et $a = b^q$. □

Soient E un anneau impotent et k un sous-corps discret de E. La **clôture séparable** de k dans E est le sous-corps de E formé par les éléments séparables sur k (théorème 1.9). Le corps k est séparablement clos dans E si k est égal à sa clôture séparable dans E. Le théorème suivant généralise le corolaire 5.5 et montre que la clôture séparable est séparablement close.

Théorème 6.7. *Soient $k \subseteq E$ des corps discrets. Si $\alpha \in E$ est algébrique (séparable) sur k et si $\beta \in E$ est séparable sur $k[\alpha]$, alors $k[\alpha, \beta] = k[\theta]$ pour un θ (β est séparable sur k).*

Démonstration. En appliquant le corolaire 6.4, on prend q égal à 1 ou à une puissance d'un nombre premier p nul dans k, avec β^q séparable sur k. Alors $k[\alpha, \beta] = k[\alpha, \beta^q]$ d'après le théorème 6.2, et $k[\alpha, \beta^q] = k[\theta]$ pour un $\theta \in E$ d'après le corolaire 5.5. Si α est séparable sur k, alors $k[\theta^p] = k[\alpha^p, \beta^p] = k[\alpha, \beta^p] = k[\alpha, \beta] = k[\theta]$, donc θ est séparable sur k d'après le théorème 6.2. Ainsi β est séparable sur k d'après le théorème 4.5. □

Soient $k \subseteq E$ des corps discrets et $\alpha \in E$ algébrique sur k. Alors, d'après le corolaire 6.4, il existe un entier q, égal à 1 ou à une puissance de la caractéristique finie de k, avec α^q séparable sur k. Si $\alpha^q \in k$, alors α est **purement inséparable** sur k. Une extension E de k est une **extension purement inséparable** si tout élément de E est purement inséparable sur k. Le théorème suivant montre que toute extension algébrique de type fini d'un corps discret est obtenue en composant une extension finie séparable et une extension purement inséparable.

Théorème 6.8. *Soit E un corps discret qui est un espace vectoriel de type fini sur un sous-corps k. Alors il existe un sous-corps K de E qui contient k, tel que K est de type fini et séparable sur k, et E est purement inséparable sur K.*

Démonstration. On considère un système générateur $\alpha_1, \ldots, \alpha_n$ de E sur k. Pour chaque α_i, il existe un $q(i)$ tel que $\alpha_i^{q(i)}$ est séparable sur k. D'après le théorème 4.5, le corps $K = k[\alpha_1^{q(1)}, \ldots, \alpha_n^{q(n)}]$ est séparable sur k. Comme chaque α_i est purement inséparable sur K, on obtient que $k[\alpha_1, \ldots, \alpha_n]$ est purement inséparable sur K. □

Exercice

1. Soient k un corps discret et $f \in k[X]$ un polynôme non constant. Montrer que f n'est pas séparable si, et seulement si, il existe un polynôme $g \in k[X]$ non constant tel que ou bien g^2 divise f, ou bien la caractéristique de k est égale à p et $g(X^p)$ divise f.

7 Corps parfaits

Si k est un corps discret de caractéristique p, alors $k^p = \{ a^p : a \in k \}$ est un sous-corps de k isomorphe à k. Un corps discret k est **parfait** si tout polynôme non nul de $k[X]$ est un produit de polynômes séparables. Le théorème suivant est une adaptation de la caractérisation en mathématiques classiques des corps parfaits, sans toutefois réclamer que l'on connaisse la caractéristique du corps.

Théorème 7.1. *Un corps discret k est parfait si, et seulement si, pour tout nombre premier p, ou bien $p \neq 0 \in k$, ou bien $k^p = k$.*

Démonstration. Supposons que k est parfait. Soient $a \in k$ et p un nombre premier tel que $p = 0$ dans k. Alors $X^p - a$ est un produit de polynômes séparables, donc il est réductible. Et $a \in k^p$ d'après le théorème 6.6.

Pour la réciproque considérons un $f \in k[X]$. D'après le théorème 6.3 nous pouvons supposer que $f(X) = g(X^q)$ avec g séparable, et ou bien $q = 1$, ou bien k est de caractéristique finie p et $q = p^e$. Si $q = 1$, f est séparable. Si $q = p^e$, la fonction $x \mapsto x^q$ est un isomorphisme de $k[X]$ vers $(k[X])^q = k^q[X^q] = k[X^q]$. Donc il existe un $h \in k[X]$ tel que $g(X^q) = h(X)^q$. Comme $n^q \equiv n \pmod p$, l'isomorphisme conserve les dérivées formelles, donc $g'(X^q) = h'(X)^q$. Comme g est séparable, h l'est également, donc f est un produit de polynômes séparables. □

Si k est un corps discret de caractéristique 0, alors k est parfait, car $p \neq 0$ dans k pour tout nombre premier p. Si k est un corps fini de caractéristique p, la fonction $x \mapsto x^p$ est un isomorphisme, donc k est parfait ; mais $k(X)$ n'est pas

parfait parce que $X \notin k(X^p)$. Si k est un corps premier, il n'est pas nécessaire de connaitre sa caractéristique pour démontrer qu'il est parfait.

Corolaire 7.2. *Un corps premier discret est parfait.*

Démonstration. Soit p un nombre premier. Si $p = 0$ dans k, alors k est le corps à p éléments, donc $k = k^p$. □

Définition 7.3. Soit k un sous-corps d'un corps discret K. Alors K est une **clôture parfaite** de k si

(i) K est parfait ;

(ii) pour tout $\alpha \in K$, ou bien $\alpha \in k$, ou bien k est de caractéristique finie p et il existe $q = p^e$ tel que $\alpha^q \in k$.

En mathématiques classiques, la clôture parfaite est souvent construite à l'intérieur de la clôture algébrique. Bien que nous ne sachions pas toujours construire une clôture algébrique, nous pouvons cependant construire une clôture parfaite en tant que limite directe.

Si $k_1 \to k_2 \to k_3 \to \cdots$ est une suite d'anneaux et d'homomorphismes d'anneaux, la **limite directe** k_∞ est définie comme suit. Les éléments de k_∞ sont les éléments de la réunion disjointe $\bigcup k_i$; deux éléments $a \in k_i$ et $b \in k_j$ sont égaux s'il existe un m tel que a et b ont pour image un même élément dans k_m. On voit facilement que k_∞ est un anneau. Si les k_i sont des corps discrets, k_∞ est un corps discret et on peut identifier chaque k_i à un sous-corps de k_∞.

Si nous connaissons la caractéristique finie d'un corps, la construction proposée dans l'exercice 1 nous donne une clôture parfaite. Si nous ne connaissons pas la caractéristique du corps, nous devons raffiner cette construction.

Théorème 7.4. *Tout corps discret possède une clôture parfaite.*

Démonstration. Soit $\{\, p_n : 1 \leqslant n \,\}$ l'énumération croissante des nombres premiers. Pour tout n, soit $k_n = k$, et définissons $\varphi_n \colon k_n \to k_{n+1}$ par

$$\varphi_n(x) = \begin{cases} x^p & \text{si } p \in \{\, p_j : j \leqslant n \,\} \text{ et } p = 0 \text{ dans } k, \\ x & \text{sinon.} \end{cases}$$

Notons K la limite directe du système et x_n l'image de x dans k_n dans K. Nous pouvons identifier l'image de k_1 dans K avec k. Pour montrer que K est parfait, considérons un $\alpha \in K$ et un nombre premier p égal à 0 dans K. Il existe un $n \in \mathbb{N}$ et un $x \in k$ tels que $\alpha = x_n$. Nous pouvons supposer n suffisamment grand pour que $p_n \geqslant p$. Alors $\varphi_n(x) = x^p$, donc

$$\alpha = x_n = \varphi_n(x)_{n+1} = (x^p)_{n+1} = x^p_{n+1}.$$

Ainsi K est parfait. Pour vérifier la condition (ii) de la définition 7.3, considérons un $\alpha \in K$ et prenons un $n \in \mathbb{N}$ et un $x \in k$ tels que $\alpha = x_n$. Si $p_1, \ldots, p_n$ sont

tous non nuls dans k, alors $\alpha = x_n = x_1 \in k$. Sinon il existe un entier $j \leqslant n$ tel que $p_j = 0$ dans k. Alors $\varphi_{n-1} \circ \cdots \circ \varphi_1(x) = x^q$ avec $q = p_j^{n-j}$. Donc

$$\alpha^q = x_n^q = (\varphi_{n-1} \circ \cdots \circ \varphi_1(x_1))_n = x_1 \in k. \qquad \square$$

La clôture parfaite est essentiellement unique.

Théorème 7.5. *Si K et L sont des clôtures parfaites du corps discret k, il existe un unique k-isomorphisme de K sur L.*

Démonstration. Nous définissons une fonction f de K vers L comme suit. Étant donné un $\alpha \in K$, ou bien $\alpha \in k$, auquel cas nous posons $f(\alpha) = \alpha$, ou bien il existe un $q = p^e$ avec p égal à la caractéristique finie de k tel que $\alpha^q \in k$. Dans ce cas il existe un $\beta \in L$ tel que $\beta^q = \alpha^q$. Comme la fonction $x \mapsto x^q$ est un automorphisme de L, l'élément β est unique et ne dépend pas du choix de q. En posant $f(\alpha) = \beta$, nous obtenons un homomorphisme de K vers L. De la même manière, en échangeant les rôles de K et L, nous construisons un homomorphisme de L vers K. Il est facile de voir que les deux fonctions sont inverses l'une de l'autre. Ce sont donc des isomorphismes. $\square$

Théorème 7.6. *Un corps discret k est parfait si, et seulement si, tout élément algébrique sur k dans un corps discret qui est une extension de k est séparable sur k.*

Démonstration. Si k est parfait, tout polynôme de $k[X]$ est un produit de polynômes séparables, donc tout élément algébrique sur k dans un corps discret qui est une extension de k est séparable. Inversement, soit p un nombre premier nul dans k. Étant donné un $a \in k$, soit $K \supseteq k$ un corps parfait et un $b \in K$ avec $b^p = a$. Comme b est séparable sur k, le théorème 6.2 nous dit que $b \in k[b^p] = k$. D'après le théorème 7.1 nous concluons que k est parfait. $\square$

Théorème 7.7. *Soit E un corps discret qui contient un corps parfait k. Si $\alpha \in E$ est algébrique sur k, alors $k[\alpha]$ est parfait.*

Démonstration. Soit p un nombre premier nul dans k. Alors $k[\alpha]^p = k^p[\alpha^p]$. Comme k est parfait, α est séparable sur k, et $k^p[\alpha^p] = k[\alpha^p] = k[\alpha]$ d'après le théorème 6.2. Donc $k[\alpha]$ est parfait. $\square$

Exercices

1. Soit k un corps discret de caractéristique finie p. Montrer que la limite directe de la suite $k \to k \to k \to \cdots$, où chaque fonction $k \to k$ envoie a sur a^p, est une clôture parfaite de k.
2. Construire un exemple brouwerien d'un corps discret k de caractéristique finie p tel que ni $k^p = k$, ni $k^p \neq k$.

8 Théorie de Galois

Soient $k \subseteq K$ et $k \subseteq E$ des anneaux commutatifs. Un homomorphisme d'anneaux $\sigma\colon K \to E$ est un **k-homomorphisme** si σ est l'identité sur k. Nous notons souvent l'image d'un élément x par l'homomorphisme σ sous la forme x^σ, et l'image de K par σ sous la forme K^σ. Nous étendons σ en un $k[X]$-homomorphisme de $K[X]$ dans $E[X]$ en posant $X^\sigma = X$. La technique fondamentale pour étendre un k-homomorphisme de corps discrets est la suivante.

Lemme 8.1. *Soient $k \subseteq K \subseteq E$ des corps discrets et $\sigma\colon K \to E$ un k-homomorphisme. Soient $f \in K[X]$ irréductible, $\alpha \in E$ une racine de f, et $\beta \in E$ une racine de f^σ. Alors σ s'étend en un homomorphisme de $K[\alpha]$ vers E qui envoie α sur β.*

Démonstration. On définit une fonction de $K[\alpha]$ vers E en envoyant $g(\alpha)$ sur $g^\sigma(\beta)$ pour tout $g \in K[X]$. Pour montrer que cette fonction est bien définie, il suffit de voir que si $g(\alpha) = 0$, alors $g^\sigma(\beta) = 0$. Supposons donc que $g(\alpha) = 0$. Alors f divise g parce que f est irréductible et $f(\alpha) = 0$; donc f^σ divise g^σ, et donc $g^\sigma(\beta) = 0$. □

Si S est un ensemble borné en nombre et si $\sigma\colon S \to S$ est injectif, alors σ est un isomorphisme (voir l'exercice I.2.11). On a un résultat analogue pour le concept de corps.

Lemme 8.2. *Soit $k \subseteq K$ une extension algébrique de corps discrets. Alors tout k-endomorphisme de K est un automorphisme.*

Démonstration. Soit σ un k-endomorphisme de K. Comme K est un corps, σ est injectif. Un $\alpha \in K$ arbitraire annule un polynôme f de $k[X]$. Soit S l'ensemble des racines de f dans K. Si $\beta \in S$, alors $f(\beta^\sigma) = f^\sigma(\beta^\sigma) = f(\beta)^\sigma = 0$, de sorte que $\beta^\sigma \in S$. Ainsi σ induit une fonction (injective) de S vers S. Mais S est borné par le degré de f, donc σ envoie S sur S, donc il existe un $\beta \in S \subseteq K$ tel que $\beta^\sigma = \alpha$. Comme $\alpha \in K$ était arbitraire, σ est surjectif. □

Soient $k \subseteq K$ des corps discrets. Si tout élément de K annule un polynôme de $k[X]$ qui est un produit de polynômes linéaires (polynômes de degré $\leqslant 1$) dans $K[X]$, K est appelé une **extension normale** de k. On dit aussi que K est **normal sur** k.

Théorème 8.3. *Soient $k \subseteq K$ des corps discrets avec K espace vectoriel de type fini sur k. Alors K est normal sur k si, et seulement si, K est un corps de décomposition d'un polynôme de $k[X]$.*

Démonstration. Supposons K normal et engendré par $\alpha_1, \ldots, \alpha_n$ sur k. Considérons des polynômes unitaires $f_i \in k[X]$ tels que $f_i(\alpha_i) = 0$ et f_i est un produit

de polynômes linéaires dans $K[X]$. Alors K est un corps de décomposition pour $f_1 f_2 \cdots f_n$.

Inversement, si K est un corps de décomposition pour un $f \in k[X]$, on a $f(X) = \prod_{i=1}^{n}(X - \alpha_i)$ avec les $\alpha_i \in K$, et pour $x \in K$, on a un $p \in k[X_1, \ldots, X_n]$ tel que $x = p(\alpha_1, \ldots, \alpha_n)$. Soit S le groupe de permutations des indéterminées $X_1, \ldots, X_n$, et posons

$$q(X, X_1, \ldots, X_n) = \prod\nolimits_{\sigma \in S}(X - p(X_1^\sigma, \ldots, X_n^\sigma)).$$

Comme q est symétrique en $X_1, \ldots, X_n$, le théorème II.8.1 nous dit que les coefficients de $q(X, \alpha_1, \ldots, \alpha_n)$ sont des polynômes en les coefficients de f, donc $q(X, \alpha_1, \ldots, \alpha_n) \in k[X]$. Clairement le polynôme $q(X, \alpha_1, \ldots, \alpha_n)$ est un produit de polynômes linéaires dans $K[X]$ et $q(x, \alpha_1, \ldots, \alpha_n) = 0$. □

Soient $k \subseteq K$ des corps discrets. L'ensemble des k-automorphismes de K forme un groupe $\mathcal{G}(K/k)$ appelé le **groupe de Galois** de K sur k. Si K est normal et séparable sur k, K est appelé une **extension de Galois** de k. Le groupe $\mathcal{G}(K/k)$ est un sous-ensemble de l'ensemble de toutes les fonctions de K vers K, donc il possède une inégalité naturelle définie par $\sigma_1 \neq \sigma_2$ s'il existe un $\alpha \in K$ tel que $\sigma_1(\alpha) \neq \sigma_2(\alpha)$. Quand nous disons que $\mathcal{G}(K/k)$ est fini, nous voulons dire fini par rapport à cette inégalité.

Théorème 8.4. *Soient $k \subseteq K$ des corps discrets. Si K est une extension galoisienne de k de dimension finie, alors $\mathcal{G}(K/k)$ est fini et $\#\mathcal{G}(K/k) = \dim_k K$.*

Démonstration. Comme K est séparable sur k, on a un θ tel que $K = k[\theta]$. Le polynôme minimal f de θ sur k est de degré $n = \dim_k K$ et il est séparable. Comme K est normal, nous pouvons écrire $f(X) = (X - \theta_1) \cdots (X - \theta_n)$ avec les $\theta_i \in K$. Comme f est séparable, les θ_i sont distincts. Les lemmes 8.1 et 8.2 disent que, pour chaque $i = 1, \ldots, n$, on a un $\sigma_i \in \mathcal{G}(K/k)$ tel que $\sigma_i(\theta) = \theta_i$. Comme $K = k[\theta]$, cela détermine complètement σ_i. D'autre part, si $\sigma \in \mathcal{G}(K/k)$, alors $f(\theta^\sigma) = f^\sigma(\theta^\sigma) = f(\theta)^\sigma = 0$, donc $\theta^\sigma = \theta_i$ pour un i, i.e. $\sigma = \sigma_i$. Ainsi $\mathcal{G}(K/k) = \{\sigma_1, \ldots, \sigma_n\}$, et les σ_i sont distincts car les θ_i sont distincts. □

Nous construisons des k-automorphismes d'une extension normale de k qui étendent des k-homomorphismes de sous-corps.

Lemme 8.5. *Soient $k \subseteq K \subseteq E$ des corps discrets avec E normal sur k et de dimension finie sur K. Alors tout k-homomorphisme de K dans E peut être étendu en un k-automorphisme de E.*

Démonstration. Soit $\sigma\colon K \to E$ un k-homomorphisme. Comme E est de dimension finie sur K, il suffit, par récurrence, de voir que si $\alpha \in E$, alors E est de dimension finie sur $K[\alpha]$ et σ peut être étendu en un k-homomorphisme de $K[\alpha]$ dans E.

Comme E est de dimension finie sur K, le théorème 1.13 dit que $K[\alpha]$ est de dimension finie sur K, donc E est de dimension finie sur $K[\alpha]$ d'après le théorème II.6.6. Comme E est normal sur k, on a un polynôme $g \in k[X]$ qui annule α et qui est un produit de polynômes linéaires de $E[X]$. Comme E est de dimension finie sur K, le théorème 1.13 dit qu'il existe un polynôme irréductible $f \in K[X]$ qui annule α. Clairement f divise g dans $K[X]$, donc f^σ divise $g^\sigma = g$. Comme g est un produit de polynômes linéaires de $E[X]$, on obtient que f^σ annule un $\beta \in E$. D'après le lemme 8.1 nous pouvons étendre σ en un k-homomorphisme de $K[\alpha]$ vers E qui envoie α sur β. □

La normalité est reliée à l'invariance par automorphismes.

Théorème 8.6. *Soient $k \subseteq K \subseteq E$ des corps discrets. Si K est normal sur k, tout k-endomorphisme de E envoie K sur K. Si E est de dimension finie et normal sur k, et si tout k-automorphisme de E envoie K dans K, alors K est normal sur k.*

Démonstration. Soient K normal sur k et σ un k-endomorphisme de E. D'après le lemme 8.2, il suffit de démontrer que $K^\sigma \subseteq K$. Soient $\alpha \in K$ et $f \in k[X]$ un produit de polynômes linéaires de $K[X]$ satisfaisant $f(\alpha) = 0$. Comme $f(\alpha^\sigma) = f^\sigma(\alpha^\sigma) = f(\alpha)^\sigma = 0$, et comme f est un produit de polynômes linéaires de $K[X]$, on a $\alpha^\sigma \in K$.

Supposons maintenant que E est de dimension finie et normal sur k, et que tout k-automorphisme de E envoie K dans K. Si $\alpha \in K$, alors α est racine d'un polynôme $f \in k[X]$ qui est un produit de polynômes linéaires de $E[X]$. Comme E est de dimension finie sur k, nous pouvons supposer que f est irréductible. Il suffit de démontrer que toute racine β de f dans E est dans K. D'après le lemme 8.1, on a un k-homomorphisme $\sigma\colon k[\alpha] \to E$ qui envoie α sur β. D'après le lemme 8.5, on peut étendre σ en un k-automorphisme de E. Mais tout k-automorphisme de E envoie K dans K. Donc l'élément $\beta = \alpha^\sigma$ est dans K. □

Une propriété cruciale d'une extension de Galois de dimension finie $k \subseteq K$ est que tout élément de $K \setminus k$ est modifié par l'action d'un élément de $\mathcal{G}(K/k)$. En fait, il s'agit d'une propriété caractéristique.

Théorème 8.7. *Soit K une extension de dimension finie d'un corps discret k. Alors les propriétés suivantes sont équivalentes.*

(i) *K est un extension de Galois de k.*

(ii) *Si $\alpha \in K \setminus k$, il existe un $\sigma \in \mathcal{G}(K/k)$ tel que $\sigma(\alpha) \neq \alpha$.*

(iii) *Si $\alpha \in K$ et si le polynôme minimal f de α sur k est de degré n, alors il existe $\sigma_1, \ldots, \sigma_n$ dans $\mathcal{G}(K/k)$ tels que $f(X) = (X - \sigma_1(\alpha)) \cdots (X - \sigma_n(\alpha))$ et $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ sont distincts.*

Démonstration. Supposons (i). Soit f le polynôme minimal sur k d'un élément $\alpha \in K \backslash k$. Comme K est séparable et normal sur k, et comme le degré de f est plus grand que 1, il y a une racine $\beta \neq \alpha$ de $f \in K$. D'après le lemme 8.1, nous pouvons construire un k-homomorphisme $\sigma\colon k[\alpha] \to K$ tel que $\sigma(\alpha) = \beta$, et nous pouvons étendre σ en un automorphisme de K d'après le lemme 8.5.

Supposons (ii). Soient α et f comme dans (iii). Nous montrons par récurrence comment construire les éléments $\sigma_1, \dots, \sigma_n$ de $\mathcal{G}(K/k)$. Supposons que nous avons construit $\sigma_1, \dots, \sigma_s$, avec $s < n$, tels que le polynôme $g(X) = (X - \sigma_1(\alpha)) \cdots (X - \sigma_s(\alpha))$ divise f et $\sigma_1(\alpha), \dots, \sigma_s(\alpha)$ sont distincts. Comme f est irréductible sur k, et comme g est un diviseur strict de f, un coefficient de g est dans $K \backslash k$. D'après (ii), on a un $\tau \in \mathcal{G}(K/k)$ tel que $g^\tau \neq g$. Comme $\tau\sigma_i(\alpha)$ est une racine de g^τ pour $1 \leqslant i \leqslant s$, on a un i tel que $\tau\sigma_i(\alpha) \notin \{\sigma_1(\alpha), \dots, \sigma_s(\alpha)\}$: on pose $\sigma_{s+1} = \tau\sigma_i$.

Le fait que (iii) implique (i) est clair. □

Si K est un corps discret et si S est un ensemble d'automorphismes de K, alors l'ensemble $\{\, x \in K : x^\sigma = x \text{ pour tout } \sigma \in S \,\}$ est un corps que l'on appelle le **corps fixe** de S. Le théorème 8.7 implique que si K est une extension de Galois de dimension finie de k, alors k est le corps fixe de $\mathcal{G}(K/k)$. L'exercice 8 montre que la condition 8.7(ii) est plus forte que la seule condition que k est le corps fixe de $\mathcal{G}(K/k)$.

Soit $k \subseteq E$ une extension de Galois de dimension finie. Le théorème fondamental de la théorie de Galois concerne la correspondance entre d'une part les sous-corps K de E qui contiennent k et sont de dimension finie sur k, et d'autre part les sous-groupes finis de $\mathcal{G}(E/k)$. Le sous-groupe de $\mathcal{G}(E/k)$ associé à K est $\mathcal{G}(E/K)$.

Théorème 8.8. *Soit E une extension de Galois de dimension finie d'un corps discret k. Soit K un sous-corps de E contenant k et de dimension finie sur k. Alors*

(i) *E est une extension de Galois de dimension finie de K ;*

(ii) *$\mathcal{G}(E/K)$ est un sous-groupe fini de $\mathcal{G}(E/k)$;*

(iii) *le corps fixe de $\mathcal{G}(E/K)$ est K ;*

(iv) *si K est normal sur k, la restriction à K est un homomorphisme de $\mathcal{G}(E/k)$ sur $\mathcal{G}(K/k)$ de noyau $\mathcal{G}(E/K)$, donc $\mathcal{G}(E/K)$ est un sous-groupe normal de $\mathcal{G}(E/k)$;*

(v) *si $\mathcal{G}(E/K)$ est un sous-groupe normal de $\mathcal{G}(E/k)$, alors K est normal sur k.*

Démonstration. Comme E est galoisien sur k, il est galoisien sur K ; donc (i) est valide. Le point (ii) est clair, et (iii) découle de la condition 8.7(ii).

Pour démontrer (iv), on prend K normal sur k et $\sigma \in \mathcal{G}(E/k)$. Le théorème 8.6 dit que $K^\sigma = K$, donc la restriction de σ à K est un élément de $\mathcal{G}(K/k)$.

Par suite, cette restriction définit un homomorphisme de $\mathcal{G}(E/k)$ vers $\mathcal{G}(K/k)$. Son noyau est clairement $\mathcal{G}(E/K)$. D'après le lemme 8.5, tout élément de $\mathcal{G}(K/k)$ peut être étendu en un k-automorphisme de K. Donc l'homomorphisme est surjectif.

Pour démontrer (v), on note que pour $\sigma, \tau \in \mathcal{G}(E/k)$, on a $\sigma \in \mathcal{G}(E/K)$ si, et seulement si, $\tau\sigma\tau^{-1} \in \mathcal{G}(E/K^\tau)$; donc $\tau\mathcal{G}(E/K)\tau^{-1} = \mathcal{G}(E/K^\tau)$. Ainsi, si $\mathcal{G}(E/K)$ est un sous-groupe normal de $\mathcal{G}(E/k)$, on a $\mathcal{G}(E/K) = \mathcal{G}(E/K^\tau)$. D'après la propriété 8.7(ii), cela implique que $K^\tau = K$, donc K est normal. □

Il nous reste à démontrer que tout sous-groupe fini de $\mathcal{G}(E/k)$ est de la forme $\mathcal{G}(E/K)$ [1]. En fait, nous allons montrer que si G est un groupe fini d'automorphismes d'un corps discret E, et si K est le corps fixe de G, alors $\dim_K E = \#G$ et E est une extension galoisienne de K de groupe de Galois G.

Soit E un corps discret et M un monoïde. Un homomorphisme de monoïdes de M vers le monoïde multiplicatif de E est appelé un **caractère** de M dans E. Tout automorphisme de E est un caractère du monoïde multiplicatif E dans E. L'ensemble E^M des fonctions de M vers E est un espace vectoriel sur E pour l'addition et la multiplication scalaire naturelles. L'inégalité naturelle sur E^M est définie en posant $f \neq g$ si on a un $m \in M$ tel que $f(m) \neq g(m)$.

Des fonctions $f_1, \ldots, f_n \in E^M$ sont **linéairement indépendantes** si, chaque fois que $a_1, \ldots, a_n$ sont des éléments non tous nuls de E, on a $a_1 f_1 + a_2 f_2 + \cdots + a_n f_n \neq 0$. Le lemme suivant donne un critère simple pour l'indépendance linéaire des caractères.

Lemme 8.9. *Soient M un monoïde, E un corps discret et $\sigma_1, \ldots, \sigma_n$ des caractères de M dans E tels que $\sigma_i \neq \sigma_j$ si $i \neq j$. Alors $\sigma_1, \ldots, \sigma_n$ sont linéairement indépendants.*

Démonstration. Nous procédons par récurrence sur n. Soient $a_1, \ldots, a_n$ des éléments non tous nuls de E. Si $n = 1$, alors $\sum_{i=1}^n a_i\sigma_i(1) = a_1 \neq 0$, donc nous pouvons renuméroter et supposer que $a_2 \neq 0$. Comme $\sigma_1 \neq \sigma_2$, il y a un $x \in M$ tel que $\sigma_1(x) \neq \sigma_2(x)$. Soit m un élément arbitraire de M et soustrayons l'expression

$$\sigma_1(x)\,(a_1\sigma_1(m) + \cdots + a_n\sigma_n(m)) \qquad (*)$$

de l'expression

$$a_1\sigma_1(xm) + \cdots + a_n\sigma_n(xm) = a_1\sigma_1(x)\sigma_1(m) + \cdots + a_n\sigma_n(x)\sigma_n(m). \qquad (**)$$

Les termes avec a_1 sont supprimés, il reste un terme $a_2(\sigma_2(x) - \sigma_1(x))\sigma_2(m)$ plus une combinaison linéaire des caractères $\sigma_3, \ldots, \sigma_n$. Par récurrence, on a un m pour lequel cette expression est non nulle, parce que $a_2(\sigma_2(x) - \sigma_1(x)) \neq 0$. Comme cette expression est la différence de $(*)$ et de $(**)$, l'une des deux doit être non nulle. Donc m ou xm montre que $\sum a_i\sigma_i \neq 0$. □

1. **NdT.** Cela résultera du théorème 8.11.

D'après le lemme 8.9, nous voyons que des automorphismes distincts d'un corps discret E sont linéairement indépendants sur E. Nous allons raffiner encore un peu ce résultat.

Lemme 8.10. *Soient K un corps discret et $\sigma_1, \dots, \sigma_n$ des automorphismes distincts de K. Il existe $\omega_1, \dots, \omega_n \in K$ tels que la matrice $\Sigma_n = \big(\sigma_i(\omega_j)\big)_{1 \leqslant i,j \leqslant n}$ est inversible.*

Démonstration. Nous procédons par récurrence sur n. Le cas $n = 1$ est obtenu en prenant $\omega_1 = 1$. Par récurrence, on a $\omega_1, \dots, \omega_{n-1} \in K$ tels que la matrice $\Sigma_{n-1} = \big(\sigma_i(\omega_j)\big)_{1 \leqslant i,j \leqslant n-1}$ est inversible. Donc il existe des éléments $a_1, \dots, a_{n-1} \in K$ tels que pour $j = 1, \dots, n-1$ on a

$$a_1\sigma_1(\omega_j) + \cdots + a_{n-1}\sigma_{n-1}(\omega_j) = \sigma_n(\omega_j)$$

D'après le lemme 8.9, on a un $\omega_n \neq 0 \in K$ tel que

$$a_1\sigma_1(\omega_n) + \cdots + a_{n-1}\sigma_{n-1}(\omega_n) \neq \sigma_n(\omega_n). \qquad (*)$$

Soit $\Sigma_n = \big(\sigma_i(\omega_j)\big)_{1 \leqslant i,j \leqslant n}$. Pour voir que Σ_n est inversible, considérons la i-ième ligne de Σ_n, notée ν_i. En remplaçant ν_n par $\nu_n - (a_1\nu_1 + \cdots + a_{n-1}\nu_{n-1})$ nous obtenons une matrice de même déterminant que Σ_n, dont la dernière ligne est nulle sauf pour la dernière entrée qui est non nulle d'après $(*)$. Le déterminant de la matrice modifiée est égal à $\det \Sigma_{n-1}$ multiplié par le coefficient non nul en position sud-est. Donc $\det \Sigma_n \neq 0$. □

Nous pouvons maintenant compléter la correspondance de Galois entre sous-groupes de $\mathcal{G}(E/k)$ et corps intermédiaires entre k et E.

Théorème 8.11. *Soient E un corps discret, G un ensemble de n automorphismes distincts de E et K le corps fixe de G. Alors il existe n éléments de E qui sont linéairement indépendants sur K. Si G est un groupe, alors $\dim_K E = n$ et E est une extension galoisienne de K de groupe de Galois G.*

Démonstration. Soit $G = \{\sigma_1, \dots, \sigma_n\}$. D'après le lemme 8.10, on a des éléments $\omega_1, \dots, \omega_n \in E$ tels que la matrice $\Sigma_n = \big(\sigma_i(\omega_j)\big)_{1 \leqslant i,j \leqslant n}$ est inversible. Soient $a_1, \dots, a_n$ des éléments de K vérifiant $a_1\omega_1 + \cdots + a_n\omega_n = 0$. Alors $a_1\sigma_i(\omega_1) + \cdots + a_n\sigma_i(\omega_n) = 0$ pour chaque i. Or la matrice Σ_n est inversible, donc les a_j sont nuls. Donc les ω_j sont linéairement indépendants.

Supposons maintenant que G est un groupe. Nous allons montrer que les ω_j engendrent E comme K-espace vectoriel. Soit $\omega \in E$. Comme Σ_n est inversible, on a $a_1, \dots, a_n \in K$ tels que

$$a_1\sigma_i(\omega_1) + \cdots + a_n\sigma_i(\omega_n) = \sigma_i(\omega) \qquad (*)$$

pour $i = 1, \ldots, n$. Comme G est un groupe, $\sigma G = G$ pour chaque $\sigma \in G$, donc en transformant $(*)$ par σ nous obtenons

$$\sigma(a_1)\sigma_i(\omega_1) + \cdots + \sigma(a_n)\sigma_i(\omega_n) = \sigma_i(\omega)$$

pour $i = 1, \ldots, n$. En soustrayant cela de $(*)$, nous obtenons

$$(a_1 - \sigma(a_1))\sigma_i(\omega_1) + \cdots + (a_n - \sigma(a_n))\sigma_i(\omega_n) = 0.$$

Mais Σ_n est inversible, donc $a_j = \sigma(a_j)$ pour tous σ et j, par suite $a_1, \ldots, a_n$ sont dans K. En prenant pour σ_i l'identité dans $(*)$, nous obtenons

$$a_1\omega_1 + \cdots + a_n\omega_n = \omega.$$

Ainsi $\omega_1, \ldots, \omega_n$ engendrent E sur K.

Le théorème 8.7 montre que E est une extension de Galois de K. Le fait que G est son groupe de Galois découle du théorème 8.4. □

Exercices

1. Soit K une extension algébrique d'un corps discret k. Montrer que K est normal si, et seulement si, tout polynôme de $k[X]$ qui a une racine dans K est divisible par un polynôme de $k[X]$ égal à un produit de polynômes linéaires de $K[X]$.
2. Définir ce qu'est un corps de décomposition pour un ensemble de polynômes. Soient $k \subseteq K$ des corps discrets. Montrer que l'extension K/k est normale si, et seulement si, il existe un ensemble de polynômes de $k[X]$ dont le corps de décomposition sur k est K.
3. Formuler et démontrer les lemmes 8.9 et 8.10 pour un anneau commutatif local K.
4. Soient k un corps discret et $K = k(X)$. On définit deux k-automorphismes σ et τ de K en posant $\sigma(X) = 1/X$ et $\tau(X) = 1 - X$.
   (i) Montrer que le groupe G engendré par σ et τ est le groupe symétrique sur trois lettres.
   (ii) Soit $I = (X^2 - X + 1)^3/X^2(X - 1)^2$. Montrer que X est une solution de l'équation polynomiale
   $$f(Y) = (Y^2 - Y + 1)^3 - IY^2(Y - 1)^2 = 0.$$
   (iii) Montrer que $k(I)$ est le corps fixe de G.
5. Soient $x_1, \ldots, x_n$ des éléments distincts d'un corps discret k et $a_1, \ldots, a_n$ des éléments de k non tous nuls. Utiliser le lemme 8.9 pour montrer qu'il existe un $m \in \mathbb{N}$ tel que $a_1x_1^m + \cdots + a_nx_n^m \neq 0$.

6. Soient $k \subseteq K$ des corps discrets. Supposons que K est un anneau factoriel de dimension finie comme k-espace vectoriel. Montrer que $\mathcal{G}(K/k)$ est fini et que $\#\mathcal{G}(K/k) \leqslant \dim_k K$.
7. Soit K un corps de décomposition de $X^3 - 2$ sur $\mathbb{Q}$. Montrer que si ω est le quotient de deux racines distinctes de $X^3 - 2$ dans K, alors $\omega^2 + \omega + 1 = 0$. En définissant un corps k intermédiaire entre $\mathbb{Q}$ et $\mathbb{Q}[\omega]$, construire un exemple brouwerien de corps discrets $k \subseteq K$ tels que $\dim_k K = 3$, mais $\mathcal{G}(K/k)$ n'est pas fini.
8. Utiliser l'exercice 7 pour construire un exemple brouwerien, utilisant le principe de Markov, de corps discrets $k \subseteq K$ tels que K est séparable et de dimension finie sur k, et k est le corps fixe de $\mathcal{G}(K/k)$, mais la condition 8.7(ii) n'est pas satisfaite.

9 Notes

Un équivalent classique du Nullstellensatz faible dit que si I est un idéal propre de $k[X_1, \ldots, X_n]$, il existe une extension K algébrique de k telle que les polynômes de I ont un zéro commun dans K^n. Cela résulte de notre version en étendant I en un idéal maximal M (par le lemme de Zorn) et en définissant $K = k[X_1, \ldots, X_n]/M$. Avec une restriction (constructive) convenable sur k, on peut prouver ce théorème de manière directe.

Pour une comparaison entre les approches constructives et récursives des corps de décomposition et des clôtures algébriques, voir [Bridges-Richman 1987].

VII. Factorisation des polynômes

Sommaire

1 Corps factoriels et corps séparablement factoriels

Dans cette section nous étudions le problème de la décomposition en produit de facteurs irréductibles d'un polynôme sur un corps discret. Nous avons déjà vu un exemple brouwerien d'un corps discret sur lequel cette décomposition est impossible (exemple IV.2.2). Un corps discret k sur lequel tout polynôme non constant peut être écrit comme un produit de facteurs irréductibles est appelé un corps **factoriel**. De manière équivalente, k est factoriel si tout polynôme non constant sur k est irréductible ou possède un facteur non trivial. Comme $k[X]$ est un anneau principal avec unités détachables (pour n'importe quel corps discret k), il revient au même de dire que k est factoriel au sens de la définition IV.2.1.

Nous disons que k est **séparablement factoriel** si tout polynôme *séparable* peut être écrit comme un produit de polynômes irréductibles. Clairement tout corps factoriel est séparablement factoriel. Par certains aspects la notion de corps séparablement factoriel est supérieure à la notion de corps factoriel : le théorème 2.4 montre qu'une extension de dimension finie d'un corps séparablement factoriel est un corps séparablement factoriel, alors que l'exercice 1.5 donne un

exemple d'une extension de dimension finie d'un corps factoriel qui n'est pas un corps factoriel.

On voit facilement que tout corps fini est factoriel : étant donné un polynôme, on le divise par tous les polynômes de degré plus petit et l'on regarde si le reste est nul ou pas. Les corps algébriquement clos discrets sont aussi factoriels, pour une raison évidente. Le premier théorème non trivial au sujet des corps factoriels est dû à Kronecker qui a montré que le corps $\mathbb{Q}$ des nombres rationnels est factoriel. Cela résulte immédiatement de « Kronecker 1 » (théorème IV.4.8), qui implique que l'anneau $\mathbb{Z}$ des nombres entiers est factoriel, et du corolaire IV.2.6, qui implique que le corps de fractions d'un anneau intègre factoriel est factoriel.

Beaucoup de corps intéressants sont de la forme $k(\alpha_1, \ldots, \alpha_n)$ où k est un corps fini ou $\mathbb{Q}$. Comme les corps finis et $\mathbb{Q}$ sont factoriels, nous sommes amenés à étudier les extensions simples $k(\alpha)$ d'un corps factoriel k ; les cas les plus importants sont lorsque α est algébrique et lorsque α est transcendant. Nous montrerons tout d'abord qu'une extension d'un corps dénombrable factoriel par un élément séparable est un corps factoriel.

Théorème 1.1. [1] *Soient $k \subseteq E$ des corps discrets, et $\alpha, \beta \in E$ avec α algébrique sur k et β séparable sur $k[\alpha]$. Si k est factoriel, alors α annule un polynôme irréductible sur $k[\beta]$.*

Démonstration. D'après le théorème VI.6.7, on a un $\theta \in E$ tel que $k[\alpha, \beta] = k[\theta]$. Si k est factoriel, alors $k[\beta]$ et $k[\theta]$ sont tous deux de dimension finie sur k d'après le théorème VI.1.13. Donc $k[\theta]$ est de dimension finie sur $k[\beta]$ d'après le théorème II.6.6. Enfin le théorème VI.1.13 nous dit que nous pouvons trouver un polynôme irréductible sur $k[\beta]$ annulé par α. □

Corolaire 1.2. *Soient E un corps discret et k un sous-corps dénombrable factoriel. Soit $\beta \in E$ séparable sur k. Alors $k[\beta]$ est factoriel.*

Démonstration. Soit $g(X)$ un polynôme non constant à coefficients dans $k[\beta]$, et soit $E' \supseteq k[\beta]$ un corps discret dénombrable qui contient une racine α de g (théorème VI.3.3). Alors α annule un polynôme irréductible sur $k[\beta]$, qui doit diviser $g(X)$ dans $k[\beta][X]$. □

Le corolaire 1.2 montre qu'une extension de type fini séparable d'un corps dénombrable factoriel est un corps factoriel. L'exercice 5 montre que la condition de séparabilité est nécessaire. Pour nous débarrasser de la condition de dénombrabilité nous allons montrer qu'un corps discret est (séparablement) factoriel si, et seulement si, tout polynôme (séparable) non constant, ou bien a une racine dans le corps, ou bien est évalué non nul en tout élément du corps.

1. **NdT.** Dans le livre original en anglais, la numérotation des énoncés commence à Theorem 1.2 ; elle est donc décalée d'un cran par rapport à la numérotation présente.

Pour cela nous construisons, à partir d'un polynôme donné f, un polynôme q tel que tout coefficient d'un diviseur unitaire de f est une racine de q.

Pour assurer que le polynôme q est un produit de polynômes séparables lorsque f est séparable, nous démontrons ce qui suit.

Lemme 1.3. *Soit K un corps, extension séparable d'un corps discret k. Si $q \in k[X]$ se décompose en un produit de facteurs linéaires dans $K[X]$, alors q est un produit de polynômes séparables.*

Démonstration. Soit $\alpha \in K$ une racine de q. L'élément α annule un polynôme séparable $f \in k[X]$. Soit $h = \operatorname{pgcd}(q, f)$. Alors $h(\alpha) = 0$ et h est séparable car il divise f. Par récurrence sur le degré, le polynôme q/h est un produit de polynômes séparables. Donc q est un produit de polynômes séparables. □

Nous utilisons un corps de décomposition pour construire q, mais nous pourrions nous en dispenser car les coefficients de q peuvent être écrits directement en termes des coefficients de f.

Théorème 1.4. *Soient k un corps discret et $f \in k[X]$ un polynôme unitaire (séparable). Alors il existe un polynôme $q \in k[X]$ (qui est un produit de polynômes séparables) tel que, pour toute extension E de k, les coefficients de tout diviseur unitaire de f dans $E[X]$ sont des racines de q.*

Démonstration. Soient k_0 le sous-corps dénombrable de k engendré par les coefficients de f et K_f un corps de décomposition pour f sur k_0. Nous écrivons

$$f(X) = (X - r_1)(X - r_2) \cdots (X - r_n)$$

dans K_f. Soit $S \subseteq k[Y_1, \ldots, Y_n]$ l'ensemble des polynômes symétriques élémentaires en les sous-ensembles finis des indéterminées $\{Y_1, \ldots, Y_n\}$, et posons

$$q(X) = \prod\nolimits_{\sigma \in S} \big(X - \sigma(r_1, \ldots, r_n)\big).$$

Comme les coefficients de f sont les polynômes symétriques élémentaires en tous les r_i, le théorème II.8.1 nous dit que $q \in k_0[X]$ et que q est indépendant du corps de décomposition K_f.

Si f est séparable, q est un produit de polynômes séparables d'après le lemme 1.3. Si g est un diviseur unitaire de f dans $E[X]$, on construit un corps de décomposition K_f pour f sur le sous-corps de E engendré par les coefficients de g et f. Clairement K_f est un corps de décomposition pour f sur k_0 et il contient les coefficients de g. Tout coefficient de g est un polynôme symétrique élémentaire en certaines des racines de f dans K_f, donc c'est une racine de q. □

Corolaire 1.5. *Si k est séparablement clos dans K, et si un polynôme séparable unitaire $f \in k[X]$ a un diviseur unitaire $g \in K[X]$, alors $g \in k[X]$. Si k est algébriquement clos dans K et si le polynôme unitaire $f \in k[X]$ a un diviseur unitaire $g \in K[X]$, alors $g \in k[X]$.*

Démonstration. Tout coefficient de tout diviseur unitaire de $f \in k[X]$ annule un polynôme de $k[X]$ (séparable si f est séparable). Comme k est algébriquement (séparablement) clos dans K, ces coefficients sont dans k. □

Le théorème 1.4 nous assure que les coefficients d'un diviseur unitaire d'un polynôme unitaire séparable sont séparables. Nous pouvons laisser tomber l'hypothèse de séparabilité si nous demandons que les deux facteurs soient premiers entre eux.

Corolaire 1.6. *Soient $k \subseteq E$ des corps discrets, $f \in k[X]$ et $g, h \in E[X]$ des polynômes unitaires tels que $f = gh$ et $\operatorname{pgcd}(g, h) = 1$. Alors les coefficients de g et h sont séparables sur k.*

Démonstration. D'après le théorème VI.6.3, nous pouvons écrire f comme un produit de polynômes unitaires dans $k[X]$ de la forme $F_i(X^{q_i})$, où F_i est séparable et q_i est égal à 1 ou à une puissance de la caractéristique de k. On a alors $F_i(X^{q_i}) = a_i(X)b_i(X)$ où $a_i(X) = \operatorname{pgcd}(F_i(X^{q_i}), g(X))$ et $b_i(X) = \operatorname{pgcd}(F_i(X^{q_i}), h(X))$. En outre les F_i sont deux à deux étrangers, donc g est le produit des a_i et h est le produit des b_i. Nous sommes ramenés au cas où $f = F(X^q)$ avec F séparable. Nous faisons une récurrence sur q. Si $q = 1$ nous avons le résultat par le théorème 1.4. Si $q > 1$, nous avons $0 = f'(X) = g'h + gh'$ donc g divise $g'h$, donc g divise g', donc $g' = 0 = h'$. Par suite $g = G(X^p)$ et $h = H(X^p)$, donc $F(X^{q/p}) = G(X)H(X)$. Par récurrence, les coefficients de G et H, qui sont les mêmes que les coefficients de g et h, sont séparables sur k. □

Nous allons montrer qu'un corps, extension de dimension finie d'un corps séparablement factoriel, est séparablement factoriel. Tout d'abord nous réduisons le problème de savoir si un corps est (séparablement) factoriel à celui de décider si un polynôme (séparable) a une racine.

Théorème 1.7 (le test de racine)**.** *Un corps discret k est (séparablement) factoriel si, et seulement si, pour tout f (séparable) dans $k[X]$, ou bien f a une racine dans k, ou bien $f(a) \neq 0$ pour tout $a \in k$.*

Dans ce cas on dit que le corps k a un **test de racine** (pour les polynômes séparables).

Démonstration. Si k est (séparablement) factoriel, nous pouvons construire tous les diviseurs unitaires linéaires de f, donc la condition est clairement nécessaire. Pour l'implication réciproque nous utilisons le théorème 1.4 qui nous permet de construire un polynôme $q \in k[X]$ (produit de polynômes séparables) tel que les coefficients de tout diviseur unitaire de $f \in k[X]$ sont racines de q. Vu l'hypothèse, nous pouvons construire l'ensemble fini des racines de q dans k. Nous obtenons ainsi un ensemble fini de polynômes qui contient tous les

diviseurs unitaires de f dans $k[X]$. On peut alors tester les éléments de cet ensemble pour savoir lesquels divisent f. □

Le prototype d'un test de racines est le **test de racine rationnelle** qui dit que si s/t (fraction réduite) est une racine dans $\mathbb{Q}$ du polynôme $a_0+a_1X+\cdots+a_nX^n \in \mathbb{Z}[X]$, alors s doit diviser a_0, et t doit diviser a_n. Ceci limite les racines possibles à un nombre fini de cas, que nous pouvons tester. Le test de racine rationnelle joint au théorème 1.7 fournit une démonstration alternative du théorème de Kronecker selon lequel le corps des nombres rationnels est factoriel. En fait,nous obtenons la version légèrement améliorée suivante du théorème « Kronecker 1 ».

Théorème 1.8. *Si R est un anneau à factorisation unique avec un nombre fini d'unités, alors il en va de même pour $R[X]$. Donc R est factoriel.*

Démonstration. Soit K le corps de fractions de R. Pour montrer que tout élément de $R[X]$ se factorise en polynômes irréductibles dans $R[X]$, il suffit d'après le lemme de Gauss de montrer que K est factoriel. D'après le théorème 1.7, il suffit de voir que K a un test de racine. L'argument esquissé ci-dessus pour le cas des zéros rationnels s'applique ici parce que R est un anneau à factorisation unique avec un nombre fini d'unités. □

Si R est un anneau à factorisation unique avec un nombre fini d'unités, alors le théorème 1.8 avec une récurrence sur n montre que $R[X_1,\ldots,X_n]$ est un anneau à factorisation unique. Donc si F est un corps fini, $F(X_1,\ldots,X_n)$ est factoriel d'après le corolaire IV.2.6. De même $\mathbb{Q}(X_1,\ldots,X_n)$ est factoriel parce que l'anneau des entiers $\mathbb{Z}$ est un anneau à factorisation unique avec deux unités. Cela ne traite cependant pas tous les cas intéressants. Le théorème « Kronecker 2 » (théorème IV.4.9) montre que si k est un corps factoriel, alors il en va de même pour $k(X)$. Nous présentons maintenant une démonstration élégante de ce théorème, basée sur le « test de racine », qui donne une information supplémentaire pour les corps séparablement factoriels.

Théorème 1.9. *Si k est un corps (séparablement) factoriel, il en va de même pour $k(X)$.*

Démonstration. Soit $f(X,Y) \in k[X,Y]$ (séparable comme polynôme en Y sur $k[X]$) ; il suffit d'après le test de racines de décider s'il existe ou non un $\alpha \in k(X)$ tel que $f(X,\alpha)=0$. On écrit

$$f(X,Y) = a_0(X) + a_1(X)Y + \cdots + a_n(X)Y^n.$$

Nous remplaçons Y par $Z/(a_n(X))$ et nous multiplions par $a_n(X)^{n-1}$, nous obtenons un polynôme unitaire en Z. Donc nous pouvons supposer que $a_n(X)=1$, et nous cherchons les racines $\alpha \in k[X]$ parmi les diviseurs de $a_0(X)$.

Dans le cas séparable, nous notons $f'(X,Y)$ la dérivée de $f(X,Y)$ comme polynôme en Y et nous calculons $s(X,Y)$ et $t(X,Y) \in k[X,Y]$ tels que

$$s(X,Y)f(X,Y) + t(X,Y)f'(X,Y) = g(X)$$

avec $g(X)$ non nul. Si k est fini, $k(X)$ est factoriel (théorème 1.8) et nous avons terminé. Ainsi le théorème VI.5.4 nous dit que, ou bien nous avons terminé, ou bien nous pouvons trouver des éléments distincts $x_1, \ldots, x_m \in k$ avec $m > \deg a_0(X)$ et avec $g(x_i) \neq 0$ pour tout i dans le cas séparable. Dans le cas séparable, chaque polynôme $f(x_i, Y)$ est séparable. Donc (dans tous les cas) nous pouvons construire les ensembles finis $A_i = \{\, y \in k : f(x_i, y) = 0 \,\}$. Si $f(X, \alpha(X)) = 0$, alors $\alpha(x_i) \in A_i$ et nous pouvons construire, par interpolation unique, un ensemble fini de candidats pour $\alpha(X)$. □

Exercices

1. Montrer qu'un corps discret k est factoriel si, et seulement si, tout polynôme non constant sur k est irréductible ou admet un diviseur non trivial.
2. Donner un exemple brouwerien d'une extension simple $k(\alpha)$ avec α ni algébrique ni transcendant sur k.
3. Un **corps premier** est un corps discret k tel que tout sous-corps de k est égal à k [1]. Notons $p_1, p_2, p_3, p_4, \ldots$ la suite des nombres premiers congrus à 1 modulo 4, et soit a une suite binaire fugitive. On définit l'anneau R comme l'anneau $\mathbb{Z}$ muni de la relation d'égalité suivante : $d = e$ s'il existe un n tel que $a_n p_n \mid d - e$. Montrer que R est un anneau intègre discret, et que son corps de fractions k est un exemple brouwerien de corps premier qui n'est pas factoriel.
4. Montrer que si $F_1 \subseteq F_2 \subseteq F_3 \subseteq \cdots$ sont des corps factoriels, et F_i est algébriquement clos dans F_{i+1} pour tout i, alors $F = \bigcup_i F_i$ est factoriel. En déduire que si k est factoriel, il en va de même pour le corps $k(X_1, X_2, \ldots)$ avec un ensemble dénombrable d'indéterminées.
5. Soit u une suite binaire croissante au sens large. Soit F un corps discret de caractéristique 2. Prenons $G_i = k$ dans le théorème VI.2.10 si $u_i = 0$, et prenons $G_i = K$ dans le même théorème si $u_i = 1$. Utilisez l'exercice 4 pour montrer que $G = \bigcup_i G_i$ est factoriel. Notez que G contient $k = F(a,b)$ (défini dans le théorème VI.2.10). Soit θ un élément d'un corps discret extension de G avec $\theta^2 = a$. En considérant le polynôme $X^2 - b$, montrez que $G[\theta]$ est un exemple brouwerien d'une extension de dimension finie d'un corps factoriel qui n'est pas factoriel ; et donc d'un corps séparablement factoriel qui n'est pas factoriel.

1. **NdT.** Par rapport à la définition donnée page 43, il est demandé en plus ici que k soit discret.

2 Extensions de corps (séparablement) factoriels

Le corolaire 1.2 dit que si k est un corps factoriel dénombrable et si α est séparable sur k, alors $k[\alpha]$ est factoriel. Dans cette section, nous supprimons l'hypothèse de dénombrabilité dans ce théorème, nous démontrons que si k est séparablement factoriel et si α est algébrique sur k, alors $k[\alpha]$ est séparablement factoriel, et nous construisons un corps de décomposition (unique) pour un polynôme séparable sur un corps séparablement factoriel.

Théorème 2.1. [1] *Soient $k \subseteq E$ des corps discrets, $\alpha \in E$ algébrique sur k, et $\beta \in E$ séparable sur $k[\alpha]$. Si k est séparablement factoriel, alors β annule un polynôme irréductible sur $k[\alpha]$.*

Démonstration. D'après le corolaire VI.5.5, on a un élément primitif θ pour $k[\alpha, \beta]$ sur k, qui est séparable sur $k[\alpha]$ d'après le théorème VI.4.5. Pour montrer que β annule un polynôme irréductible, il suffit d'après le théorème VI.1.13 de montrer que $k[\alpha, \beta]$ est un espace vectoriel de dimension finie sur $k[\alpha]$. On applique le corolaire VI.6.4 : on prend $q = p^e$ avec $e \geqslant 0$ tel que l'élément $\lambda = \theta^q$, et donc α^q, est séparable sur k (q est égal à 1 ou à une puissance convenable de la caractéristique de finie de k). Alors $k[\lambda]$ et $k[\alpha^q]$ sont de dimension finie sur k, car k est séparablement factoriel. Par suite, d'après le théorème II.6.6, $k[\lambda]$ est de dimension finie sur $k[\alpha^q]$. Soit $1, \lambda, \lambda^2, \ldots, \lambda^s$ une base de $k[\lambda]$ sur$k[\alpha^q]$. Comme $\theta^q = \lambda \in k[\lambda, \alpha]$, et comme θ est séparable sur $k[\alpha]$, on a $\theta \in k[\lambda, \alpha]$ d'après le théorème VI.6.2, donc $k[\theta] = k[\lambda, \alpha]$. Ainsi $1, \lambda, \lambda^2, \ldots, \lambda^s$ engendrent $k[\theta]$ sur $k[\alpha]$. Supposons que $\sum_{i=0}^{s} a_i \lambda^i = 0$ avec $a_i \in k[\alpha]$. Alors

$$0 = \big(\sum\nolimits_{i=0}^{s} a_i \lambda^i\big)^q = \sum\nolimits_{i=0}^{s} (a_i)^q \lambda^{iq}$$

où $(a_i)^q \in k[\alpha^q]$. Comme λ est séparable sur k, le théorème VI.6.2 nous dit que $k[\alpha^q, \lambda] = k[\alpha^q, \lambda^q]$. Ainsi $1, \lambda^q, \lambda^{2q}, \ldots, \lambda^{sq}$ est une base de $k[\alpha^q, \lambda]$ sur $k[\alpha^q]$. Par suite $(a_i)^q = 0$, donc les a_i sont nuls. Donc $1, \lambda, \ldots, \lambda^s$ est une base de $k[\theta]$ sur $k[\alpha]$, et $k[\theta]$ est de dimension finie sur $k[\alpha]$. □

Lemme 2.2. *Soit k un sous-corps discret d'un anneau E. Soit θ un élément de E qui annule un polynôme unitaire de $k[X]$ de degré $n > 0$. Si $\alpha \in k[\theta]$, alors $\theta \in k[\alpha]$ ou α annule un polynôme de $k[X]$ de degré $< n$.*

Démonstration. Écrivons $\alpha^i = \sum_{j=1}^{n-1} a_{ij} \theta^j$ pour $i = 0, \ldots, n-1$. Par des manipulations élémentaires de lignes nous mettons la matrice $\{a_{ij}\}$ en forme triangulaire supérieure. S'il y a un zéro sur la diagonale, $1, \alpha, \ldots, \alpha^{n-1}$ sont

1. **NdT.** Dans le livre original en anglais, la numérotation des énoncés commence à Theorem 2.0 ; elle est donc décalée d'un cran par rapport à la numérotation présente.

linéairement dépendants sur k, donc α annule un polynôme de degré $< n$. Si les éléments diagonaux sont tous non nuls, le déterminant de $\{a_{ij}\}$ est non nul, donc $\theta \in k[\alpha]$. □

Le théorème suivant, qui a un contenu classique, sera utilisé pour éliminer l'hypothèse de dénombrabilité dans le corolaire (classiquement trivial) 1.2.

Théorème 2.3. *Soient $K \subseteq E$ des anneaux impotents et k un sous-corps discret de K, séparablement clos dans K. Soit $\alpha \in E$ algébrique sur k. Alors $k[\alpha]$ est séparablement clos dans $K[\alpha]$. Si, en outre, α est séparable et k est algébriquement clos dans K, alors $k[\alpha]$ est algébriquement clos dans $K[\alpha]$.*

Démonstration. Soit $\beta \in K[\alpha]$ séparable sur $k[\alpha]$. D'après le théorème VI.6.7, on a un $\theta \in k[\alpha, \beta]$ tel que $k[\theta] = k[\alpha, \beta]$. Pour montrer que $\beta \in k[\alpha]$ il suffit de montrer que $\theta \in k[\alpha]$. D'après le corolaire VI.6.4, il existe un entier q tel que θ^q, qui est dans $K[\alpha^q]$, est séparable sur k, avec q égal à 1 ou à une puissance p^e, k étant de caractéristique finie p. Alors, d'après le théorème VI.4.5, le corps $k[\alpha^q] \subseteq k[\theta^q]$ est séparable sur k. On a donc un polynôme séparable $f \in k[X]$, de degré n, annulé par α^q. Nous procédons par récurrence sur n pour montrer que $\theta^q \in k[\alpha^q]$; et alors $\theta \in k[\alpha]$, d'après le théorème VI.6.2, parce que θ est séparable sur $k[\alpha]$.

Si $n = 1$, alors $\alpha^q \in k$, donc $\theta^q \in K$, et donc $\theta^q \in k$ parce que k est séparablement clos dans K. Supposons maintenant $n > 1$. Comme $\theta^q \in K[\alpha^q]$, d'après le corolaire VI.1.3, on sait que θ^q annule un polynôme de degré n sur K. Mais θ^q annule un polynôme séparable sur k. En prenant le pgcd de ces deux polynômes, et en utilisant le théorème VI.4.1(iii), nous obtenons un polynôme séparable de degré au plus n dans $k[X]$ annulé par θ^q. Comme $\alpha^q \in k[\theta^q]$, le lemme 2.2 nous dit que, ou bien $\theta^q \in k[\alpha^q]$, et nous avons terminé, ou bien α^q annule un polynôme de degré $< n$ et nous terminons par récurrence. Ainsi $\theta^q \in k[\alpha^q]$.

Supposons maintenant que α est séparable sur k et que k est algébriquement clos dans K. Soit θ un élément de $K[\alpha]$ algébrique sur $k[\alpha]$; il nous faut montrer que $\theta \in k[\alpha]$. D'après le corolaire VI.5.5, nous pouvons supposer que $k[\alpha, \theta] = k[\theta]$. L'élément α annule un polynôme unitaire de degré n dans $k[X]$. Nous procédons par récurrence sur n pour montrer que $\theta \in k[\alpha]$. Comme $\theta \in K[\alpha]$, le corolaire VI.1.3 nous dit que θ annule un polynôme unitaire de $K[X]$ de degré n. L'élément θ est aussi algébrique sur k. En appliquant le corolaire 1.5 au pgcd des polynômes que θ annule sur k et K, nous obtenons un polynôme de degré au plus n dans $k[X]$ annulé par θ. D'après le lemme 2.2, ou bien $\theta \in k[\alpha]$, et nous avons terminé, ou bien α annule un polynôme unitaire de degré $< n$. Dans ce dernier cas l'hypothèse de récurrence montre que $\theta \in k[\alpha]$. □

Nous pouvons maintenant éliminer la restriction concernant la dénombrabilité dans le corolaire 1.2 et démontrer le résultat analogue pour les corps séparablement factoriels.

Théorème 2.4. *Soit k un sous-corps séparablement factoriel d'un corps discret E, et soit $\alpha \in E$ algébrique sur k. Alors $K = k[\alpha]$ est séparablement factoriel. Si α est séparable et si k est factoriel, alors K est factoriel.*

Démonstration. Soit $f \in K[X]$ séparable. Soit k_0 la clôture séparable dans k du corps dénombrable engendré par les coefficients d'un polynôme non nul de $k[X]$ annulé par α et par les coefficients des puissances de α présentes dans les coefficients de f. Comme k est séparablement factoriel, k_0 est un corps dénombrable. Comme nous pouvons décider si un polynôme séparable sur k_0 a une racine dans k, et donc dans k_0, le théorème 1.7 dit que k_0 est un corps séparablement factoriel. Pour compléter la démonstration de la première affirmation, il suffit d'après le théorème 1.7 de trouver les racines de f qui sont dans $k_0[\alpha]$, car le théorème 2.3 dit que $k_0[\alpha]$ est séparablement clos dans $k[\alpha]$, et les coefficients de f sont dans $k_0[\alpha]$.

Comme $k_0[\alpha]$ est dénombrable, nous pouvons construire, d'après le théorème VI.3.4, un corps de décomposition L de f sur $k_0[\alpha]$. Soient $r_1, \ldots, r_s$ les racines de f dans L. D'après le théorème 2.1, nous trouvons des polynômes g_i irréductibles dans $k_0[\alpha][X]$ annulés par les r_i. Si l'un des g_i est linéaire, alors $r_i \in k_0[\alpha]$, et nous avons trouvé une racine de f dans $k_0[\alpha]$. Si aucun g_i n'est linéaire, alors f n'a pas de racines dans $k_0[\alpha]$.

La deuxième affirmation est démontrée exactement la même manière que la première, à ceci près que nous prenons pour k_0 la clôture algébrique au lieu de la clôture séparable. □

Dans la section 1, nous avons montré comment construire un corps de décomposition pour un polynôme sur un corps dénombrable. Pour un polynôme séparable sur un corps séparablement factoriel, nous pouvons nous débarrasser de l'hypothèse de dénombrabilité.

Corolaire 2.5. *Soit k un corps séparablement factoriel, et soit $f \in k[X]$ un polynôme séparable. Alors il existe un corps de décomposition séparablement factoriel K pour f sur k.*

Démonstration. Nous procédons par récurrence sur le degré n de f. Si $n = 1$, on prend $K = k$. Supposons $n > 1$. Comme k est séparablement factoriel, f possède un facteur irréductible p. Soit alors $F = k[Y]/(p(Y))$: F est un corps et l'élément $\alpha = Y$ de F est une racine de f, donc $f(X) = (X - \alpha)q(X)$ dans $F[X]$. D'après le théorème 2.4, le corps F est séparablement factoriel. Donc par récurrence, q a un corps de décomposition séparablement factoriel sur F. Ce corps de décomposition est le corps de décomposition voulu pour f sur k. □

Finalement nous montrons que deux corps de décomposition pour un polynôme séparable sur un corps séparablement factoriel k sont toujours isomorphes sur k.

Théorème 2.6. *Soient k_1 et k_2 des corps séparablement factoriels et $\varphi\colon k_1 \to k_2$ un isomorphisme. Soient p_1 un polynôme séparable de $k_1[X]$ et p_2 l'image de p_1 par φ. Soient K_1 et K_2 des corps de décomposition pour p_1 sur k_1 et p_2 sur k_2 respectivement. Alors φ peut être étendu en un isomorphisme $K_1 \to K_2$.*

Démonstration. Il est clair que le polynôme p_2 est séparable sur k_2. Si $\deg p_1 = 0$, il n'y a rien à démontrer, donc supposons que α_1 est une racine de p_1 dans K_1. Comme k_1 est séparablement factoriel, α_1 est une racine d'un facteur irréductible q_1 de p_1 dans $k_1[X]$. Soit q_2 l'image de q_1 par φ. Alors q_2 est un facteur de p_2, donc $q_2(\alpha_2) = 0$ pour un $\alpha_2 \in K_2$. L'isomorphisme φ s'étend en un isomorphisme, que nous notons encore φ, de $k_1[\alpha_1]$ vers $k_2[\alpha_2]$ en imposant $\varphi(\alpha_1) = \alpha_2$. Comme le corps $k_1[\alpha_1]$ est séparablement factoriel, nous pouvons étendre cet isomorphisme, par récurrence sur le degré de p_1, en un isomorphisme $K_1 \to K_2$. □

Exercices

1. Soit k un corps dénombrable séparablement factoriel. Montrer qu'il existe une extension séparable dénombrable K de k telle que tout polynôme séparable sur K a une racine dans K. Le corps K est appelé une **clôture séparable** de k.
2. Soit k un corps dénombrable séparablement factoriel. Montrer que si K et L sont des clôtures séparables de k, alors K et L sont k-isomorphes.
3. Utiliser le théorème VI.2.10 pour construire un exemple classique qui montre que l'hypothèse que α est séparable est nécessaire dans le théorème 2.3.
4. Soit k un corps séparablement factoriel contenu dans un anneau commutatif discret R. Supposons que R est une extension algébrique séparable de type fini de k. Montrer que R est de dimension finie sur k. (Chercher les idempotents non nuls minimaux $e \in R$; notons que ke est un sous-corps de l'anneau Re et qu'il est isomorphe à k.)

3 Corps de Seidenberg : la condition P

Soit k un corps discret de caractéristique finie p. La condition P de Seidenberg apparait lorsqu'on veut savoir si un élément donné de k a une racine p-ième dans k, c'est-à-dire si le sous-corps k^p des puissances p-ièmes d'éléments de k est détachable dans k. La condition introduite par Seidenberg est la première condition dans le théorème suivant.

Théorème 3.1. *Soit k un corps discret de caractéristique finie p. Les propriétés suivantes sont équivalentes.*

(i) *Étant donnés $a_{ij} \in k$ ($1 \leqslant i \leqslant m$ et $1 \leqslant j \leqslant n$), ou bien il existe des $x_j \in k^p$ non tous nuls tels que $\sum a_{ij}x_j = 0$ pour tout i, ou bien, lorsque $\sum a_{ij}x_j = 0$ pour tout i avec les $x_j \in k^p$, les x_j sont tous nuls.*

(ii) *Si K est un corps extension de dimension finie de k, K^p est détachable dans K.*

(iii) *Si K est une extension de dimension finie purement inséparable de k, K^p est détachable dans K.*

(iv) *Tout corps K extension de type fini de k avec $K^p \subseteq k$ est de dimension finie.*

(v) *Tout sous-k^p-espace vectoriel de type fini de k est de dimension finie.*

Démonstration. Pour déduire (ii) de (i), soit $\omega_1, \ldots, \omega_n$ une base de K sur k et notons $\omega_i^p = \sum_{j=1}^n b_{ij}\omega_j$. Alors un élément $\sum a_j\omega_j$ arbitraire de K est dans K^p si, et seulement si, il existe des $x_i \in k^p$ tels que

$$\sum\nolimits_{j=1}^{n} a_j\omega_j = \sum\nolimits_{i=1}^{n} x_i\omega_i^p = \sum\nolimits_{j=1}^{n}\sum\nolimits_{i=1}^{n} x_i b_{ij}\omega_j,$$

i.e. $a_j = \sum_{i=1}^n x_i b_{ij}$ pour tout j ou, puisque les ω_i^p sont indépendants sur k^p, que le système d'équations

$$x_0 a_j - \sum\nolimits_{i=1}^{n} x_i b_{ij} = 0$$

a une solution non triviale dans k^p.

Le point (iii) résulte clairement de (ii). Pour montrer que (iv) découle de (iii), on considère un corps K extension de type fini de k avec $K^p \subseteq k$. Soit ω l'un des générateurs de K sur k. Puisque k^p est détachable dans k, ou bien $\omega^p \in k^p$ et donc $\omega \in k$ et nous terminons par récurrence sur le nombre de générateurs, ou bien $X^p - \omega$ est un polynôme irréductible sur k (théorème VI.6.6) donc $k(\omega)$ est une extension de k de dimension p. Dans ce cas, $k(\omega)$ satisfait clairement aussi (iii). Mais K est une extension de type fini de $k(\omega)$, donc K est de dimension finie sur $k(\omega)$, donc aussi sur k, par récurrence sur le nombre de générateurs.

Pour déduire (v) de (iv), on considère un sous-k^p-espace V de type fini de k. Alors V engendre un sous-corps F de k qui est de type fini sur k^p. Soit $K = F^{-p} \supseteq k$. Alors K est de type fini, donc de dimension finie sur k ; donc $F = K^p$ est de dimension finie sur k^p et par suite le sous-espace V de type fini de F est de type fini sur k^p.

Pour déduire (i) de (v), on considère une base pour le sous-k^p-espace de k engendré par les a_{ij}. Alors la question dans (i) est réduite à l'existence d'une solution non triviale dans k^p pour un système d'équations linéaires homogènes à coefficients dans k^p, ce qui est décidable d'après le théorème II.6.2. □

Nous disons qu'un corps discret k satisfait **la condition P de Seidenberg**, ou que k est un **corps de Seidenberg**, si, pour tout nombre premier p nul dans k, les propriétés équivalentes du théorème 3.1 sont satisfaites.

Le point (ii) du théorème 3.1 nous montre que la condition P est héritée par les extensions de corps de dimension finie. Nous montrons maintenant qu'elle est aussi héritée par les extensions purement transcendantes.

Théorème 3.2. *Si k est un corps de Seidenberg, il en va de même pour $k(X)$.*

Démonstration. Nous allons montrer que le point (i) du théorème 3.1 est satisfait par $k(X)$. Soit

$$\sum\nolimits_j a_{ij}x_j = 0$$

un système d'équations sur $k(X)$ pour lequel nous cherchons une solution non triviale dans $k(X)^p = k^p(X^p)$. Nous pouvons supposer que les a_{ij} appartiennent à $k[X]$, et nous cherchons une solution non triviale dans $k^p[X^p]$. En répartissant les exposants de X dans les classes résiduelles modulo p, nous obtenons un système d'équations équivalent dans lequel les a_{ij} appartiennent à $k[X^p]$.

Les coefficients des a_{ij} engendrent un sous-k^p-espace de k qui, d'après le point (v) du théorème 3.1, est de dimension finie. Soit $\lambda_1, \ldots, \lambda_m$ une base de ce sous-espace. Nous écrivons $a_{ij} = \sum_k a_{ijk}\lambda_k$ avec les $a_{ijk} \in k^p[X^p]$. Alors nous pouvons trouver une solution non triviale dans $k^p(X^p)$ du système original si, et seulement si, nous pouvons trouver une solution non triviale dans $k^p[X^p]$ pour le système

$$\sum\nolimits_j a_{ijk}x_j = 0,$$

mais maintenant les coefficients et la solution recherchée sont tous dans le même corps $k^p(X^p)$, donc le résultat découle du théorème II.6.2. □

L'exercice 1.5 montre qu'une extension de dimension finie d'un corps factoriel n'est pas nécessairement un corps factoriel ; l'ingrédient manquant est la condition P. Appelons un corps discret k **pleinement factoriel** si tout corps extension de dimension finie de k est factoriel.

Théorème 3.3. *Soit k un corps discret. Alors k est pleinement factoriel si, et seulement si, k est séparablement factoriel et satisfait la condition P.*

Démonstration. Supposons que k est pleinement factoriel. Comme k est une extension de dimension finie de lui-même, k est (séparablement) factoriel. Pour montrer que k satisfait la condition P, nous allons vérifier le point (ii) du théorème 3.1. Soit K une extension de dimension finie de k. Alors K est factoriel, donc pour chaque $a \in K$ ou bien le polynôme $X^p - a \in K[X]$ est irréductible, auquel cas $a \notin K^p$, ou bien il est réductible, auquel cas $a \in K^p$ d'après le théorème VI.6.6.

Inversement, supposons que k est séparablement factoriel et satisfait la condition P. Soit K un corps extension de dimension finie de k. Alors K est séparablement factoriel d'après le théorème 2.4, et il satisfait la condition P d'après le théorème 3.1. Soit f un polynôme unitaire de $K[X]$; nous allons

montrer que f a ou n'a pas une racine dans K (donc K est factoriel d'après le théorème 1.7). D'après le théorème VI.6.3, nous pouvons écrire f comme un produit de polynômes unitaires de la forme $g(X^q)$ où g est séparable et q est égal à 1 ou à une puissance de la caractéristique de k, donc par récurrence sur le degré nous pouvons supposer que f est de cette forme. Comme K est séparablement factoriel, nous pouvons supposer que g est irréductible. Par suite, si $g(X^q)$ a une racine dans K, g est linéaire, donc $g(X^q) = X^q - a$. Nous pouvons décider si $X^q - a$ a une racine dans K d'après le point (ii) du théorème 3.1. □

Nous obtenons comme corolaire que toute extension purement transcendante d'un corps pleinement factoriel est pleinement factorielle.

Corolaire 3.4. *Si k est un corps pleinement factoriel alors il en va de même pour $k(X)$.*

Démonstration. Le théorème 3.3 montre que k est un corps de Seidenberg, donc $k(X)$ est un corps de Seidenberg d'après le théorème 3.2. Mais $k(X)$ est factoriel d'après le théorème 1.9, donc $k(X)$ est pleinement factoriel d'après le théorème 3.2. □

Exercices

1. Montrer directement que le corps F de l'exercice 1.5 ne satisfait pas la condition P.
2. Montrer que deux clôtures algébriques d'un corps dénombrable pleinement factoriel k sont toujours isomorphes sur k.
3. Montrer qu'un corps dénombrable discret k est pleinement factoriel si, et seulement si, tout corps extension algébrique de type fini de k est de dimension finie.
4. Construire un exemple brouwerien d'un anneau commutatif discret extension de $\mathbb{Q}$ qui est de type fini et algébrique, mais pas de dimension finie, sur $\mathbb{Q}$.
5. Montrer que si k satisfait la condition P, alors il en va de même pour le corps $k(X_1, X_2, \ldots)$ en une infinité dénombrable d'indéterminées.

4 Le théorème fondamental de l'algèbre

Les nombres complexes algébriques sur $\mathbb{Q}$ forment un corps discret $\mathbb{C}^a$ (théorème VI.1.9), appelé le corps des **nombres algébriques**. Nous allons montrer dans cette section que $\mathbb{C}^a$ est algébriquement clos (théorème 4.5). Nous utiliserons de nombreux résultats de la théorie de Galois et, sans en donner de démonstration, l'existence des 2-sous-groupes de Sylow dans les groupes finis.

Une démonstration du *théorème fondamental de l'algèbre* sous la forme que tout polynôme unitaire non constant sur $\mathbb{C}$ a une racine dans $\mathbb{C}$ est indiquée dans les exercices comme corolaire du théorème 4.5.

Lemme 4.1 (théorème des valeurs intermédiaires pour les polynômes à coefficients rationnels)**.** *Soit $f \in \mathbb{Q}[X]$. Si a et b sont des nombres rationnels tels que $f(a) < 0 < f(b)$, il existe $c \in \mathbb{R}$ qui annule f.*

Démonstration. Nous pouvons supposer que $a < b$. Nous définissons pas récurrence deux suites $\{a_n\}$ et $\{b_n\}$ de nombres rationnels. On initialise $a_0 = a$ et $b_0 = b$. On définit ensuite a_n et b_n pour $n > 0$, comme suit : tout d'abord on calcule $c_n = (a_{n-1} + b_{n-1})/2$, puis on pose

(i) $a_n = b_n = c_n$ si $f(c_n) = 0$,

(ii) $a_n = c_n$ et $b_n = b_{n-1}$ si $f(c_n) < 0$,

(iii) $a_n = a_{n-1}$ et $b_n = c_n$ si $f(c_n) > 0$.

Clairement $a_{n-1} \leqslant a_n \leqslant b_n \leqslant b_{n-1}$, et $b_n - a_n \leqslant (b-a)/2^n$ pour tout $n > 0$. Par conséquent la suite $\{c_n\}$ est une suite de Cauchy, qui représente un nombre réel c. Pour montrer que $f(c) = 0$, nous devons montrer que $f(c_n)$ converge vers 0.

En appliquant le théorème du reste à $f(X)$ comme polynôme sur $\mathbb{Q}[Y]$, nous obtenons une égalité $f(X) = (X-Y)g(X,Y) + f(Y)$ avec un polynôme $g \in \mathbb{Q}[X,Y]$. On obtient facilement une borne M sur $\{\, |g(x,y)| : a \leqslant x, y \leqslant b \,\}$, donc $|f(x)-f(y)| \leqslant M|x-y|$ si $a \leqslant x, y \leqslant b$. Comme les suites $c_n - a_n$ et $b_n - c_n$ convergent vers 0, on déduit que $f(c_n) - f(a_n)$ et $f(b_n) - f(c_n)$ convergent vers 0. Comme $f(a_n) \leqslant 0 \leqslant f(b_n)$ pour tout n, il s'ensuit que $f(c_n)$ converge vers 0. □

Corolaire 4.2. *Soit $f \in \mathbb{Q}[X]$ de degré impair. Alors f a une racine dans $\mathbb{R}$.*

Démonstration. Comme f est de degré impair, il existe des nombres rationnels a et b qui satisfont les hypothèses du lemme 4.1. □

Lemme 4.3. *Si $a+bi \in \mathbb{C}^a$, alors il existe $c+di \in \mathbb{C}^a$ tel que $(c+di)^2 = a+bi$.*

Démonstration. Tout d'abord le cas réel, i.e. $b = 0$. Comme $\mathbb{C}^a$ est discret, $a = 0$ ou $a > 0$ ou $a < 0$. Si $a > 0$, le lemme 4.1 nous dit que le polynôme $X^2 - a$ a une racine dans $\mathbb{R}^a$, que nous notons $\sqrt{a}$. Si $a < 0$, $i\sqrt{-a}$ est une racine de $X^2 - a$. Voyons le cas général. Nous prenons pour c et d des racines convenables [1] des polynômes

$$X^2 - \frac{a + \sqrt{a^2+b^2}}{2} \quad \text{et} \quad X^2 - \frac{-a + \sqrt{a^2+b^2}}{2}.$$

Alors $c + di$ est une racine carrée de $a + bi$. □

1. **NdT.** Le réel cd doit avoir le même signe que b.

La démonstration du théorème final nécessite deux résultats de la théorie des groupes finis.

(i) Si G est un groupe fini et si 2^n divise $\#G$, G contient un sous-groupe d'ordre 2^n.

(ii) Tout groupe fini G contient un sous-groupe T tel que $\#T$ est une puissance de 2 et l'indice de T dans G est impair.

Un sous-groupe T de G qui satisfait (ii) est appelé un **2-sous-groupe de Sylow de** G, ou plus simplement un **2-Sylow de** G. Ces résultats classiques de la théorie des groupes finis ne présentent aucun problème de constructivité.

Lemme 4.4. *Soit $f \in \mathbb{Q}[X]$. Alors f a une racine dans $\mathbb{C}^a$.*

Démonstration. Soit E un corps de décomposition de f sur $\mathbb{Q}$. Il suffit d'immerger E dans $\mathbb{C}^a$. Comme E est de dimension finie sur $\mathbb{Q}$, le groupe de Galois G de E sur $\mathbb{Q}$ est fini. Soit T un 2-Sylow de G et K le corps fixe de T. D'après le corolaire VI.5.5, il existe un $\alpha \in K$ tel que $K = \mathbb{Q}[\alpha]$. Alors α annule un polynôme irréductible g de degré $\dim_{\mathbb{Q}} K$, qui est impair car il est égal à l'indice de T dans G. D'après le corolaire 4.2, le polynôme g a une racine $\theta \in \mathbb{C}^a$. D'après le lemme VI.8.1, il y a un homomorphisme injectif $\sigma\colon K \to \mathbb{C}^a$ qui envoie α sur θ.

Supposons que $\#T = 2^n$. D'après (i), nous pouvons trouver des sous-groupes $T_0 \subseteq \cdots \subseteq T_n = T$ tels que $\#T_i = 2^i$. Soit K_i le corps fixe de T_i. Nous allons étendre progressivement σ, qui est défini sur K_n, pour en faire une immersion de $K_0 = E$ dans $\mathbb{C}^a$. Supposons que σ est défini sur K_{i+1}. La dimension de K_i sur K_{i+1} est 2, donc $K_i = L[\beta]$ où β annule un polynôme irréductible h de degré 2 sur K_{i+1}. D'après le lemme 4.3 et les formules pour une racine carrée, h^σ a une racine dans $\mathbb{C}^a$, donc nous pouvons étendre σ à K_i en application du lemme VI.8.1. □

Théorème 4.5 (le théorème fondamental de l'algèbre, version discrète)**.** *Le corps $\mathbb{C}^a$ est algébriquement clos.*

Démonstration. Soit $f \in \mathbb{C}^a[X]$ un polynôme non constant ; nous devons montrer que f a une racine dans $\mathbb{C}^a$. Soit K le sous-corps de $\mathbb{C}^a$ engendré par les coefficients de f. Le théorème VI.3.3 nous dit comment construire un corps dénombrable discret qui contient K et une racine θ de f, et l'on considère un polynôme $g \in \mathbb{Q}[X]$ annulé par θ. Si f ne divise pas g, on remplace f par le pgcd de f et g dans $\mathbb{C}^a[X]$. On peut donc supposer que f divise g. D'après le théorème VI.3.4, on sait construire un corps de décomposition dénombrable E pour g sur $\mathbb{Q}$. Comme E est une extension séparable de type fini de $\mathbb{Q}$, nous pouvons construire un $\alpha \in E$ tel que $E = \mathbb{Q}(\alpha)$. Soit $h \in \mathbb{Q}[X]$ le polynôme minimal de α, et soit β une racine de h dans $\mathbb{C}^a$. Alors g est un produit de facteurs linéaires sur $\mathbb{Q}(\beta)$, car $\mathbb{Q}(\beta) \simeq E$ est normal. Comme f divise g, il a une racine dans $\mathbb{C}^a$. □

Une démonstration du théorème fondamental de l'algèbre, sous la forme que tout polynôme unitaire non constant sur $\mathbb{C}$ a une racine dans $\mathbb{C}$, est indiquée dans les exercices qui suivent.

Exercices

1. Soit f un polynôme unitaire de $\mathbb{C}^a[X]$ de degré $n > 0$. Montrer que pour chaque $x \in \mathbb{C}^a$ il existe une racine r de f dans $\mathbb{C}^a$ telle que $|r - x|^n \leqslant |f(x)|$.
2. Soit f un polynôme unitaire de $\mathbb{C}[X]$ de degré $n > 0$.
   (i) Utiliser l'exercice 1 pour montrer que pour tout $x \in \mathbb{C}$ et tout $\varepsilon > 0$ il existe un $r \in \mathbb{Q}(i)$ tel que $|f(r)| < \varepsilon$ et $|r - x|^n < |f(x)| + \varepsilon$.
   (ii) Utiliser le point (i) pour construire une suite de Cauchy $r_1, r_2, \ldots$ dans $\mathbb{Q}(i)$ telle que $f(r_i)$ converge vers 0. En déduire que f a une racine dans $\mathbb{C}$.

5 Notes

Kronecker (1882) a démontré que les corps de nombres algébriques sont factoriels. Le résultat selon lequel les extensions finies séparables de corps factoriels sont des corps factoriels se trouve dans [van der Waerden 1953], mais la démonstration est incomplète (voir la discussion dans [Mines-Richman 1982]). Un exemple montrant que la condition de séparabilité est nécessaire (exercice 1.5) apparait pour la première fois dans [Seidenberg 1974].

La condition P a été introduite dans [Seidenberg 1970]. Dans cet article, il a été démontré que les extensions de corps (factoriels) satisfaisant la condition P, de dimension finie ou purement transcendantes, satisfont également la condition P (et sont factoriels). Le théorème 3.1 se trouve dans [Richman 1981].

Brouwer et de Loor (1924) ont donné une démonstration constructive que tout polynôme unitaire non constant sur $\mathbb{C}$ a une racine dans $\mathbb{C}$. Bishop (1967) a démontré le résultat en supposant seulement que le polynôme a un coefficient non nul pour une puissance strictement positive de X.

VIII. Anneaux commutatifs noethériens

Sommaire

1 Le théorème de la base de Hilbert

Le théorème de la base de Hilbert établit que $R[X]$ est noethérien lorsque R est noethérien. Personne n'a donné de démonstration constructive de ce théorème pour notre définition présente d'*anneau noethérien*, mais d'autres définitions ont permis une telle démonstration. Les démonstrations classiques usuelles du théorème sont constructives si l'on entend par *anneau noethérien* un anneau où tous les idéaux sont de type fini. Mais seul l'anneau trivial est noethérien en ce sens d'un point de vue constructif. La première démonstration d'un théorème de la base de Hilbert constructivement intéressant a été donnée par Jon Tennenbaum ;

nous présentons certaines de ses idées dans la section 4. Dans la section présente, nous démontrons le théorème pour les anneaux cohérents noethériens. Du point de vue classique, ce sont exactement les anneaux noethériens.

Pour un anneau R nous notons le R-module $\{ f \in R[X] : \deg f < n \}$ par $R[X]_n$. Clairement, le R-module $R[X]_n$ est libre de rang n. Si I est un idéal à gauche de $R[X]$, alors $I \cap R[X]_n = \{ f \in I : \deg f < n \}$. Si M est un sous-R-module de $R[X]_n$, alors $X^m M$ est un sous-R-module de $R[X]_{n+m}$.

Lemme 1.1. *Soient R un anneau cohérent noethérien (à gauche) et I l'idéal à gauche de $R[X]$ engendré par $f_1, \dots, f_s$. Si $f_i \in R[X]_n$ pour chaque i, il existe un R-module de type fini $M \subseteq R[X]_n$ tel que $XM \cap R[X]_n \subseteq M$ et $I \cap R[X]_m = \sum_{i=0}^{m-n} X^i M$ pour tout $m \geqslant n$.*

Démonstration. Le corolaire III.2.8 dit que $R[X]_m$ est un R-module cohérent noethérien. On construit une chaine $N_1 \subseteq N_2 \subseteq \cdots$ de sous-modules de type fini de $I \cap R[X]_n$ comme suit. Soient $N_1 = Rf_1 + \cdots + Rf_s$ et $N_{k+1} = N_k + XN_k \cap R[X]_n$. Comme $R[X]_{n+1}$ est cohérent, les modules N_k sont de type fini ; comme $R[X]_n$ est noethérien, il y a un k tel que $N_k = N_{k+1}$. On pose $M = N_k$. Clairement $XM \cap R[X]_n \subseteq M$.

Comme $M \subseteq I \cap R[X]_n$, on a $\sum_{i=0}^{m-n} X^i M \subseteq I \cap R[X]_m$ pour tout $m \geqslant n$. Montrons que $I \cap R[X]_m \subseteq \sum_{i=0}^{m-n} X^i M$: soit $f \in I \cap R[X]_m$. On écrit $f = \sum_{i=1}^{s} g_i f_i$, où les $g_i \in R[X]_d$, et l'on procède par récurrence sur d. Si $d = 1$, alors $f \in M$ et c'est terminé. Si $d > 1$, on définit $h_i \in R[X]$ par $g_i = g_i(0) + Xh_i$ et l'on pose $f^* = \sum_{i=1}^{s} h_i f_i \in I$. Notez que $h_i \in R[X]_{d-1}$. Alors $f = \sum_{i=1}^{s} g_i(0) f_i + Xf^*$, donc $Xf^* \in I \cap R[X]_m$ et par suite $f^* \in R[X]_{m-1}$. Si $m = n$, alors par récurrence sur d on a $f^* \in M$ donc $Xf^* \in XM \cap R[X]_n \subseteq M$ où $f \in N_1 + M = M$. Si $m > n$, alors par récurrence sur d on a $f^* \in \sum_{i=0}^{m-1-n} X^i M$, donc $f \in N_1 + X \sum_{i=0}^{m-1-n} X^i M \subseteq \sum_{i=0}^{m-n} X^i M$. □

Théorème 1.2. *Soient R un anneau cohérent noethérien, I un idéal à gauche de type fini de $R[X]$, et k un entier > 1. Alors $I \cap R[X]_k$ est un R-module de type fini. En particulier, $I \cap R$ est un idéal à gauche de type fini de R.*

Démonstration. Soient $n \geqslant k$ et $M = I \cap R[X]_n$ comme dans le lemme 1.1. Alors $I \cap R[X]_k = M \cap R[X]_k$ est de type fini car $R[X]_n$ est cohérent et M est de type fini. □

Lemme 1.3. *Si R est un anneau cohérent noethérien, $R[X]$ est un anneau cohérent. Si, en outre, R est fortement discret (à gauche), il en va de même pour $R[X]$.*

Démonstration. On montre d'abord la deuxième affirmation. Soit I un idéal à gauche de type fini de l'anneau $R[X]$ et soit $f \in R[X]$. On prend un n tel que $R[X]_n$ contient f et une famille finie de générateurs de I. D'après le

lemme 1.1, on sait que le module $M = I \cap R[X]_n$ est de type fini. Si R est fortement discret (à gauche), M est détachable dans $R[X]_n$ d'après le corolaire III.2.8, donc on peut décider si $f \in I \cap R[X]_n$. Ainsi I est détachable dans $R[X]$.

Soit $g_1, \ldots, g_k$ un système générateur de $M \cap R[X]_{n-1}$; on pose $g_{k+i} = Xg_i$ pour $i = 1, \ldots, k$ et on note $g_{2k+1}, \ldots, g_\ell$ des générateurs de M. Donc $g_1, \ldots, g_\ell$ engendrent I comme idéal de $R[X]$. Soit $e_1, \ldots, e_\ell$ la base naturelle du $R[X]$-module $R[X]^\ell$, et soit φ l'application linéaire de $R[X]^\ell$ sur I qui envoie e_i sur g_i. Nous allons construire une famille finie qui engendre $\ker\varphi$, ce qui montrera que $R[X]$ est cohérent.

Comme $R[X]_n$ est un R-module cohérent, le R-module $R^\ell \cap \ker\varphi$ est de type fini. Soit K le sous-$R[X]$-module de $R[X]^\ell$ engendré par ces éléments et les éléments $Xe_i - e_{k+i}$ pour $i = 1, \ldots, k$. Nous allons montrer que $K = \ker\varphi$. Clairement $K \subseteq \ker\varphi$.

Supposons que $\sum_{i=1}^{\ell} r_i g_i = 0$ et montrons que $\sum_{i=1}^{\ell} r_i e_i \in K$. On prend un m tel que $\deg r_i \leqslant m$ pour tout i. Nous procédons par récurrence sur m. Si $m = 0$, chaque $r_i \in R$, donc nous avons terminé car $R^\ell \cap \ker\varphi \subseteq K$. Si $m > 0$, on écrit $r_i = s_i + a_i X^m$, où $a_i \in R$ et $\deg s_i < m$. L'égalité $\sum s_i g_i + X^m \sum a_i g_i = 0$ nous dit que $\sum a_i g_i \in M \cap R[X]_{n-1}$, donc $\sum_{i=1}^{\ell} a_i g_i = \sum_{i=1}^{k} b_i g_i$ avec $b_i \in R$. Ainsi $\sum_{i=1}^{\ell} a_i e_i - \sum_{i=1}^{k} b_i e_i \in K$, donc il suffit de démontrer que

$$\sum\nolimits_{i=1}^{\ell} s_i e_i + X^m \sum\nolimits_{i=1}^{k} b_i e_i \in K.$$

Comme $Xe_i - e_{k+i} \in K$ pour $i = 1, \ldots, k$, il suffit de démontrer que

$$\sum\nolimits_{i=1}^{\ell} s_i e_i - X^{m-1} \sum\nolimits_{i=1}^{k} b_i e_{k+i} \in K,$$

et ceci est vrai par récurrence sur m. Ainsi, I est de présentation finie. □

Si R est un anneau et I est un idéal à gauche de $R[X]$, on définit

$$L(I) = \{\, a_n \in R : a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0 \in I \,\}$$

comme l'ensemble des coefficients formellement dominants des polynômes de I. Notez qu'un polynôme peut avoir différents coefficients formellement dominants (certains nuls) selon la manière dont il est écrit, et notez que $L(I)$ est un idéal à gauche de R.

Lemme 1.4. *Soient R un anneau cohérent noethérien et I un idéal à gauche de type fini de $R[X]$. Alors l'idéal à gauche $L(I)$ de R est de type fini*[1]*. Soit $J \supseteq I$ un idéal à gauche de $R[X]$ tel que $L(I) = L(J)$, et soit $m > 0$. Si $I \cap R[X]_m$ engendre I, alors $J \cap R[X]_m$ engendre J.*

1. **NdT.** Ce lemme contient en filigrane un algorithme de Buchberger généralisé pour un anneau cohérent noethérien R (à la place d'un corps discret) et les anneaux de polynômes sur R, au moins lorsque l'ordre monomial considéré est un ordre lexicographique sur les variables.

Démonstration. Soient n et $M = I \cap R[X]_n$ comme dans le lemme 1.1, et notons $L_n(I) \subseteq L(I)$ l'ensemble des coefficients formellement dominants des polynômes dans M. Comme $XM \cap R[X]_n \subseteq M$, le R-module $L_n(I)$ est l'image de l'application R-linéaire qui envoie un polynôme de M sur son coefficient en X^{n-1}. Comme M est de type fini, il en va de même pour $L_n(I)$. Nous complétons la démonstration de la première affirmation en montrant que $L_n(I) = L(I)$. Soit $h = h_{m-1}X^{m-1} + \cdots + h_1X + h_0 \in I$ avec les $h_i \in R$. Si $m \leqslant n$, $h_{m-1} \in L_n(I)$. Si $m > n$, $h \in \sum_{i=0}^{m-n} X^i M$, donc nous pouvons trouver un $g \in M$ ayant h_{m-1} pour coefficient formellement dominant, donc $h_{m-1} \in L_n(I)$.

Maintenant soient J et m comme dans la deuxième affirmation. On peut supposer que $m = n$, en changeant n et M si nécessaire [1]. Soit $h = h_{d-1}X^{d-1} + \cdots + h_1X + h_0 \in J$; nous allons montrer que h est dans l'idéal à gauche engendré par $J \cap R[X]_n$. Si $d \leqslant n$, $h \in J \cap R[X]_n$. Si $d > n$, alors, comme $L_n(I) = L(I) = L(J)$, nous pouvons trouver un $g = g_{n-1}X^{n-1} + \cdots + g_1X + g_0$ dans M tel que $g_{n-1} = h_{d-1}$. Donc $h - X^{d-n}g \in J \cap R[X]_{d-1}$, donc, par récurrence sur d, il est dans l'idéal à gauche engendré par $J \cap R[X]_n$. Ainsi h est dans l'idéal à gauche engendré par $J \cap R[X]_n$. □

Théorème 1.5 (théorème de la base de Hilbert)**.** *Si R est un anneau cohérent noethérien (à gauche), alors il en va de même pour $R[X]$. Si en outre R est fortement discret (à gauche), alors il en va de même pour $R[X]$.*

Démonstration. Le lemme 1.3 dit que $R[X]$ est un anneau cohérent et qu'il est fortement discret à gauche si R l'est. Il reste à montrer que $R[X]$ est noethérien. Soit $I_1 \subseteq I_2 \subseteq \cdots$ une chaine d'idéaux à gauche de type fini de $R[X]$. Nous construisons deux suites d'entiers $1 = v(1) < v(2) < \cdots$ et $n(1), n(2), \ldots$ de la manière suivante. On pose $v(1) = 1$. Si $v(m)$ a été construit, on prend un $n(m)$ tel que $I_{v(m)} \cap R[X]_{n(m)}$ engendre l'idéal à gauche $I_{v(m)}$. Si $v(m-1)$ et $n(m-1)$ ont été construits, on utilise le fait que $R[X]_{n(m-1)}$ est noethérien et $I_i \cap R[X]_{n(m-1)}$ de type fini pour chaque i (théorème 1.2) pour trouver un $v(m) > v(m-1)$ tel que

$$I_{v(m)} \cap R[X]_{n(m-1)} = I_{v(m)+1} \cap R[X]_{n(m-1)}.$$

Les idéaux à gauche $L(I_{v(1)}) \subseteq L(I_{v(3)}) \subseteq L(I_{v(5)}) \subseteq \cdots$ sont de type fini d'après le lemme 1.4, donc on peut trouver un m tel que $L(I_{v(m-1)}) = L(I_{v(m+1)})$. On a alors $L(I_{v(m-1)}) = L(I_{v(m)})$. Mais $I_{v(m-1)} \cap R[X]_{n(m-1)}$ engendre $I_{v(m-1)}$, donc le lemme 1.4 nous dit que $I_{v(m)} \cap R[X]_{n(m-1)}$ engendre $I_{v(m)}$. De la même manière $I_{v(m)+1} \cap R[X]_{n(m-1)}$ engendre $I_{v(m)+1}$. Donc $I_{v(m)} = I_{v(m)+1}$. □

1. **NdT.** Il se peut que le R-module $I \cap R[X]_m$ engendre I comme idéal de $R[X]$ pour un m plus petit que le n du lemme 1.1. On remplace alors l'entier n et le module M du lemme 1.1 par l'entier m et le R-module $I \cap R[X]_m$ donnés dans l'hypothèse. Il n'est pas nécessaire ici que le nouveau module M soit de type fini.

En particulier, $\mathbb{Z}[X_1, \ldots, X_n]$ est un anneau cohérent noethérien fortement discret, de même que $k[X_1, \ldots, X_n]$ pour un corps discret k.

Exercices

1. Soient G le groupe abélien $\mathbb{Z} \oplus \mathbb{Z}$ et P le sous-monoïde de G formé par les couples (m, n) tels que $m > 0$, ou $m = 0$ et $n \geqslant 0$. On considère l'algèbre $k^{(P)}$ du monoïde P sur un corps discret k. Comme P est en notation additive, nous écrivons les éléments de $k^{(P)}$ comme des sommes formelles $\sum a_p Y^p$ où $p \in P$ et $a_p \in k$. Soit S le sous-monoïde multiplicatif de $k^{(P)}$ des éléments $\sum a_p Y^p$ tels que $a_{(0,0)} \neq 0$, et notons R l'anneau $S^{-1}k^{(P)}$.
   (i) Montrer que R est un domaine de Bézout avec unités détachables, en fait un anneau de valuation, et donc un anneau cohérent fortement discret.
   (ii) Soit I l'idéal de $R[X]$ engendré par les éléments $1 + Y^{(0,1)}X$ et $Y^{(1,0)}$. Montrer que ni $I \cap R$, ni $I \cap R[X]_2$ ne sont des R-modules de type fini.
2. Montrer que tout idéal de $\mathbb{Z}[X]$ engendré par un nombre fini de polynômes de degré au plus 1 est ou bien principal ou bien, de manière unique, de la forme $a(X + b, c)$ avec a et c positifs et $0 \leqslant b < c$. Donner un théorème analogue pour les idéaux engendrés par un nombre fini de polynômes de degré au plus 2.

2 Le théorème de normalisation de Noether et le lemme d'Artin-Rees

On dit qu'un homomorphisme $\varphi\colon R \to S$ d'anneaux commutatifs **réfléchit les idéaux de type fini** si $\varphi^{-1}I$ est un idéal de type fini de R pour tout idéal de type fini I de S. Le théorème 1.2 dit que si R est un anneau commutatif cohérent noethérien, le morphisme $R \to R[X]$ réfléchit les idéaux de type fini ; donc par récurrence il en va de même pour le morphisme $R \to R[X_1, \ldots, X_n]$. En mathématiques classiques, ce n'est pas un résultat très excitant car *tout* idéal de R est de type fini ; mais c'est un outil très efficace pour construire des systèmes générateurs d'idéaux. Dans cette section nous donnons quelques applications importantes de cette technique.

Tout d'abord nous notons que le théorème du reste admet la généralisation suivante pour les polynômes en plusieurs variables.

Lemme 2.1. *Soient R un anneau commutatif et $\varphi\colon R[X_1, \ldots, X_n] \to R$ l'homomorphisme d'évaluation des X_i en les a_i. Alors* $\ker \varphi = (X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n)$.

Démonstration. On considère le morphisme

$$\theta\colon R[X_1,\dots,X_n] \to R[X_1,\dots,X_n]$$

défini par $\theta(a) = a$ pour $a \in R$ et $\theta(X_i) = X_i - a_i$ pour chaque i. L'homomorphisme $\varphi\theta$ envoie les X_i sur 0, donc son noyau est formé par les polynômes avec terme constant nul, i.e. les éléments de l'idéal $(X_1,\dots,X_n)$. Mais θ est un automorphisme, avec $\theta^{-1}X_i = X_i + a_i$. Donc $\ker\varphi = \theta(\ker\varphi\theta) = (X_1 - a_1,\dots,X_n - a_n)$. □

Nous utilisons le théorème 1.2 pour calculer des relations dans les anneaux de polynômes modulo les idéaux de type fini ; i.e. étant donnés des polynômes $p_1,\dots,p_n$ et un idéal de type fini I, nous construisons un système générateur fini pour les polynômes f tels que $f(p_1,\dots,p_n) \in I$.

Théorème 2.2. *Soient R un anneau commutatif cohérent noethérien et $\varphi\colon R[X_1,\dots,X_m] \to R[Y_1,\dots,Y_n]$ un homomorphisme d'anneaux égal à l'identité sur R. Alors φ réfléchit les idéaux de type fini.*

Démonstration. Soit I un idéal de type fini de $R[Y_1,\dots,Y_n]$. On doit montrer que $\varphi^{-1}I$ est de type fini. On étend φ en un homomorphisme

$$\varphi^*\colon R[X_1,\dots,X_m,Y_1,\dots,Y_n] \to R[Y_1,\dots,Y_n].$$

en posant $\varphi^*(Y_i) = Y_i$. Comme φ^* est l'identité sur $R[Y_1,\dots,Y_n]$, $\ker\varphi^* = (X_1 - \varphi(X_1),\dots,X_m - \varphi(X_m))$ est un idéal de type fini (lemme 2.1), et donc $J = (\varphi^*)^{-1}I$ est un idéal de type fini. Enfin $\varphi^{-1}I$, qui est égal à $J \cap R[X_1,\dots,X_m]$, est un idéal de type fini de $R[X_1,\dots,X_m]$ d'après le théorème 1.2. □

Soit k un corps discret. Un anneau commutatif R qui contient k est dit **de présentation finie sur** k si R est isomorphe à $k[X_1,\dots,X_n]/I$ pour un idéal de type fini I. Si R et S sont deux anneaux commutatifs qui contiennent le corps discret k, un **morphisme de k-algèbres** est un homomorphisme d'anneaux de R vers S égal à l'identité sur k. Un anneau de présentation finie sur k est aussi appelé une **k-algèbre de présentation finie** [1].

Corolaire 2.3. *Si R est une k-algèbre de présentation finie, tout morphisme de k-algèbres $k[X_1,\dots,X_n] \to R$ a un noyau de type fini.*

Démonstration. Soient $R = k[Y_1,\dots,Y_m]/I$ et $\varphi\colon k[X_1,\dots,X_n] \to R$ un morphisme de k-algèbres. Relevons le morphisme φ en un morphisme $\psi\colon k[X_1,\dots,X_n] \to k[Y_1,\dots,Y_m]$. Le morphisme ψ réfléchit les idéaux de type fini d'après le théorème 2.2. Donc $\psi^{-1}I$, qui est le noyau de φ, est de type fini. □

1. **NdT.** Les définitions ci-dessus sont aussi bien valables avec un anneau commutatif arbitraire k.

Tout anneau commutatif de présentation finie sur un corps discret k peut être vu comme une extension entière d'un anneau de polynômes sur k.

Théorème 2.4 (théorème de normalisation de Noether)**.** *Soient k un corps discret et $R = k[x_1, \dots, x_n]$ une k-algèbre de présentation finie. Alors il existe des éléments $z_1, \dots, z_n \in R$ et un entier $m \leqslant n$ tels que $R = k[z_1, \dots, z_n]$ est entier sur $k[z_1, \dots, z_m]$ et $z_1, \dots, z_m$ sont algébriquement indépendants sur k.*

Démonstration. Nous procédons par récurrence sur n. Si $x_1, \dots, x_n$ sont algébriquement indépendants, ce qui est décidable d'après le corolaire 2.3, alors nous avons terminé. Nous supposons donc qu'il y a une relation non triviale

$$\sum\nolimits_{j \in L} a_j x_1^{j_1} \cdots x_n^{j_n} = 0,$$

où j est le n-uplet $j_1, \dots, j_n$, les $a_j \neq 0$ sont dans k, et L est fini non vide. Soit d un entier strictement plus grand que les j_i pour les $j \in L$. Posons $y_i = x_i - x_n^{d^{n-i}}$ pour $i < n$, et remplaçons x_i par $y_i + x_n^{d^{n-i}}$ dans l'égalité ci-dessus. En développant, nous obtenons

$$\sum a_j x_n^{j^*} + f(y_1, \dots, y_{n-1}, x_n) = 0,$$

où $j^* = j_1 d^{n-1} + j_2 d^{n-2} + \cdots + j_n$, et où le degré en x_n de chaque terme de f est strictement inférieur à j^* pour un j. Comme les j^* sont distincts, ceci est une équation de dépendance intégrale de x_n sur $k[y_1, \dots, y_{n-1}]$. Donc $R = k[y_1, \dots, y_{n-1}, x_n]$ est entier sur $k[y_1, \dots, y_{n-1}]$, qui est une k-algèbre de présentation finie d'après le corolaire 2.3. Par récurrence, on obtient $k[y_1, \dots, y_{n-1}] = k[z_1, \dots, z_{n-1}]$ entier sur $k[z_1, \dots, z_m]$ avec $z_1, \dots, z_m$ algébriquement indépendants sur k. On termine en posant $z_n = x_n$. □

Un corps discret K qui contient k est appelé **une extension de présentation finie de** k s'il est le corps de fractions d'une k-algèbre de présentation finie. Le théorème de normalisation de Noether nous donne le moyen de construire une base de transcendance particulièrement agréable pour une extension de présentation finie de k.

Corolaire 2.5. *Soient $k \subseteq K$ des corps discrets avec K une extension de présentation finie de k. Il existe une base de transcendance finie B de K sur k telle que K est de dimension finie sur $k(B)$.*

Démonstration. Par hypothèse, K est le corps de fractions d'une k-algèbre de présentation finie R. D'après le théorème de normalisation de Noether, nous pouvons écrire R sous la forme $k[X_1, \dots, X_r, Y_1, \dots, Y_s]/P = k[X, Y]/P$ où $k[X] \cap P = 0$ et R est entier sur $k[X]$. Alors on a

$$K = k(X)[Y]/(k(X)P) = k(X)[y_1, \dots, y_s],$$

qui est une algèbre de présentation finie, et algébrique, sur le corps $k(X)$. Il suffit de montrer que K est de dimension finie sur $k(X)$, c'est-à-dire de montrer ce corolaire quand le degré de transcendance r est nul.

Dans ce cas on a $K = k[Y_1, \ldots, Y_s]/P = k[y_1, \ldots, y_s]$. Le sous-corps $k[y_s]$ est un espace vectoriel de dimension finie sur k d'après le corolaire 2.3. Mais $K = k[Y_1, \ldots, Y_{s-1}, y_s]/P'$, où P' est l'image de P dans $k[Y_1, \ldots, Y_{s-1}, y_s]$. Par récurrence sur s, K est de présentation finie sur le corps $k[y_s]$, et donc est de dimension finie sur $k[y_s]$. Nous avons terminé : K est de dimension finie sur k. □

Nous obtenons aussi le résultat suivant pour les corps pleinement factoriels.

Théorème 2.6. *Soit K un corps extension de présentation finie d'un corps discret k. Si k est pleinement factoriel, il en va de même pour K.*

Démonstration. Soit B une base de transcendance de K sur k comme dans le corolaire 2.5. Le corps $k(B)$ est pleinement factoriel d'après le corolaire VII.3.4. Comme K est de dimension finie sur $k(B)$, il est pleinement factoriel. □

Comme autre application du théorème 2.2, nous démontrons le **lemme d'Artin-Rees**.

Théorème 2.7 (Artin-Rees)**.** *Soit I un idéal de type fini d'un anneau commutatif cohérent noethérien R. Soit N un sous-module de type fini d'un R-module de présentation finie M. Alors il existe un entier k tel que pour tout $n \geqslant k$ on a*

$$I^{n-k}(I^k M \cap N) = I^n M \cap N.$$

Démonstration. En passant à l'anneau $R \oplus M$, où $m_1 m_2 = 0$ pour $m_1, m_2 \in M$, nous pouvons supposer que M est un idéal de type fini de R. Avec $I = (a_1, \ldots, a_m)$, nous définissons le R-morphisme $\varphi\colon R[X_1, \ldots, X_m] \to R[Y]$ en posant $\varphi(X_i) = a_i Y$. Le noyau de φ est de type fini d'après le théorème 2.2, donc l'image $R[IY]$ de φ est un $R[X_1, \ldots, X_m]$-module de présentation finie, donc un anneau cohérent noethérien. Maintenant $N[Y]$ est un $R[Y]$-idéal de type fini, donc

$$R[IY] \cap N[Y] = \varphi\varphi^{-1}(N[Y])$$

est un $R[IY]$-idéal de type fini d'après le théorème 2.2. Donc $M[IY] \cap N[Y]$ est un $R[IY]$-idéal de type fini, parce que $M[IY]$ est un $R[IY]$-idéal de type fini et que $R[IY]$ est cohérent. Mais

$$M[IY] \cap N[Y] = \sum\nolimits_{i=0}^{\infty} (I^i M \cap N) Y^i.$$

On prend alors pour k un entier tel que $M[IY] \cap N[Y]$ soit engendré, comme $R[IY]$-idéal, par $\sum_{i=0}^{k} (I^i M \cap N) Y^i$. □

L'anneau $R[IY]$ dans la démonstration précédente est connu sous le nom d'**anneau de Rees**.

Théorème 2.8 (théorème d'intersection de Krull)**.** *Soient M un module de présentation finie sur un anneau commutatif cohérent noethérien R et I un idéal de type fini de R. Notons $A = \bigcap_n I^n M$. Alors $a \in Ia$ pour tout $a \in A$, et donc $IA = A$.*

Démonstration. Soit $N = Ra$. D'après le lemme d'Artin-Rees, il existe un entier k tel que pour tout $n \geqslant k$ on a $I^n M \cap N = I^{n-k}(I^k M \cap N)$. Mais $N \subseteq I^n M$, donc en prenant $n = k+1$ on obtient $N = IN$. □

Corolaire 2.9. *Soit M un module de présentation finie sur un anneau commutatif cohérent noethérien R et I un idéal de type fini contenu dans le radical de Jacobson de R. Alors $\bigcap_n I^n M = 0$.*

Démonstration. Si $a \in \bigcap_n I^n M$, alors $a \in Ia$ d'après le théorème 2.8. Donc $a = \lambda a$ pour un $\lambda \in I$, $(1-\lambda)a = 0$, et $a = 0$. □

Exercices

1. Soient k un corps discret et $R = k[X_1, X_2]/(X_1 X_2)$. Donner $z_1, z_2 \in R$ comme dans le théorème de normalisation de Noether.
2. *Théorème d'intersection de Krull à la Herstein.* Soient R un anneau commutatif, I un idéal de type fini de R, et $r \in I$. Soient M un R-module noethérien de présentation finie et K et N des sous-modules de type fini de M tels que $K \cap N = IN$.
   (i) Montrer que la suite $L_n(r) = \{\, x \in M : r^n x \in K \,\}$ est une chaine croissante de sous-modules de type fini.
   (ii) Montrer que si $L_n(r) = L_{n+1}(r)$, alors $(r^n M + K) \cap N = IN$.
   (iii) Montrer que K est contenu dans un sous-module de type fini K' de M tel que $K' \cap N = IN$ et $I^n M \subseteq K'$ pour un n.
   (iv) Utiliser (iii) pour démontrer le théorème d'intersection de Krull.

3 Le Nullstellensatz

Soient k un corps discret et K un corps, extension algébrique de k. Pour $\alpha = (\alpha_1, \ldots, \alpha_n) \in K^n$, le k-morphisme naturel de $k[X] = k[X_1, \ldots, X_n]$ sur le corps $k[\alpha_1, \ldots, \alpha_n]$ a pour noyau

$$M = \{\, f \in k[X] : f(\alpha_1, \ldots, \alpha_n) = 0 \,\},$$

de sorte que M est un idéal maximal détachable. Dans cette section nous allons démontrer, avec des hypothèses convenables sur k, que tout idéal propre de

type fini de $k[X]$ est contenu dans un tel idéal maximal M, et que M est de type fini si K est de dimension finie.

Théorème 3.1. *Soient $k \subseteq K \subseteq E$ des corps discrets avec E extension de présentation finie de K et K extension de présentation finie de k. Alors E est une extension de présentation finie de k.*

Démonstration. Soient $X = (X_1, \ldots, X_m)$ et $Y = (Y_1, \ldots, Y_n)$ des indéterminées et $x \in K^m$ et $y \in E^n$ des éléments tels que les morphismes $k[X] \to k(x) = K$ et $K[Y] \to K(y) = E$ ont des noyaux de type fini. Alors chacun des morphismes

$$k[X, Y] \to k[x, Y] \to k(x)[Y] \to k(x)[y]$$

réfléchit les idéaux de type fini ; le premier est surjectif et son noyau est engendré par le noyau de $k[X] \to k[x]$, le deuxième réfléchit les idéaux de type fini d'après le théorème 2.2 parce que la localisation $k[x] \to k(x)$ le fait, et le troisième est surjectif avec un noyau de type fini. Donc le morphisme composé réfléchit les idéaux de type fini ; en particulier, son noyau est de type fini. □

Nous avons vu qu'une extension de corps de présentation finie est une extension purement transcendante suivie d'une extension algébrique de dimension finie (corolaire 2.5). La réciproque se déduit du théorème 3.1.

Corolaire 3.2. *Soient $k \subseteq K$ des corps discrets. S'il existe une base de transcendance finie B de K sur k telle que K soit de dimension finie sur $k(B)$, K est une extension de présentation finie de k.*

Démonstration. Supposons qu'une telle base de transcendance B existe. Clairement $k(B)$ est de présentation finie sur k. Donc, d'après le théorème 3.1, il suffit de traiter le cas où K est de dimension finie sur k. Si $K = k$ nous avons terminé ; sinon soit $x \in K \setminus k$ et soit $f \in k[X]$ un polynôme irréductible annulé par x. Alors $k(x) \simeq k[X]/(f)$ est une extension de présentation finie de k, et K est une extension de présentation finie de $k(x)$ par récurrence sur la dimension. Donc K est une extension de présentation finie de k d'après le théorème 3.1. □

Du théorème 3.1 et du corolaire 2.3 on déduit que si K est de dimension finie sur k, et $\alpha \in K^n$, alors $\{ f \in k[X] : f(\alpha) = 0 \}$ est un idéal de type fini.

Soit I un idéal de type fini propre de l'anneau de polynômes $k[X_1, \ldots, X_n]$. Si nous voulons construire un idéal maximal *de type fini* qui contient I, nous devons supposer k factoriel, même si $n = 1$. Cependant, nous pouvons obtenir le résultat plus faible suivant sans avoir à factoriser les polynômes.

Lemme 3.3. *Soient k un corps discret et I un idéal de type fini propre de $k[X_1, \ldots, X_n] = k[X]$. Alors il existe un idéal propre de type fini $J \supseteq I$ tel que $k[X]/J$ est entier sur k.*

Démonstration. Soit $k[x_1,\dots,x_n] = k[x] = k[X]/I$. D'après le théorème de normalisation de Noether, il existe $y_1,\dots,y_r \in k[x]$, algébriquement indépendants sur k, tels que $k[x]$ est entier sur $k[y_1,\dots,y_r]$. Si $r = 0$, il n'y a rien à faire. Si $r \geqslant 1$, nous allons montrer que y_1 n'est pas une unité de $k[x]$. Nous pourrons alors remplacer I par $I + (Y_1)$, où Y_1 est un élément de $k[X]$ égal à y_1 modulo I, et nous terminerons par récurrence sur r.

Supposons que $zy_1 = 1$ pour un $z \in k[x]$. Comme $k[x]$ est entier sur $k[y_1,\dots,y_r]$, il existe des $a_i \in k[y_1,\dots,y_r]$ tels que

$$z^m + a_{m-1}z^{m-1} + \cdots + a_0 = 0$$

et donc

$$1 + a_{m-1}y_1 + \cdots + a_0 y_1^m = 0,$$

mais cette égalité contredit l'indépendance algébrique de $y_1,\dots,y_r$ sur k. □

On dit qu'un corps discret k **admet des corps de décomposition** si pour tout polynôme $f \in k[X]$ il existe un corps de décomposition discret pour f sur k. Les corps pleinement factoriels et les corps dénombrables admettent des corps de décomposition.

Lemme 3.4. *Soit k un corps discret qui admet des corps de décomposition et soit I un idéal de type fini propre de $k[X_1,\dots,X_n] = k[X]$. Alors il existe un corps K extension algébrique de k tel que les polynômes dans I ont un zéro commun dans K^n.*

Démonstration. D'après le lemme 3.3, nous pouvons supposer que la k-algèbre $k[x] = k[X]/I$ est entière sur k. Pour chaque x_i on a un polynôme unitaire $f_i \in k[Y]$ annulé par x_i. Soient K un corps de décomposition de $f = \prod_i f_i$ et J l'idéal engendré par I dans $K[X]$. Comme $I \cap k = 0$, l'idéal J est propre d'après le théorème III.3.3. On écrit $f_1(Y) = \prod_i (Y - \alpha_i) \in K[Y]$. Comme $f_1(X_1) \in I$, on a l'inclusion

$$J = J + \textstyle\prod_i (X_1 - \alpha_i) \supseteq \prod_i (J + (X_1 - \alpha_i)),$$

de sorte que $J + (X_1 - \beta_1) \neq K[X]$ pour un zéro β_1 de f_1. Remplaçons J par $J + (X_1 - \beta_1)$, et répétons cette procédure pour $f_2,\dots,f_m$. Nous construisons ainsi un idéal propre $J + N$ où $N = (X_1 - \beta_1,\dots,X_n - \beta_n)$. Il est clair que N est un idéal maximal détachable, que $N \supseteq J$ et que $\beta = (\beta_1,\dots,\beta_n)$ est un zéro commun pour les polynômes de J, donc β est aussi un zéro commun pour les polynômes de I. □

Théorème 3.5 (Nullstellensatz [1])**.** *Soient k un corps discret qui admet des corps de décomposition, I un idéal de type fini de $k[X] = k[X_1,\dots,X_n]$ et*

1. **NdT.** Une version constructive un peu plus générale du Nullstellensatz, dans laquelle k est seulement supposé être un corps discret, se trouve dans l'ouvrage *Algèbre commutative. Méthodes constructives* (référence [5] de la postface), théorèmes VII-1.8 et VII-1.9.

$f \in k[X]$. Ou bien $f \in \sqrt{I}$, ou bien il existe un corps K, extension algébrique de k, et un élément $\alpha \in K^n$ tels que $f(\alpha) \neq 0$ mais $g(\alpha) = 0$ pour tout $g \in I$.

Démonstration. On considère l'idéal I' de $k[X, Y]$ engendré par I et $1 - Yf$. Si I' est propre, alors, d'après le lemme 3.4, il existe un corps, extension algébrique K de k, et des éléments $\alpha \in K^n$ et $\beta \in K$ tels que $g(\alpha) = 0$ pour tout $g \in I$ et $1 - \beta f(\alpha) = 0$. Si $I' = k[X, Y]$, alors on a des polynômes $h_i \in k[X, Y]$ et $g_i \in I$ tels que

$$1 = h_0 \cdot (1 - Yf) + \sum\nolimits_{i>0} h_i \cdot g_i. \qquad (*)$$

On fait la substitution $Y = 1/f$ [1] et l'on choisit un r strictement plus grand que les degrés de Y dans les h_i. Alors $f^r \in I$, donc $f \in \sqrt{I}$. □

Exercices

1. Dans la démonstration du lemme 3.3, utiliser l'exercice VI.1.1 pour voir directement que $J = I + (Y_1, \ldots, Y_r)$ est l'idéal propre souhaité (les Y_i sont des éléments égaux aux y_i modulo I).
2. Montrer que si k est un corps discret qui admet des corps de décomposition et si I est un idéal de $k[X_1, \ldots, X_n]$, alors $\sqrt{I}$ est l'intersection des idéaux maximaux détachables qui contiennent I.
3. Soient $k \subseteq K$ des corps discrets avec K algébriquement clos. Une **k-variété** dans K^n est un ensemble de la forme $\{\, x \in K^n : f_i(x) = 0 \text{ pour } i = 1, .., n \,\}$, où $f_1, \ldots, f_n$ sont dans $k[X] = k[X_1, \ldots, X_n]$. L'**idéal** d'une k-variété V est l'ensemble $\{\, f \in k[X] : f(v) = 0 \text{ pour tout } v \in V \,\}$. Une k-variété V est **irréductible** si, lorsque V est la réunion de deux k-variétés A et B, on a $V = A$ ou $V = B$.
   (i) Montrer que l'idéal de la k-variété définie par $f_1, \ldots, f_n$ est le radical de l'idéal engendré par $f_1, \ldots, f_n$, et que ce radical est détachable.
   (ii) Montrer qu'une k-variété est irréductible si, et seulement si, son idéal est premier.

4 L'approche de Tennenbaum pour le théorème de la base de Hilbert

Soient R un anneau et M un R-module discret. Une **fonction génératrice noethérienne** [2] pour M est une fonction φ de M^n vers R^{n-1}, pour $n = 2, 3, \ldots$,

1. **NdT.** Il s'agit d'un raccourci du langage. On a ici $1 = 0$ dans $k[X, Y]/I' \simeq (k[X]/I)[1/f]$, ce qui implique $f^r = 0$ dans $k[X]/I$ pour un r assez grand, i.e. $f \in \sqrt{I}$. L'égalité $(*)$ permet d'ajouter une précision au résultat de l'énoncé : on peut prendre pour r un entier strictement plus grand que les degrés de Y dans les h_i.

2. **NdT.** Noetherian basis function. Cette terminologie anglaise, que l'on retrouve dans le « théorème de la base de Hilbert » dit qu'un système générateur d'un module est une base de

telle que si $x_1, x_2, \ldots$ est une suite infinie d'éléments de M, alors il existe des entiers n arbitrairement grands tels que $x_n = \sum_{i=1}^{n-1} r_i x_i$, où $(r_1, \ldots, r_{n-1}) = \varphi(x_1, \ldots, x_n)$.

La fonction $\rho(x_1, \ldots, x_n) = x_n - \sum_{i=1}^{n-1} r_i x_i$ sera souvent appelée la **fonction génératrice**, sans expliciter φ, qui est implicite quand nous écrivons $x_n = \sum_{i=1}^{n-1} r_i x_i$ comme conséquence de $\rho(x_1, \ldots, x_n) = 0$. Le terme **fonction génératrice** provient du fait que les éléments $\rho(x_1), \rho(x_1, x_2), \ldots, \rho(x_1, \ldots, x_n)$ engendrent le même sous-module que $x_1, \ldots, x_n$, donc ρ réalise un changement de système générateur.

Nous disons qu'une fonction génératrice ρ est **consistante** lorsque l'on a $\rho(x_1, \ldots, x_n) = 0$ chaque fois que $\rho(x_{i(1)}, \ldots, x_{i(m)}, x_n) = 0$ pour une suite $1 \leqslant i(1) < i(2) < \cdots < i(m) < n$. Clairement tout module discret qui admet une fonction génératrice noethérienne en admet une qui est consistante.

Théorème 4.1. *Tout module discret qui admet une fonction génératrice noethérienne est noethérien.*

Démonstration. Soit ρ une fonction génératrice noethérienne consistante pour M, et soit $I_1 \subseteq I_2 \subseteq \cdots$ une chaine de sous-modules de type fini de M. On construit une suite $x_1, x_2, \ldots$ d'éléments de M et une suite $\alpha(1) < \alpha(2) < \cdots$ d'entiers strictement positifs tels que I_j est engendré par $x_{\alpha(j)}, \ldots, x_{\alpha(j+1)-1}$. Ensuite on construit une suite $\beta(1), \beta(2), \ldots$ d'entiers strictement positifs telle que

(i) $\alpha(j) \leqslant \beta(j) < \alpha(j+1)$;

(ii) si $\rho(x_1, \ldots, x_{\alpha(j)-1}, x_{\beta(j)}) = 0$, alors $\rho(x_1, \ldots, x_{\alpha(j)-1}, x_i) = 0$ pour $\alpha(j) \leqslant i < \alpha(j+1)$.

Il existe un entier n tel que $\rho(x_{\beta(1)}, \ldots, x_{\beta(n)}) = 0$, donc

$$\rho(x_1, \ldots, x_{\alpha(n)-1}, x_{\beta(n)}) = 0$$

car ρ est consistante. Par suite $\rho(x_1, \ldots, x_{\alpha(n)-1}, x_i) = 0$ si $\alpha(n) \leqslant i < \alpha(n+1)$, donc $I_n = I_{n-1}$. □

Théorème 4.2. *L'anneau $\mathbb{Z}$ des entiers, comme module sur lui-même, admet une fonction génératrice noethérienne.*

Démonstration. Soit d le pgcd $\geqslant 0$ de $x_1, x_2, \ldots, x_{n-1}$. Si $d = 0$, on pose $\rho(x_1, \ldots, x_n) = x_n$; sinon on prend $\rho(x_1, \ldots, x_n)$ égal au reste $(\geqslant 0)$ de la division de x_n par d. □

Théorème 4.3. *Soit B un R-module discret et soit A un sous-module détachable de B. Si A et B/A admettent des fonctions génératrices noethériennes, il en va de même pour B. En outre on peut prendre pour fonction génératrice pour B une fonction qui étend celle donnée pour A.*

ce module, ce qui entre en conflit avec la notion de base d'un module libre.

Démonstration. Soit π l'application linéaire naturelle de B vers B/A, et soient $b_1, \ldots, b_n$ des éléments de B. On considère l'ensemble $J = \{j_1, \ldots, j_m\}$ des indices j tels que $\rho_{B/A}(\pi b_1, \ldots, \pi b_j) = 0$. Pour $j \in J$, on considère

$$(r_1^j, \ldots, r_{j-1}^j) = \varphi_{B/A}(\pi b_1, \ldots, \pi b_j),$$

et on pose

$$a_j = b_j - \sum\nolimits_{i=1}^{j-1} r_i^j b_i \in A.$$

On définit $\rho_B(b_1, \ldots, b_n) = b_n$ sauf si $n = j_m \in J$ auquel cas nous avons

$$b_n = a_n + \sum\nolimits_{i=1}^{n-1} r_i^n b_i$$

de sorte que, en posant $(s_1, s_2, \ldots, s_{m-1}) = \varphi_A(a_{j_1}, \ldots, a_{j_m})$, nous avons

$$b_n = \rho_A(a_{j_1}, \ldots, a_{j_m}) + \sum\nolimits_{i=1}^{m-1} s_i a_{j_i} + \sum\nolimits_{i=1}^{n-1} r_i^n b_i.$$

En remplaçant chaque a_j par l'expression $b_j - \sum_{i=1}^{j-1} r_i^j b_i$, nous calculons des éléments $t_i \in R$ tels que

$$b_n = \rho_A(a_{j_1}, \ldots, a_{j_m}) + \sum\nolimits_{i=1}^{n-1} t_i b_i.$$

On définit $\varphi_B(b_1, \ldots, b_n) = (t_1, \ldots, t_{n-1})$, donc

$$\rho_B(b_1, \ldots, b_n) = \rho_A(a_{j_1}, \ldots, a_{j_m}).$$

Nous pouvons supposer que $\varphi_{B/A}(x_1, \ldots, x_{n-1}, 0) = (0, \ldots, 0)$, donc si tous les b_i sont dans A, alors $J = \{1, \ldots, n\}$ et $a_j = b_j$ pour tout $j \in J$. Ainsi ρ_B étend ρ_A. Étant donnée une suite infinie $b_1, b_2, \ldots \in B$, nous obtenons une suite infinie $a_{j_1}, a_{j_2}, \ldots \in A$ et $\rho_A(a_{j_1}, \ldots, a_{j_m}) = 0$ pour une infinité de valeurs m. □

Pour un R-module M, notons $M[X]$ l'ensemble des polynômes en X à coefficients dans M. L'ensemble $M[X]$ est un $R[X]$-module de manière naturelle. Pour $M = R$, le théorème suivant est le théorème de la base de Hilbert pour les anneaux qui admettent une fonction génératrice noethérienne.

Théorème 4.4. *Si le R-module M admet une fonction génératrice noethérienne, il en va de même pour le $R[X]$-module $M[X]$.*

Démonstration. Dans ce qui suit, nous attribuons le degré 0 au polynôme nul. Soit $M[X]_N$ l'ensemble des polynômes de $M[X]$ de degré $< N$. Soit ρ une fonction génératrice noethérienne consistante pour M et soit ρ_N la fonction

génératrice pour le R-module $M[X]_N$ définie par récurrence sur N en regardant $M[X]_N$ comme une «extension de $M[X]_{N-1}$ par M» (précisément, on prend dans le théorème 4.3 $B = M[X]_N$ et $A = M[X]_{N-1}$, et le quotient B/A est isomorphe à M).

Pour $f_1, \dots, f_n \in M[X]$ on définit $g_1, \dots, g_n$ comme suit. On pose $g_1 = f_1$. Supposons avoir défini g_i pour $i < n$. Soit alors $N_n = \max\{\, 1 + \deg g_i : 1 \leqslant i < n \,\}$. On définit g_n par la procédure itérative suivante. Si $\deg f_n < N_n$, on pose $g_n = f_n$. Si $\deg f_n \geqslant N_n$, soit c_j le coefficient dominant de g_j et c le coefficient dominant de f_n. Si $\rho(c_1, \dots, c_{n-1}, c) \neq 0$, on pose $g_n = f_n$. Sinon soient $e(i) = \deg f_n - \deg g_i$ et $(r_1, \dots, r_{n-1}) = \varphi(c_1, \dots, c_{n-1}, c)$, et remplaçons f_n par $f_n - \sum_{i=1}^{n-1} r_i x^{e(i)} g_i$. Ceci diminue le degré de f_n, et nous recommençons en haut du paragraphe. Notons que cette construction garantit que $\rho(c_1, \dots, c_n) \neq 0$ si $\deg g_n \geqslant N_n$.

Résumons ce que nous venons de faire : étant donnés $f_1, \dots, f_n \in M[X]$, on construit $g_1, \dots, g_n, N_n$ comme ci-dessus. Posons alors $\rho(f_1, \dots, f_n) = \rho_{N_n}(g_1, \dots, g_n)$.

Si $f_1, f_2, \dots$ est une suite infinie dans $M[X]$, on construit la suite $g_1, g_2, \dots$ comme ci-dessus et on pose $N(k) = \max\{\, 1 + \deg g_i : 1 \leqslant i \leqslant k \,\}$. Pour tout k il existe un $n > k$ tel que ou bien $N(k) < N(n)$, ou bien $\rho(f_1, \dots, f_n) = 0$; en effet, en notant $\pi_{N(k)}$ la projection de $M[X]$ sur $M[X]_{N(k)}$, il existe un $n > k$ tel que

$$\rho_{N(k)}(\pi_{N(k)} g_1, \dots, \pi_{N(k)} g_n) = 0.$$

Donc, ou bien $N(k) < N(n)$, ou bien $N(k) = N(n)$ et $\rho(f_1, \dots, f_n) = \rho_{N(n)}(g_1, \dots, g_n) = 0$.

Nous pouvons construire une suite $\alpha(1) < \alpha(2) < \cdots$ d'entiers strictement positifs telle que pour chaque k

(i) ou bien $N(\alpha(k)) < N(\alpha(k+1))$, ou bien $\rho(f_1, \dots, f_{\alpha(k+1)}) = 0$;

(ii) $N(\alpha(k)) = N(\alpha(k)+1) = \cdots = N(\alpha(k+1)-1)$.

Si c_j est le coefficient dominant de g_j, il y a des entiers n arbitrairement grands tels que $\rho(c_{\alpha(1)}, \dots, c_{\alpha(n)}) = 0$. Mais cela arrive seulement si $N(\alpha(n)) = N(\alpha(n)-1)$, et donc $\rho(f_1, \dots, f_n) = 0$. □

Exercices

1. Montrer que tout module fini admet une fonction génératrice noethérienne.
2. Montrer que tout module discret qui admet une fonction génératrice noethérienne en admet une consistante.
3. Supprimer *arbitrairement grand* dans la définition d'une fonction génératrice noethérienne. Montrer que si M admet une fonction génératrice noethérienne dans ce nouveau sens, alors il en admet une dans le sens

ancien. Pourquoi demander des n arbitrairement grands ? C'est utilisé dans les démonstrations des théorèmes 4.3 et 4.4 ; est-ce qu'on peut éviter facilement cette condition ?

4. Soit M un R-module noethérien fortement discret. Est-ce que M admet nécessairement une fonction génératrice noethérienne ? (probablement pas).
5. Disons qu'un R-module M est un **module de Tennenbaum** s'il existe un R'-module discret M' qui admet une fonction génératrice noethérienne, un homomorphisme d'anneaux $\varphi\colon R' \to R$, et un épimorphisme $\psi\colon M' \to M$ de groupes abéliens tels que $\psi(rx) = \varphi(r)\psi(x)$ pour tous $r \in R'$ et $x \in M'$. Montrer que tout module de Tennenbaum est noethérien. Montrer que le théorème de la base de Hilbert est satisfait par les anneaux de Tennenbaum.
6. Soit a une suite binaire, et soit I l'idéal de $\mathbb{Z}$ engendré par les éléments $a_n n!$. Montrer que $\mathbb{Z}/I$ est un exemple brouwerien d'anneau de Tennenbaum qui n'est pas cohérent. Est-ce que tout anneau noethérien est un anneau de Tennenbaum ?

5 Idéaux primaires

Un idéal premier dans un anneau commutatif est l'analogue d'un nombre premier – plus précisément de l'ensemble des multiples d'un nombre premier. Un *idéal primaire* est l'analogue d'une puissance d'un nombre premier, et le théorème qui dit que tout nombre est un produit de puissances de nombres premiers admet une version adéquate dans certains anneaux plus généraux, comme les anneaux de polynômes en plusieurs variables sur un corps discret : le théorème de décomposition de Lasker-Noether affirme que tout idéal de type fini est intersection finie d'idéaux de type fini primaires. Dans les sections 7 et 8, nous étudions ces anneaux de *Lasker-Noether*. Dans la section présente, nous donnons quelques propriétés de base des idéaux primaires dans un anneau commutatif.

Soit R un anneau commutatif. Un idéal Q de R est **primaire** si $xy \in Q$ implique $x \in Q$ ou $y^n \in Q$ pour un n. Ainsi un idéal détachable Q est primaire si, et seulement si, R/Q est un anneau discret dans lequel tout diviseur de zéro est nilpotent.

Proposition 5.1. *Soit Q un idéal primaire d'un anneau commutatif ; alors $\sqrt{Q}$ est un idéal premier.*

Démonstration. Si $xy \in \sqrt{Q}$, alors $(xy)^n \in Q$, donc $x^n \in Q$ ou $y^{nm} \in Q$ pour un m. Donc $x \in \sqrt{Q}$ ou $y \in \sqrt{Q}$. □

Si Q est un idéal primaire d'un anneau commutatif R et si $\sqrt{Q} = P$, nous disons que Q **appartient à** P, ou que P **appartient à** Q.

Théorème 5.2. *Soient P et Q des idéaux d'un anneau commutatif. Alors Q est un idéal primaire appartenant à P si, et seulement si, les trois propriétés suivantes sont satisfaites.*

(i) $Q \subseteq P$.

(ii) *Si* $r \in P$, $r^m \in Q$ *pour un* m.

(iii) *Si* $rs \in Q$, $r \in Q$ *ou* $s \in P$.

Démonstration. Clairement, les conditions (i) et (ii) sont équivalentes à $Q \subseteq P \subseteq \sqrt{Q}$. Supposons (iii). Si $rs \in Q$, $r \in Q$ ou $s \in P$; comme $P \subseteq \sqrt{Q}$, cela implique que $r \in Q$ ou $s^n \in Q$ pour un n ; donc Q est primaire. Montrons que $\sqrt{Q} \subseteq P$. Soit $q \in \sqrt{Q}$. Alors $q^n \in Q \subseteq P$ pour un n. D'après (iii), nous avons $q^{n-1} \in Q$ ou $q \in P$; donc par récurrence sur n on obtient $q \in P$. Donc $\sqrt{Q} = P$. Inversement, supposons que Q est primaire et $\sqrt{Q} = P$. Si $rs \in Q$, $r \in Q$ ou $s^n \in Q$ pour un n ; mais $s^n \in Q$ implique $s \in \sqrt{Q} = P$. Donc la condition (iii) est satisfaite. □

Corolaire 5.3. *Soient Q_1 et Q_2 des idéaux primaires appartenant à P. Alors $Q_1 \cap Q_2$ est un idéal primaire appartenant à P.* □

Théorème 5.4. *Soit P un idéal maximal détachable d'un anneau commutatif R. Soit Q un idéal tel que $Q \subseteq P \subseteq \sqrt{Q}$. Alors Q est un idéal primaire appartenant à P.*

Démonstration. On vérifie la condition (iii) du théorème 5.2. Supposons que $rs \in Q$. Si $s \in P$ nous avons terminé, donc nous pouvons supposer que $s \notin P$. Comme P est maximal, il existe $x \in R$ et $p \in P$ tels que $p + xs = 1$. On prend un n tel que $p^n \in Q$. Alors $(p + xs)^n = p^n + ys = 1$ pour un y dans R. Donc $r = rp^n + yrs \in Q$. □

Corolaire 5.5. *Soient P un idéal maximal détachable d'un anneau commutatif R et Q un idéal tel que $P^n \subseteq Q \subseteq P$ pour un n. Alors Q est un idéal primaire appartenant à P.* □

La proposition suivante étend la propriété caractéristique d'un idéal primaire des éléments aux idéaux de type fini.

Lemme 5.6. *Soient Q un idéal primaire d'un anneau commutatif R et $P = \sqrt{Q}$. Soient I et J des idéaux de type fini tels que $IJ \subseteq Q$. Alors $I \subseteq Q$ ou $J \subseteq P$.*

Démonstration. Soit $I = (a_1, \ldots, a_m)$ et $J = (b_1, \ldots, b_n)$. Comme $a_i b_j \in Q$, on a $a_i \in Q$ ou $b_j \in P$. Si $b_j \in P$ pour tous les j, $J \subseteq P$; sinon $a_i \in Q$ pour tout i, donc $I \subseteq Q$. □

Théorème 5.7. *Soient Q un idéal primaire d'un anneau commutatif R et $P = \sqrt{Q}$. Soit I un idéal de type fini de R. Si $Q : I$ est de type fini, ou bien $I \subseteq Q$, ou bien $Q : I$ est un idéal primaire appartenant à P.*

Démonstration. Comme $I(Q : I) \subseteq Q$, le lemme 5.6 nous dit que $I \subseteq Q$ ou $Q : I \subseteq P$. Dans le second cas nous montrons que $Q : I$ est un idéal primaire appartenant à P. Nous utilisons la caractérisation du théorème 5.2. Nous avons déjà la condition (i) en hypothèse, tandis que (ii) est satisfaite parce que $Q \subseteq Q : I$. Pour vérifier (iii) on suppose que $rs \in Q : I$. Alors $rsI \subseteq Q$, donc $rI \subseteq Q$ ou $s \in P$; i.e. $r \in Q : I$ ou $s \in P$. □

Proposition 5.8. *Soient $\varphi\colon R \to R'$ un homomorphisme d'anneaux commutatifs et P et Q des idéaux de R'.*

- *Si Q est détachable, il en va de même pour $\varphi^{-1}(Q)$.*
- *Si Q est un idéal primaire appartenant à P, $\varphi^{-1}(Q)$ est un idéal primaire appartenant à $\varphi^{-1}(P)$.*

Démonstration. On suppose que Q est détachable et que $x \in R$. Alors $x \in \varphi^{-1}(Q)$ si, et seulement si, $\varphi(x) \in Q$; donc $\varphi^{-1}(Q)$ est détachable.

Supposons que Q est un idéal primaire appartenant à P. Nous utilisons la caractérisation du théorème 5.2. Clairement $\varphi^{-1}(Q) \subseteq \varphi^{-1}(P)$. Si $r \in \varphi^{-1}(P)$, i.e. $\varphi(r) \in P$, on a un n tel que $\varphi(r)^n \in Q$, i.e. $r^n \in \varphi^{-1}(Q)$. Enfin, si $rs \in \varphi^{-1}(Q)$, i.e. $\varphi(rs) \in Q$, on a $\varphi(r) \in Q$ ou $\varphi(s) \in P$. Donc $r \in \varphi^{-1}(Q)$ ou $s \in \varphi^{-1}(P)$. □

Exercices

1. Soient k un corps discret et $R = k[X, Y]$. Montrer que R est un anneau cohérent noethérien fortement discret. Soit $P = (X, Y)$ et $Q = (X, Y^2)$. Montrer que les inclusions $P^2 \subseteq Q \subseteq P$ sont propres. Montrer que Q est un idéal primaire appartenant à P. Conclure qu'un idéal primaire n'est pas nécessairement une puissance d'un idéal premier.
2. Soient k un corps discret et $R = k[X, Y, Z]/(XY - Z^2)$. Soient $x, y, z \in R$ les images de X, Y, Z dans R. Montrer que $P = (x, z)$ est un idéal premier détachable de R, mais que P^2 n'est pas primaire. Comparer avec le corolaire 5.5.
3. Soient Q_1 et Q_2 des idéaux primaires appartenant à un idéal maximal détachable P. Montrer que $Q_1 + Q_2$ et Q_1Q_2 sont des idéaux primaires appartenant à P. Montrer que dans l'anneau $\mathbb{Q}[X, Y, Z_1, Z_2]$ les idéaux

$$Q_1 = ((X, Y)^3,\ Z_1X + Z_2Y) \text{ et } Q_2 = ((X, Y)^3,\ Z_1Y + Z_2X)$$

sont des idéaux primaires appartenant à (X, Y), mais que $Q_1 + Q_2$ n'est pas primaire parce qu'il contient $Z_1(X^2 - Y^2)$ (Seidenberg).

4. Soient φ un épimorphisme d'un anneau R sur un anneau R' et Q un idéal qui contient le noyau de φ. Montrer que Q est un idéal primaire appartenant à P si, et seulement si, $\varphi(Q)$ est un idéal primaire appartenant à $\varphi(P)$.

6 Localisation

Soit S un sous-monoïde multiplicatif d'un anneau commutatif R. Pour un R-module M on définit le **sous-module de S-torsion** de M comme

$$\tau_S(M) = \{\, x \in M : sx = 0 \text{ pour un } s \text{ dans } S \,\}.$$

On vérifie facilement que $\tau_S(M)$ est bien un sous-module de M. Si $M = \tau_S(M)$, on dit que M est un **module de S-torsion** [1].

Le théorème suivant implique que le morphisme $R \to S^{-1}R$ réfléchit les idéaux de type fini si, et seulement si, $\tau_S(R/I)$ est de type fini pour tout idéal de type fini I de R [2].

Théorème 6.1. *Soient S un sous-monoïde multiplicatif d'un anneau commutatif R, I un idéal de R et $x \in R$. Alors les propriétés suivantes sont équivalentes.*

(i) *$x/1 \in S^{-1}I$ dans $S^{-1}R$.*

(ii) *$sx \in I$ pour un $s \in S$.*

(iii) *$x \bmod I$ est un élément de $\tau_S(R/I)$.*

Démonstration. Clairement les points (ii) et (iii) sont équivalents. Si la condition (i) est satisfaite, on a $x/1 = y/s_1$ pour un $y \in I$ et un $s_1 \in S$. Par suite il existe un $s_2 \in S$ tel que $s_2(s_1x - y) = 0$, donc nous pouvons prendre $s = s_2s_1$ dans (ii). Inversement, si la condition (ii) est satisfaite, alors $x/1 = (sx)/s \in S^{-1}I$. □

Nous disons qu'un module M est **S-borné** s'il existe un $s \in S$ tel que $sM = 0$. On voit facilement que tout module de S-torsion de type fini est S-borné. Pour les sous-modules de S-torsion de modules de présentation finie sur un anneau cohérent, la réciproque est vraie.

Théorème 6.2. *Soit S un sous-monoïde multiplicatif d'un anneau commutatif cohérent R. Si M est un R-module de présentation finie et si $\tau_S(M)$ est S-borné, $\tau_S(M)$ est de type fini.*

1. **NdT.** On a facilement $\tau_S(\tau_S(M)) = \tau_S(M)$: le sous-module de S-torsion de M est donc bien un module de S-torsion.

2. **NdT.** Notons $\varphi_S\colon R \to S^{-1}R$ et $\pi_I : R \to R/I$ les morphismes canoniques. Le théorème démontre que $\varphi_S^{-1}(\varphi_S(I)) = \pi_I^{-1}(\tau_S(R/I))$. Un idéal arbitraire de $S^{-1}R$ s'écrit $S^{-1}I$ pour un idéal de R. Son image réciproque par φ_S est donc de type fini si, et seulement si, $\pi_I^{-1}(\tau_S(R/I))$ est de type fini si, et seulement si, $\tau_S(R/I)$ de type fini.

Démonstration. Soit $s \in S$ tel que $s\tau_S(M) = 0$. Alors $\tau_S(M)$ est le noyau de l'endomorphisme de M induit par la multiplication par s, donc $\tau_S(M)$ est de type fini d'après le théorème III.2.2 et le corolaire III.2.6. □

Lemme 6.3. *Soient S un sous-monoïde multiplicatif d'un anneau commutatif R, M un R-module, et M' un sous-R-module de M. Si $\tau_S(M')$ et $\tau_S(M/M')$ sont S-bornés, il en va de même pour $\tau_S(M)$.*

Démonstration. On prend s et $t \in S$ tels que $s\tau_S(M') = 0$ et $t\tau_S(M/M') = 0$. Un $x \in \tau_S(M)$ représente un élément de $\tau_S(M/M')$, donc $tx \in M'$ et par suite $tx \in \tau_S(M')$. Ainsi $stx = 0$, et nous avons démontré que $st\tau_S(M) = 0$. □

Théorème 6.4. *Soit S un sous-monoïde multiplicatif d'un anneau commutatif cohérent R. Si $\tau_S(R/I)$ est S-borné pour tout idéal de type fini I de R (en particulier si $R \to S^{-1}R$ réfléchit les idéaux de type fini*[1]*), alors*

(i) *$\tau_S(M)$ est de type fini pour tout R-module de présentation finie M ;*

(ii) *si R est fortement discret, il en va de même pour $S^{-1}R$.*

Démonstration. Pour démontrer le point (i), nous considérons un système générateur $x_1, \ldots, x_n$ de M et nous notons M' le sous-module de M engendré par $x_1, \ldots, x_{n-1}$. Par récurrence sur n, $\tau_S(M')$ est S-borné. L'idéal $I = \{\, r \in R : rx_n \in M' \,\}$ est de type fini parce que R est cohérent et M est de présentation finie. Par hypothèse $\tau_S(R/I)$ est S-borné, donc $\tau_S(M/M') \simeq \tau_S(R/I)$ est S-borné. Donc $\tau_S(M)$ est S-borné d'après le lemme 6.3. Il est de type fini d'après le théorème 6.2.

Pour démontrer le point (ii), nous considérons un idéal J de type fini de $S^{-1}R$. Donc $J = S^{-1}I$ pour un idéal de type fini I de R. On prend un $t \in S$ tel que $t\tau_S(R/I) = 0$. Si $x \in R$ et $tx \in I$, alors $x/s = (tx)/(ts) \in J$ pour tout $s \in S$. Inversement, si $x/s \in J$, $x/1 \in J$, donc $s_1 x \in I$ pour un $s_1 \in S$ d'après le théorème 6.1, et par suite $tx \in I$. Donc nous pouvons décider si $x/s \in J$ en testant $tx \in I$. □

Théorème 6.5. *Soit P un idéal premier propre de type fini détachable d'un anneau commutatif cohérent R, et soit M un R-module de présentation finie tel que $P^n M = 0$ pour un entier $n > 0$. Alors $\tau_{R\setminus P}(M)$ est de type fini.*

Démonstration. Soit $S = R \setminus P$. Comme M est un module sur R/P^n, nous sommes ramenés au cas où $P^n = 0$ et nous procédons par récurrence sur n. Si $n = 1$, $P = 0$, donc R est un anneau intègre discret et S est l'ensemble des éléments non nuls de R. Soit I un idéal de type fini de R. Si $I = 0$, on a $\tau_S(R/I) = 0$; et s'il y a un $s \neq 0$ dans I, on a $s\tau_S(R/I) = 0$. Nous pouvons

1. **NdT.** D'après la remarque avant le théorème 6.1 expliquée dans la note 2, cela signifie que $\tau_S(R/I)$ est de type fini pour tout idéal de type fini I. Et si $\tau_S(R/I)$ est de type fini, il est S-borné car c'est un module de S-torsion.

décider laquelle de ces alternatives est satisfaite parce que R est discret et I est de type fini. On voit ainsi que $\tau_S(R/I)$ est S-borné pour tout idéal de type fini I. On en déduit que $\tau_S(M)$ est de type fini d'après le théorème 6.4.

Si $n > 1$, les modules PM et M/PM sont de présentation finie et ils sont annulés par P^{n-1}. Alors $\tau_S(PM)$ et $\tau_S(M/PM)$ sont de type fini par récurrence sur n, et sont donc S-bornés. Par suite, $\tau_S(M)$ est S-borné d'après le lemme 6.3, et il est de type fini d'après le théorème 6.2. □

Théorème 6.6. *Soit S un sous-monoïde multiplicatif d'un anneau commutatif noethérien R. Alors l'anneau $S^{-1}R$ est noethérien.*

Démonstration. Soit $J_1 \subseteq J_2 \subseteq \cdots$ une chaine d'idéaux de type fini de $S^{-1}R$. Alors nous pouvons construire une chaine $I_1 \subseteq I_2 \subseteq \cdots$ d'idéaux de type fini de R telle que $J_j = S^{-1}I_j$ pour tout j. Il existe un n tel que $I_n = I_{n+1}$, donc $J_n = J_{n+1}$. □

Corolaire 6.7. *Soit R un anneau cohérent noethérien fortement discret. Soit P un idéal premier de type fini de R tel que $P^n = 0$ pour un n. Alors R_P est un anneau cohérent noethérien fortement discret.*

Démonstration. Le théorème 6.6 montre que R_P est noethérien. La cohérence résulte de l'exercice III.3.4. Comme $P^n = 0$, le théorème 6.5 nous dit que $\tau_{R\setminus P}(M)$ est de type fini pour tout R-module de présentation finie M, donc R_P est fortement discret d'après le théorème 6.4. □

Voir l'exercice 8.5 pour une version plus forte du corolaire 6.7.

Nous étudions maintenant le comportement des idéaux primaires par localisation.

Lemme 6.8. *Soient S un sous-monoïde multiplicatif d'un anneau commutatif R et Q un idéal primaire de R tel que $Q \cap S = \emptyset$. Alors $x/1 \in S^{-1}Q$ si, et seulement si, $x \in Q$. Si Q appartient à l'idéal premier P, $S^{-1}Q$ est un idéal primaire appartenant à l'idéal premier $S^{-1}P$.*

Démonstration. Il est évident que $x/1 \in S^{-1}Q$ si $x \in Q$. Inversement, si $x/1 \in S^{-1}Q$, alors $sx \in Q$ pour un $s \in S$ d'après le théorème 6.1. Donc $x \in Q$ ou $s^n \in Q$ pour un n, mais ce dernier cas est impossible car $Q \cap S$ est vide.

Clairement $S^{-1}Q \subseteq S^{-1}P$ et tout élément de $S^{-1}P$ a une puissance dans $S^{-1}Q$. Supposons que $(x/s_1)(y/s_2) \in S^{-1}Q$. Alors $sxy \in Q$ pour un $s \in S$, donc ou bien $x \in P$, et alors $x/s_1 \in S^{-1}P$, ou bien $sy \in Q$, et alors $y/s_2 \in S^{-1}Q$. □

Théorème 6.9. *Soient S un sous-monoïde multiplicatif d'un anneau commutatif R, $Q_1, \ldots, Q_n$ des idéaux primaires détachables de R tels que $Q_i \cap S$ est vide pour $i = 1, \ldots, m$, $Q_i \cap S$ est non vide pour $i = m+1, \ldots, n$, et $I = Q_1 \cap \cdots \cap Q_n$. On a $S^{-1}I = \bigcap_{i=1}^{m} S^{-1}Q_i$.*

Démonstration. Si $Q_i \cap S$ est non vide, $S^{-1}Q_i = S^{-1}R$. Clairement, $S^{-1}I \subseteq \bigcap_{i=1}^{n} S^{-1}Q_i = \bigcap_{i=1}^{m} S^{-1}Q_i$. Inversement, supposons que $x/s \in \bigcap_{i=1}^{m} S^{-1}Q_i$. D'après le lemme 6.8, nous avons $x \in I$, donc $x/s \in S^{-1}I$. □

Le lemme 6.8 et le théorème 6.9 impliquent que si R est un anneau commutatif fortement discret tel que tout idéal de type fini est une intersection finie d'idéaux primaires de type fini, et si P est un idéal premier de type fini de R, alors R_P est un anneau commutatif fortement discret (mais voyez l'exercice 8).

Soit P un idéal premier détachable d'un anneau commutatif R, et soit un $n > 0$. Si P^n est un idéal primaire, P^n appartient à P. Même si P^n n'est pas nécessairement primaire lorsque P n'est pas maximal (voir le corolaire 5.5 et l'exercice 5.2), il y a toujours un idéal voisin qui est primaire. La **puissance symbolique** $P^{(n)}$ de P est l'idéal

$$P^{(n)} = \{\, x \in R : sx \in P^n \text{ pour un } s \text{ dans } S = R \setminus P \,\}.$$

Observez que $P^{(n+1)} \subseteq P^{(n)} \subseteq P^{(1)} = P$, que $P^{(n)}/P^n = \tau_S(R/P^n)$, et que $P^{(n)}$ est l'image réciproque de $S^{-1}P^n$ dans R.

Théorème 6.10. *Soit P un idéal premier détachable d'un anneau commutatif R, et soit $n > 0$. Alors $P^{(n)}$ est un idéal primaire appartenant à P. Si P^n est primaire, $P^{(n)} = P^n$.*

Démonstration. Si $xy \in P^{(n)}$, $sxy \in P^n$ pour un $s \in R \setminus P$. Si $x \in R \setminus P$, $sx \in R \setminus P$, donc $y \in P^{(n)}$. Si P^n est primaire et si $x \in P^{(n)}$, alors $sx \in P^n$ pour un $s \in R \setminus P$, donc $x \in P^n$ ou $s^m \in P^n$ pour un m. Donc $x \in P^n$. □

Soit P un idéal premier d'un anneau commutatif R. Alors P est un **idéal premier minimal au-dessus d'un** idéal I si $P \supseteq I$ et si pour tout idéal premier P' tel que $P \supseteq P' \supseteq I$ on a $P = P'$. Un **idéal premier minimal de** R est un idéal premier minimal au-dessus de 0.

Théorème 6.11. *Soit P un idéal premier propre de type fini d'un anneau commutatif R. Si $P^{(n)} = P^{(n+1)}$ pour un n, P est un idéal premier minimal au-dessus de* 0.

Démonstration. Soit Q un idéal premier de R tel que $P \supseteq Q$. L'égalité $P^{(n)} = P^{(n+1)}$ implique que $(P_P)^n = (P_P)^{n+1} = P_P(P_P)^n$. Le R_P-module $(P_P)^n$ est de type fini et P_P est un idéal quasi-régulier de R_P [1], donc d'après le lemme de Nakayama, (lemme III.1.4), nous avons $(P_P)^n = 0_P \subseteq Q_P$. Donc $P^n \subseteq Q$ d'après le lemme 6.8 [2], et par suite $P \subseteq Q$ d'après le théorème II.2.4. □

1. **NdT.** L'idéal premier P est propre, donc R_P est non trivial et P_P est quasi-régulier : si $x/s \in P_P$, avec $x \in P$ et $s \notin P$, alors $1 + x/s = (s + x)/s$ avec $x + s \notin P$, donc $1 + x/s$ est inversible dans R_P.

2. **NdT.** Dans le lemme on prend $S = R \setminus P$. Comme Q est premier, il est primaire. La première affirmation du lemme dit que si l'image dans R_P d'un x de R est dans Q_P, alors $x \in Q$. On applique cela pour les $x \in P^n$.

Avec des hypothèses supplémentaires de cohérence et de décidabilité, la puissance symbolique $P^{(n)}$ est un idéal de type fini.

Théorème 6.12. *Soit P un idéal premier propre de type fini d'un anneau commutatif cohérent fortement discret R, et soit $n > 0$. Alors $P^{(n)}$ est un idéal primaire de type fini appartenant à P.*

Démonstration. D'après le théorème 6.10, il suffit de démontrer que $P^{(n)}$ est de type fini. Mais $P^{(n)}/P^n = \tau_{R\setminus P}(R/P^n)$ est de type fini d'après le théorème 6.5, donc $P^{(n)}$ est de type fini. □

Exercices

1. On considère les anneaux $\mathbb{Z} \subseteq \mathbb{Z}[X]/(2X-4)$. Montrer que l'idéal P engendré par 2 est premier dans chacun d'eux. Montrer que $2 \in P^{(2)}$ dans l'un et $2 \notin P^{(2)}$ dans l'autre. Construire un exemple brouwerien d'un anneau R fortement discret et d'un idéal premier de type fini P tels que $P^{(2)}$ n'est pas détachable.
2. Soit S un sous-monoïde multiplicatif de type fini d'un anneau commutatif cohérent noethérien R. Montrer que si M est un R-module de présentation finie, $\tau_S(M)$ est de type fini. (Suggestion : considérer le produit s des générateurs de S et étudier $M_n = \{\, x \in M : s^n x = 0 \,\}$.)
3. Soit S un sous-monoïde multiplicatif de type fini d'un anneau commutatif cohérent noethérien R fortement discret. Montrer que $S^{-1}R$ est un anneau cohérent noethérien fortement discret.
4. Soit R l'anneau des polynômes sur $\mathbb{Z}$ en les indéterminées $s, x_1, x_2, \ldots$ modulo l'idéal engendré par les éléments sx_i, et soit S le sous-monoïde multiplicatif de R engendré par s. Montrer que $\tau_S(R)$ est S-borné mais n'est pas de type fini. Pourquoi le théorème 6.2 ne s'applique-t-il pas ?
5. Soient a une suite binaire et S le sous-monoïde multiplicatif de $\mathbb{Z}$ engendré par $\{\, 1 + a_n : n = 1, 2, \ldots \,\}$. Montrer que $S^{-1}\mathbb{Z}$ est un exemple brouwerien d'un anneau non fortement discret. Pourquoi le théorème 6.4 ne s'applique-t-il pas ?
6. Pour un nombre premier p, notons A_p l'anneau des couples (x, y) avec $x \in \mathbb{Z}$ et $y \in \mathbb{Z}_p$ (l'anneau des entiers modulo p), en définissant la multiplication par

$$(x_1, y_1)(x_2, y_2) = (x_1 y_1, x_1 y_2 + x_2 y_1 + y_1 y_2).$$

   Soit p_n le n-ième nombre premier impair, et soit a une suite binaire. Si $a_i = 0$ pour tout $i \leqslant n$, on pose $R_n = \mathbb{Z}$; sinon on prend pour R_n l'anneau A_{p_i} avec i le premier indice inférieur ou égal à n tel que $a_i \neq 0$. Soit R la réunion (la limite directe) des anneaux R_n. Montrer que R

est un anneau cohérent noethérien fortement discret. Soit P l'idéal de R engendré par 2. Montrer que $\tau_{R\setminus P}(R)$ est un exemple brouwerien d'un R-module qui n'est pas de type fini. Pourquoi le théorème 6.5 ne s'applique-t-il pas ?

7. Soit S un sous-monoïde multiplicatif d'un anneau commutatif R, et soit φ le morphisme naturel de R vers $S^{-1}R$. Montrer que $\tau_S(R/I)$ est de type fini pour tout idéal de type fini I de R si, et seulement si, $\varphi^{-1}(J)$ est de type fini pour tout idéal de type fini J de $S^{-1}R$.
8. En utilisant les anneaux $\mathbb{Z} \subseteq \mathbb{Z}[X]/(2X)$, construire un exemple brouwerien d'un anneau R avec un idéal premier P engendré par 2 tel que R est fortement discret alors que R_P n'est pas discret.
9. Soit K un corps discret et $R = K[S, X, Y, Z]/(SXY - Z^2)$. En utilisant les deux idéaux premiers $I = (x, z)$ et $J = (x, y, z)$ de R, construire un exemple brouwerien d'un idéal premier P de R tel que $xy \in P^{(2)}$, mais pour lequel on n'a pas $x \in P$ ou $y \in P^{(2)}$. Pourquoi le théorème 6.10 ne s'applique-t-il pas ?

7 Décompositions primaires

Un idéal I d'un anneau commutatif admet une **décomposition primaire** s'il existe des idéaux primaires de type fini $Q_1, \ldots, Q_n$, appartenant à des idéaux premiers de type fini, tels que $I = \bigcap_i Q_i$. On dit aussi dans ce cas que l'idéal I est **décomposable** [1]. En mathématiques classiques, tout idéal d'un anneau noethérien admet une décomposition primaire (voir l'exercice 4).

Une décomposition primaire est **réduite** [2] si d'une part aucun idéal primaire de la décomposition ne contient l'intersection des autres idéaux primaires, et d'autre part deux idéaux primaires de la décomposition appartenant au même idéal premier sont égaux. Dans un anneau cohérent fortement discret, nous pouvons remplacer les idéaux primaires appartenant à un même idéal premier par leur intersection (corolaire 5.3), et nous pouvons supprimer les idéaux primaires qui contiennent l'intersection des autres idéaux primaires, de sorte que tout idéal décomposable admet une décomposition primaire réduite.

Soit I un idéal d'un anneau commutatif R et soit P un idéal premier propre de type fini de R. Nous disons que P est un **idéal premier associé** à I si $P = \sqrt{I : a}$ pour un $a \in R$.

Théorème 7.1. *Soit R un anneau commutatif cohérent fortement discret. Soit $I = \bigcap_i Q_i$ une décomposition primaire réduite d'un idéal propre I de R. Alors l'ensemble des idéaux premiers associés à I est formé par les idéaux $\sqrt{Q_i}$.*

1. **NdT.** L'idéal $I = R$ est décomposable : prendre $n = 0$ et la famille vide d'idéaux premiers de type fini.
2. **NdT.** Irredundant.

Démonstration. Pour voir que $\sqrt{Q_i}$ est un idéal premier associé à I, on prend un $a \in \bigcap_{j\neq i} Q_j$ tel que $a \notin Q_i$. Alors $I : a = \bigcap_j (Q_j : a)$, et $Q_j : a = R$ si $j \neq i$, donc $I : a = Q_i : a$. Enfin le théorème 5.7 nous dit que $Q_i : a$ est un idéal primaire appartenant à $\sqrt{Q_i}$.

Inversement, pour tout a, le théorème 5.7 nous dit que l'idéal $\sqrt{I : a} = \bigcap_i \sqrt{Q_i : a}$ est égal à l'intersection des idéaux $\sqrt{Q_i}$ tels que $a \notin Q_i$; donc si $\sqrt{I : a}$ est un idéal premier, $\sqrt{I : a} = \sqrt{Q_i}$ pour un i d'après le théorème II.2.4. □

Théorème 7.2. *Soient R un anneau commutatif cohérent fortement discret et I un idéal décomposable de R. Alors tout idéal premier minimal au-dessus de I est un idéal premier associé à I.*

Démonstration. Soient $P_1, \ldots, P_n$ les idéaux premiers associés à I, et soit P un idéal premier minimal au-dessus de I. Alors $P \supseteq \sqrt{I} = \bigcap_i P_i$, donc $P \supseteq P_i$ pour un i (théorème II.2.4). Par minimalité $P = P_i$. □

Dans la situation du théorème 7.2, les idéaux premiers associés à I qui ne sont pas minimaux au-dessus de I sont appelés des **idéaux premiers immergés**. Les idéaux primaires appartenant à un idéal premier immergé ne sont pas nécessairement uniques (voir l'exercice 1), mais les idéaux primaires appartenant aux idéaux premiers minimaux sont uniques.

Théorème 7.3. *Soient R un anneau commutatif cohérent fortement discret et $I = \bigcap_i Q_i$ une décomposition primaire réduite d'un idéal I avec les idéaux premiers associés P_i. Pour chaque i on définit $Q'_i = \{\, x \in R : sx \in I \text{ pour un } s \in R \setminus P_i \,\}$. Alors Q'_i est un idéal détachable contenu dans Q_i, et $Q'_i = Q_i$ si P_i est un idéal premier minimal au-dessus de I.*

Démonstration. On vérifie facilement que Q'_i est un idéal de R. Comme R est cohérent, l'idéal $I : x$ est de type fini, donc nous pouvons décider si $I : x \subseteq P_i$. Ainsi l'idéal Q'_i est détachable. Si $x \in Q'_i$, $sx \in I \subseteq Q_i$ pour un $s \notin P_i$, donc $x \in Q_i$. Donc $Q'_i \subseteq Q_i$. Si P_i est un idéal premier minimal au-dessus de I, P_i ne contient pas $\bigcap_{j\neq i} P_j$ (les idéaux P_j sont distincts parce que la décomposition primaire est réduite), donc en utilisant la cohérence nous pouvons trouver un $a \in \bigcap_{j\neq i} P_j \setminus P_i$. Alors $a^m \in \bigcap_{j\neq i} Q_j \setminus P_i$ pour un m, et $a^m Q_i \subseteq I$. Donc $Q_i \subseteq Q'_i$. □

Corolaire 7.4. *Soient R un anneau commutatif cohérent fortement discret, I un idéal de R décomposable et P un idéal premier minimal au-dessus de I. Alors l'idéal primaire qui appartient à P dans une décomposition primaire réduite de I est l'ensemble $\{\, x \in R : sx \in I \text{ pour un } s \in R \setminus P \,\}$. Donc les idéaux primaires appartenant à des idéaux premiers minimaux sont les mêmes pour toutes les décompositions primaires réduites.* □

Lemme 7.5. *Soit I un idéal d'un anneau commutatif R.*

(i) *Si l'idéal I est décomposable, il en va de même pour $\sqrt{I}$.*

(ii) *L'idéal $\sqrt{I}$ est décomposable si, et seulement si, il est égal à l'intersection d'un nombre fini d'idéaux premiers de type fini.*

(iii) *Si R est un anneau cohérent fortement discret et si $\sqrt{I}$ est décomposable, les idéaux premiers minimaux au-dessus de I sont exactement les idéaux premiers associés à $\sqrt{I}$, et $\sqrt{I}$ est leur intersection.*

Démonstration. Si I, ou $\sqrt{I}$, est égal à $\bigcap_i Q_i$, $\sqrt{I} = \bigcap_i \sqrt{Q_i}$. Ce fait, en notant que les idéaux premiers sont primaires et s'appartiennent à eux-mêmes, démontre les propriétés (i) et (ii). Pour démontrer (iii), on considère un idéal $\sqrt{I}$ décomposable. D'après (ii), nous pouvons écrire $\sqrt{I}$ comme une intersection d'un nombre fini d'idéaux premiers de type fini, et nous obtenons une décomposition primaire réduite de $\sqrt{I}$ à partir de ces idéaux premiers. D'après le théorème 7.2, ce sont des idéaux premiers associés à $\sqrt{I}$, car ils sont tous évidemment minimaux. Comme les idéaux premiers minimaux au-dessus de $\sqrt{I}$ sont les mêmes que les idéaux premiers minimaux au-dessus de I, la propriété (iii) est établie. □

Soient R un anneau commutatif cohérent fortement discret, et I et P des idéaux propres de type fini de R avec P idéal premier minimal au-dessus de I. Considérons l'idéal $Q = \{\, x \in R : sx \in I \text{ pour un } s \in R \setminus P \,\}$. On vérifie facilement que Q est un idéal détachable qui contient I, et que $Q/I = \tau_{R\setminus P}(R/I)$. Si Q est de type fini, alors $Q = I : s$ pour un $s \notin P$, donc l'idéal $I : Q$ n'est pas contenu dans P. Si I est décomposable, le théorème 7.3 nous dit que Q est l'idéal primaire de I appartenant à P. Même sans supposer I décomposable, il est également vrai dans certains cas que l'idéal Q est un idéal primaire de type fini.

Lemme 7.6. *Soient I et P des idéaux de type fini d'un anneau commutatif cohérent fortement discret R. Si P est premier et $P^n \subseteq I \subseteq P$ pour un n, alors P est l'unique idéal premier minimal au-dessus de I, et l'idéal*

$$Q = \{\, x \in R : sx \in I \text{ pour un } s \in R \setminus P \,\}$$

est un idéal primaire de type fini appartenant à P.

Démonstration. Comme $P^n \subseteq I$, l'idéal P est contenu dans tout idéal premier qui contient I. Il reste à voir que Q est un idéal primaire de type fini appartenant à P. Comme I est de type fini, nous pouvons supposer que $I = 0$. Dans ce cas, $Q = P^{(n)}$, et c'est un idéal primaire de type fini appartenant à P d'après le théorème 6.12. □

Théorème 7.7. *Soient R un anneau commutatif cohérent fortement discret, I un idéal de type fini tel que $\sqrt{I}$ est décomposable, et P un idéal premier minimal au-dessus de I. Alors l'idéal*

$$Q^* = \{\, x \in R : sx \in I \text{ pour un } s \in R \setminus P \,\}$$

est un idéal primaire de type fini appartenant à P.

Démonstration. Soit K le produit des idéaux premiers minimaux au-dessus de I différents de P. Il existe un n tel que $(PK)^n \subseteq I$. Soit $J = I : K^n$. Alors $P^n \subseteq J \subseteq P$. D'après le lemme 7.6, l'idéal

$$Q = \{\, x \in R : sx \in J \text{ pour un } s \in R \setminus P \,\}$$

est un idéal primaire de type fini appartenant à P. Comme I est contenu dans J, l'idéal Q^* est contenu dans Q ; nous allons montrer qu'ils sont égaux. Si $r \in Q$, $srK^n \subseteq I$ pour un $s \in R \setminus P$. Si $t \in K^n \setminus P$, $str \in I$ donc $r \in Q^*$. □

L'idéal Q^* du théorème 7.7 est appelé l'**idéal primaire isolé au-dessus de I appartenant à P**.

Exercices

1. Soit $R = \mathbb{Z}[X]$. Montrer que (2) est un idéal premier de R, et que $(4, X)$ et $(4, X-2)$ sont des idéaux primaires de R appartenant à l'idéal premier $(2, X)$. Conclure que $(4, X) \cap (2)$ et $(4, X-2) \cap (2)$ sont des décompositions primaires réduites de $(2X, 4)$. Ainsi les idéaux primaires appartenant à des idéaux premiers immergés ne sont pas nécessairement uniques.
2. Soit k l'anneau des entiers modulo 2. Considérons les anneaux $k \subseteq k[X]/(X^2)$. Construire un exemple brouwerien d'un anneau R cohérent noethérien fortement discret, tel que tout idéal de type fini de R est primaire, R contient un idéal premier détachable propre, alors que R n'a pas d'idéaux de type fini propres ; donc 0 est un idéal primaire sans décomposition primaire.
3. Soient R un anneau cohérent noethérien, I un idéal de type fini de R, et $a, b \in R$ avec $ab \in I$. Montrer qu'il existe un n tel que $I = (I + (a)) \cap (I + (b^n))$. Idée : considérer la chaine des idéaux $I : (b^n)$.
4. Nous disons qu'un idéal I est **irréductible** si lorsque I est écrit comme l'intersection de deux idéaux, alors l'un de ces idéaux est égal à I. Utiliser l'exercice 3 pour montrer que si R est un anneau cohérent noethérien, et si I est un idéal de type fini irréductible, alors I est primaire. Donner une démonstration en mathématiques classiques que tout idéal dans un anneau noethérien est une intersection d'idéaux primaires en utilisant les principes que tout idéal est primaire ou ne l'est pas, et que tout ensemble d'idéaux dans un anneau noethérien contient un élément maximal.

8 Anneaux de Lasker-Noether

Un **anneau de Lasker-Noether** est un anneau commutatif cohérent noethérien fortement discret tel que le radical de tout idéal de type fini est l'intersection d'un nombre fini d'idéaux premiers de type fini. En particulier le radical d'un idéal de type fini est de type fini, et il admet une décomposition primaire (lemme 7.5(ii)). En mathématiques classiques, tout anneau commutatif noethérien est un anneau de Lasker-Noether (voir l'exercice 7.4). Les corps discrets sont des anneaux de Lasker-Noether, de même que l'anneau des entiers. Le nom *Lasker-Noether* fait référence à la décomposition de Lasker-Noether du théorème 8.5.

Si k est un corps discret, $k[X]$ est un anneau cohérent noethérien fortement discret d'après le théorème de la base de Hilbert (théorème 1.5). Tout idéal de type fini de $k[X]$ est principal, donc si le radical de l'idéal principal (f) est l'intersection d'un nombre fini d'idéaux premiers de type fini, tout diviseur premier de f correspond à un générateur de l'un de ces idéaux premiers (principaux). Donc si $k[X]$ est un anneau de Lasker-Noether, k est un corps factoriel.

Le lemme 7.5(iii) garantit que dans un anneau de Lasker-Noether nous pouvons calculer les idéaux premiers minimaux au-dessus d'un idéal de type fini donné, qui sont eux-mêmes de type fini. La classe des anneaux de Lasker-Noether est stable par localisation en un idéal premier de type fini (théorème 8.1), et par passage au quotient modulo un idéal de type fini (théorème 8.2).

Théorème 8.1. *Soit S un sous-monoïde multiplicatif d'un anneau de Lasker-Noether R tel que $I \cap S$ est vide ou non vide pour tout idéal de type fini I de R. Alors $S^{-1}R$ est un anneau de Lasker-Noether*[1].

Démonstration. L'anneau $S^{-1}R$ est noethérien d'après le théorème 6.6 et cohérent d'après l'exercice III.3.4. Soit J un idéal de type fini de $S^{-1}R$. Nous devons montrer que $\sqrt{J}$ est l'intersection d'un nombre fini d'idéaux premiers de type fini de $S^{-1}R$. On écrit $J = S^{-1}I$ pour un idéal de type fini I de R. Alors $\sqrt{J} = S^{-1}\sqrt{I} = S^{-1}(P_1 \cap \cdots \cap P_n)$ avec les P_i des idéaux premiers de type fini de R. Nous pouvons supposer que P_i a une intersection vide avec S pour $i \leqslant m$, et non vide pour $i > m$. Le théorème 6.9 dit que nous avons $\sqrt{J} = \bigcap_{i=1}^{m} S^{-1}P_i$. Et $S^{-1}P_i$ est un idéal premier (de type fini) d'après le lemme 6.8. □

Théorème 8.2. *Soient R un anneau de Lasker-Noether et I un idéal de type fini de R. Alors R/I est un anneau de Lasker-Noether.*

Démonstration. Trivial. □

1. **NdT.** Si $S = R \setminus P$ pour un idéal premier P, la condition « $I \cap S$ est vide ou non vide » signifie « I est ou n'est pas contenu dans P ». Comme I est de type fini, le test est effectif si, et seulement si, P est détachable. Une conséquence du théorème 8.1 est donc que pour tout idéal premier détachable, et en particulier pour tout idéal premier de type fini, le localisé R_P est un anneau de Lasker-Noether, comme indiqué juste avant l'énoncé du théorème.

Une **série de composition** pour un module de type fini cohérent fortement discret M est une chaine finie maximale dans le treillis des sous-modules de type fini de M. On vérifie facilement qu'un espace vectoriel de dimension finie sur un corps a une série de composition.

Comme le treillis des sous-modules de type fini de M est modulaire, le théorème de Jordan-Hölder-Dedekind (I.5.2) s'applique, donc un module avec une série de composition est noethérien et il satisfait la condition de chaine descendante sur les sous-modules de type fini.

Théorème 8.3. *Soient R un anneau de Lasker-Noether et P un idéal premier minimal de R tel que tout élément de $R\setminus P$ est inversible. Alors le R-module R a une série de composition.*

Démonstration. L'idéal P est de type fini et l'anneau $F = R/P$ est un corps discret [1]. Comme P est l'unique idéal premier minimal au-dessus de 0 [2], il existe un n tel que $P^n = 0$. Les modules P^i/P^{i+1} sont des espaces vectoriels sur F, et sont de dimension finie parce que R est cohérent fortement discret. Donc R admet une série de composition formée d'idéaux de type fini détachables. □

Lemme 8.4. *Soit R un anneau commutatif, I un idéal de R, et $P_1, \dots, P_n$, $Q_1, \dots, Q_n$ des idéaux détachables de R tels que $I \subseteq \bigcap_i Q_i$ et Q_i est un idéal primaire appartenant à l'idéal premier P_i pour chaque i. Soit $f \in (I : \bigcap_i Q_i) \setminus (\bigcup_i P_i)$. Alors*

(i) $I : f = \bigcap_i Q_i$.

(ii) $I : f = I : f^2$.

(iii) $I = (I : f) \cap (I, f)$.

Démonstration. Si $x \in \bigcap_i Q_i$, alors $xf \in I$, donc $\bigcap_i Q_i \subseteq I : f$. Inversement, si $xf \in I$, alors $xf \in Q_i$, donc $x \in Q_i$ car $f \notin P_i$. Donc $I : f \subseteq \bigcap_i Q_i$.

Comme $f^2 \in (I : \bigcap_i Q_i) \setminus (\bigcup_i P_i)$, la propriété (i) dit que $I : f = \bigcap_i Q_i = I : f^2$.

De manière évidente $I \subseteq (I : f) \cap (I, f)$. Si $x \in (I : f) \cap (I, f)$, alors il existe un $a \in I$ et un $r \in R$ tels que $x = a + rf \in I : f$. Donc $af + rf^2 \in I$, et par suite $rf^2 \in I$. D'après (ii), cela implique $rf \in I$, donc $x = a + rf \in I$. □

Théorème 8.5 (théorème de décomposition primaire)**.** *Soit R un anneau de Lasker-Noether. Alors tout idéal de type fini de R est décomposable.*

1. **NdT.** D'après le lemme 7.5(iii), P est un idéal premier associé à 0, donc de type fini, donc détachable. L'anneau $F = R/P$ est donc un anneau non trivial discret avec tout élément non nul inversible.

2. **NdT.** La décomposition primaire de 0 dans R donne celle de 0 dans R/P, qui est triviale. Donc $\sqrt{0} = P$.

Démonstration. Soit I un idéal de type fini propre de R. Nous construisons tout d'abord deux idéaux de type fini J et K tels que J admet une décomposition primaire, $I = J \cap K$, et K contient proprement I.

D'après le théorème 7.7, les idéaux primaires isolés $Q_1, \dots, Q_k$ de I appartenant aux idéaux premiers minimaux $P_1, \dots, P_k$ au-dessus de I sont de type fini. On pose $J = Q_1 \cap \cdots \cap Q_k$. Comme $I : Q_i$ n'est pas contenu dans P_i, l'idéal $I : J$ n'est contenu dans aucun P_i, donc il existe un $f \in (I : J) \setminus (\bigcup_i P_i)$ d'après le théorème II.2.3. On prend $K = (I, f)$, et l'on a $I = J \cap K$ d'après le lemme 8.4.

Nous construisons maintenant une chaine ascendante d'idéaux de type fini H_n de R de la manière suivante. D'abord $H_1 = I$. Ensuite $H_{n+1} = R$ si $H_n = R$; sinon nous prenons un H_{n+1} tel que $H_n = J \cap H_{n+1}$, où J est décomposable et H_{n+1} contient proprement H_n. Notez que si H_n est décomposable, alors il en va de même pour H_{n-1}, et donc il en va de même pour I. Comme R est noethérien, il existe un n tel que $H_n = H_{n+1}$; mais cela arrive seulement si $H_n = R$, auquel cas H_n, et par suite I, est décomposable. □

Théorème 8.6. *Soit P un idéal premier détachable propre d'un anneau de Lasker-Noether R, et soit $\varphi\colon R \to R_P$ le morphisme naturel. Alors R_P est un anneau de Lasker-Noether, et φ réfléchit les idéaux de type fini.*

Démonstration. L'anneau R_P est de Lasker-Noether d'après le théorème 8.1. Soit I un idéal de type fini de R_P ; on a un idéal de type fini $J \subseteq R$ tel que $I = J_P$. D'après le théorème 8.5, l'idéal J admet une décomposition primaire $J = Q_1 \cap \cdots \cap Q_n$. Si $Q_1, \dots, Q_s$ sont les idéaux primaires de cette décomposition contenus dans P, alors, d'après le lemme 6.8 et le théorème 6.9 où l'on prend $S = R \setminus P$, on a $\varphi^{-1}(I) = \varphi^{-1}(J_P) = Q_1 \cap \cdots \cap Q_s$, qui est de type fini. □

Exercices

1. Soit R un anneau de Lasker-Noether qui est un anneau principal. Montrer que R est un anneau à factorisation unique.
2. Soit G l'exemple brouwerien dans l'exercice VII.1.5 d'un corps qui est factoriel mais pas pleinement factoriel. Montrer que $G[X, Y]$ est un anneau intègre à factorisation unique et un anneau cohérent noethérien fortement discret. Montrer que tout idéal principal de $G[X, Y]$ admet une décomposition primaire. Montrer que $G[X, Y]$ n'est pas un anneau de Lasker-Noether.
3. Soit k un corps discret. Montrer que k est factoriel si, et seulement si, $k[X]$ est un anneau de Lasker-Noether.
4. Soit I un idéal de type fini d'un anneau de Lasker-Noether. Montrer que $\sqrt{I}$ est de type fini et que I contient une puissance de $\sqrt{I}$.

5. Soient R un anneau cohérent noethérien fortement discret et P un idéal premier de type fini de R tel que $P^n = 0$. Montrer que R_P est un anneau de Lasker-Noether avec une série de composition.
6. Soit I un idéal de type fini d'un anneau de Lasker-Noether R, et soit $P \supseteq I$ un idéal premier détachable propre de R. Montrer que P est un idéal premier minimal de I si, et seulement si, il existe un n tel que $(P_P)^n \subseteq I_P$ dans R_P.
7. Soit R un anneau de Lasker-Noether et I un idéal de R formé de diviseurs de zéro. Montrer que $rI = 0$ pour un élément non nul r de I. (Suggestion : utiliser le théorème II.2.3. On devrait pouvoir affaiblir l'hypothèse à être cohérent noethérien, voire seulement noethérien.)

9 Anneaux complètement de Lasker-Noether

La propriété de Lasker-Noether ne passe pas toujours d'un anneau à l'anneau des polynômes : tout corps discret k est un anneau de Lasker-Noether, mais $k[X]$ est un anneau de Lasker-Noether seulement si k est factoriel.

Soit R un anneau tel que $R[X_1, \ldots, X_m]$ est un anneau de Lasker-Noether pour tout m. Soit P un idéal premier de type fini propre de R, et K le corps de fractions de R/P. Soit E un corps, extension algébrique de dimension finie de K. Nous pouvons écrire $E = K[\alpha_1, \ldots, \alpha_n]$ avec α_i entier sur R/P pour chaque i. Alors E est isomorphe au corps de fractions de $R[X_1, \ldots, X_n]/I$, où l'idéal premier I est engendré d'une part par P, et d'autre part, pour chaque i, par le relèvement dans $R[X_1, \ldots, X_i]$ du polynôme minimal de α_i sur $K[\alpha_1, \ldots, \alpha_{i-1}]$. Donc tout corps qui est une extension algébrique de dimension finie de K est factoriel, et K est pleinement factoriel. Cela suggère la définition suivante.

On dit qu'un anneau R est **pleinement Lasker-Noether** si c'est un anneau de Lasker-Noether et si pour chaque idéal premier de type fini P de R, le corps de fractions de R/P est pleinement factoriel. Notez que l'anneau des entiers $\mathbb{Z}$ est pleinement Lasker-Noether, de même que tout corps pleinement factoriel.

Théorème 9.1. *Soit I un idéal de type fini d'un anneau pleinement Lasker-Noether R. Alors R/I est un anneau pleinement Lasker-Noether.*

Démonstration. D'après le théorème 8.2, l'anneau R/I est un anneau de Lasker-Noether. Soit P un idéal premier de type fini de R/I. L'image réciproque P' de P dans R est un idéal premier de type fini de R, donc le corps de fractions de $(R/I)/P \simeq R/P'$ est pleinement factoriel. □

Théorème 9.2. *Si P est un idéal premier détachable d'un anneau pleinement Lasker-Noether R, le localisé R_P est un anneau pleinement Lasker-Noether.*

Démonstration. D'après le théorème 8.1, l'anneau R_P est un anneau de Lasker-Noether. Soit Q un idéal premier de type fini de R_P. L'image réciproque Q' de Q dans R est un idéal premier de type fini d'après le théorème 8.6, donc le corps de fractions de R_P/Q, qui est isomorphe au corps de fractions de R/Q', est pleinement factoriel. □

Si $R[X_1, \dots, X_n]$ est un anneau de Lasker-Noether pour chaque n, R est un anneau pleinement Lasker-Noether. Nous allons démontrer la réciproque.

Lemme 9.3. *Soit S un sous-ensemble multiplicatif d'un anneau commutatif cohérent noethérien R. Si le morphisme $R \to S^{-1}R$ réfléchit les idéaux de type fini, il en va de même pour $R[X] \to S^{-1}R[X]$.*

Démonstration. Comme $R \to S^{-1}R$ réfléchit les idéaux de type fini, le noyau de $R \to S^{-1}R$ est de type fini, donc nous pouvons supposer que $R \subseteq S^{-1}R$. L'anneau $S^{-1}R$ est cohérent et noethérien. Soit I un idéal de type fini de $S^{-1}R[X]$, et soit $R[X]_m = \{ f \in R[X] : \deg f < m \}$. D'après le lemme 1.1, il existe un m tel que $M = I \cap S^{-1}R[X]_m$ est un $S^{-1}R$-module de type fini, et $I \cap S^{-1}R[X]_n = \sum_{i=0}^{n-m} MX^i$ pour chaque $n \geqslant m$. Soit M' le R-module engendré par un système générateur fini du $S^{-1}R$-module M. Alors le module $\tau_S(R[X]_m/M') = (R[X]_m \cap I)/M'$ est de type fini d'après le théorème 6.4, donc le R-module $R[X]_m \cap I = M \cap R[X]$ est de type fini.

Soit J l'idéal de $R[X]$ engendré par $M \cap R[X]$. C'est un idéal de type fini de $R[X]$ contenu dans $I \cap R[X]$. Soit A l'idéal (de type fini) de $S^{-1}R$ formé par les coefficients de X^{m-1} des éléments de M. Comme $R \to S^{-1}R$ réfléchit les idéaux de type fini, $A \cap R$ est de type fini, donc il existe $f_1, \dots, f_k \in M$ dont les coefficients de X^{m-1} engendrent $A \cap R$. On prend un $s \in S$ tel que $sf_i \in R[X]$ pour chaque i. Comme $R[X]$ est cohérent et noethérien, il existe un p tel que $J : s^p = J : s^{p+1}$. Nous allons montrer que l'idéal $I \cap R[X] = J : s^p$, et donc que cet idéal est de type fini.

Supposons que $s^p h \in J$ pour un $h \in R[X]$. Alors $s^p h \in I$, donc $h \in I$, et $h \in I \cap R[X]$. Inversement, supposons que $h \in I \cap R[X]$. Alors $h \in R[X]_n$ pour un n, et nous procédons par récurrence sur n. Si $n \leqslant m$, alors $h \in J \subseteq J : s^p$. Si $n > m$, alors $h = \sum_i r_i f_i X^{n-m} + g$, où $g \in S^{-1}R[X]_{n-1}$ et $r_i \in R$. Donc $sh = \sum_i r_i s f_i X^{n-m} + sg$, et $sg \in I \cap R[X]_{n-1}$. Par récurrence sur n nous avons $sg \in J : s^p$. Ainsi $h \in J : s^{p+1} = J : s^p$. □

Lemme 9.4. *Soit R un anneau pleinement Lasker-Noether et I un idéal propre de type fini de $R[X]$. Soient M un idéal premier minimal au-dessus de $I \cap R$, K le corps de fractions de R/M, et J l'idéal engendré par I dans $K[X]$. Si J est propre, l'image réciproque P de $\sqrt{J}$ dans $R[X]$ est une intersection finie d'idéaux premiers de type fini, et $I : P \neq I$.*

Démonstration. Comme K est un corps factoriel, $\sqrt{J}$ est l'intersection d'un nombre fini d'idéaux premiers principaux de $K[X]$. D'après le lemme 9.3, nous

voyons que l'intersection de chacun de ces idéaux premiers avec $(R/M)[X]$ est de type fini, et donc P est l'intersection d'un nombre fini d'idéaux premiers de type fini.

Pour démontrer que $I : P \neq I$, on considère d'abord le cas spécial où $M \subseteq \sqrt{R \cap I}$ et $K = R/M$. Comme $\sqrt{J}$ est un idéal principal de $K[X]$, il existe un $g \in R[X]$ dont l'image engendre $\sqrt{J}$. Comme $M \subseteq \sqrt{R \cap I}$, il existe un $n \geqslant 1$ tel que $M^n \subseteq I$ et $M^{n-1} \setminus I$ est non vide. On prend un $t \in M^{n-1} \setminus I$ et on note que $tM \subseteq I$. Comme $g \in \sqrt{I + M[X]}$, il existe un $m \in \mathbb{N}$ tel que $tg^m \notin I$ et $tg^{m+1} \in I$. Alors $tg^m \in (I : P) \setminus I$. Notez que nous n'avons pas besoin du lemme 9.3 dans ce cas puisque P est une intersection d'idéaux premiers de la forme $(p) + M[X]$ qui sont clairement de type fini.

Pour traiter le cas général on pose $S = R \setminus M$. Alors $S^{-1}R$ est un anneau de Lasker-Noether, $S^{-1}M$ est le radical de $S^{-1}I \cap S^{-1}R$, et $S^{-1}R/S^{-1}M = K$. L'image réciproque de $\sqrt{J}$ dans $S^{-1}R[X]$ est $S^{-1}P$. Le cas spécial nous donne $S^{-1}I : S^{-1}P \neq S^{-1}I$, donc $I : P \neq I$. □

Lemme 9.5. *Si R est un anneau pleinement Lasker-Noether, alors $R[X]$ est un anneau cohérent noethérien fortement discret tel que pour tout idéal premier de type fini P de $R[X]$, le corps de fractions de $R[X]/P$ est pleinement factoriel.*

Démonstration. D'après le théorème de la base de Hilbert, (théorème 1.5), nous savons que $R[X]$ est un anneau cohérent noethérien fortement discret. L'idéal $P' = P \cap R$ est un idéal premier de type fini de R d'après le théorème 1.2, donc le corps de fractions de R/P' est pleinement factoriel. Le corps de fractions de $R[X]/P \simeq (R/P')[X]/(P/P'[X])$ est une extension de présentation finie d'un corps pleinement factoriel, donc il est pleinement factoriel d'après le théorème 2.6. □

Théorème 9.6. *Si R est un anneau pleinement Lasker-Noether, il en va de même pour $R[X]$.*

Démonstration. D'après le lemme 9.5, il suffit de démontrer que si I est un idéal propre de type fini de $R[X]$, alors il existe un nombre fini d'idéaux premiers de type fini qui contiennent I tels qu'une puissance de l'intersection de ces idéaux premiers est contenue dans I. Comme un certain produit d'idéaux premiers minimaux au-dessus de $R \cap I$ est contenu dans $R \cap I$, il existe un idéal premier minimal M au-dessus de $R \cap I$ tel que $I + M[X] \neq R[X]$. Si K est le corps de fractions de R/M, l'idéal J engendré par l'image de I dans $K[X]$ est propre. D'après le lemme 9.4, l'image réciproque P de $\sqrt{J}$ dans $R[X]$ est une intersection finie d'idéaux premiers de type fini, et $I : P \neq I$. Soit L l'intersection de ces idéaux P lorsque M parcourt les idéaux premiers minimaux de R tels que J est propre. Remplaçons I par $I_2 = I : L \supsetneq I : P \neq I$ et recommençons. Ceci nous fournit une chaine ascendante d'idéaux $I = I_1 \subseteq I_2 \subseteq \cdots$ et des intersections finies d'idéaux premiers de type fini $L = L_1, L_2, \ldots$ telles que

$I_{n+1} = I_n : L_n$, et $I_n \neq I_{n+1}$ sauf si $I_n = R[X]$. Il existe un n tel que $I_n = I_{n+1}$ donc $R[X] = I_n \subseteq I : L_1 L_2 \cdots L_{n-1}$ et par suite $L_1 L_2 \cdots L_{n-1} \subseteq I$. □

Exercices

1. Montrer qu'un corps discret est pleinement factoriel si, et seulement si, c'est un anneau pleinement Lasker-Noether.
2. Montrer que l'anneau des entiers est pleinement Lasker-Noether. Conclure que le corps des nombres rationnels est pleinement factoriel.
3. En considérant les anneaux $\mathbb{Q} \subseteq \mathbb{Q}[X]$, construire un exemple brouwerien d'un anneau pleinement Lasker-Noether qui n'a pas d'idéal maximal de type fini.
4. **Un anneau noethérien désagréable (Nagata)**. Soient k un corps discret et $X_1, X_2, \ldots$ un ensemble dénombrable d'indéterminées. Soit $m_1, m_2, \ldots$ une suite d'entiers strictement positifs avec $0 < m_i - m_{i-1} < m_{i+1} - m_i$ pour tout i. Soit P_i l'idéal (premier) de $K = k[X_1, X_2, \ldots]$ engendré par $\{ X_j : m_i \leqslant j < m_{i+1} \}$, soit S l'ensemble des polynômes sur K qui n'appartiennent à aucun P_i, et soit $R = S^{-1}K$. Montrer les propriétés suivantes.
   (i) K, et donc aussi R, est cohérent.
   (ii) Si I est un idéal de type fini propre non nul de R, l'ensemble $\{ i : I \subseteq S^{-1}P_i \}$ est fini non vide.
   (iii) La localisation R_i de K en P_i est un anneau noethérien.
   (iv) R est un anneau (pleinement) de Lasker-Noether si k est (pleinement) factoriel.
   (v) R contient des chaines arbitrairement longues d'idéaux premiers de type fini.
5. Soit S un sous-ensemble multiplicatif de type fini d'un anneau pleinement Lasker-Noether R. Montrer que $S^{-1}R$ est pleinement Lasker-Noether.
6. Soit K un corps pleinement factoriel. Soient $R = K[X, Y, Z]$ et $I = (X^2 - YZ, Y^2 - XZ)$. Déterminer les idéaux premiers minimaux au-dessus de I.

10 Le théorème de l'idéal principal

La **hauteur** d'un idéal premier de type fini détachable d'un anneau noethérien R est définie comme sa hauteur dans l'ensemble des idéaux premiers de type fini détachables de R, ordonné par inclusion (voir les définitions de la hauteur et de la profondeur page 23).

Théorème 10.1 (théorème de l'idéal principal)**.** *Soient a un élément non inversible d'un anneau de Lasker-Noether R et P un idéal premier de type fini propre minimal au-dessus de (a). Alors P est de hauteur au plus* 1*.*

Démonstration. Soit Q un idéal premier de type fini de R tel que $P \supseteq Q$. Nous allons montrer que Q est égal à P ou qu'il est minimal au-dessus de 0. D'après le lemme 6.8, nous pouvons localiser en P et donc supposer que tout élément de $R \setminus P$ est inversible. Si $a \in Q$, on a $Q = P$ en raison de la minimalité de P ; nous pouvons donc supposer que $a \notin Q$. Nous montrons alors que Q est minimal au-dessus de 0. Considérons la suite décroissante des puissances symboliques $Q^{(1)} \supseteq Q^{(2)} \supseteq \cdots$ de Q. Les idéaux $Q^{(i)} + (a)$ forment une suite décroissante d'idéaux qui contiennent (a). Comme l'idéal $P/(a)$ est un idéal premier minimal de $R/(a)$, l'anneau $R/(a)$ est un anneau de Lasker-Noether avec une série de composition d'après le théorème 8.3. D'après le théorème 6.12, les idéaux $Q^{(i)}$ sont de type fini, donc il y a un n tel que $Q^{(n)} + (a) = Q^{(n+1)} + (a)$. Donc, si $q \in Q^{(n)}$, il existe un $r \in Q^{(n+1)}$ et un $x \in R$ tels que $q = r + xa$. Or $a \notin Q$, alors que $xa = q - r \in Q^{(n)}$, donc $x \in Q^{(n)}$. Donc $Q^{(n)} = Q^{(n+1)} + Q^{(n)}a$. D'après le lemme de Nakayama, on a $Q^{(n)} = Q^{(n+1)}$, donc Q est un idéal premier minimal au-dessus de 0 d'après le théorème 6.11. □

Lemme 10.2. *Soit R un anneau de Lasker-Noether. Soit $P_0 \supset \cdots \supset P_{n-1} \supset P_n$ une suite strictement décroissante d'idéaux premiers de type fini propres et soit $x \in P_0$. Alors il existe des idéaux premiers de type fini $P_1^*, \ldots, P_{n-1}^*$ tels que la suite $P_0 \supset P_1^* \supset \cdots \supset P_{n-1}^* \supset P_n$ est strictement décroissante et $x \in P_{n-1}^*$.*

Démonstration. Il suffit de traiter le cas où $n = 2$, $x \notin P_1$, et $P_2 = 0$. Soit P_1^* un idéal premier minimal au-dessus de (x) qui est contenu dans P_0. Il est clair que P_1^* est non nul. L'idéal premier P_0 a une hauteur au moins égale à 2, tandis que l'idéal premier P_1^* est un idéal premier minimal au-dessus de l'idéal principal (x). Le théorème de l'idéal principal (10.1) nous dit que P_1^* a une hauteur au plus 1. Donc P_0 contient proprement P_1^*. □

Corolaire 10.3. *Soit R un anneau de Lasker-Noether. Soient $P_0 \supset \cdots \supset P_{n-1} \supset P_n$ une suite strictement décroissante d'idéaux premiers de type fini propres et $Q_1, \ldots, Q_m$ des idéaux premiers de type fini propres qui ne contiennent pas P_0. Alors il existe des idéaux premiers de type fini $P_1^*, \ldots, P_{n-1}^*$ avec la suite $P_0 \supset P_1^* \supset \cdots \supset P_{n-1}^* \supset P_n$ strictement décroissante, et tels qu'aucun Q_i ne contient P_{n-1}^*.*

Démonstration. D'après le théorème II.2.3, l'idéal P_0 n'est pas contenu dans la réunion $Q_1 \cup \cdots \cup Q_m$. On prend un $x \in P_0 \setminus (Q_1 \cup \cdots \cup Q_m)$ et on applique le lemme 10.2. □

Théorème 10.4 (théorème de l'idéal principal généralisé)**.** *Soient R un anneau de Lasker-Noether et $I = (a_1, \ldots, a_n)$. Alors tout idéal premier minimal au-dessus de I est de hauteur au plus n.*

Démonstration. Soit P un idéal premier minimal au-dessus de I. Nous procédons par récurrence sur n. Si $n = 0$, alors $I = 0$ et P est un idéal premier minimal de R, donc P est de hauteur 0.

Soit $J = (a_1, \ldots, a_{n-1})$. Si P est un idéal premier minimal au-dessus de J, alors P et de hauteur au plus $n-1$ par hypothèse de récurrence. Il suffit donc de traiter le cas où P n'est contenu dans aucun des idéaux premiers minimaux au-dessus de J.

Il nous faut montrer qu'il ne peut pas exister une suite strictement décroissante $P = P_0 \supset P_1 \supset \cdots \supset P_n \supset P_{n+1}$ d'idéaux premiers de type fini. Si nous avions une telle suite, d'après le corolaire 10.3, nous pourrions construire une suite strictement décroissante d'idéaux premiers de type fini $P = P_0^* \supseteq P_1^* \supseteq \cdots \supseteq P_n^* \supseteq P_{n+1}$ où P_n^* ne serait contenu dans aucun des idéaux premiers minimaux au-dessus de J. L'idéal premier P/J de R/J est un idéal premier minimal au-dessus de l'idéal principal I/J, donc il est de hauteur 1 d'après le théorème de l'idéal principal, (théorème 10.1). L'idéal $(P_n^* + J)/J$ n'est contenu dans aucun idéal premier minimal de R/J, mais $P/J \supseteq (P_n^* + J)/J$. Donc P/J est un idéal premier minimal au-dessus de $(P_n^* + J)/J$. Donc P est un idéal premier minimal au-dessus de $P_n^* + J$, et P/P_n^* est un idéal premier minimal au-dessus de l'idéal $(P_n^* + J)/P_n^*$ de R/P_n^*. Dans l'anneau R/P_n^*, l'idéal $(P_n^* + J)/P_n^*$ est engendré par $n-1$ éléments. Par récurrence P/P_n^* est de hauteur au plus $n-1$. Donc $P_i^*/P_n^* = P_{i+1}^*/P_n^*$ pour un $i < n$, et $P_i^* = P_{i+1}^*$, ce qui est une contradiction. □

Le théorème 10.1 implique qu'un idéal premier principal propre dans un anneau de Lasker-Noether est de hauteur au plus 1. La réciproque n'est pas vraie : un idéal premier de hauteur au plus 1 n'est pas nécessairement principal (exercice 3). On a cependant le résultat suivant.

Théorème 10.5. *Soit P un idéal premier de type fini propre d'un anneau de Lasker-Noether R. Alors il existe un m tel que P est de hauteur m et est un idéal premier minimal au-dessus d'un idéal engendré par m éléments.*

Démonstration. Comme P est minimal au-dessus de P, d'après le théorème 10.4, il existe un n tel que P est de hauteur en plus n. Nous procédons par récurrence sur n. Il y a un nombre fini d'idéaux premiers minimaux $Q_1, \ldots, Q_k$ de R contenus dans P. Si $P = Q_i$ pour un i, alors P est de hauteur 0 et minimal au-dessus de l'idéal 0, qui est engendré par 0 élément. Sinon, nous pouvons trouver pour chaque i un $x_i \in P \setminus Q_i$. Il y a alors un nombre fini d'idéaux premiers minimaux au-dessus de $Q_i + (x_i)$, et si $\hat{Q}$ est l'un d'entre eux, alors $P/\hat{Q}$ est de hauteur au plus $n-1$, donc par récurrence $P/\hat{Q}$ a une hauteur. Soit $m-1$ le maximum des hauteurs des $P/\hat{Q}$ avec $\hat{Q} \subseteq P$ un idéal premier minimal au-dessus d'un $Q_i + (x_i)$. Nous allons montrer que P est de hauteur m.

Clairement P est de hauteur au moins m parce que chaque $\hat{Q}$ est de hauteur au moins 1. Soit $P = P_0 \supset \cdots \supset P_n$ une suite strictement décroissante d'idéaux

premiers de type fini. Alors $P_n \supseteq Q_i$ pour un i. D'après le lemme 10.2, il y a une suite strictement décroissante $P = P_0 \supset P_1^* \supset \cdots \supset P_{n-1}^* \supset P_n$ telle que $x_i \in P_{n-1}^*$. Donc P_{n-1}^* contient l'un les idéaux premiers $\hat{Q}$ minimaux au-dessus de $Q_i + (x_i)$. Donc $n \leqslant m+1$ et P est de hauteur au plus m.

Nous venons de montrer que P a une hauteur bien définie.

Si P est de hauteur m, nous allons montrer que P est un idéal premier minimal au-dessus d'un idéal I engendré par m éléments. Nous procédons par récurrence sur m. Nous pouvons supposer que $m > 0$. Soient $Q_1, \ldots, Q_n$ les idéaux premiers minimaux de R contenus dans P. Comme P contient proprement chaque Q_i, le théorème II.2.3 nous dit qu'il existe un $x \in P \setminus (Q_1 \cup \cdots \cup Q_n)$. Donc $P/(x)$ est de hauteur au plus $m-1$ dans $R/(x)$. Par récurrence il existe un idéal $J \subseteq R$ tel que J est engendré par $m-1$ éléments et $P/(x)$ est un idéal premier minimal au-dessus de $(J+(x))/(x)$. Donc P est un idéal premier minimal au-dessus de $I = J + (x)$. □

Corolaire 10.6. *Tout idéal premier de type fini propre d'un anneau de Lasker-Noether a une hauteur*[1]. □

Exercices

1. Soit R un anneau cohérent noethérien fortement discret. Montrer que tout idéal premier de type fini de R de hauteur 1 est un idéal premier minimal au-dessus d'un idéal principal.
2. Soit R un anneau de Lasker-Noether intègre. Montrer que R est un anneau à factorisation unique si, et seulement si, tout idéal premier de hauteur 1 est principal.
3. Soit $R = \mathbb{Z}[\sqrt{-5}]$, et soit P l'idéal engendré par 2 et $1+\sqrt{-5}$. Montrer que R est un anneau de Lasker-Noether intègre. Montrer que R/P est un corps discret à 2 éléments, donc P est un idéal premier de type fini. Montrer que P est de hauteur 1 mais n'est pas principal.

11 Notes

Une version constructive du théorème de la base de Hilbert a été donnée par Jonathan Tennenbaum dans sa thèse de 1973 sous la direction d'Errett Bishop à l'Université de Californie à San Diego. Tennenbaum a utilisé une *opération* génératrice noethérienne plutôt qu'une *fonction*. C'est l'un des rares exemples où la notion d'opération de A vers B, due à Bishop, ne peut pas être interprétée comme une fonction de A vers l'ensemble des sous-ensembles non vides de B. La forme originale et l'esprit du résultat de Tennenbaum peuvent

1. **NdT.** En particulier un anneau local de Lasker-Noether dont l'idéal maximal est de type fini a une dimension de Krull bien définie.

être retrouvées en ignorant la fonction φ dans la section 3 et en considérant la fonction ρ comme une opération. Les exercices 4.5 et 4.6 sur les anneaux de Tennenbaum constituent une tentative de retrouver la forme du résultat de Tennenbaum sans s'appuyer sur la notion d'opération.

Le théorème de la base de Hilbert pour les anneaux cohérents noethériens fortement discrets a été démontré par Richman (1974) en s'appuyant sur le résultat de Tennenbaum. Seidenberg (1974a) a montré comment se débarrasser de la dépendance par rapport au résultat de Tennenbaum, et en même temps il a démontré que le théorème de la base de Hilbert est également valable pour les anneaux cohérents noethériens (sans référence à la détachabilité des idéaux de type fini). Notez que cet autre théorème de la base de Hilbert n'est ni moins général ni plus général que celui qui s'applique aux anneaux fortement discrets : aussi bien l'hypothèse que la conclusion sont plus faibles.

Le théorème principal sur la décomposition primaire des idéaux dans les anneaux noethériens – à savoir que $R[X]$ est un anneau pleinement Lasker-Noether si R est pleinement Lasker-Noether – a d'abord été démontré par Seidenberg (1984), qui ne peut cependant pas être blâmé pour la terminologie.

L'anneau noethérien désagréable de l'exercice 9.4 provient de [Nagata 1962]. Il fournit un exemple d'un anneau pleinement Lasker-Noether qui n'est pas construit à partir d'un corps discret (ou d'un anneau principal) par ajout d'un nombre fini d'indéterminées puis par passage à un quotient et à une localisation.

IX. Algèbres de dimension finie

Sommaire

1 Représentations

Soit k un corps discret [1]. Une **k-algèbre** est un anneau A, qui est aussi un espace vectoriel sur k, avec $\lambda(ab) = (\lambda a)b = a(\lambda b)$ pour tous $\lambda \in k$ et $a, b \in A$. Si A et B sont des k-algèbres, un **homomorphisme** de A vers B est un homomorphisme d'anneaux qui est aussi une application k-linéaire. Le terme **de dimension finie**, appliqué à une structure S qui est un k-espace vectoriel, comme une k-algèbre, signifie que S est un espace vectoriel de dimension finie sur k.

Si M est un espace vectoriel de dimension n sur k, les applications k-linéaires de M vers M forment une k-algèbre de dimension finie $\mathrm{E}_k(M)$ qui peut être identifiée à l'algèbre des matrices $n \times n$ sur k. Toute k-algèbre de dimension finie A est isomorphe à une sous-algèbre de dimension finie de $\mathrm{E}_k(A)$ en faisant correspondre à tout élément a de A l'application linéaire T_a de A vers A donnée par $T_a(x) = ax$.

Une **représentation** d'une k-algèbre de dimension finie A est donnée par un k-espace vectoriel de dimension finie M et un homomorphisme de k-algèbres $\varphi\colon A \to \mathrm{E}_k(M)$. Si nous laissons tomber la référence explicite à φ et si nous

1. **NdT.** Dans ce chapitre, k désigne toujours un corps discret. Et une k-algèbre de dimension finie est toujours (implicitement) non nulle.

écrivons am pour $\varphi(a)m$, nous avons la notion d'un A-module de dimension finie (sur k). Si le noyau K de la représentation φ est nul, nous disons que φ (ou M) est **fidèle**. Si M est un A-module fidèle, la k-algèbre A peut être identifiée à une sous-algèbre de $\mathrm{E}_k(M)$. Le théorème suivant donne plusieurs constructions importantes qui fournissent des espaces vectoriels de dimension finie.

Théorème 1.1. *Soient A une k-algèbre de dimension finie, M un A-module de dimension finie, I un sous-espace de dimension finie de A, et N un sous-espace de dimension finie de M. Alors on obtient les k-espaces vectoriels de dimension finie suivants.*

(i) *Le sous-espace IN de M engendré par $\{\, ax : a \in I \text{ et } x \in N \,\}$.*

(ii) *La sous-algèbre $k + I + I^2 + I^3 + \cdots$ de A engendrée par I.*

(iii) *Le **centre** de A : $\{\, a \in A : ax = xa \text{ pour tout } x \in A \,\}$.*

(iv) *Le **noyau de la représentation** M : $K = \{\, a \in A : aM = 0 \,\}$.*

(v) *Le **centralisateur** de A/K : $\{\, b \in \mathrm{E}_k(M) : ab = ba \text{ pour tout } a \in A \,\}$.*

Démonstration. Le sous-espace IN est clairement de type fini, donc de dimension finie. Pour chaque n le sous-espace $S_n = I + I^2 + \cdots + I^n$ est de dimension finie, donc nous pouvons trouver un n tel que $S_n = S_{n+1}$, d'où ensuite $S_m = S_n$ pour chaque $m \geqslant n$. Le centre de A est l'intersection des noyaux des applications k-linéaires $f_x \colon A \to A$ données par $f_x(a) = ax - xa$, où x parcourt une base de A. Le noyau K de la représentation M est l'intersection des noyaux des applications k-linéaires $g_m \colon A \to M$ données par $g_m(a) = am$, où m parcourt une base de M. Le centralisateur de A/K est l'intersection des noyaux des applications k-linéaires $h_a \colon \mathrm{E}_k(M) \to \mathrm{E}_k(M)$ données par $h_a(b) = ab - ba$, où a parcourt une base de A. □

D'après le théorème 1.1(iv), nous pouvons décider si M est fidèle ou pas. Dans chaque cas, nous pouvons regarder M comme un module fidèle sur A/K. L'anneau des endomorphismes de M [1] est le centralisateur de l'algèbre A/K vue comme une sous-algèbre de $\mathrm{E}_k(M)$.

Si a et b sont des éléments non nuls d'une k-algèbre de dimension finie A et si $ab = 0$, nous disons que a est un **diviseur de zéro à gauche**, et que b est un **diviseur de zéro à droite**.

Corolaire 1.2. *Soit A une k-algèbre de dimension finie. Tout élément non nul de A est ou bien inversible, ou bien un diviseur de zéro à droite et à gauche.*

Démonstration. Pour $a \in A$, définissons $\rho_a \colon A \to A$ en posant $\rho_a(x) = xa$. D'après le théorème II.6.2, ou bien ρ_a a un noyau non nul, auquel cas a est un diviseur de zéro à droite, ou bien ρ_a est surjective, auquel cas a a un inverse à gauche b. Dans ce dernier cas, ρ_a est aussi injective, on a $ba = 1$ et

1. **NdT.** M vu comme module sur A/K.

$\rho_a(ab) = a = \rho_a(1)$, ce qui implique $ab = 1$, donc a est inversible. Ainsi ou bien a est inversible, ou bien a est un diviseur de zéro à droite. De même, ou bien a est inversible, ou bien a est un diviseur de zéro à gauche. □

Notons que $Aa = A$ si, et seulement si, a est inversible. Donc une algèbre de dimension finie A a un idéal à gauche non trivial de dimension finie si, et seulement si, A contient un diviseur de zéro. Nous ne pouvons pas toujours décider si *tout* élément non nul de A possède un inverse, c'est-à-dire, si A est une **algèbre à division** ou pas.

Exemple 1.3. Soient a une suite binaire et $k = \bigcup_n \mathbb{Q}(ia_n)$. Soit X une indéterminée et A la k-algèbre $k[X]/(X^2+1)$, qui est de dimension 2. On vérifie facilement que A est une algèbre à division exactement lorsque $a_n = 0$ pour tout n. □

Une k-algèbre de dimension finie A est une algèbre à division si, et seulement si, elle ne contient aucun diviseur de zéro. C'est un théorème de mathématiques classiques que tout module sur une algèbre à division est libre. Donc, en mathématiques classiques, ou bien A contient un diviseur de zéro, ou bien tout A-module à gauche de dimension finie sur k est libre. Même si nous ne pouvons pas décider laquelle de ces alternatives est satisfaite, nous pouvons néanmoins, étant donné un A-module M, ou bien construire une base de M sur A, ou bien construire un diviseur de zéro dans A.

Théorème 1.4. *Soit A une k-algèbre de dimension finie, M un A-module de dimension finie sur k, et u un élément non nul de M* [1]*. Ou bien A contient un diviseur de zéro, ou bien M est un A-module libre avec une base qui contient u.*

Démonstration. L'ensemble $\{\, a \in A : au = 0 \,\}$ est un idéal à gauche de A, de dimension finie. S'il est non nul, nous avons terminé d'après le corolaire 1.2, donc supposons que Au est un A-module libre de rang 1. Alors $N = M/Au$ est un A-module de dimension finie plus petite que la dimension de M. Si $N = 0$, alors $\{u\}$ est une base du A-module M. Sinon, par récurrence sur la dimension de M, ou bien A contient un diviseur de zéro, ou bien N est un A-module libre. Dans ce dernier cas, M est un A-module libre avec une base qui contient u. □

Soit K une k-algèbre de dimension finie. De nombreuses constructions qui peuvent être effectuées lorsque K est un anneau à division peuvent être tentées, que K soit un anneau à division ou pas ; le résultat sera la construction souhaitée, ou sinon la construction d'un diviseur de zéro dans K. Le théorème 1.4 est un exemple de cette technique. Un autre exemple est la construction du polynôme minimal.

Soient A une k-algèbre de dimension finie, K une sous-algèbre du centre de A, et $a \in A$. Un polynôme unitaire $f \in K[X]$ est appelé le **polynôme minimal**

1. **NdT.** Si la dimension du k-espace vectoriel M est > 0, un tel u existe toujours.

de a sur K si pour tout $g \in K[X]$ on a $g(a) = 0$ si, et seulement si, f divise g. On vérifie facilement que le polynôme minimal est unique s'il existe, et que dans ce cas $K[a] \simeq K[X]/(f)$.

Théorème 1.5. *Soient A une k-algèbre de dimension finie, K une sous-algèbre de dimension finie du centre de A, et $a \in A$. Alors nous pouvons construire, ou bien un diviseur de zéro dans K, ou bien le polynôme minimal de a sur K.*

Démonstration. Pour $n \in \mathbb{N}$, notons $M_n = K + Ka + \cdots + Ka^n$. On considère l'application K-linéaire $\varphi_n \colon K \to M_n/M_{n-1}$ qui envoie 1 sur a^n, et on prend le plus petit n tel que $\ker \varphi_n \neq 0$: nous pouvons trouver un tel $n \leqslant 1 + \dim A$ parce que nous avons $M_n = M_{n-1}$ à un certain point. Si $\ker \varphi_n \neq K$, alors K contient un diviseur de zéro. Sinon, on voit facilement que $1, a, \ldots, a^{n-1}$ est une base de $M_n = M_{n-1}$ sur K, et si $a^n = c_0 + c_1 a + \cdots + c_{n-1}a^{n-1}$, alors $p(X) = X^n - c_{n-1}X^{n-1} - \cdots - c_1 X - c_0$ est le polynôme minimal de a sur K. □

Exercices

1. Soit A une k-algèbre de dimension finie. Montrer que A est un anneau cohérent noethérien fortement discret.
2. Montrer que l'algèbre A de l'exemple 1.3 est une algèbre à division exactement lorsque $a_n = 0$ pour tout n.
3. Construire un contre-exemple brouwerien pour le théorème qui affirme que si A est une k-algèbre de dimension finie, alors ou bien A contient un diviseur de zéro, ou bien tout A-module est libre.
4. L'**algèbre des quaternions** H sur k est la k-algèbre de dimension 4 avec une base $\{1, i, j, ij\}$ qui satisfait les égalités
$$i^2 = j^2 = -1, \quad ij = -ji.$$
Pour quels corps discrets k l'algèbre H est-elle une algèbre à division ? Pour quels k l'algèbre H contient-elle un diviseur de zéro ?
5. Montrer que si k est algébriquement clos et si A est une k-algèbre de dimension finie, alors ou bien A est une algèbre à division, ou bien A contient un diviseur de zéro.

2 Le théorème de densité

Un module M est dit **réductible**[1] s'il a un sous-module propre non nul – sinon il est dit **simple** (ou **irréductible**). En mathématiques classiques, le

1. **NdT.** Reducible module : pas de traduction dans la littérature mathématique française usuelle.

théorème de densité affirme que si M est un A-module fidèle simple, alors le centralisateur B de A est un anneau à division (lemme de Schur) et A est un anneau dense d'endomorphismes du B-espace vectoriel M. Cette terminologie renvoie à la situation où M est de dimension infinie sur B, et la conclusion est que A est dense au sens que tout ensemble fini B-indépendant $\{x_1, \ldots, x_k\}$ de M peut être envoyé sur n'importe quel sous-ensemble $\{y_1, \ldots, y_k\}$ au moyen de la multiplication par un élément de A.

Dans le cas de la dimension finie, qui est celui que nous allons traiter, nous pouvons conclure que A est l'anneau de tous les B-endomorphismes du module M, c'est-à-dire que A est le centralisateur de B dans $\mathrm{E}_k(M)$. D'un point de vue constructif, le théorème de densité est beaucoup plus utile si nous pouvons l'appliquer à un module qui n'est pas nécessairement simple.

Théorème 2.1 (théorème de densité)**.** *Soit A une k-algèbre de dimension finie d'endomorphismes d'un k-espace vectoriel de dimension finie M, et soit u un élément non nul de M. Notons B le centralisateur de A dans $\mathrm{E}_k(M)$. Alors l'une des propriétés suivantes est satisfaite*[1]*.*

(i) *M contient un sous-A-module non trivial.*

(ii) *M est un B-module libre avec une base qui contient u, et A est le centralisateur de B*[2]*.*

Démonstration. En regardant M comme un B-module, le théorème 1.4 nous dit que, ou bien B contient un diviseur de zéro, ou bien M est un B-module libre avec une base qui contient u. Si l'on a un diviseur de zéro b dans B, bM est un sous-A-module non trivial de M.

Nous supposons maintenant que M est un B-module libre avec une base $u_1, \ldots, u_n$ qui contient u. Pour $j = 0, \ldots, n$ nous posons

$$L_j = \{\, a \in A : au_i = 0 \text{ pour tout } i \leqslant j \,\}.$$

Il est clair que L_j est un idéal à gauche de A, de dimension finie. Nous pouvons supposer que le sous-A-module (de dimension finie) $L_j u_i$ de M est égal à 0 ou à M pour tous j, i[3]. Nous notons

$$M_j = \{\, x \in M : L_j x = 0 \,\}.$$

1. **NdT.** Dans ce théorème, on regarde M comme un A-module à gauche. Si le cas (i) est exclu, c'est-à-dire si M est un A-module simple, le théorème affirme donc que le centralisateur du centralisateur de A est A lui-même. Le théorème de densité à la Richman est donc une forme constructive précise du théorème du bicommutant des mathématiques classiques. Richman nous a prévenu que cette forme constructive est plus utile par la suite que le simple théorème du bicommutant pour les modules simples.

2. **NdT.** Ainsi M, vu comme B-module, est isomorphe à un certain B^n et $A \simeq E_{B^{op}}(B^n)$.

3. **NdT.** Si l'un des $L_j u_i$ est non trivial, nous avons terminé ; il suffit donc de traiter le cas où tous les $L_j u_i$ sont égaux à 0 ou à M. Voici la démarche du reste de la démonstration. L'algèbre A est incluse dans le centralisateur de B et pour montrer qu'elle lui est égale, il suffit de montrer que les u_i peuvent être envoyés sur n'importe quels v_i par un $a \in A$. Posons $L_0 = A$; on a $L_0 u_1 \neq \{0\}$ et donc $L_0 u_1 = M$. Il existe donc $a_1 \in L_0$ tel que $a_1 u_1 = v_1$.

Ce sous-B-module M_j de M contient $\sum_{i=1}^{j} Bu_i$. Nous démontrons ensuite, par récurrence sur j, que

$$M_j = \sum\nolimits_{i=1}^{j} Bu_i.$$

Comme $L_0 = A$, les deux membres sont nuls pour $j = 0$. Supposons l'égalité satisfaite pour un $j < n$. Alors $L_j u_{j+1} = M$ parce que $u_{j+1} \notin M_j$. Soit $x \in M_{j+1}$. Comme $L_{j+1}x = 0$, en posant $b(\ell u_{j+1}) = \ell x$ pour $\ell \in L_j$ nous définissons un élément b de B, avec $L_j(x - bu_{j+1}) = 0$. Donc $x - bu_{j+1} \in M_j = \sum_{i=1}^{j} Bu_i$, donc $x \in \sum_{i=1}^{j+1} Bu_i$.

Pour montrer que A est le centralisateur de B, nous construisons, pour des éléments donnés $v_1, \dots, v_n \in M$, un élément $a \in A$ tel que $au_i = v_i$ $(1 \leqslant i \leqslant n)$. Comme $L_{i-1}u_i = M$, nous pouvons construire par récurrence des $a_i \in L_{i-1}$ tels que

$$a_i u_i = v_i - (a_1 + \cdots + a_{i-1})u_i.$$

On prend alors $a = a_1 + a_2 + \cdots + a_n$. □

Une k-algèbre est dite **simple** [1] si tout idéal bilatère est trivial. Nous utilisons le théorème de densité pour réduire la question de savoir si une algèbre est simple au cas commutatif.

Théorème 2.2. *Soit A une k-algèbre de dimension finie de centre C. L'une des propriétés suivantes est satisfaite.*

— *A possède un idéal non trivial.*

— *On a une bijection entre idéaux I de A et idéaux J de C donnée par*

$$J = I \cap C, \quad I = AJ.$$

Démonstration. Soit R la sous-algèbre (de dimension finie) de $\mathrm{E}_k(A)$ engendrée par les endomorphismes de multiplication à droite et à gauche par des éléments de A. Le centralisateur de R est le centre C de A, et les sous-R-modules de A sont exactement les idéaux de A. D'après le théorème de densité, ou bien A possède un idéal non trivial, ou bien A est un C-module libre avec une base qui contient 1 et R est le centralisateur de C. Dans le second cas, soient I un idéal de A et J un idéal de C. Le fait que $J = (AJ) \cap C$ est une conséquence

Posons $L_1 = \{\, a \in A : au_1 = 0 \,\}$; si on trouve $a_2 \in L_1$ tel que $a_2u_2 = v_2 - a_1u_2$, on aura $(a_1 + a_2)u_i = v_i$ pour $i = 1, 2$. Il suffit d'établir que $L_1u_2 = M$, i.e. $L_1u_2 \neq \{0\}$. Pour cela, posons $M_1 = \{\, x \in M : L_1x = 0 \,\}$ et montrons que $M_1 = Bu_1$, i.e. pour $x \in M_1$ trouvons $b \in B$ tel que $x = bu_1$. Comme cela équivaut à ce que $\ell x = \ell bu_1 = b(\ell u_1)$ pour tout $\ell \in L_0$, il suffit de faire deux constats. (1) Cette équation définit bien une application k-linéaire $b : L_0u_1 = M$; si $\ell u_1 = 0$ alors $\ell \in L_1$ or $x \in M_1$ et donc $\ell x = 0$. (2) En outre b commute avec tout $a \in A$: $b(a(\ell u_1)) = b((a\ell)u_1) = (a\ell)x = a(\ell x) = a(b(\ell u_1))$. Etc.

1. **NdT.** Fred Richman propose de définir un anneau simple comme un anneau dans lequel tout idéal bilatère qui ne contient pas 1 est nul. Selon cette définition, un corps de Heyting est un anneau simple. Lorsque l'anneau est discret, comme dans le cas présent, la définition revient à dire que si un élément est non nul, l'idéal bilatère qu'il engendre contient 1.

immédiate du fait que A est un C-module libre avec une base qui contient 1. Nous devons montrer que $I = (I \cap C)A$. Soit $1 = u_0, \ldots, u_n$ une base de A sur C, et prenons des $r_i \in R$ tels que $r_i u_i = 1$ et $r_i u_j = 0$ si $j \neq i$ [1]. Si $x \in I$, alors $x = \sum c_i u_i$, donc $r_i x = c_i$ et par suite $x \in (I \cap C)A$. □

Nous améliorerons ce théorème dans la section suivante, en remplaçant la condition « A possède un idéal non trivial » par « $\operatorname{rad} A \neq 0$ ».

Exercices

1. *Lemme de Schur.* Soit M un module de dimension finie fidèle irréductible sur une k-algèbre de dimension finie A. Montrer que le centralisateur de A est un anneau à division.
2. *Théorème de Burnside.* Soient M un espace vectoriel de dimension finie sur un corps algébriquement clos k et A une sous-algèbre de $\mathrm{E}_k(M)$. Montrer que, ou bien M contient un sous-A-module non trivial, ou bien $A = \mathrm{E}_k(M)$.
3. Soit A une k-algèbre de dimension finie. Montrer que, ou bien le centre de A est de dimension > 1, ou bien A possède un idéal non trivial, ou bien tout idéal de A est trivial.
4. On se rapporte aux deux premières affirmations dans la démonstration du théorème 2.2. Montrer que le centralisateur de R est le centre C de A.

3 Le radical et les facteurs directs

Soit A une k-algèbre de dimension finie. Un idéal à gauche L de A est **nilpotent** si $L^n = 0$ pour un n. Le **radical** de A est défini par

$$\operatorname{rad} A = \{\, x \in A : Ax \text{ est nilpotent} \,\}.$$

On vérifie facilement que $\operatorname{rad} A$ est un idéal de A. De plus $\operatorname{rad} A$ est détachable dans A, car si L est un idéal à gauche de dimension n, alors L^n est de dimension finie, et $L^n = 0$ si, et seulement si, L est nilpotent [2].

Le théorème de structure de Wedderburn pour les algèbres A de dimension finie telles que $\operatorname{rad} A = 0$ repose sur la construction d'idempotents de A. En mathématiques constructives, nous avons besoin d'une information supplémentaire donnée par un algorithme qui construit un idempotent ou un élément non nul de $\operatorname{rad} A$.

1. **NdT.** L'endomorphisme r_i du C-module A défini sur la base $u_0, \ldots, u_n$ par $u_i \mapsto u_0 = 1$ et $u_j \mapsto 0$ pour $j \neq i$ est dans le centralisateur de C dans $\mathrm{E}_k(A)$, c'est-à-dire dans R.
2. **NdT.** La suite des idéaux L^k est décroissante et devient stationnaire dès que $L^k = L^{k+1}$.

Lemme 3.1. *Soit L un idéal à gauche non nul d'une k-algèbre de dimension finie A. Alors, ou bien L contient un idéal à gauche nilpotent non nul, ou bien il contient un idempotent non nul.*

Démonstration. En considérant $Ax \subseteq L$ nous pouvons supposer que L est de dimension finie et nous procédons par récurrence sur la dimension de L. Si $L^2 = 0$ nous avons trouvé notre idéal à gauche nilpotent non nul ; si $0 \neq L^2 \neq L$, nous avons terminé par récurrence. Nous pouvons donc supposer que $L^2 = L$.

Comme $L^2 = L \neq 0$, nous pouvons trouver un $x \in L$ tel que $Lx \neq 0$. On définit $f\colon L \to L$ en posant $f(y) = yx$. D'après le théorème II.6.2, ou bien $\ker f$ est un idéal à gauche non nul contenu proprement dans L, ou bien f est un isomorphisme. Dans le premier cas nous terminons par récurrence. Voyons le dernier cas. On a $yx = x$ pour un $y \in L$, donc $y^2x = yx = x$ et par suite $(y^2 - y)x = 0$, donc $y = y^2$ est un idempotent non nul dans L. □

Le lemme suivant est un résultat standard reliant idempotents et facteurs directs.

Lemme 3.2. *Soit L un idéal à gauche de dimension finie d'une k-algèbre de dimension finie A. Alors $L = Ae$ pour un idempotent $e \in A$ si, et seulement si, $A = L \oplus K$ pour un idéal à gauche K.*

Démonstration. Si e est un idempotent, $A = Ae \oplus A(1 - e)$. Si $A = L \oplus K$, on écrit $1 = e + f$ avec $e \in L$ et $f \in K$. Pour $x \in L$, on a $x = xe + xf$, donc $xf = 0$ et $x = xe$. Inversement, si $x = xe$, alors $x \in L$. Donc $L = Ae$ et $e^2 = e$. □

Théorème 3.3. *Soit A une k-algèbre de dimension finie et soit L un idéal (à gauche) de A de dimension finie. Alors, ou bien $L \cap \operatorname{rad} A \neq 0$, ou bien $A = L \oplus N$ pour un idéal (à gauche) N.*

Démonstration. Nous pouvons supposer $L \neq 0$. D'après le lemme 3.1, ou bien $L \cap \operatorname{rad} A \neq 0$, ou bien L contient un idempotent non nul et donc, d'après le lemme 3.2, un idéal à gauche non nul K facteur direct de A. Ainsi $A = K \oplus M$ et $L = K \oplus (M \cap L)$. Par récurrence sur $\dim L$, nous pouvons supposer que $M \cap L$ est un facteur direct de A, donc de M, donc $A = K \oplus (M \cap L) \oplus N = L \oplus N$. Si L est un idéal, et $R = \{\, r \in A : Lr = 0 \,\}$, alors $N \subseteq R$. Comme $R \cap L$ est un idéal à droite nilpotent de dimension finie contenu dans l'idéal L, ou bien L contient l'idéal nilpotent non nul $A(R \cap L)$, ou bien $R \cap L = 0$ et donc $N = R$ est un idéal. □

Si A_1 et A_2 sont des k-algèbres, alors $A_1 \times A_2$ est une k-algèbre de manière naturelle, on l'appelle le **produit** de A_1 et A_2. Les algèbres A_1 et A_2 peuvent être identifiées avec les idéaux de $A_1 \times A_2$ engendrés par les idempotents $(1, 0)$ et $(0, 1)$ respectivement. Inversement, si une algèbre A peut être écrite comme somme directe de deux idéaux bilatères L et N comme dans le théorème 3.3,

alors L et N sont des k-algèbres pour elles-mêmes, et A est isomorphe à leur produit.

Si l'idéal L dans le théorème 3.3 est un idéal bilatère, ou bien nous obtenons un élément non nul de $L \cap \operatorname{rad} A$, ou bien A se décompose en un produit de k-algèbres. Cette dernière décomposition sera souvent utilisée dans les démonstrations par récurrence sur la dimension de A. Un exemple est la version suivante, plus forte, du théorème 2.2.

Théorème 3.4. *Soit A une k-algèbre de dimension finie de centre C. L'une des propriétés suivantes est satisfaite.*

— $\operatorname{rad} A \neq 0$.

— *On a une bijection entre idéaux I de A et idéaux J de C donnée par*

$$J = I \cap C, \quad I = AJ.$$

Démonstration. D'après le théorème 2.2, nous pouvons supposer que A possède un idéal non trivial de dimension finie. D'après le théorème 3.3, ou bien $\operatorname{rad} A \neq 0$, ou bien A est un produit d'algèbres, auquel cas nous terminons par récurrence sur la dimension de A. □

Lemme 3.5. *Soit K une k-algèbre commutative de dimension finie avec $\operatorname{rad} K = 0$. Si f est un polynôme séparable dans $K[X]$, alors $\operatorname{rad}(K[X]/(f)) = 0$.*

Démonstration. Si K contient un diviseur de zéro, il existe un idéal non trivial, donc K est un produit d'après le théorème 3.3, et nous terminons par récurrence sur la dimension de K. Nous allons montrer maintenant que si $g \in K[X]$ et f divise g^2, ou bien f divise g, ou bien K contient un diviseur de zéro. L'algorithme d'Euclide nous fournit, ou bien un diviseur de zéro dans K, ou bien un générateur d de l'idéal (f, g). Dans ce dernier cas écrivons $f = da$ et $g = db$. Comme f est séparable, a est séparable et étranger avec d. Comme $f = da$ divise $g^2 = d^2b^2$, ou bien a divise db^2, ou bien K contient un diviseur de zéro. Mais puisque a et d sont étrangers, a divise b^2. Par suite, ou bien K contient un diviseur de zéro, ou bien a divise b par récurrence sur le degré de f. Ainsi f divise g ou K contient un diviseur de zéro. □

Lemme 3.6. *Soit R anneau commutatif, p un nombre premier tel que $pR = 0$ et r un élément de R. Soit q une puissance de p, et f et g des polynômes unitaires de $R[X]$ avec $fg = X^q - r$. Si f et g sont étrangers, alors f ou g est une constante.*

Démonstration. Si $q = 1$, le théorème est clairement vrai. Supposons que $q > 1$. Écrivons $sf + tg = 1$. En différenciant $fg = X^q - r$ nous obtenons $f'g + fg' = 0$. Comme $sf + tg = 1$, nous concluons que f divise f', donc $f' = 0$. De la même manière nous obtenons $g' = 0$. Donc (théorème VI.6.1) nous pouvons écrire $f(X) = f_0(X^p)$ et $g(X) = g_0(X^p)$. Notons $s(X) = \sum_{i=0}^{p-1} X^i s_i(X^p)$ et

$t(X) = \sum_{i=0}^{p-1} X^i t_i(X^p)$. Alors $s_0 f_0 + t_0 g_0 = 1$ et $f_0 g_0 = X^{q/p} - r$, donc nous terminons par récurrence sur q. □

Le lemme suivant généralise le théorème VI.6.6 du cas des corps à celui des algèbres commutatives de dimension finie réduites. En mathématiques classiques, ces dernières sont des produits de corps et la généralisation est immédiate. Comme il peut arriver que nous ne sachions pas écrire l'algèbre comme un produit de corps, la démonstration constructive est plus délicate.

Lemme 3.7. *Soient k un corps discret de caractéristique p, q une puissance de p, K une k-algèbre commutative de dimension finie, et a un élément de K. Si $X^q - a = fg$ avec f et g unitaires et non constants dans $K[X]$, l'une des propriétés suivantes est satisfaite.*

(i) $a \in K^p$.

(ii) $\operatorname{rad} K \neq 0$.

Démonstration. Si nous trouvons un idéal non trivial L de K, alors d'après le théorème 3.3, ou bien $\operatorname{rad} K \neq 0$, ou bien $K = L \oplus N$ pour deux idéaux non triviaux L et N. Dans ce cas, le théorème est satisfait pour L et N par récurrence sur la dimension. Par suite, ou bien $\operatorname{rad} L$ ou $\operatorname{rad} N$ est non nul, ou bien les composantes de a dans L et N sont dans L^p et N^p respectivement, et alors $a \in K^p$.

Nous supposons maintenant que tout élément non nul de K que nous construisons est inversible. Il nous faut écrire $X^q - a$ comme une puissance non triviale. Supposons que $X^q - a = fg^i$ avec f et g des polynômes unitaires de degrés > 0. Soit d le pgcd unitaire de f et g. Si $d = 1$, le lemme 3.6 est en défaut, donc nous pouvons supposer que $\deg d > 0$. Soient f_1 et g_1 les polynômes unitaires qui satisfont $f = f_1 d$ et $g = g_1 d$. Alors $X^q - a = f_1 d (g_1 d)^i = (f_1 g_1^i) d^{i+1}$. Si $f_1 g_1^i = 1$, nous avons écrit $X^q - a$ sous la forme voulue ; sinon nous continuons avec $f_1 g_1^i$ en tant que nouvel f, d en tant que nouveau g et $i+1$ en tant que nouvel i. Après au plus q étapes, nous avons écrit $X^q - a = h(X)^m$ avec un polynôme unitaire $h(X)$ et un entier $m > 0$. Clairement m divise q, donc m est une puissance de p. Par suite $a = (-h(0)^{m/p})^p \in K^p$. □

Lemme 3.8. *Soient k un corps discret de caractéristique p qui satisfait la condition P, K une k-algèbre commutative de dimension finie, $a \in K$, et $L = K[X]/(X^p - a)$. L'une des propriétés suivantes est satisfaite.*

(i) $\operatorname{rad} L \neq 0$.

(ii) $\operatorname{rad} L \neq 0$ *implique* $\operatorname{rad} K \neq 0$.

Démonstration. Soit $e_1, \ldots, e_n$ une base de K sur k. Comme k satisfait la condition P, ou bien les éléments $e_1^p, \ldots, e_n^p$ sont indépendants sur k^p, ou bien ils sont dépendants sur k^p. Si $\sum a_j^p e_j^p = 0$, alors $\sum a_j e_j \in \operatorname{rad} K$, donc nous

pouvons supposer qu'ils sont indépendants, auquel cas l'application naturelle de K vers K^p est un isomorphisme d'anneaux.

Comme k satisfait la condition P, nous pouvons décider si des éléments de K sont linéairement dépendants sur k^p ou pas, donc $K^p[a]$ est une k^p-algèbre de dimension finie. D'après le théorème 1.5, nous pouvons construire, ou bien un diviseur de zéro dans K^p, et donc dans K, ou bien le polynôme minimal de a sur K^p. Dans le premier cas, le lemme 3.1 nous donne, ou bien un idempotent de K, et nous avons terminé par récurrence sur $\dim K$, ou bien un élément non nul de $\operatorname{rad} K$, et la propriété (ii) et satisfaite de manière triviale. Sinon, notons g le polynôme minimal de a sur K^p. Nous pouvons supposer que g est unitaire. Ou bien on a $g = X^p - a^p$, ou bien $X^p - a^p$ se factorise sur K^p. Dans le dernier cas, on a $\operatorname{rad} K \neq 0$ ou $a \in K^p$ d'après le lemme 3.7, donc $\operatorname{rad} L \neq 0$ et la propriété (i) est satisfaite. Si $X^p - a^p$ est le polynôme minimal de a sur K^p, alors $K^p[a]$ est isomorphe à $K^p[X]/(X^p - a^p)$ qui est isomorphe, en tant qu'anneau, à L. Puisque $K^p[a] \subseteq K$, nous obtenons la propriété (ii). □

Exercices

1. Soit L un idéal à gauche de dimension n d'une k-algèbre de dimension finie. Montrer que L^n est de dimension finie, et que L est nilpotent si, et seulement si, $L^n = 0$.
2. Montrer que le radical d'une k-algèbre de dimension finie A est le radical de Jacobson de A. Montrer que $\operatorname{rad}(A_1 \times A_2) = \operatorname{rad} A_1 \times \operatorname{rad} A_2$.
3. Soit A une k-algèbre de dimension finie avec un radical J de dimension finie. Le **socle à gauche** de A est l'ensemble $\{ x \in A : Jx = 0 \}$. Montrer que le socle à gauche est un idéal bilatère qui a une intersection non nulle avec tout idéal à gauche non nul. Identifier le radical, et les socles à droite et à gauche, de l'algèbre des matrices triangulaires inférieures $n \times n$ sur un corps discret.
4. Montrer que les quatre propriétés suivantes pour une k-algèbre de dimension finie A sont équivalentes.
   (i) $\operatorname{rad} A = 0$.
   (ii) Tout idéal à gauche de dimension finie de A est un facteur direct.
   (iii) Tout sous-module de dimension finie d'un A-module de dimension finie est un facteur direct.
   (iv) Tout A-module de dimension finie est projectif.
5. *Théorème de Maschke.* Soient G un groupe fini, k un corps discret tel que l'entier $n = \#G$ n'est pas nul dans k, et A l'algèbre du groupe G sur k. Soit M un A-module de dimension finie et $\varphi\colon M \to M$ une application k-linéaire telle que $\varphi^2 = \varphi$ et $\varphi(M)$ est un A-module à gauche. Soit $\psi(x) = \frac{1}{n} \sum_{g \in G} g\varphi(g^{-1}x)$. Montrer que ψ est un homomorphisme

de A-modules, $\psi^2 = \psi$, et $\varphi(M) = M$. Conclure que $\operatorname{rad} A = 0$ (voir l'exercice 4).

4 Théorème de Wedderburn, première partie

Pour démontrer le théorème de Wedderburn concernant les algèbres de dimension finie et de radical nul, nous devons faire des hypothèses supplémentaires sur le corps k.

Lemme 4.1. *Soit A une k-algèbre de dimension finie et $K \neq A$ une sous-algèbre de dimension finie du centre de A. L'une des propriétés suivantes est satisfaite.*

- *K possède un idempotent non trivial.*
- *K possède un nilpotent non trivial.*
- *Il existe un $x \in A \setminus K$ qui possède un polynôme minimal g sur K, et ce polynôme est de l'une des formes suivantes :*
  - *g est séparable,*
  - *$g(X) = X^p - r$ avec p la caractéristique de k,*
  - *$g(X) = X^m$.*

Démonstration. Nous pouvons supposer que $A = K[a]$ et nous construisons, d'après le théorème 1.5, ou bien un diviseur de zéro dans K, ou bien le polynôme minimal $g(X)$ de a sur K. Si K contient un diviseur de zéro, alors K contient un idempotent non trivial ou un nilpotent non trivial d'après le lemme 3.1. D'après le théorème VI.6.3, ou bien K contient un idéal non trivial, ou bien nous pouvons factoriser g en un produit de polynômes deux à deux étrangers de la forme $f^m(X^q)$ où m est un entier strictement positif, q est égal à 1 ou à une puissance de la caractéristique finie p de k, et f est séparable. Ceci donne une décomposition de A en un produit d'algèbres de la forme $K[X]/f^m(X^q)$, donc nous pouvons supposer que $g(X) = f^m(X^q)$. Si $a^q \in K$, alors $g(X) = X^q - r$. Si $q = p$, nous avons terminé ; sinon $a^p \notin K$ alors que $(a^p)^{q/p} \in K$, donc $K[a^p]$ est une sous-algèbre non triviale de A et nous avons terminé par récurrence sur $\dim A$. Si $a^q \notin K$ et $m = 1$, alors f est le polynôme minimal de a^q sur K et il est séparable. Si $a^q \notin K$ et $m > 1$, alors le polynôme minimal de $f(a^q)$ sur K est X^m. □

Théorème 4.2. *Un corps discret k est séparablement factoriel si, et seulement si, toute k-algèbre de dimension finie A de radical nul est simple ou possède un idéal non trivial.*

Démonstration. D'après le théorème 2.2, nous pouvons restreindre notre attention aux k-algèbres commutatives. Soit A une k-algèbre commutative de dimension finie. Si $A = k$ nous avons terminé ; sinon nous pouvons trouver un $a \in A \setminus k$ avec un polynôme minimal g.

Supposons d'abord que k est séparablement factoriel et que $\operatorname{rad} A = 0$. Alors g ne peut pas être de la forme X^m. Si $g(X) = X^p - r$, g est irréductible d'après le théorème VI.6.6, à moins que $r \in k^p$, auquel cas $\operatorname{rad} A \neq 0$. Si g est irréductible, nous pouvons remplacer k par $k[X]/(g)$ et nous terminons par récurrence sur $\dim A$. Donc, d'après le lemme 4.1, nous pouvons supposer que g est séparable. On décompose g en produit de polynômes irréductibles. Si a annule l'un des facteurs, alors $k(a)$ est un corps et, comme A est commutatif, A est une $k(a)$-algèbre de dimension finie. Alors, comme $k(a)$ est aussi séparablement factoriel, nous avons terminé par récurrence sur $\dim A$. Si a n'annule aucun des facteurs f de g, alors chaque $f(a)$ engendre un idéal non trivial de A.

Voyons l'implication réciproque. Soient K un corps, extension de dimension finie de k et $f \in K[X]$ un polynôme séparable. Nous considérons la k-algèbre commutative de dimension finie $A = K[X]/(f)$. D'après le lemme 3.5, on a $\operatorname{rad} A = 0$. Les idéaux de type fini de A sont en correspondance bijective avec les diviseurs unitaires de f, donc f est irréductible ou possède une factorisation non triviale. □

Nous caractérisons maintenant les corps séparablement factoriels en termes de décomposition d'une algèbre en produit d'algèbres simples. Ceci constitue la première partie du théorème de Wedderburn [1].

Théorème 4.3 (théorème de Wedderburn, première partie)**.** *Un corps discret k est séparablement factoriel si, et seulement si, toute k-algèbre de dimension finie de radical nul est un produit d'algèbres simples.*

Démonstration. Soit A une k-algèbre de dimension finie. D'après le théorème 4.2, A est simple ou contient un idéal non trivial L. Dans le premier cas nous avons terminé. Dans l'autre cas nous appliquons le théorème 3.3 et nous écrivons A comme un produit non trivial d'algèbres, et nous terminons par récurrence sur la dimension de A.

Inversement, si toute algèbre A de radical nul est un produit d'algèbres simples, alors A ou bien est simple, ou bien contient un idéal non trivial, donc k est séparablement factoriel d'après le théorème 4.2. □

Théorème 4.4. *Un corps discret k satisfait la condition P si, et seulement si, toute k-algèbre de dimension finie a un radical de dimension finie.*

Démonstration. Supposons que k satisfait la condition P. Si nous construisons un élément non nul a de $\operatorname{rad} A$, alors en passant à $A/(AaA)$ nous avons terminé par récurrence sur $\dim A$. Notons C le centre de A. D'après le théorème 3.4, ou bien $\operatorname{rad} A \neq 0$, ou bien $\operatorname{rad} A = A \cdot \operatorname{rad} C$. Donc nous sommes ramenés à traiter le cas où A est commutative. Si nous construisons un idempotent non

1. **NdT.** En mathématiques classiques, tout corps est séparablement factoriel, et l'énoncé est beaucoup plus pauvre.

trivial de A, alors nous pouvons écrire A comme un produit de deux algèbres de dimensions plus petites et nous avons terminé par récurrence sur $\dim A$. Soit K une sous-k-algèbre de dimension finie de A avec $\operatorname{rad} K = 0$. Nous commençons en prenant $K = k$, et nous procédons par récurrence sur $\dim A - \dim K$.

Ou bien $K = A$, auquel cas nous avons terminé, ou bien nous pouvons appliquer le lemme 4.1 pour construire un élément $a \in A \setminus K$ avec un polynôme minimal g. Ou bien g est séparable, ou bien g s'écrit $g(X) = X^p - r$ avec p la caractéristique de k, ou bien $g(X) = X^m$. Si $g(X) = X^m$, a est un élément non nul de $\operatorname{rad} A$. Si $g(X) = X^p - r$, alors, comme k satisfait la condition P, le lemme 3.8 nous dit que, ou bien $\operatorname{rad} K[a] \neq 0$, ou bien $\operatorname{rad} K[a] = 0$. Dans le dernier cas, nous remplaçons K par $K[a]$ et nous avons terminé par récurrence sur $\dim A - \dim K$. Si g est séparable, alors $\operatorname{rad} K[a] = 0$ d'après le lemme 3.5, et nous remplaçons K par $K[a]$ comme précédemment.

Voyons l'implication réciproque. Nous allons démontrer la propriété caractéristique (ii) dans le théorème VII.3.1. Soient K un corps, extension de dimension finie de k, et $a \in K$. Considérons la k-algèbre $L = K[X]/(X^p - a) = K[x]$. Si $\operatorname{rad} L = 0$, $a \notin K^p$ car si $a = r^p$, $x - r$ est un élément non nul de $\operatorname{rad} L$. Si $\operatorname{rad} L \neq 0$, il existe un polynôme $f \in K[X]$ tel que $X^p - a$ divise f^2 mais ne divise pas f. Dans ce cas, le pgcd de $X^p - a$ et f est un diviseur propre de $X^p - a$, et $a \in K^p$ d'après le théorème VI.6.6. □

Corolaire 4.5. *Un corps discret k est pleinement factoriel si, et seulement si, toute k-algèbre de dimension finie contient un idéal nilpotent de dimension finie I tel que A/I est un produit de k-algèbres simples.*

Démonstration. Un corps discret k est pleinement factoriel si, et seulement si, il est séparablement factoriel et satisfait la condition P. Le résultat est donc une conséquence directe des théorèmes 4.3 et 4.4. □

Exercices

1. Soit K une k-algèbre commutative de dimension finie et $g \in K[X]$. Supposons que $g = f_1 f_2 \cdots f_n$ avec les f_i deux à deux étrangers. Montrer que $K[X]/(g)$ est isomorphe au produit des k-algèbres $K[X]/(f_i)$.

2. Soit k un corps factoriel et $f \in k[X]$. Identifier le radical I de $A = k[X]/(f)$, et décrire A/I comme un produit de k-algèbres simples.

3. Soient G le groupe symétrique sur $\{1, 2, 3\}$ et A l'algèbre du groupe G sur $\mathbb{Q}$. Décomposer A en un produit de $\mathbb{Q}$-algèbres simples (voir l'exercice 3.5).

5 Anneaux de matrices et algèbres à division

La seconde partie du **théorème de structure de Wedderburn** pour les algèbres semi-simples dit qu'une algèbre simple de dimension finie est isomorphe à un anneau de matrices carrées sur une algèbre à division [1]. Ce théorème repose sur la capacité de construire des idéaux à gauche non triviaux. Lorsque nous avons un idéal à gauche non trivial, nous pouvons l'utiliser pour décomposer l'algèbre de départ.

Théorème 5.1 (théorème de structure de Wedderburn)**.** *Soit A une k-algèbre de dimension finie qui contient un idéal à gauche non trivial. L'une des propriétés suivantes est satisfaite.*

(i) *Le radical de A est non nul.*

(ii) *A est un produit de k-algèbres de dimension finie (de dimensions plus petites que A).*

(iii) *Il existe un entier $n > 1$ tel que A est isomorphe à l'anneau des matrices carrées $n \times n$ sur une k-algèbre de dimension inférieure à celle de A.*

Démonstration. Soit L l'idéal à gauche non trivial dans l'hypothèse. En considérant l'idéal à gauche engendré par un élément non nul de L, nous pouvons supposer que L est de dimension finie. Si L n'est pas un A-module fidèle, le noyau de la représentation L est un idéal non nul de A ; donc d'après le théorème 3.3 [2], ou bien $\operatorname{rad} A \neq 0$, ou bien A est un produit.

Supposons maintenant que L est fidèle. L'algèbre A peut être vue comme une sous-k-algèbre de $\mathrm{E}_k(L)$. Soit B le centralisateur de A sur L (i.e. l'anneau $\mathrm{E}_A(L)$). D'après le théorème de densité, (théorème 2.1), ou bien L est réductible (et nous terminons par récurrence sur la dimension de L), ou bien A est isomorphe à un anneau complet de matrices à coefficients dans l'anneau opposé à B. Il reste à montrer que la dimension de B est inférieure à celle de A [3]. D'après le théorème 3.3, ou bien $\operatorname{rad} A \neq 0$, ou bien L est un facteur direct de A. Dans ce dernier cas, l'algèbre B est une sous-algèbre propre du centralisateur de A sur A, qui est l'anneau opposé à A. □

Le problème fondamental et de savoir reconnaitre si une k-algèbre de dimension finie est une algèbre à division ou pas, à savoir, être capable d'affirmer que c'est une algèbre à division ou alors de construire un idéal à gauche non trivial. Si nous sommes capables de faire cela, alors le théorème 5.1 implique que toute

1. **NdT.** Voir le commentaire après le théorème 5.1, qui explique pourquoi ce théorème est une version constructive du théorème de structure de Wedderburn des mathématiques classiques.

2. **NdT.** Le noyau est un idéal bilatère, on se reporte alors au commentaire qui suit le théorème 3.3.

3. **NdT.** À moins que l'on ne se retrouve dans le cas (i).

k-algèbre de dimension finie a un radical de dimension finie, et que modulo ce radical elle est un produit d'anneaux de matrices carrées $n \times n$ sur des algèbres à division. Cette condition est équivalente à la capacité de reconnaitre si une représentation de dimension finie arbitraire d'une k-algèbre de dimension finie est réductible.

Théorème 5.2. *Les propriétés suivantes pour un corps discret k sont équivalentes.*

(i) *Toute k-algèbre de dimension finie est une algèbre à division ou sinon contient un idéal à gauche non trivial.*

(ii) *Tout k-module à gauche de dimension finie M sur une k-algèbre de dimension finie A est réductible ou irréductible.*

(iii) *Toute k-algèbre de dimension finie A a un radical de dimension finie, et $A/\operatorname{rad} A$ est un produit d'anneaux complets de matrices sur des algèbres à division.*

Démonstration. Clairement les points (ii) et (iii) impliquent chacun le point (i).

Montrons que (i) implique (ii). Nous pouvons supposer que M est un A-module fidèle. Soit B le centralisateur de A sur M. Si B contient un diviseur de zéro b, bM est un sous-A-module non trivial de M. Si B est une algèbre à division, alors d'après le théorème de densité, ou bien M est réductible, ou bien A est le centralisateur de B, et M est irréductible.

Montrons que (i) implique (iii). Si A est une algèbre à division, nous avons terminé. Si A contient un idéal à gauche non trivial, alors d'après le théorème 5.1, ou bien A contient un idéal nilpotent non nul de dimension finie I, auquel cas nous passons à A/I et nous terminons par récurrence sur $\dim A$, ou bien A est un produit de k-algèbres de dimension finie et nous terminons par récurrence sur $\dim A$, ou bien A est isomorphe à un anneau complet de matrices et nous terminons par récurrence sur $\dim A$. □

Pour quels corps k les conditions du théorème 5.2 sont-elles satisfaites ? Les corps finis et les corps algébriquement clos fournissent des exemples faciles. Le corps des nombres réels algébriques $\mathbb{R}^a$ admet seulement trois algèbres à division, et une démonstration constructive de cette assertion montre que ce corps satisfait les conditions du théorème 5.2.

Théorème 5.3. *Soient k un sous-corps discret du corps des nombres réels $\mathbb{R}$, algébriquement clos dans $\mathbb{R}$, $H = k(i, j)$ l'algèbre des quaternions sur k, et A une k-algèbre de dimension finie. Ou bien A contient un diviseur de zéro, ou bien A est isomorphe à l'une des algèbres k, $k(i)$, ou H.*

Démonstration. Si $A = k$, nous avons terminé ; sinon en considérant un $\alpha \in A \backslash k$, comme A est de dimension finie, nous pouvons construire un polynôme non trivial annulé par α. Le corps $k(i) \subseteq \mathbb{C}$ est discret et algébriquement clos, donc

k est factoriel, et tout polynôme irréductible sur k est de degré au plus 2. Donc, ou bien A contient un diviseur de zéro, ou bien α est de degré 2. Nous pouvons donc supposer que $\alpha \in k(i)$ avec $i \in A$ et $i^2 = -1$. Le centralisateur de i dans A est une algèbre de dimension finie sur le corps algébriquement clos $k(i)$, donc il contient un diviseur de zéro ou est égal à $k(i)$. Nous traitons le deuxième cas. Si $A = k(i)$ nous avons terminé. Sinon nous pourrons construire un $\beta \in A \setminus k(i)$ tel que $\beta^2 = -1$ exactement comme nous avons construit $i \in A$. Comme $i\beta + \beta i$ commute avec i et β, nous pouvons supposer que $i\beta + \beta i \in k(i) \cap k(\beta) = k$. On pose $i\beta + \beta i = r \in k$ et $j = \beta + ri/2$. Alors $ij + ji = 0$ et $j^2 \in k$. Si $j^2 = s^2$ pour un $s \in k$, alors $j - s$ est un diviseur de zéro non nul dans A. Sinon $j^2 < 0$ et nous pouvons normaliser j pour avoir $j^2 = -1$. Si j' est un autre tel élément j, alors jj' commute avec i, donc $jj' \in k(i)$ et par suite $j' \in k(i, j)$. □

Est-ce que le corps $\mathbb{Q}$ des nombres rationnels satisfait les conditions du théorème 5.2 ? Nous n'allons certainement pas produire un contre-exemple brouwerien avec $k = \mathbb{Q}$. Une analyse détaillée de la théorie classique des algèbres à division sur $\mathbb{Q}$, en analogie avec le théorème 5.3, donnera probablement une démonstration.

Exercice

1. Soit k un corps pleinement factoriel et A une k-algèbre commutative de dimension finie. Alors, ou bien A est un corps discret, ou bien A contient un idéal non trivial. Soit k un corps factoriel et A une k-algèbre qui a pour dimension un nombre premier. Alors, ou bien A est une algèbre à division, ou bien A contient un idéal à gauche non trivial.

6 Notes

La majeure partie du matériau contenu dans ce chapitre est parue dans [Richman 1982]. Il serait intéressant de voir comment la théorie peut être développée pour les anneaux qui possèdent une série de composition (les anneaux artiniens). Les algèbres de Frobenius, les anneaux quasi-Frobenius [1] et les algèbres de Lie constituent également des sujets de recherche intéressants.

1. **NdT.** Voir par exemple `https://fr.wikipedia.org/wiki/Algèbre_de_Frobenius` et `https://fr.wikipedia.org/wiki/Anneau_quasi-Frobenius`.

X. Groupes libres

Sommaire

1 Existence et unicité

Un groupe F est un **groupe libre** sur un sous-ensemble S de F si pour tout groupe H et toute fonction f de S vers H, il y a un unique homomorphisme de F vers H qui prolonge f. Si F est un groupe libre sur S, S est appelé un **système générateur libre** [1] ou une **base (libre)** de F. Avant de montrer comment construire les groupes libres nous démontrons qu'il y a, à un isomorphisme unique près, un unique groupe libre sur un ensemble donné.

Théorème 1.1. *Soient F_1 et F_2 deux groupes libres sur des ensembles S_1 et S_2. Si f est une bijection de S_1 sur S_2, il y a un unique isomorphisme de F_1 vers F_2 qui prolonge f.*

Démonstration. Soit g la bijection réciproque de f. Comme F_1 est un groupe libre sur S_1, il y a un unique homomorphisme f_* de F_1 vers F_2 qui prolonge f. De la même manière il y a un unique homomorphisme g_* de F_2 vers F_1 qui prolonge g. L'homomorphisme f_*g_* de F_2 vers F_2 prolonge l'application identique de S_2. Comme F_2 est un groupe libre sur S_2, et comme l'application identique sur F_2 prolonge également l'application identique sur S_2, l'homomorphisme identique sur F_2 est égal à f_*g_*. De la même manière g_*f_* est l'homomorphisme identique

1. **NdT.** (Free) basis.

sur F_1. Donc f_* est l'isomorphisme demandé ; f_* est unique parce que F_1 est libre sur S_1. □

Pour construire un groupe libre sur un ensemble arbitraire S, on définit d'abord l'ensemble $S \cup S^{-1}$ comme $S \times \{1, -1\}$, en identifiant S avec $S \times \{1\}$, et $(s, -\varepsilon)$ est noté $(s, \varepsilon)^{-1}$. Soit $F(S)$ le monoïde libre sur $S \cup S^{-1}$. Nous définissons deux égalités sur $F(S)$. La première, notée par le symbole « $\equiv$ », est l'égalité usuelle sur un monoïde libre. Pour définir la seconde égalité, nous prenons au sérieux la notation x^{-1} : on dit que deux mots dans $F(S)$ sont **adjacents** si l'un peut être écrit sous la forme vw et l'autre sous la forme $vxx^{-1}w$ avec v et $w \in F(S)$, et $x \in S \cup S^{-1}$. Deux mots v et w sont **égaux** dans $F(S)$, ce que l'on écrit $v = w$, s'il existe une suite de mots $v \equiv w_1, w_2, \ldots, w_n \equiv w$, tels que w_i est adjacent à w_{i+1} pour chaque $i < n$.

Nous devons d'abord montrer que l'application naturelle de S dans $F(S)$ fait de S un sous-ensemble de $F(S)$: i.e. si s et $s' \in S$ et $s = s'$ comme éléments de $F(S)$, alors $s = s'$ comme éléments de S. À cette fin, et aussi pour son utilité générale, nous allons établir la **propriété de Church-Rosser** pour $F(S)$. Si $x_i \in S \cup S^{-1}$ pour $i = 1, \ldots, n$, la **longueur** de $z \equiv x_1 x_2 \cdots x_n$ est définie comme $\ell(z) = n$. La longueur est une fonction sur $F(S)$ par rapport à « $\equiv$ » mais pas par rapport à « $=$ », par exemple les mots x et $xx^{-1}x$ sont égaux mais leurs longueurs sont respectivement égales à 1 et 3.

Théorème 1.2 (la propriété de Church-Rosser)**.** *Soient u et v des mots égaux dans $F(S)$. Nous pouvons trouver un entier n et une chaine $u \equiv w_1, \ldots, w_n \equiv v$ de mots adjacents telle que si $\ell(w_{i-1}) < \ell(w_i)$ pour un $i < n$, alors $\ell(w_i) < \ell(w_{i+1})$.*

Démonstration. Comme $u = v$, on a une suite de mots adjacents $u \equiv w_1, \ldots, w_n \equiv v$. Nous allons démontrer le résultat par récurrence sur la longueur totale $N = \sum \ell(w_i)$ de la suite. Nous pouvons supposer que $n > 1$. Si pour un i nous avons $\ell(w_{i-1}) < \ell(w_i)$ et $\ell(w_i) > \ell(w_{i+1})$, alors w_{i-1} est obtenu à partir de w_i en supprimant un morceau xx^{-1}, et w_{i+1} est obtenu à partir de w_i en supprimant un morceau yy^{-1}. Si ces deux morceaux coïncident, w_i et w_{i+1} peuvent être omis dans la suite et nous terminons par récurrence. Si ces deux morceaux se superposent sans coïncider, w_i contient un morceau $zz^{-1}z$ et w_{i-1} et w_{i+1} sont tous les deux obtenus en remplaçant ce morceau par z, donc $w_{i-1} \equiv w_{i+1}$ une fois de plus, et w_i et w_{i+1} peuvent être omis. Dans le cas restant, où les deux morceaux sont disjoints, nous pouvons supprimer les deux morceaux de w_i pour obtenir une nouvelle suite de longueur totale $N - 4$ et nous terminons par récurrence. □

C'est une conséquence facile du théorème 1.2 que S est un sous-ensemble de $F(S)$.

La multiplication (associative) sur $F(S)$ respecte l'égalité « = » ; i.e. si $v = v'$ et $w = w'$, alors $vw = v'w'$. Si $v \equiv x_1 x_2 \cdots x_n$, on pose $v^{-1} \equiv x_n^{-1} \cdots x_2^{-1} x_1^{-1}$. Alors $vv^{-1} = v^{-1}v = 1$, où 1 est le mot vide. Donc $F(S)$ est un groupe.

Pour montrer que $F(S)$ est un groupe libre sur S, on considère une fonction f de S vers un groupe H. Si $\bar{f}$ est un homomorphisme de $F(S)$ vers H qui prolonge f, alors $\bar{f}(x_1 \cdots x_n)$ doit être égal à $f(x_1) \cdots f(x_n)$, donc $\bar{f}$ est unique. De plus, en posant $\bar{f}(x_1 \cdots x_n) = f(x_1) \cdots f(x_n)$ on définit un homomorphisme parce que $\bar{f}(w) = \bar{f}(w')$ si $w = w'$. Donc $F(S)$ est un groupe libre sur S, auquel nous nous référons comme **le groupe libre sur** S. Nous résumons la discussion précédente comme suit.

Théorème 1.3. *Pour un ensemble S, $F(S)$ est un groupe libre sur S.* □

Un mot $w \equiv x_1 x_2 \cdots x_n \in F(S)$, avec les $x_i \in S \cup S^{-1}$, est dit **réductible** si $x_i x_{i+1} = 1$ pour un $i = 1, \ldots, n-1$. Si w n'est pas réductible, nous disons que w est **réduit**. Notez que si u et $v \in F(S)$ et si uv est réduit, alors u et v sont réduits. Si S est un ensemble discret et si u et v sont des mots réduits de $F(S)$, alors, ou bien uv est réduit, ou bien $u \equiv ax$ et $v \equiv x^{-1}b$ pour un $x \in F(S)$ avec ab reduit.

Si $w = w'$ et si w' est réduit, alors w' est appelé la **forme réduite** de w ; la propriété de Church-Rosser de $F(S)$ implique que si $w = w'$ et si w et w' sont tous les deux réduits, alors $w \equiv w'$, donc la forme réduite est unique [1]. Si S est discret, tout élément de $F(S)$ a une forme réduite unique. Ceci nous donne le résultat suivant.

Théorème 1.4. *Si S est un ensemble discret, $F(S)$ est un groupe discret.* □

Théorème 1.5. *Si $w \in F(S)$ et $w^n = v$ avec $\ell(v) \leqslant \ell(w)$ pour un $n > 1$, alors $w = 1$ ou w est réductible. En particulier, un groupe libre est sans torsion ; i.e. si $w^n = 1$ pour un $n > 0$, alors $w = 1$.*

Démonstration. Écrivons $w \equiv u^{-1} w_1 u$ (par exemple : $u \equiv 1$ et $w_1 \equiv w$) et raisonnons par récurrence sur $\ell(w_1)$. Si $w^n = v$ avec $\ell(v) \leqslant \ell(w)$ pour un $n > 1$, alors d'après le théorème 1.2, ou bien $\ell(u^{-1} w_1^n u) \leqslant \ell(v)$, ou bien w est réductible, ou bien $w_1 \equiv x^{-1} w_2 x$ pour un $x \in S \cup S^{-1}$. Dans le premier cas $w_1 \equiv 1$ donc $w = 1$, dans le second nous avons terminé, et dans le troisième nous terminons par récurrence sur $\ell(w_1)$. □

Théorème 1.6. *Soient F et F' des groupes libres sur des ensembles finis S et S'. Alors F et F' sont isomorphes si, et seulement si, $\#S = \#S'$.*

1. **NdT.** En mathématiques classiques, on a l'habitude d'identifier $(F(S), =)$ avec l'ensemble des mots réduits, muni de la relation $\equiv$. La situation est à priori plus compliquée constructivement lorsque S n'est pas discret. Néanmoins, la théorie développée ici pour le cas général, en munissant $F(S)$ des deux relations $\equiv$ et $=$, s'avère conceptuellement plus simple que celle dans les exposés de mathématiques classiques, basés sur les mots réduits.

Démonstration. Si $\#S = \#S'$, alors F et F' sont isomorphes d'après le théorème 1.1. Pour la réciproque nous devons montrer comment retrouver le nombre d'éléments $\#S$ à partir (de la structure) du groupe F. Soit N le sous-groupe de F engendré par les éléments v^2 pour $v \in F$. Clairement N est un sous-groupe normal. Le groupe quotient F/N est abélien : le carré de tout élément est égal à 1, donc $xyx^{-1}y^{-1} = xyxy = 1$. Nous montrons maintenant que F/N est un ensemble fini à $2^{\#S}$ éléments.

Si $w \equiv x_1 x_2 \cdots x_n \in F$ et $s \in S$, notons $\nu_s(w)$ le nombre des indices i tels que $x_i = s$ ou $x_i = s^{-1}$. Si $w = w'$, $\nu_s(w)$ est congruent à $\nu_s(w')$ modulo 2. On note

$$D = \{\, w \in F : \nu_s(w) \text{ est pair pour chaque } s \in S \,\}.$$

Clairement $N \subseteq D$ et D est un sous-ensemble détachable de F. Inversement, comme le groupe F/N est abélien, et comme le carré de tout élément de F/N est égal à 1, nous obtenons $D \subseteq N$, et tout élément de F/N peut être écrit de manière unique comme un produit d'éléments distincts de S. □

Lorsque S est un ensemble fini, le nombre entier $\#S$ est un invariant de tout groupe F libre sur S, appelé le **rang** de F. Si S est un ensemble infini dénombrable, on dit que le groupe libre $F(S)$ est de **rang dénombrable**.

Théorème 1.7. *Pour tout groupe G, il existe un groupe libre F et un épimorphisme $f\colon F \to G$. Si G est discret, on peut trouver un F discret.*

Démonstration. Soit $F = F(G)$ le groupe libre sur l'ensemble G. En utilisant la fonction identique de G vu comme ensemble vers G vu comme groupe, nous obtenons, d'après la définition d'un groupe libre, un unique homomorphisme f de $F(G)$ vers G égal à l'identité sur G. □

Lemme 1.8. *Soit U un sous-ensemble d'un groupe G tel que $U \cap U^{-1} = \emptyset$. Alors U est une base d'un sous-groupe libre de G si, et seulement si, chaque fois que $u_1 u_2 \cdots u_n = 1$ avec $n \geqslant 1$ et les u_i dans $U \cup U^{-1}$, on a une égalité $u_i u_{i+1} = 1$ pour un i.*

Démonstration. Si U est une base d'un sous-groupe libre de G, l'ensemble U satisfait les conditions du lemme d'après le théorème 1.2. Inversement, supposons que U satisfasse les conditions du lemme et considérons le groupe $F(U)$ libre sur U. La fonction injective naturelle de U vers G se prolonge de manière unique en un homomorphisme de groupes $f\colon F(U) \to G$ dont l'image est le sous-groupe engendré par U. Supposons que

$$1 = f(u_1 \cdots u_n) = f(u_1) \cdots f(u_n),$$

avec chaque $u_i \in U \cup U^{-1}$. Comme f est injective sur U, nous avons $f(u_i) \in U \cup U^{-1}$ dans G, donc il y a un i tel que $f(u_i) f(u_{i+1}) = 1$, et donc $u_i u_{i+1} = 1$. Par suite le noyau de f est trivial, donc $F(U)$ est isomorphe au sous-groupe engendré par U. □

Exercices

1. Montrer que si $F(S)$ est abélien et si $a, b \in S$, alors $a = b$.
2. Montrer que si $w \in F(S)$, $s \in S$ et $sw = ws$, alors $w = s^n$ pour un entier n.
3. Montrer que tout mot dans $F(S)$ possède une forme réduite si, et seulement si, S est discret.
4. Montrer que $F(S) \simeq F(T)$ implique que S est isomorphe à T dans les cas suivants :
   (i) S est fini,
   (ii) S est l'ensemble $\mathbb{N}$,
   (iii) S est un sous-ensemble initial [1] (sans trous) détachable de $\mathbb{N}$.
5. Soit S un ensemble fini de cardinalité m. Montrer que si T est un sous-ensemble fini de $F(S)$ de cardinalité strictement plus grande que m, il existe un produit non vide d'éléments distincts de T qui est égal à un produit de carrés.
6. Soient $S = \{s_1, \ldots, s_m\}$ et $T = \{t_1, \ldots, t_n\}$ (non nécessairement discrets). Utiliser l'exercice 5 pour montrer que si $F(S) \simeq F(T)$ et $m < n$, alors $t_i = t_j$ pour un $i < j$.

2 Ensembles de Nielsen

Soit S un ensemble discret. Nous étudions les conditions sur un sous-ensemble U de $F(S)$ qui assurent que U est un système générateur libre du sous-groupe $\langle U \rangle$ engendré par U. La **longueur réduite** d'un élément $w \in F(S)$ est la longueur de sa forme réduite, et nous la notons $|w|$.

Un sous-ensemble U du groupe libre $F(S)$ est appelé un **ensemble de Nielsen** si

(N0) $U \cap U^{-1} = \emptyset$,

et pour tous $x, y, z \in U \cup U^{-1}$ nous avons :

(N1) si $xy \neq 1$, alors $|xy| \geqslant \max\{|x|, |y|\}$,

(N2) si $xy \neq 1$ et $yz \neq 1$, alors $|xyz| > |x| - |y| + |z|$.

Notez que la condition N0 assure que $1 \notin U$. Nous allons démontrer que si U satisfait les conditions N0 et N2, alors U est un système générateur libre pour $\langle U \rangle$.

1. **NdT.** Un sous-ensemble S de $\mathbb{N}$ est dit **initial** si $n \in S$ et $m < n$ impliquent $m \in S$.

Exemple 2.1 (*les conditions N1 et N2 sont indépendantes*)**.** Soit $S = \{s, t, u, v\}$. Alors l'ensemble $U = \{s^2, st, ts\}$ satisfait la condition N1 mais, comme $(st)^{-1}(s^2)(ts)^{-1} = t^{-2}$, il ne satisfait pas la condition N2. L'ensemble $V = \{tuv, suv\}$ satisfait la condition N2 mais pas la condition N1. □

Si u et v sont des mots réduits, il existe des mots réduits uniques a, b et c tels que $u \equiv ab^{-1}$, $v \equiv bc$, et ac est réduit. Nous appelons b **le morceau de** v **qui disparait dans le produit** uv. De la même manière b^{-1} est appelé **le morceau de** u **qui disparait dans le produit** uv. Le lemme suivant aide à comprendre la signification de la condition N1.

Lemme 2.2. *Soit U un ensemble fini de mots réduits qui satisfait la condition N1 dans le groupe libre $F(S)$. Si u et v sont des mots dans U et si b est le morceau de v qui disparait dans le produit uv, alors $2|b| \leqslant \min(|u|, |v|)$.*

Démonstration. Il s'agit d'une conséquence facile de la condition N1. □

Le lemme suivant explique la signification de la condition N2, et il donne le moyen d'invoquer le lemme 1.8.

Lemme 2.3. *Soient S un ensemble discret et U un ensemble de mots réduits dans $F(S)$ qui satisfait les conditions N0 et N2. Soit $w \equiv u_1 u_2 \cdots u_n$ avec les $u_i \in U \cup U^{-1}$ et $u_i u_{i+1} \neq 1$ pour $i < n$. Alors il existe des mots a_i, b_i, c_i tels que $u_i \equiv a_i b_i c_i$, $b_i \neq 1$, et $b_1 b_2 \cdots b_n$ est la forme réduite de w.*

Démonstration. On définit $a_0 \equiv c_n \equiv 1$. Soient c_i le morceau de u_i et $a_{i+1} \equiv c_i^{-1}$ le morceau de u_{i+1} qui disparaissent dans le produit $u_i u_{i+1}$ pour $i < n$. D'après la condition N2, nous avons

$$|u_{i-1} u_i u_{i+1}| > |u_{i-1}| - |u_i| + |u_{i+1}|,$$

et donc $u_i \equiv a_i b_i c_i$, avec $b_i \neq 1$, si $1 < i < n$. D'après le théorème 1.5, nous savons que $u_1 u_1 \neq 1$ et $u_n u_n \neq 1$, donc N2 nous dit que $|u_1 u_1 u_2| > |u_2|$ et $|u_{n-1} u_n u_n| > |u_{n-1}|$; par suite $b_1 \neq 1$ et $b_n \neq 1$. Comme c_i est le morceau de u_i qui disparait dans le produit $u_i u_{i+1}$, nous obtenons que $a_i b_i b_{i+1} c_{i+1}$ est la forme réduite de $u_i u_{i+1}$, donc le mot $b_1 b_2 \cdots b_n$ est réduit. □

Corolaire 2.4. *Si U est un ensemble de mots qui satisfait les conditions N0 et N2 dans un groupe libre sur un ensemble discret, c'est un système générateur libre pour $\langle U \rangle$.*

Démonstration. Cela résulte des lemmes 2.3 et 1.8. □

Dans l'exemple 2.1, l'ensemble V satisfait les conditions N0 et N2, donc V est un système générateur libre de $\langle V \rangle$.

Contrairement à ce qui se passe dans le cas des groupes abéliens, un groupe libre de petit rang peut avoir comme sous-groupe un groupe libre de grand rang.

En fait, il y a même des sous-groupes libres de rang infini parmi les sous-groupes de groupes libres de rang fini.

Théorème 2.5. *Un groupe libre sur un ensemble fini à deux éléments contient un sous-groupe libre de rang dénombrable.*

Démonstration. Soit $\{x, y\}$ la base du groupe libre. On considère l'ensemble

$$U = \{\, y,\ xyx^{-1},\ x^2yx^{-2},\ x^3yx^{-3}, \dots\}.$$

On vérifie facilement que U est un ensemble de Nielsen, donc c'est un système générateur libre pour le groupe qu'il engendre. □

Exercices

1. Dans un groupe G, un élément de la forme $aba^{-1}b^{-1}$ est appelé le *commutateur de a et b*. L'ensemble des commutateurs engendre un sous-groupe distingué appelé le **groupe dérivé de** G, noté $\mathrm{D}(G)$. On l'appelle aussi le **sous-groupe des commutateurs** de G. Le quotient $G/\mathrm{D}(G)$ est le groupe abélien engendré par G.
   Soit F le groupe libre sur l'ensemble fini à deux éléments $\{x, y\}$. Montrer que $\{\, x^m y^n x^{-m} y^{-n} : m, n \in \mathbb{Z} \setminus \{0\}\,\}$ est un système générateur libre pour le sous-groupe des commutateurs de F.
2. Montrer que si U est un ensemble de Nielsen de mots dans un groupe libre discret et si $w \equiv u_1 \cdots u_n$ avec $u_i \in U \cup U^{-1}$ et chaque $u_i u_{i+1} \neq 1$, alors $|w| \geqslant \max\{|u_1|, \dots, |u_n|\}$.
3. Montrer que le sous-groupe construit dans le théorème 2.5 est détachable.

3 Sous-groupes de type fini de groupes libres

Nous démontrons dans cette section comment transformer un ensemble fini de générateurs d'un sous-groupe d'un groupe libre sur un ensemble fini S en un ensemble de Nielsen.

Définition 3.1. Soient U et V des ensembles finis de mots. Nous disons que V est obtenu à partir de U par une **transformation de Nielsen** si l'on se trouve dans l'un des cas suivants :

(T0) $V = U \setminus \{1\}$;

(T1) $V = (U \setminus \{u\}) \cup \{u^{-1}\}$ où $u \in U$;

(T2) $V = (U \setminus \{u\}) \cup \{v\}$ où v est égal à uu', ou $u'u$, pour un $u' \in U \cup U^{-1}$ différent de u et u^{-1}.

On réfère à une transformation de type T2 en disant que l'on a **remplacé** u **par** v **dans** U. Notez que si V est obtenu à partir de U par une transformation de Nielsen, alors on a $\langle U\rangle = \langle V\rangle$ et $\#U \geqslant \#V$. (Les transformations de types T1 et T2 peuvent faire décroitre le nombre d'éléments de l'ensemble U. Par exemple si $U = \{a, ab, b\}$, la transformation de type T2 qui remplace b par ab diminue le nombre d'éléments.) De plus, si V est obtenu à partir de U par une transformation de type T1 ou T2, et si $\#U = \#V$, alors U est obtenu à partir de V par une transformation du même type.

Si S est un ensemble fini, nous pouvons mettre un ordre total sur les mots de $F(S)$, par rapport à « $\equiv$ », de la manière suivante. On fixe un ordre total sur $S \cup S^{-1}$ et on l'étend en l'ordre lexicographique sur les mots de $F(S)$. Si u et v sont des mots de $F(S)$, on définit $u < v$ comme suit :

(i) $\ell(u) < \ell(v)$, ou

(ii) $\ell(u) = \ell(v)$ et u précède v pour l'ordre lexicographique.

Notez que tout mot a un nombre fini de prédécesseurs pour cette relation d'ordre.

Théorème 3.2. *Soient S un ensemble fini et U un sous-ensemble fini de $F(S)$. Alors il existe une suite de transformations de Nielsen qui transforme U en un ensemble de Nielsen.*

Démonstration. Tout d'abord nous définissons une mesure de la taille de U pour laquelle nous pourrons faire une démonstration par récurrence. Si w est un mot, nous pouvons écrire la forme réduite de w de manière unique sous la forme $w_L w_R$ où $|w_L|$ est le plus grand entier inférieur ou égal à $(|w|+1)/2$. On définit ensuite une fonction φ de $F(S)$ vers $\mathbb{N}$, de manière un peu cryptique, en prenant $\varphi(w)$ égal au nombre de mots v tels que $v < w_L w_R^{-1}$. Notez que si $|u_1| < |u_2|$, alors $\varphi(u_1) < \varphi(u_2)$. Enfin on pose $\varphi U = \sum_{u\in U} \varphi(u)$.

Nous procédons par récurrence sur φU. À l'aide d'une suite de transformations de type T0 et T1, nous pouvons supposer que $U \cap U^{-1} = \emptyset$. Si $|xy| < |x|$ pour $x, y \in U \cup U^{-1}$ et $xy \neq 1$, alors $x \neq y$ d'après le théorème 1.5 et nous pouvons remplacer x par xy (ou x^{-1} par $y^{-1}x^{-1}$) et faire décroitre φU. Donc nous pouvons supposer que U satisfait N1.

Soient x, y et z des mots réduits dans $U \cup U^{-1}$ avec $xy \neq 1$ et $yz \neq 1$. Supposons que $|xyz| \leqslant |x| - |y| + |z|$. Alors nous pouvons écrire

$$x \equiv ap^{-1},\ y \equiv pq^{-1},\ z \equiv qc.$$

Si $|p| > |q|$, $|xy| < |x|$; si $|p| < |q|$, $|yz| < |z|$; si $|p| > |a|$, $|xy| < |y|$; si $|q| > |c|$, $|yz| < |y|$; donc aucun de ces cas ne peut se produire car U satisfait la condition N1. Donc $|p| = |q| \leqslant \min(|a|, |c|)$, $|xy| = |x|$, et $|yz| = |z|$. Notez que $p \neq q$ parce que $y \neq 1$. Si $p < q$ (pour l'ordre lexicographique), alors $\varphi(yz) < \varphi(z)$; tandis que si $q < p$, alors $\varphi(xy) < \varphi(x)$. Dans chaque cas,

nous pouvons utiliser une transformation de Nielsen qui diminue $\varphi(u)$ pour un élément $u \in U$ sans changer les autres éléments, ce qui fait décroitre φU. □

Corolaire 3.3. *Tout sous-groupe de type fini d'un groupe libre de rang fini est libre, avec un ensemble de Nielsen comme système générateur libre.* □

Théorème 3.4. *Si F est un groupe libre de rang fini n et si U est un système générateur de F, alors U contient au moins n éléments. En outre, si U a exactement n éléments, c'est un système générateur libre de F.*

Démonstration. Comme chaque élément d'un système générateur libre de F est le produit d'un nombre fini de mots dans U, nous pouvons supposer que U est fini. D'après le théorème 3.2, nous pouvons transformer U en un ensemble de Nielsen V par une suite de transformations de Nielsen. Donc on a $\langle U\rangle = \langle V\rangle$ et $\#V \leqslant \#U$. Comme V est un ensemble de Nielsen, et comme U est un système générateur, V est un système générateur libre de F, donc V a n éléments. Si U a n éléments, aucune transformation de type T0 n'a été utilisée pour transformer U en V. Par suite V peut être transformé en U par des transformations de types T1 et T2. Mais ces transformations peuvent être utilisées pour définir une fonction surjective du système générateur libre V sur U, fonction qui peut être étendue en un endomorphisme de F qui est un isomorphisme. □

Théorème 3.5. *Tout sous-groupe de type fini G d'un groupe libre de rang fini F est détachable.*

Démonstration. Comme G est de type fini, le corolaire 3.3 nous dit que G contient un ensemble de Nielsen U qui est un système générateur libre. Soit $w \in F$. D'après le lemme 2.3, tout $w \in G$ peut être écrit comme un produit d'au plus $|w|$ éléments de $U \cup U^{-1}$. Comme F est discret, nous pouvons tester si w peut s'écrire de cette manière. □

Exercices

1. Montrer que le sous-groupe des commutateurs d'un groupe libre sur un ensemble à deux éléments n'est pas de type fini (voir l'exercice 2.1).
2. Donner un exemple brouwerien d'un sous-groupe dénombrable d'un groupe libre de rang fini qui n'est pas libre.
3. Montrer qu'un groupe libre de rang fini F est **hopfien** au sens que tout morphisme de F sur F est injectif.
4. Montrer que tout sous-groupe de type fini d'un groupe libre discret est libre et détachable.

4 Sous-groupes détachables de groupes libres de rang fini

Nous démontrons dans cette section que les sous-groupes détachables d'un groupe libre de rang fini sont libres. De plus, un sous-groupe d'indice fini n dans un groupe libre de rang fini r est libre de rang $n(r-1)+1$.

Soit F un groupe et G un sous-groupe de F. Une fonction T de F vers F est appelée une **transversale** (**à droite**) pour G si $T(x) \in Gx$ pour chaque $x \in F$, et si $T(x) = T(y)$ chaque fois que $Gx = Gy$. En d'autres termes, T est une fonction de choix pour l'ensemble des classes à droite de G dans F. Notez que $T(T(x)y) = T(xy)$ pour tous $x, y \in F$.

Soit F le groupe libre sur un ensemble fini S. Si $w \equiv uv$ est un mot réduit dans F, u est appelé un **segment initial** de w et v est appelé un **segment final** de w. Une transversale T pour un sous-groupe G de F est une **transversale de Schreier** si c'est une fonction de l'ensemble F muni de l'égalité « $=$ » vers l'ensemble F muni de l'égalité « $\equiv$ » qui vérifie les conditions suivantes : tous les mots $T(w)$ sont réduits et l'ensemble $T(F) = \{\, T(w) : w \in F \,\}$ est clos par segments initiaux. Si $T(F)$ est également clos par segments finaux, T est une **transversale de Schreier bilatère**.

Théorème 4.1. *Soient F le groupe libre sur un ensemble fini S et G un sous-groupe détachable de F. Alors G possède une transversale de Schreier, et si G est un sous-groupe normal, il possède une transversale de Schreier bilatère.*

Démonstration. On munit l'ensemble F de l'ordre total défini juste avant le théorème 3.2. Tout élément de F a un nombre fini de prédécesseurs et G est détachable, donc pour chaque $w \in F$ on peut définir $T(w)$ comme le premier mot dans Gw (notez que Gw est l'ensemble des mots égaux à un mot de la forme gw).

Si $w \equiv uv$ est le plus petit élément de Gw, alors u est le plus petit élément de Gu, car s'il y a un $g \in G$ avec $gu = c < u$, alors $gw = cv < uv \equiv w$. Donc T est une transversale de Schreier.

Si G est normal, on a $Gw = wG$, donc v est le plus petit élément de $Gv = vG$, et par suite T est une transversale de Schreier bilatère. □

Lemme 4.2. *Soit F le groupe libre sur un ensemble fini S et T une transversale de Schreier pour un sous-groupe G de F. Soient s et s' des éléments de $S \cup S^{-1}$, et t et t' des éléments de $T(F)$ tels que ni ts ni $t's'$ n'est égal à un élément de $T(F)$. Soit u la forme réduite de $T(ts)^{-1}t'$. Alors :*

(i) *$tsT(ts)^{-1}$ et $t's'T(t's')^{-1}$ sont réduits ;*

(ii) *si $tsT(ts)^{-1} = t's'T(t's')^{-1}$, alors $t \equiv t'$ et $s \equiv s'$;*

(iii) *sus' est réduit sauf dans le cas où $u = 1$ et $s' = s^{-1}$.*

Démonstration. Si ts n'est pas réduit, $t \equiv t''s^{-1}$ pour un $t'' \in T(F)$, car T est une transversale de Schreier, et donc $ts = t'' \in T(F)$, contrairement à l'hypothèse. Si $sT(ts)^{-1}$ n'est pas réduit, $T(ts) \equiv t''s$ avec $t'' \in T(F)$, car T est une transversale de Schreier. Mais alors

$$t'' = T(t'') = T(T(ts)s^{-1}) = T(tss^{-1}) = T(t) = t,$$

donc $ts = t''s \in T(F)$, contrairement à l'hypothèse. Comme ts et $sT(ts)^{-1}$ sont tous deux réduits, le mot $tsT(ts)^{-1}$ est réduit. De la même manière $t's'T(t's')^{-1}$ est réduit.

Si $tsT(ts)^{-1} = t's'T(t's')^{-1}$, comme ils sont tous deux réduits, ts est un segment initial de $t's'$ ou vice versa, mais ts n'est pas un segment initial de t' (car $t' \in T(F)$ et $ts \notin T(F)$), et de même $t's'$ n'est pas un segment initial de t. On a donc nécessairement $ts = t's'$, donc $t = t'$ et $s = s'$ [1].

Pour démontrer le point (iii), il suffit de démontrer que su et us' sont réduits. On a $u = T(ts)^{-1}t'$, et u et $sT(ts)^{-1}$ sont réduits. Si su n'est pas réduit, $T(ts)^{-1}$ doit disparaitre dans le produit $T(ts)^{-1}t'$ en laissant s^{-1} sur la gauche, donc $T(ts)s^{-1}$ est un segment initial de t'. Donc $T(ts)s^{-1}$ est dans $T(F)$ car T est une transversale de Schreier. Ainsi $t = T(T(ts)s^{-1}) = T(ts)s^{-1}$, d'où l'on déduit $ts = T(ts) \in T(F)$, contrairement à l'hypothèse. Donc su est réduit.

De la même manière, si $us' = T(ts)^{-1}t's'$ n'est pas réduit, alors, comme $t's'$ est réduit, $t's'$ est un segment initial de $T(ts)$, donc il est dans $T(F)$, contrairement à l'hypothèse. □

Lemme 4.3. *Soient T une transversale pour un sous-groupe d'un groupe F, $t, t' \in T(F)$ et $s \in F$. Alors les propriétés suivantes sont équivalentes.*

(i) $t' = T(ts)$.

(ii) $t = T(t's^{-1})$.

En outre, lorsque ces conditions sont satisfaites, en notant $f(w) = wT(w)^{-1}$, on a

(iii) $f(ts)f(t's^{-1}) = 1$.

Démonstration. Si $t' = T(ts)$, alors

$$T(t's^{-1}) = T(T(ts)s^{-1}) = T(tss^{-1}) = T(t) = t,$$

donc (i) implique (ii), et par suite (ii) implique (i). Si les conditions (i) et (ii) sont satisfaites, on a

$$\begin{aligned} f(ts)^{-1} &= T(ts)s^{-1}t^{-1} = T(T(t's^{-1})s)s^{-1}t^{-1} \\ &= T(t')s^{-1}t^{-1} = t's^{-1}t^{-1} = (t's^{-1})t^{-1} = f(t's^{-1}). \end{aligned}$$ □

1. **NdT.** Notez que pour les mots réduits, $=$ et $\equiv$ coïncident.

Théorème 4.4. *Soit G un sous-groupe du groupe libre F sur un ensemble discret S. Soit T une transversale de Schreier pour G. On définit la fonction f de F vers G par $f(w) = wT(w)^{-1}$. Alors l'ensemble*

$$Y = \{\, f(ts) : s \in S,\, t \in T(F) \text{ et } f(ts) \neq 1 \,\}$$

est un système générateur libre de G.

Démonstration. Si $w \in G$, $T(w) = 1$, donc $f(w) = w$. Donc pour démontrer que $G = \langle Y \rangle$, il suffit de démontrer que $f(w) \in \langle Y \rangle$ pour tout $w \in F$. Soit $w \in F$ et $s \in S$. Alors

$$f(w)f(T(w)s) = wT(w)^{-1}T(w)sT(T(w)s)^{-1} = wsT(ws)^{-1} = f(ws).$$

Comme $f(T(w)s) \in Y \cup \{1\}$, on a $f(ws) \in \langle Y \rangle$ si, et seulement si, $f(w) \in \langle Y \rangle$.

Soit maintenant un mot réduit $w \in F$. Ou bien $w = 1 \in \langle Y \rangle$, ou bien $|ws^{-1}| < |w|$ pour un $s \in S$, ou bien $|ws| < |w|$ pour un $s \in S$. Dans les deux derniers cas, par récurrence sur la longueur, ou bien $f(ws^{-1}) \in \langle Y \rangle$, ou bien $f(ws) \in \langle Y \rangle$. Donc $w \in \langle Y \rangle$.

Nous montrons maintenant que Y est un système générateur libre en faisant appel au lemme 1.8. On observe d'abord que l'on a

$$Y^{-1} = \{\, f(ts^{-1}) : s \in S,\, t \in T(F), \text{ et } f(ts^{-1}) \neq 1 \,\}$$

d'après le lemme 4.3. Donc si $y \in Y \cup Y^{-1}$, on a $y = f(ts)$ avec $s \in S \cup S^{-1}$ et $t \in T(F)$. Ensuite on note que $Y \cap Y^{-1} = \emptyset$ d'après le lemme 4.2(ii). Nous supposons maintenant que $y_1 y_2 \cdots y_n = 1$ avec les $y_i \in Y \cup Y^{-1}$. On écrit $y_i \equiv f(t_i s_i) \equiv t_i s_i T(t_i s_i)^{-1}$, avec $s_i \in S \cup S^{-1}$ et $t_i \in T(F)$. D'après le lemme 4.2(i) les y_i sont réduits. Soit u_i la forme réduite de $T(t_i s_i)^{-1} t_{i+1}$ pour $i < n$ et $u_n = T(t_n s_n)^{-1}$. Alors

$$y_1 y_2 \cdots y_n = t_1 s_1 u_1 s_2 u_2 \cdots u_{n-1} s_n u_n. \qquad (*)$$

Nous devons montrer que $y_i y_{i+1} = 1$ pour un $i < n$. Si $t_i s_i$ était égal à un élément de $T(F)$, y_i serait égal à 1 ; nous pouvons donc appliquer le lemme 4.2(iii). Ainsi, ou bien les éléments $s_i u_i s_{i+1}$ sont tous réduits pour $i < n$, ou bien on a $u_i = s_i s_{i+1} = 1$ pour un $i < n$. Dans le premier cas, le membre de droite de $(*)$ est réduit parce que $t_1 s_1$ et $s_n u_n$ sont aussi réduits d'après le lemme 4.2(i) ; or c'est impossible car $y_1 y_2 \cdots y_n = 1$. Dans le deuxième cas, on a $t_{i+1} = T(t_i s_i)$ pour un i, donc $y_i y_{i+1} = 1$ d'après le lemme 4.3. □

Les théorèmes 4.1 et 4.4 impliquent que les sous-groupes détachables de groupes libres de rang fini sont libres. Si le sous-groupe est d'indice fini, nous pouvons calculer son rang comme suit.

Théorème 4.5. *Soit $F = F(S)$ un groupe libre de rang r et G un sous-groupe d'indice fini n. Alors G est un groupe libre de rang $n(r-1)+1$.*

Démonstration. Soit T une transversale de Schreier pour G, et Y le système générateur libre défini dans le théorème 4.4. Il nous faut montrer que Y a $n(r-1)+1$ éléments. On définit les fonctions λ et μ

$$\lambda\colon T(F)\setminus\{1\}\to T(F)\times S,\quad \mu\colon Y\to T(F)\times S$$

par

$$\mu(y)=(t,s)\text{ tel que }f(ts)=y\ \text{ et }\ \lambda(t)=\begin{cases}(t',s) & \text{si } t\equiv t's \text{ avec } s\in S\\ (t,s) & \text{si } t\equiv t's^{-1} \text{ avec } s\in S.\end{cases}$$

Le lemme 4.2 assure que la fonction μ est bien définie ; elle est clairement injective. La fonction λ a son image dans $T(F)\times S$ parce que T est une transversale de Schreier ; on voit facilement que λ est injective. L'image de λ est l'ensemble des couples $(t,s)\in T(F)\times S$ tels que $ts\in T(F)$, ce qui est la même chose que l'ensemble des couples (t,s) tels que $f(ts)=1$. Donc les images de λ et de μ partitionnent $T(F)\times S$ en deux ensembles disjoints. Le premier contient $n-1$ éléments et le second contient le même nombre d'éléments que Y. Comme $T(F)\times S$ a nr éléments, on voit que $\#Y = nr-(n-1) = n(r-1)+1$. □

Exercices

1. Montrer que si G est un sous-groupe d'un groupe libre discret, alors G est détachable si, et seulement si, il possède une transversale de Schreier.
2. Construire un exemple brouwerien d'un sous-groupe libre d'un groupe libre de rang fini qui n'est pas détachable.
3. Soit G un sous-groupe de type fini d'un groupe libre de rang fini. Montrer comment on peut déterminer si G a un indice fini.
4. Utiliser le théorème 2.5 pour montrer qu'un sous-groupe détachable d'un groupe libre discret dénombrable est libre.

5 Sous-groupes conjugués

Soit S un ensemble et $u,v\in F(S)$. Les éléments u et v sont dits **conjugués** dans $F(S)$ s'il existe un $c\in F$ tel que $u=c^{-1}vc$. Un mot $w\equiv x_1\cdots x_n$, avec les $x_i\in S\cup S^{-1}$ est **cycliquement réduit** s'il est réduit et $x_nx_1\neq 1$. Si S est discret, tout mot réduit w de $F(S)$ peut être écrit de manière unique sous la forme $w\equiv v^{-1}w'v$ avec w' cycliquement réduit.

Théorème 5.1. *Si F est un groupe libre sur un ensemble discret S, deux éléments arbitraires $u,v\in F$ sont ou ne sont pas conjugués.*

Démonstration. Nous pouvons supposer que u et v sont réduits. On écrit $u \equiv a^{-1}u'a$ et $v \equiv b^{-1}v'b$ avec u' et v' cycliquement réduits. Alors u et v sont conjugués si, et seulement si, u' et v' sont conjugués. Nous allons montrer que si $u' \neq v'$ et $u' = c^{-1}v'c$, alors u' est une permutation cyclique de v'. Nous pouvons supposer que c est réduit. Comme u' est cycliquement réduit, $c^{-1}v'$ ou $v'c$ n'est pas réduit. Dans le premier cas, on a $c \equiv sd$ et $v' \equiv sw$, avec $s \in S \cup S^{-1}$. Alors $u' = d^{-1}s^{-1}swsd = d^{-1}wsd$ et ws est une permutation cyclique de v'. Comme $|d| < |c|$, nous terminons par récurrence sur $|c|$. Le second cas est similaire. Donc u et v sont conjugués si, et seulement si, u' et v' sont des permutations cycliques l'un de l'autre. □

Soit F un groupe et U un sous-ensemble de F. Pour $w \in F$, on note $w^{-1}Uw = \{\, w^{-1}uw : u \in U \,\}$. Si U est un sous-groupe, $w^{-1}Uw$ est un sous-groupe. Les sous-groupes G et H sont dits **conjugués** s'il existe un $w \in F$ tel que $H = w^{-1}Gw$.

Théorème 5.2. *Soit F un groupe libre de rang fini et soient G et H des sous-groupes de type fini de F. Alors, ou bien G est conjugué d'un sous-groupe de H, ou bien il ne l'est pas. De même, ou bien G est conjugué de H, ou bien il ne l'est pas.*

Démonstration. Soit U un système générateur libre fini de G, et V un système générateur libre fini de H. Nous pouvons supposer que V est un ensemble de Nielsen de générateurs pour H et, en remplaçant G par un sous-groupe conjugué, que U contient un élément u qui est cycliquement réduit (le cas $U = \emptyset$ est trivial). Soit $m = \max\{\, |w| : w \in U \cup V \,\}$. Nous montrons que, pour chaque $w \in F$,

$$\begin{aligned} &\text{si } w^{-1}Gw \subseteq H \text{ et } |w| > m, \text{ nous pouvons trouver} \\ &\text{un } w' \in GwH \text{ tel que } |w'| < |w|. \end{aligned} \tag{$*$}$$

Si $(*)$ est démontré, comme $w' \in GwH$, on a $w'^{-1}Gw' \subseteq H$; donc, par récurrence, nous pouvons trouver un $w' \in GwH$ tel que $|w'| \leqslant m$. Le théorème résulte alors du raisonnement suivant. Puisque F est de rang fini, il y a seulement un nombre fini de mots w tels que $|w| \leqslant m$. Pour chaque mot w de ce type, nous testons si $w^{-1}Uw \subseteq H$; on peut le faire parce que U est fini et H est détachable. Si un tel w n'existe pas, G n'est pas conjugué d'un sous-groupe de H. Si un tel w existe, $w^{-1}Gw$ est un sous-groupe de H conjugué de G. Si $w^{-1}Uw \subseteq H$, nous pouvons décider si $\langle w^{-1}Uw \rangle = H$ parce que H est de type fini et $\langle w^{-1}Uw \rangle$ est détachable. Si c'est le cas, G et H sont conjugués ; sinon, ils ne le sont pas.

Pour démontrer $(*)$, nous supposons que w est réduit avec $|w| > m$ et $w^{-1}Gw \subseteq H$. Soit un $u \in U$ cycliquement réduit. Alors $u^{-1}w$ ou uw est réduit. Nous pouvons supposer, en remplaçant u par u^{-1} si nécessaire, que uw est réduit. Si $|w| > |u^{-1}w|$, nous pouvons prendre $w' = u^{-1}w$, sinon on a

$|w^{-1}u| \geqslant |w^{-1}|$. Dans ce cas, c'est au plus la moitié de u qui disparait dans le produit $w^{-1}u$. Comme uw est réduit et $|w^{-1}| = |w| > m \geqslant |u|$, nous voyons que la forme réduite du produit $w^{-1}uw$ commence avec plus que la moitié du facteur w^{-1}, et se termine avec le facteur w. En particulier, $|w^{-1}uw| > |w| > m$.

Écrivons $w^{-1}uw$ sur le système générateur libre V de H : $w^{-1}uw = v_1v_2\cdots v_n$ avec les v_i dans $V \cup V^{-1}$ et $v_iv_{i+1} \neq 1$ pour tout $i < n$. Comme $|w^{-1}uw| > m \geqslant |v_1|$, on a nécessairement $n > 1$. Si $|wv_1| < |w|$, nous pouvons prendre $w' = wv_1$, et nous pouvons supposer que $|w| \leqslant |wv_1|$. Comme V est un ensemble de Nielsen, les lemmes 2.2 et 2.3 nous disent que la forme réduite de $w^{-1}uw = v_1\cdots v_n$ commence avec au moins la moitié de v_1, et d'après ce qui précède il commence aussi par au moins la moitié de w^{-1}. Comme $|w| > m \geqslant |v_1|$, cela implique que w^{-1} commence avec au moins la moitié de v_1. Cependant $|w| \leqslant |wv_1|$, donc w^{-1} commence avec au plus la moitié de v_1. Donc la forme réduite de $w^{-1}uw$ commence avec exactement la moitié de v_1, et la moitié de v_1 disparait dans v_1v_2. De la même manière, il se termine avec exactement la moitié de v_n. Supposons que $|v_1| \leqslant |v_n|$. Comme w^{-1} commence avec la moitié de v_1 et w se termine avec la moitié de v_n, la moitié de v_1 disparait dans le produit v_nv_1, et tout v_1 disparait dans le produit $v_nv_1v_2$. Comme $v_1v_2 \neq 1$, et comme V est un ensemble de Nielsen, on obtient $v_1 = v_n^{-1}$. De la même manière, si $|v_n| \leqslant |v_1|$, $v_1 = v_n^{-1}$. Donc $v_1 = v_n^{-1}$. Comme w se termine avec la moitié de $v_n = v_1^{-1}$, au moins la moitié de v_1 disparait dans le produit $w' = wv_1$, donc $|w'| \leqslant |w|$. Mais $w'^{-1}uw' = v_2\cdots v_{n-1}$ et nous terminons récurrence sur n. □

Exercices

1. Montrer que le théorème 5.2 est vrai pour tout groupe libre discret.
2. Construire des contre-exemples brouweriens pour des généralisations du théorème 5.2, la première avec G de rang dénombrable et la seconde avec H de rang dénombrable.

6 Notes

Le **problème des mots** pour un groupe G est celui de décider si deux éléments de G sont égaux ; autrement dit, résoudre le problème des mots pour G, c'est démontrer que G est discret. La terminologie provient de la considération de groupes quotients F/N où F est un groupe libre et N un sous-groupe normal de F ; dans cette situation le problème devient celui de reconnaitre si un mot de F est ou n'est pas dans N. Il pourrait sembler plausible de résoudre le problème des mots quand F est de rang fini et N est de type fini comme sous-groupe normal, i.e. lorsqu'il y a un sous-ensemble fini A de N tel que tout élément de N peut être écrit comme un produit de conjugués d'éléments de A. Cependant, une construction célèbre de Novikov et Boone donne de tels F et A pour lesquels

le problème des mots ne peut pas être résolu par un machine de Turing, et donc aucun algorithme ne peut être écrit dans un langage de programmation standard pour décider si un mot de F est dans N.

Le **problème des mots généralisé** pour un groupe G relativement à un sous-groupe H est de décider si un élément de G est dans H. Le problème des mots généralisé pour un groupe libre de rang fini relativement à un sous-groupe de type fini est résolu par la construction de Nielsen (théorème 3.5).

La construction de Schreier montre, en mathématiques classiques, que tout sous-groupe d'un groupe libre est libre. Pour construire une transversale de Schreier, on munit $S \cup S^{-1}$ d'une relation de bon ordre et on procède comme dans le cas fini.

XI. Groupes abéliens

Sommaire

1 Groupes sans torsion de rang fini

Un groupe abélien est un module sur l'anneau des entiers. Ainsi, quand nous étudions les groupes abéliens, nous pouvons faire appel aux faits généraux concernant les modules que nous avons développés dans le chapitre III, ainsi qu'à ceux que nous avons établis pour les modules sur les anneaux principaux dans le chapitre V. Le théorème de structure pour les groupes abéliens de présentation finie est un cas particulier du théorème de structure pour les modules de présentation finie sur les anneaux principaux (théorème V.2.3). Dans cette section, nous étudions les cas les plus simples de groupes abéliens sans torsion qui ne sont pas de présentation finie.

Si G est un module sur l'anneau commutatif R et si $r \in R$, alors $rG = \{\, rx : x \in G \,\}$ est un sous-module de G. Pour un $x \in G$, il est utile de savoir pour quels $r \in R$ nous avons $x \in rG$. Lorsque $R = \mathbb{Z}$, cette question se ramène celle de savoir si $x \in qG$ pour un nombre q égal à une puissance d'un nombre premier.

Lemme 1.1. *Si G est un module sur un anneau commutatif R, et si a et b sont des éléments étrangers de R, alors $abG = aG \cap bG$.*

Démonstration. Clairement $abG \subseteq aG \cap bG$, et si nous supposons que $x = ay = bz \in aG \cap bG$, nous pouvons écrire $1 = sa + tb$, de sorte que $x = sax + tbx = sabz + tbay = ab(sz + ty) \in abG$. □

Un groupe abélien G est **sans torsion** si pour tout entier non nul n et tout $x \in G$, $nx = 0$ implique $x = 0$. Si G est un groupe abélien sans torsion, l'application naturelle $G \to \mathbb{Q} \otimes G$ qui envoie x sur $1 \otimes x$, est un monomorphisme. Notez que $\mathbb{Q} \otimes G$ est discret si, et seulement si, G est discret, et que $\mathbb{Q} \otimes G$ est un espace vectoriel sur $\mathbb{Q}$. On dit qu'un groupe abélien sans torsion est de **rang** n si $\mathbb{Q} \otimes G$ est un espace vectoriel discret de dimension n sur $\mathbb{Q}$. Un groupe abélien sans torsion est de rang 1 si, et seulement si, il est isomorphe à un sous-groupe non nul du groupe additif $\mathbb{Q}$. En mathématiques classiques, les groupes abéliens sans torsion de rang 1 sont classifiés par les classes d'équivalence de fonctions de l'ensemble $\mathbf{P}$ des nombres premiers vers $\mathbb{N} \cup \{\infty\}$.

Si x est un élément d'un groupe sans torsion G, nous définissons la **p-hauteur** de x comme $h_p x = \sup\{\, n : x \in p^n G \,\}$, où le supremum est pris dans $\mathbb{N} \cup \{\infty\}$. Naturellement il n'y a aucune raison de croire que nous pouvons calculer $h_p x$ en général [1] ; si nous pouvons le faire pour chaque nombre premier p et chaque $x \in G$, nous disons que le groupe G **possède des hauteurs**. Lorsque $G = A \oplus B$, on voit facilement que G possède des hauteurs si, et seulement si, A et B possèdent des hauteurs, auquel cas $h_p^G x = \min(h_p^A x, h_p^B x)$.

Lemme 1.2. *Soit G un groupe abélien sans torsion qui possède des hauteurs. Pour $p \in \mathbf{P}$, $m \in \mathbb{N}$ et $x \in G$, les propriétés suivantes sont satisfaites.*

— *On a $h_p mx \geqslant h_p x$ avec égalité dans le cas où $(p, m) = 1$.*

— *Si $h_p x \in \mathbb{N}$, alors $h_p px = h_p x + 1$* [2].

Démonstration. Clairement $h_p mx \geqslant h_p x$. Supposons que $(p, m) = 1$ et $mx = p^n y$. Écrivons $sp^n + tm = 1$. Alors $x = sp^n x + tmx = p^n(sx + y)$; donc $h_p x \geqslant h_p mx$.

Enfin, on a $px = p^{n+1} y$ si, et seulement si, $x = p^n y$ parce que G est sans torsion. □

Un **type** est une fonction de $\mathbf{P}$ vers $\mathbb{N} \cup \{\infty\}$; deux types sont dits **égaux** s'ils sont égaux sauf peut-être en un nombre fini de nombres premiers, où ils sont tous les deux finis. L'ensemble des types est muni d'un ordre partiel naturel en posant $\tau_1 \leqslant \tau_2$ si $\tau_1(p) \leqslant \tau_2(p)$ sauf peut-être en un nombre fini de nombres premiers, où ils sont tous les deux finis. On voit alors facilement que l'ensemble des types forme un treillis distributif avec un élément maximum et un élément minimum.

Le **type d'un élément** x dans un groupe sans torsion G qui possède des hauteurs est la fonction $p \mapsto h_p x$ vue comme un type. D'après le lemme 1.2, si $x \in G$ et si m est un entier naturel non nul, alors le type de x est égal au type de mx. Comme deux éléments non nuls d'un groupe sans torsion de rang 1 ont un multiple commun, nous pouvons définir le **type d'un groupe sans torsion de**

1. **NdT.** Si le groupe est fortement discret, on peut à priori seulement décider si $h_p x \geqslant n$.
2. **NdT.** Avec la convention usuelle $\infty + 1 = \infty$.

rang 1 qui possède des hauteurs comme étant le type de n'importe quel élément non nul du groupe. Le théorème qui suit montre que deux groupes de cette sorte qui ont le même type sont isomorphes.

Théorème 1.3. *Soient G et G' des groupes abéliens sans torsion de rang 1 qui possèdent des hauteurs, de types respectifs τ et τ'.*

— *Il existe un morphisme non nul de G vers G' si, et seulement si, $\tau \leqslant \tau'$.*

— *Si $\tau = \tau'$, les groupes G et G' sont isomorphes.*

Démonstration. Soit un morphisme non nul $\varphi\colon G \to G'$. Clairement $h_p\varphi x \geqslant h_p x$ pour tout $x \in G$, donc $\tau \leqslant \tau'$.

Supposons maintenant que $\tau \leqslant \tau'$, et soient x et x' des éléments non nuls de G et G'. D'après le lemme 1.2, il existe des entiers non nuls m et m' tels que $h_p mx \leqslant h_p m'x'$ pour tous les nombres premiers p, avec égalité si $\tau = \tau'$. Soit H le sous-groupe de $G \oplus G'$ engendré par $(mx, m'x')$, et soit

$$K = \{\, w \in G \oplus G' : nw \in H \text{ pour un entier non nul } n \in \mathbb{N} \,\}.$$

Clairement, K est un sous-groupe de $G \oplus G'$. Si $y \in G$, alors $ny = \ell mx$ pour des entiers non nuls ℓ et n, car G est de rang 1. Donc $\ell m'x' \in nG'$ d'après les lemmes 1.1 et 1.2. Par suite, il existe un $y' \in G'$ tel que $ny' = \ell m'x'$, et donc $(y, y') \in K$. Si $\tau = \tau'$, alors, par symétrie, pour tout $y' \in G'$ il existe un $y \in G$ tel que $(y, y') \in K$. Si (y, y') et $(y, z') \in K$, alors $(0, y' - z') \in K$, et donc $y' = z'$ puisque G et G' sont sans torsion. En posant $\varphi(y) = y'$, nous obtenons un morphisme non nul qui est un isomorphisme si $\tau = \tau'$. □

Les groupes abéliens sans torsion de rang 1 qui possèdent des hauteurs forment une **classe semirigide** au sens suivant.

Corolaire 1.4. *Soient A et B des groupes abéliens sans torsion de rang 1 qui possèdent des hauteurs. S'il existe des morphismes non nuls de A vers B et de B vers A, A et B sont isomorphes.* □

L'hypothèse que A et B possèdent des hauteurs ne peut pas être supprimée dans le corolaire 1.4 ; un exemple est proposé dans l'exercice 7.

En mathématiques classiques, tout groupe abélien sans torsion de type fini est une somme directe de groupes cycliques. Cela n'est pas vrai d'un point de vue constructif (voir l'exercice 2) mais on a le théorème suivant.

Théorème 1.5. *Tout sous-groupe de type fini d'un groupe abélien sans torsion de rang fini est une somme directe de groupes cycliques.*

Démonstration. Il suffit de considérer les sous-groupes de type fini $G \subseteq \mathbb{Q}^n$. En multipliant G par un dénominateur commun des coordonnées des générateurs de G, nous sommes ramenés au cas où $G \subseteq \mathbb{Z}^n$. Alors G est de présentation finie en tant que sous-module de type fini d'un module cohérent, donc G est une somme directe de groupes cycliques d'après le théorème de structure V.2.3. □

Les groupes abéliens sans torsion de rang fini les plus simples sont les sommes directes finies de groupes abéliens sans torsion de rang 1 qui possèdent des hauteurs. Un tel groupe peut être spécifié, à isomorphisme près, par une famille finie de types. Il est à priori possible que deux familles distinctes de types correspondent à des groupes isomorphes, mais il se trouve que ce n'est pas le cas. Dans le contexte des mathématiques classiques, nous pouvons calculer, de manière invariante, le nombre de facteurs de rang 1 et de type τ en considérant le sous-groupe

$$G(\tau) = \{\, x \in G : \mathrm{type}(x) \geqslant \tau \,\}$$

et le sous-groupe $G(\tau^*)$ engendré par $\{\, G(\sigma) : \sigma > \tau \,\}$: le rang du groupe quotient $G(\tau)/G(\tau^*)$ est égal au nombre de facteurs de type τ. Mais comme l'ensemble des types n'est pas discret, cela ne nous permet pas de déterminer ce rang dans un contexte constructif. Notre approche repose sur le lemme suivant au sujet des bases des espaces vectoriels de dimension finie.

Lemme 1.6. *Soient $e_1, \ldots, e_n$ et $e_{n+1}, \ldots, e_{2n}$ des bases d'un espace vectoriel de dimension finie sur un corps discret. Soit $\pi_i(x)$ le multiple scalaire de e_i dans l'expression de x sur la base concernée. Soit R la clôture transitive de la relation $\pi_i(e_j) \neq 0$ sur $\{1, \ldots, 2n\}$. Alors chaque classe d'équivalence d'éléments de $\{1, \ldots, 2n\}$ pour la relation « $i \equiv j$ si $R(i,j)$ et $R(j,i)$ » a exactement la moitié de ses éléments dans le sous-ensemble $\{1, \ldots, n\}$.*

Démonstration. Soit C une classe d'équivalence d'éléments de $\{1, \ldots, 2n\}$. Écrivons $C = A \cup B$ avec $A = C \cap \{1, \ldots, n\}$ et $B = C \cap \{n+1, \ldots, 2n\}$. Pour S égal à A ou à B notons $\pi_S = \sum_{i \in S} \pi_i$ et V_S le sous-espace engendré par $\{\, e_i : i \in S \,\}$, i.e. l'image de π_S. Nous allons montrer que V_A a la même dimension que V_B. Par symétrie, il suffit de montrer que $\pi_A V_B = V_A$. Nous montrons que $e_i = \pi_A \pi_B e_i$ pour tout $i \in A$. On a $\pi_A \pi_B e_i = \sum_{k \in A} \sum_{j \in B} \pi_k \pi_j e_i$, mais d'après la définition des classes d'équivalence, $\pi_k \pi_j e_i = 0$ si $i, k \in A$ et $j \in \{n+1, \ldots, 2n\} \setminus B$. Donc $\pi_A \pi_B e_i = \sum_{k \in A} \sum_{j=n+1}^{2n} \pi_k \pi_j e_i = \pi_A e_i = e_i$. □

Théorème 1.7. *Supposons que $G = H_1 \oplus H_2 \oplus \cdots \oplus H_n = K_1 \oplus K_2 \oplus \cdots \oplus K_m$, où les H_i et K_j sont des groupes abéliens sans torsion de rang 1 qui possèdent des hauteurs. Alors $m = n$, et il existe une permutation σ de $\{1, \ldots, n\}$ telle que $H_i \simeq K_{\sigma(i)}$ pour tout i.*

Démonstration. Soient $e_1, \ldots, e_n$ des éléments non nuls de $H_1, \ldots, H_n$ respectivement, et $e_{n+1}, \ldots, e_{n+m}$ des éléments non nuls de $K_1, \ldots, K_m$ respectivement. Alors $e_1, \ldots, e_n$ et $e_{n+1}, \ldots, e_{n+m}$ sont des bases de $\mathbb{Q} \otimes G$, donc $m = n$. Pour le confort de la notation, nous posons $H_{n+i} = K_i$ pour $i = 1, \ldots, n$. On considère la fonction π_i comme dans le lemme 1.6, et on note que $\pi_i G = H_i$, donc si $\pi_i e_j \neq 0$ nous avons une fonction non nulle de H_j vers H_i. Le résultat se déduit maintenant du lemme 1.6 et du corolaire 1.4. □

Exercices

1. Montrer que tout groupe abélien fini est de présentation finie.

2. Soit a une suite binaire fugitive. Soit S le sous-groupe de $\mathbb{Z} \oplus \mathbb{Z}$ engendré par l'ensemble $\{ (1, na_n) : n \in \mathbb{N} \}$. Montrer que $(\mathbb{Z} \oplus \mathbb{Z})/S$ est un exemple brouwerien d'un groupe abélien sans torsion discret de type fini qui n'est pas égal à une somme directe de groupes cycliques.

3. Pour tout entier $i > 0$, soit A_i le sous-groupe de $\mathbb{Q}$ engendré par l'ensemble $\{ 1/p^i : p \text{ est un nombre premier} \}$. Montrer que A_i possède des hauteurs, et que A_i et A_j ne sont pas isomorphes si $i \neq j$. Pour quelles valeurs de i le groupe A_i est-il de type fini ?

4. Soit a une suite binaire, et A le sous-groupe de $\mathbb{Q}$ engendré par 1 et par l'ensemble $\{ 1/2^n : a_n = 1 \}$. Montrer que A est un exemple brouwerien d'un groupe sans torsion de rang 1 qui ne possède pas de hauteurs. Montrer que A est une partie détachable de $\mathbb{Q}$ si a est décroissante, mais pas en général.

5. Étant donnée une fonction $f : \mathbf{P} \to \mathbb{N} \cup \{\infty\}$, construire un groupe sans torsion de rang 1, et un élément x, tels que $h_p x = f(p)$ pour tout nombre premier p.

6. Un sous-groupe A d'un groupe abélien B est **plein** si B/A est un groupe de torsion. Montrer qu'un groupe abélien sans torsion est de rang n si, et seulement si, il contient un sous-groupe plein isomorphe à $\mathbb{Z}^n$.

7. Soient a une suite binaire et A le sous-groupe de $\mathbb{Q}$ engendré par 1 et $\{ a_n/2 : n \in \mathbb{N} \}$. Construire des applications non nulles de $\mathbb{Z}$ vers A et de A vers $\mathbb{Z}$, mais montrer que A est un exemple brouwerien d'un groupe qui n'est pas isomorphe à $\mathbb{Z}$. Pourquoi le corolaire 1.4 ne s'applique-t-il pas ? Construire un exemple de cette sorte où A et B ont la propriété que mA et mB sont des sous-groupes détachables pour tout m.

8. Construire un exemple brouwerien qui montre que l'hypothèse dans le théorème 1.7 selon laquelle les groupes ont des hauteurs est nécessaire.

9. *Un exemple d'un groupe sans torsion indécomposable de rang 2 qui possède des hauteurs.* Soit G le sous-groupe de $\mathbb{Q} \oplus \mathbb{Q}$ engendré par les éléments de la forme $(2^{-m}, 0)$, $(0, 3^{-m})$, et $(5^{-m}, 5^{-m})$. Calculer $h_p(x)$ pour $p > 5$, calculer $h_p(30^m x)$ dans $\mathbb{Z} \oplus \mathbb{Z}$. Dans le calcul de $h_2(x)$, nous pouvons ignorer $(2^{-m}, 0)$, et de manière analogue pour h_3 et h_5. Le fait que G est indécomposable résulte de ce qu'il a des éléments de trois types deux à deux incomparables.

2 Groupes divisibles

Un groupe est **p-divisible** si $pG = G$, **divisible** s'il est p-divisible pour tout nombre premier p. Le lemme 1.1 nous dit que G est divisible si, et seulement si, $nG = G$ pour tout entier $n \neq 0$. Le groupe additif des nombres rationnels $\mathbb{Q}$ est un groupe divisible sans torsion. L'exemple le plus simple d'un groupe de torsion divisible non trivial est le sous-groupe p-primaire du groupe de torsion $\mathbb{Q}/\mathbb{Z}$, noté $\mathbb{Z}(p^\infty)$, le groupe cyclique d'ordre p^∞ pour ainsi dire.

Dans un groupe sans torsion divisible, l'endomorphisme induit par la multiplication par un entier non nul est bijectif, donc est un isomorphisme. Par suite un groupe sans torsion divisible admet une unique structure d'espace vectoriel sur le corps $\mathbb{Q}$. Inversement, il est clair que le groupe additif d'un $\mathbb{Q}$-espace vectoriel est sans torsion et divisible.

Un **groupe abélien cohérent** est un groupe abélien qui est cohérent comme $\mathbb{Z}$-module [1]. On voit facilement qu'un groupe cohérent est fortement discret, et que tout groupe discret de torsion est cohérent.

Théorème 2.1. *Soit D un sous-groupe divisible d'un groupe G tel que G/D est dénombrable et cohérent. Alors on peut construire un sous-groupe dénombrable K de G tel que $G = K \oplus D$.*

Démonstration. Soient $x_1, x_2, \ldots$ des éléments de G qui énumèrent G/D. Comme G/D est cohérent, nous pouvons faire que,

ou bien $\langle x_{i+1}\rangle \cap (\langle x_1, \ldots, x_i\rangle + D) = 0$,

ou bien $px_{i+1} \in \langle x_1, \ldots, x_i\rangle + D$ pour un nombre premier p [2].

Nous allons construire une suite de sous-groupes de type fini $K_1 \subseteq K_2 \subseteq \cdots$ de G telle que $K_i + D = \langle x_1, \ldots, x_i\rangle + D$ et $K_i \cap D = 0$. Alors $K = \bigcup_i K_i$ sera le groupe voulu.

On pose $K_0 = 0$. Étant donné K_i, on construit K_{i+1} comme suit. Si $x_{i+1} \in K_i + D$ (ce qui est décidable), alors nous posons $K_{i+1} = K_i$. Si $x_{i+1} \notin K_i + D$, alors ou bien $\langle x_{i+1}\rangle \cap (K_i + D) = 0$, ou bien $px_{i+1} \in K_i + D$. Dans le premier cas, on pose $K_{i+1} = \langle x_{i+1}\rangle + K_i$. Dans le deuxième cas, on écrit $px_{i+1} = k_i + d$, où $k_i \in K_i$ et $d \in D$. Comme D est divisible, nous pouvons trouver un élément $d' \in D$ tel que $d = pd'$. Soit $y = x_{i+1} - d'$. Alors $py = k_i$, et nous posons $K_{i+1} = \langle y\rangle + K_i$. On a bien $K_{i+1} + D = \langle x_1, \ldots, x_{i+1}\rangle + D$; nous devons montrer que $K_{i+1} \cap D = 0$. Pour $w \in K_{i+1} \cap D$, nous écrivons $w = ny + z$ avec

1. **NdT.** La condition de cohérence est invisible en mathématiques classiques pour lesquelles tout module sur un anneau noethérien est cohérent.

2. **NdT.** Le transporteur $\langle x_1, \ldots, x_i\rangle : x_{i+1}$ dans G/D est un sous-groupe de type fini de $\mathbb{Z}$, donc de la forme $d\mathbb{Z}$ pour un $d \geqslant 0$. Si $d = 0$ on est dans le premier cas. Si $d = 1$ on peut supprimer x_{i+1}, ou le remplacer par 0. Si $d > 1$, on le décompose en facteurs premiers et on utilise cette décomposition pour remplacer x_{i+1} par une suite finie d'éléments $a_k x_{i+1} = x_{k,i+1}$. Par exemple si $d = 45$, on utilisera $(x_{1,i+1}, x_{2,i+1}, x_{3,i+1}) = (9x_{i+1}, 3x_{i+1}, x_{i+1})$: $5x_{1,i+1} \in \langle x_1, \ldots, x_i\rangle + D$, $3x_{2,i+1} \in \langle x_{1,i+1}\rangle$ et $3x_{3,i+1} \in \langle x_{2,i+1}\rangle$.

$z \in K_i$. Donc $ny = w - z \in D + K_i$. Mais $py \in K_i$, donc si $(p, n) = 1$, alors $y \in K_i + D$, et $x_{i+1} \in K_i + D$ contrairement à notre hypothèse. Par suite p divise n, donc $ny \in K_i$ et ainsi $w \in K_i \cap D = 0$. □

Nous pouvons utiliser le théorème 2.1 pour obtenir un théorème de structure pour les groupes dénombrables cohérents divisibles.

Théorème 2.2. *Soit G un groupe dénombrable cohérent divisible. Alors G est une somme directe dénombrable de sous-groupes isomorphes à $\mathbb{Q}$ ou à $\mathbb{Z}(p^\infty)$ pour des nombres premiers p.*

Démonstration. Soit T le sous-groupe de torsion de G. Le groupe G/T est cohérent parce que, comme G est cohérent, les sous-groupes de type fini de G sont des sommes directes de groupes cycliques finis ou infinis. Donc le théorème 2.1 dit que nous pouvons écrire $G = T \oplus F$, avec F sans torsion. Il suffit donc de démontrer le théorème dans les cas où G est de torsion, ou sans torsion.

Si G est sans torsion et divisible, alors G admet une unique structure de $\mathbb{Q}$-espace vectoriel, donc tout élément non nul de G est contenu dans un unique sous-groupe de G isomorphe au groupe additif de $\mathbb{Q}$. Soit $x_0, x_1, \ldots$ une énumération de G. Définissons un sous-ensemble détachable S de $\mathbb{N}$ en posant $i \in S$ si x_i n'est pas dans l'espace vectoriel engendré par $x_0, \ldots, x_{i-1}$; ceci est décidable parce que G est cohérent. On voit facilement que G est la somme directe des sous-espaces $\mathbb{Q}x_i \simeq \mathbb{Q}$ pour $i \in S$.

Si G est de torsion, alors G est la somme directe de ses composantes primaires G_p, donc nous pouvons supposer que G est un p-groupe [1]. Il suffit alors de démontrer que tout élément d'un p-groupe discret divisible est contenu dans un sous-groupe isomorphe à $\mathbb{Z}(p^\infty)$; nous pouvons ensuite appliquer le théorème 2.1 de manière répétée. Étant donné un tel élément x, nous pouvons construire une suite $x = y_0, y_1, \ldots$ telle que $py_{i+1} = y_i$ pour tout i. Le sous-groupe engendré par les y_i est le sous-groupe recherché. □

Un sous-groupe A d'un groupe abélien discret B est **essentiel** si pour tout élément b non nul de B il existe un $n \in \mathbb{Z}$ tel que nb est un élément non nul de A ; en particulier, B/A est de torsion (mais ce n'est pas suffisant). Une **enveloppe divisible** [2] d'un groupe abélien discret A est un groupe abélien discret divisible B qui contient A comme sous-groupe essentiel.

Théorème 2.3. *Tout groupe abélien dénombrable discret a une enveloppe divisible dénombrable discrète.*

Démonstration. Nous pouvons supposer que le groupe est de la forme F/K, avec F groupe abélien libre de rang dénombrable, et K un sous-groupe détachable de

1. **NdT.** Un groupe fini est appelé p-groupe si son ordre est une puissance de p. Une définition plus générale est donnée au début de la section 3.
2. **NdT.** Divisible hull.

F. Nous notons $\mathbb{Q}F = \mathbb{Q} \otimes F$ et nous construisons un sous-groupe dénombrable N de $\mathbb{Q}F$ comme suit. Tout d'abord on note que si A est un sous-groupe de type fini de $\mathbb{Q}F$, alors $A \cap F$ est de type fini, car A et les éléments de la base de F qui interviennent peuvent être mis dans un sous-groupe libre de rang fini de $\mathbb{Q}F$. Soit $a_0, a_1, \ldots$ une énumération de $\mathbb{Q}F$; nous posons

$$N_0 = 0$$
$$N_{i+1} = \begin{cases} N_i + \mathbb{Z}a_i & \text{si } (N_i + \mathbb{Z}a_i) \cap F \subseteq K, \\ N_i & \text{sinon.} \end{cases}$$

La décision pour savoir si l'on doit mettre a_i dans N_{i+1} est possible parce que $N_i + \mathbb{Z}a_i$ est de type fini.

On pose $N = \bigcup_i N_i$ et $D = \mathbb{Q}F/N$. Le sous-groupe N est détachable dans $\mathbb{Q}F$ parce que $a_i \in N$ si, et seulement si, $(N_i + \mathbb{Z}a_i) \cap F \subseteq K$; donc D est discret. Clairement $N \cap F = K$, de sorte que nous pouvons voir F/K comme un sous-groupe de $\mathbb{Q}F/N = D$. Enfin, si $a_i \in \mathbb{Q}F \setminus N$ est un élément non nul de D, il existe un $x \in N_i$ et un $n \in \mathbb{Z}$ tels que $x + na_i \in F \setminus K$. Donc na_i est égal à un élément non nul de F/K. □

L'enveloppe divisible d'un groupe abélien dénombrable discret *cohérent* est un groupe cohérent. En fait, on a le résultat plus général suivant.

Théorème 2.4. *Soient $A \subseteq B$ des groupes abéliens discrets. Si B/A est un groupe de torsion, et si A est cohérent, alors B est cohérent.*

Démonstration. Nous montrons d'abord que si B/A est de torsion et si A est de présentation finie, alors B est discret. Étant donné $b \in B$, on a un $n \neq 0$ tel que $nb \in A$. Si $nb \notin nA$ (décidable car A est de présentation finie), alors $b \notin A$. Si $nb = na$ pour un $a \in A$, alors il suffit de décider si $b - a \in A$ ou non. Mais il y a seulement un nombre fini d'éléments de torsion dans A.

Dans le cas général, soit φ un homomorphisme d'un groupe abélien libre de rang fini F vers B. On a un $n \neq 0$ tel que $\varphi(nF) \subseteq A$. Le groupe $B/\varphi(nF)$ est discret, d'après le premier cas, et $A/\varphi(nF)$ est cohérent d'après le théorème III.2.5 ; donc les hypothèses du théorème sont satisfaites dans la situation $A/\varphi(nF) \subseteq B/\varphi(nF)$. Si $B/\varphi(nF)$ est cohérent, il en va de même pour B d'après le théorème III.2.5, donc nous pouvons supposer que $\varphi(nF) = 0$. Mais F/nF est fini et B est discret, donc le morphisme induit de F/nF vers B a un noyau fini, et le noyau de φ est de type fini. □

Exercices

1. Montrer que tout groupe de torsion est égal à la somme directe de ses sous-groupes p-primaires.

2. Montrer que tout sous-groupe de type fini de $\mathbb{Z}(p^\infty)$ est cyclique, que les sous-groupes de type fini de $\mathbb{Z}(p^\infty)$ forment une chaine pour l'inclusion, et que pour tout n il existe un sous-groupe fini cyclique de $\mathbb{Z}(p^\infty)$ d'ordre p^n. Montrer que tout groupe G qui satisfait ces conditions est isomorphe à $\mathbb{Z}(p^\infty)$.
3. Soit a une suite binaire fugitive, et soit H le sous-$\mathbb{Q}$-espace de $\mathbb{Q}$ engendré par $\{\, a_n : n = 1, 2, \ldots\}$. Montrer que H est un exemple brouwerien d'un sous-groupe dénombrable divisible de $\mathbb{Q}$, en fait une somme directe dénombrable de copies de $\mathbb{Q}$, qui n'est pas un facteur direct. Pourquoi le théorème 2.1 ne s'applique-t-il pas ?
4. Trouver deux endroits où l'axiome du choix dépendant est utilisé dans la démonstration du théorème 2.2, autres que (de manière indirecte) l'appel au théorème 2.1.
5. Soit G un p-groupe discret divisible, et soit X une base de $\{\, x \in G : px = 0\,\}$, vu comme espace vectoriel sur le corps $\mathbb{F}_p$. Pour tout $x \in X$, construire une suite $x = y_0, y_1, \ldots$ telle que $py_{i+1} = y_i$, et soit A_x le sous-groupe de G engendré par les y_i. Montrer que chaque A_x est isomorphe à $\mathbb{Z}(p^\infty)$, et que G est somme directe des sous-groupes A_x.
6. Construire un exemple brouwerien d'un groupe abélien dénombrable entre $\mathbb{Z}$ et $\mathbb{Q}$ qui n'est détachable dans aucune enveloppe divisible.

3 Fonctions de hauteur sur les p-groupes

Soit G un groupe abélien et p un nombre premier. Nous disons que G est un **p-groupe** si pour chaque $x \in G$ il y a un entier $n > 0$ tel que $p^n x = 0$. Un point important dans la théorie des groupes abéliens est la classification des p-groupes dénombrables au moyen des dimensions de certains espaces vectoriels définis en termes de la notion de *hauteur*. Si $x \in G$, rappelons que la p-hauteur de x est l'entier naturel n lorsque $x \in p^n G$ et $x \notin p^{n+1}G$. Nous avons déjà vu qu'il peut y avoir des problèmes pour calculer les hauteurs dans les groupes sans torsion. En outre, pour obtenir un théorème de classification pour les p-groupes dénombrables, nous devons étendre la notion de hauteur à des valeurs transfinies.

Soit G un groupe abélien, p un nombre premier, λ un ordinal et $\lambda_\infty = \lambda \cup \{\infty\}$. Une **fonction de p-hauteur** sur G est une fonction surjective h de G sur λ_∞ qui satisfait les propriétés suivantes.

(i) On a $hpx \geqslant hx$ pour tout x ; de plus, si $hx < \infty$, alors $hpx > hx$.

(ii) Si $(m, p) = 1$, alors $hmx = hx$.

(iii) Si $a < hx$ ou si $a = hx = \infty$, il existe un y tel que $py = x$ et $a \leqslant hy$.

L'ordinal λ est appelé la **p-longueur** de G. Notez que (i) implique que $h0 = \infty$. Lorsque $hx = \infty$ implique $x = 0$ nous disons que G est **p-réduit**. Si G est un p-groupe, alors (i) et (ii) impliquent que si q est un nombre premier autre que p, la q-hauteur de tout élément de G est ∞ ; dans ce cas nous laissons tomber le préfixe « p » dans « p-hauteur » et « p-longueur ». Une telle fonction de hauteur est unique ; en fait, λ et h sont tous deux des invariants de (la classe d'isomorphisme de) G au sens suivant.

Théorème 3.1. *Soient G et G' des groupes abéliens avec des fonctions de p-hauteur h et h' et des p-longueurs λ et λ' respectivement. Soit $\varphi\colon G \to G'$ un isomorphisme. Alors il existe un isomorphisme $\rho\colon \lambda_\infty \to \lambda'_\infty$ tel que $h'\varphi = \rho h$.*

Démonstration. Nous disons que ρ **est défini en** a si chaque fois que $x, y \in G$ avec $hx = hy = a$, on a $h'\varphi x = h'\varphi y$. Si ρ est défini en a, nous posons $\rho a = h'\varphi x$ pour tout x tel que $hx = a$. Définissons $[0, a] = \{\, b \in \lambda : b \leqslant a \,\}$ et

$$S = \{\, a \in \lambda : \rho \text{ est défini en tout élément de } [0, a] \\ \text{et, restreint à } [0, a], \text{ c'est un plongement} \,\}$$

Nous allons montrer que $S = \lambda$. Supposons que $a \in S$ pour tout $a < b$. Si $hx = b$, nous allons voir que

(i) si $a < b$, alors $\rho a < h'\varphi x$,

(ii) si $c < h'\varphi x$, alors il y a un $a < b$ tel que $\rho a = c$.

Ceci montrera que $b \in S$; donc S est héréditaire, d'où $S = \lambda$.

Pour montrer (i), on suppose que $a < b$. Comme h est une fonction de hauteur, il y a un z tel que $a \leqslant hz < b$ et $pz = x$. Donc $p\varphi z = \varphi x$ et $h'\varphi z = \rho h z \geqslant \rho a$. Ainsi $\rho a < h'\varphi x$.

Pour montrer (ii), on suppose que $c < h'\varphi x$. Comme h' est une fonction de hauteur, il existe un z tel que $h'z \geqslant c$ et $pz = \varphi x$. Alors $p\varphi^{-1}z = x$, donc $h\varphi^{-1}z = d < b = hx$. Par suite $h'z = h'\varphi\varphi^{-1}z = \rho h\varphi^{-1}z = \rho d$ et ρ est un plongement sur $[0, d]$. Il existe donc un $a \leqslant d < b$ tel que $\rho a = c$.

Comme $S = \lambda$, la fonction ρ est un *plongement* (définition page 27) de λ dans λ'. De la même manière nous obtenons un plongement de λ' dans λ. Leur composition est un plongement de λ (ou de λ') dans lui-même, donc c'est l'identité d'après le théorème I.6.5. Enfin nous posons $\rho\infty = \infty$. □

Pour illustrer le type de structure que nous traitons, considérons l'exemple le plus simple d'un p-groupe abélien qui possède des éléments d'une hauteur transfinie autre que ∞. Ce groupe est construit en imposant aux générateurs $x_0, x_1, \ldots$ les relations $px_0 = 0$, et $p^n x_n = x_0$ pour $n > 0$.

Exemple 3.2. Soit F le groupe abélien libre sur l'ensemble discret $\{\, x_n : n \in \mathbb{N} \,\}$. Soit P le quotient de F par le sous-groupe R de F engendré par

les éléments px_0, $px_1 - x_0$, $p^2x_2 - x_0$, ... Un exercice facile établit que R est une partie détachable de F, que P est donc discret, et que tout élément de P a un **représentant canonique** dans F de la forme $\sum n_i x_i$ avec $0 \leqslant n_0 < p$ et $0 \leqslant n_i < p^i$ pour $i > 0$. Clairement, P est un p-groupe.

Soit λ l'ensemble bien ordonné $\{0, 1, 2, \ldots, \omega\}$. On définit une fonction h de P vers λ_∞ comme suit. Soit $\sum n_i x_i$ le représentant canonique de l'élément $y \in P$. On définit $h(y) = \infty$ si tous les n_i sont nuls ; on prend $h(y) = \omega$ si n_0 est l'unique n_i non nul ; sinon, on prend $h(y) = \min\{ v_p n_i : i \neq 0 \}$, où $v_p m$ est l'exposant de p dans la décomposition de m en facteurs premiers. On vérifie facilement que h est une fonction de hauteur sur P. □

Le théorème suivant montre que les homomorphismes augmentent (faiblement) les hauteurs, dans la mesure où l'on peut donner un sens à cette affirmation.

Théorème 3.3. *Soient G et H des groupes avec des fonctions de p-hauteur et dont les longueurs sont des segments initiaux d'un même ordinal λ. Si φ est un homomorphisme de G vers H, alors $h\varphi x \geqslant hx$ pour tout $x \in G$.*

Démonstration. Posons $S = \{ a \in \lambda : h\varphi x \geqslant a \text{ si } hx = a \}$, et supposons que $a \in S$ pour tout $a < b$. Si $hx = b$ et $h\varphi x < b$, alors $x = py$ pour un y tel que $hy \geqslant h\varphi x$. Comme $b = hx = hpy > hy$, nous avons $h\varphi y \geqslant hy$. Mais $h\varphi x = hp\varphi y > h\varphi y$, donc $hy > h\varphi y$, une contradiction. Donc $S = \lambda$.

Maintenant posons $S = \{ a \in \lambda : h\varphi x > a \text{ si } hx = \infty \}$, et supposons que $a \in S$ pour tout $a < b$. Si $hx = \infty$, alors il existe un y tel que $hy = \infty$ et $py = x$. Si $h\varphi y \geqslant b$, alors $h\varphi x > b$, donc nous avons montré que $b \in S$. Sinon, $h\varphi y = a < b$, ce qui conduit à une contradiction $h\varphi y > a$ car $a \in S$. Donc $S = \lambda$. □

Jusqu'à maintenant, la seule interaction entre une fonction de p-hauteur sur un groupe et la structure additive du groupe que nous ayons considérée concerne les relations entre hmx et hx. Nous examinons maintenant la relation fondamentale entre hauteur et addition.

Théorème 3.4. *Soit h une fonction de p-hauteur sur un groupe G. On a*

$$h(x + y) \geqslant \min(hx, hy)$$

pour tous $x, y \in G$, avec égalité lorsque $hx \neq hy$.

Démonstration. Soit λ la longueur de G, et soit S l'ensemble des $b \in \lambda$ pour lesquels $h(x_1 + x_2) \geqslant b$ chaque fois que $b \leqslant hx_1, hx_2$. Nous allons montrer que si $a \in S$ pour tout $a < b$, alors $b \in S$. Supposons au contraire que

$$a = h(x_1 + x_2) < b \leqslant hx_1, hx_2.$$

Alors $x_1 = py_1$ et $x_2 = py_2$ avec $hy_1 \geqslant a$ et $hy_2 \geqslant a$ d'après la condition (iii) sur la fonction de p-hauteur. Posons $z = y_1 + y_2$. On a $hz < \infty$ car $hpz < \infty$ et donc

$$a = hpz > hz.$$

Or $a \in S$ et donc $hz \geqslant a$. Contradiction. On vient de prouver $S = \lambda$. Si hx_1 ou $hx_2 < \infty$ on a terminé avec $b = \min(hx_1, hx_2)$.
Si $hx = hy = \infty$, on obtient $h(x + y) \geqslant b$ pour tout $b \in \lambda$. Comme λ_∞ est discret, et comme tout élément b de λ est de la forme $hz < hpz$, cela implique $h(x + y) = \infty$.
Il reste à démontrer la dernière affirmation. Si $hx < hy$, alors

$$hx = h((x + y) + (-y)) \geqslant \min(h(x + y), hy),$$

donc $hx \geqslant h(x + y)$, et $hx = h(x + y)$. □

Comme conséquence du théorème 3.4, pour tout $a \in \lambda$, l'ensemble $\{\, x \in G : hx \geqslant a \,\}$ est un sous-groupe de G.

Exercices

1. Soit p un nombre premier et G un groupe abélien fini. Montrer que G possède une fonction de p-hauteur. Quelle est la p-longueur de G (en termes des invariants dans la section V.3) ?
2. Soit G un groupe avec une fonction de p-hauteur h. Montrer que $h^{-1}(\infty)$ est un sous-groupe p-divisible de G qui contient tout sous-groupe p-divisible de G.
3. Soit $G = A \oplus B$ un groupe abélien avec une fonction de p-hauteur h_G. Montrer que A possède une fonction de p-hauteur qui est égale à la restriction de h_G à A, et que la p-longueur de A est un segment initial de la p-longueur de G.
4. Donner un exemple d'un p-groupe abélien G avec une fonction de p-hauteur, et un sous-groupe A de G tels que A possède une fonction de p-hauteur, alors que la fonction de p-hauteur sur G ne se restreint pas en une fonction de p-hauteur sur A.
5. Vérifier les affirmations concernant le p-groupe P dans l'exemple 3.2.
6. Soit a une suite binaire. Soit G le sous-groupe du groupe P de l'exemple 3.2 engendré par les éléments $a_n x_n$. Montrer que G est un p-groupe dénombrable discret avec une fonction de hauteur. Quelle est la longueur de G ?

4 Le théorème d'Ulm

On considère un nombre premier fixé p. Si G est un p-groupe dénombrable avec une fonction de hauteur h, alors le sous-groupe $D = h^{-1}(\infty)$ est un sous-groupe dénombrable divisible détachable de G, et G/D est un p-groupe, par conséquent cohérent. D'après le théorème 2.1, nous obtenons $G = D \oplus R$, avec D un groupe dénombrable cohérent divisible, donc de structure connue (théorème 2.2), et R un p-groupe dénombrable réduit avec une fonction de hauteur. Nous sommes ainsi amenés à étudier de tels groupes R, que nous appelons des **groupes d'Ulm**. Les p-groupes finis sont clairement des groupes d'Ulm. Le théorème suivant montre comment construire de nombreux groupes d'Ulm plus grands.

Théorème 4.1. *Pour tout ordinal λ, il existe un p-groupe réduit avec une fonction de hauteur, et de longueur λ. En particulier, pour tout ordinal dénombrable λ, il existe un groupe d'Ulm de longueur λ.*

Démonstration. Soit F le groupe abélien libre construit sur les suites finies $\sigma = (a_1, \dots, a_n)$ d'éléments de λ telles que $a_1 < a_2 < \cdots < a_n$ avec $n \geqslant 1$. Soit K le sous-groupe de F engendré par les éléments de la forme

$$p(a_1), \text{ et } \ p(a_1, a_2, \dots, a_n) - (a_2, \dots, a_n) \text{ pour } n > 1,$$

et soit G le groupe quotient F/K. Nous disons qu'un élément de F est **en forme standard** si on peut l'écrire $\sum n_i \sigma_i$, où les σ_i sont des générateurs libres distincts de F, et $0 \leqslant n_i < p$. Tout élément de G provient d'un unique élément de F en forme standard : vu la nature des générateurs de K il est clair qu'on peut trouver un tel élément ; qu'un tel élément soit unique résulte du fait que tout élément non nul $\sum k_i \sigma_i$ de K a une coordonnée non nulle k_i divisible par p. On définit $h\colon G \to \lambda_\infty$ en prenant pour hx le plus petit élément de λ qui apparait dans une suite ayant un coefficient non nul dans la forme standard de x, et $hx = \infty$ si $x = 0$. On voit facilement que h est une fonction de hauteur réduite sur G pour laquelle G est de longueur λ. Clairement G est un groupe d'Ulm si λ est un ordinal dénombrable. □

Un système complet d'invariants pour les groupes d'Ulm est fourni par certains espaces vectoriels dénombrables discrets sur le corps à p éléments $\mathbb{F}_p$, que l'on appellera les *invariants d'Ulm*. Il est utile de définir ces invariants dans le cadre plus général des groupes valués.

Définition 4.2. Un **p-groupe valué** est un p-groupe H avec un ordinal λ et une fonction $v\colon H \to \lambda_\infty$ qui satisfait les propriétés suivantes.

(i) Si $vx < \infty$, alors $vx < vpx$.

(ii) Si $(p, m) = 1$, alors $vmx = vx$.

(iii) $v(x+y) \geqslant \min(vx, vy)$.

La fonction v sera appelée la **valuation** du p-groupe valué. Nous dirons que H (ou v) est **réduit(e)** si $v^{-1}(\infty) = 0$.

Un p-groupe valué typique est donné par un sous-groupe H d'un p-groupe avec une fonction de hauteur h : la fonction v est la restriction de h à H. Tout p-groupe avec une fonction de hauteur h est un groupe valué pour $v = h$. Si λ est un ordinal et si a, b sont des éléments de λ_∞, nous écrivons $a \ll b$ si $a < b = \infty$ ou s'il existe un c tel que $a < c < b$. Notons que si $vx > a$, alors $vpx \gg a$.

Définition 4.3. Soit H un p-groupe valué à valeurs dans l'ordinal λ. Pour chaque $a \in \lambda$ nous définissons le a-ième **invariant d'Ulm** de H comme le groupe

$$f_H(a) = \frac{\{\, x \in H : vx \geqslant a \text{ et } vpx \gg a \,\}}{\{\, x \in H : vx > a \,\}}.$$

La fonction f_H est appelée la **fonction d'Ulm** de H. Notons que $f_H(a)$ est un espace vectoriel discret sur le corps $\mathbb{F}_p$.

Un espace vectoriel dénombrable discret sur un corps fini a une base dénombrable, donc un invariant d'Ulm d'un groupe d'Ulm est déterminé par sa dimension, qui est la cardinalité d'un certain sous-ensemble détachable de $\mathbb{N}$. En mathématiques classiques, les invariants d'Ulm sont pensés comme des éléments de $\mathbb{N} \cup \{\infty\}$. Une vertu de notre définition des invariants comme des espaces vectoriels est d'en faire des foncteurs additifs.

Si H est un groupe cyclique fini d'ordre p^n et si v est la fonction de hauteur, alors la longueur de H est $\{0, 1, \ldots, n-1\}$ et $\dim f_H(n-1) = 1$, tandis que $f_H(a) = 0$ pour $a < n-1$. Les invariants d'Ulm sont clairement additifs en ce sens que si G est une somme directe d'une famille de sous-groupes $H(i)$, alors $f_G(a)$ est la somme directe des espaces vectoriels $f_{H(i)}(a)$. Comme tout p-groupe fini est une somme directe finie de p-groupes cycliques, les invariants d'Ulm fournissent un système complet d'invariants pour les p-groupes finis ; plus généralement, ils fournissent un système complet d'invariants pour les sommes directes de p-groupes cycliques finis.

Nous abordons maintenant la preuve du théorème d'Ulm : un groupe d'Ulm est déterminé à un isomorphisme près par ses invariants d'Ulm. Si H est un sous-groupe d'un groupe d'Ulm G et si $x \in G$, nous disons que x est H**-propre** si x est de hauteur maximum parmi les éléments de $x + H$.

Théorème 4.4 (théorème d'Ulm)**.** *Soient G et G' des groupes d'Ulm de longueur λ avec des invariants d'Ulm isomorphes, et soit φ un isomorphisme préservant les hauteurs d'un sous-groupe fini H de G sur un sous-groupe fini H' de G'. Alors φ se prolonge en un isomorphisme de G sur G'.*

Démonstration. Soit $x_1, x_2, \dots$ une énumération de G telle que px_i est dans le sous-groupe engendré par $x_1, \dots, x_{i-1}$ pour chaque i [1], et soit $x'_1, x'_2, \dots$ une énumération de G' du même type. Nous allons construire des suites de sous-groupes finis $H_1 \subseteq H_2 \subseteq \cdots$ de G, et $H'_1 \subseteq H'_2 \subseteq \cdots$ de G', et des isomorphismes préservant les hauteurs $\varphi_n \colon H_n \to H'_n$, telles que $x_n \in H_{2n-1}$ et $x'_n \in H'_{2n}$, et de façon à ce que φ_{n+1} prolonge φ_n. Par symétrie, il suffit de montrer que si φ est un isomorphisme préservant les hauteurs entre un sous-groupe fini H de G et un sous-groupe fini H' de G', et si $x \in G$ et $px \in H$, alors φ peut être prolongé en un isomorphisme préservant les hauteurs défini sur le sous-groupe $H + \langle x \rangle$ [2].

Si $x \in H$, il n'y a rien à faire. Sinon, en prenant un élément de hauteur maximum dans l'ensemble fini $x + H$, nous pouvons supposer que x est H-propre. Parmi de tels x, on en prend un qui maximise hpx. Notez que $h(x+z) = \min(hx, hz)$ pour tout $z \in H$ parce que x est H-propre. On note $a = hx$. Nous devons définir φx.

Comme $h'\varphi px = hpx > a$, nous pouvons trouver un $x' \in G'$ tel que $h'x' \geqslant a$ et $px' = \varphi px$. Si $h'x' = a$, et si x' est H'-propre (notez que ces questions sont décidables), alors nous pouvons prolonger φ en posant $\varphi x = x'$. Si $h'x' = a$ mais x' n'est pas H'-propre, alors il existe un $z \in H$ tel que

$$h'(x' + \varphi z) > a,$$

donc $h'(px' + \varphi pz) \gg a$, et donc $h(px + pz) \gg a$. Mais $h(x + z) \geqslant a$, car $hz = h'\varphi z = a$, donc $x + z$ est H-propre. Ainsi, vu notre choix de x, nous avons $hpx \geqslant h(px + pz)$, donc $hpx \gg a$. Enfin, si $h'x' > a$, nous avons aussi $hpx = h'px' \gg a$.

Nous examinons maintenant le cas où $hpx \gg a$, et donc $x \in f_G(a)$, mais, x étant H-propre, $x \notin f_H(a) \subseteq f_G(a)$. Il nous faut trouver un élément $x'_* \in f_{G'}(a)$ qui n'est pas dans $f_{H'}(a)$. Soit σ un isomorphisme de $f_G(a)$ vers $f_{G'}(a)$. Notez que l'ensemble fini $f_{H'}(a)$ est un sous-espace détachable de l'espace discret $f_{G'}(a)$. Si $\sigma x \notin f_{H'}(a)$, nous avons terminé. Sinon, en appliquant de manière répétée φ^{-1} et σ, nous pouvons trouver un sous-espace fini V de $f_H(a)$ tel que $\sigma x \in \varphi V = \sigma V$, ou trouver l'élément x'_* que nous cherchons. Mais si $\sigma x \in \sigma V$, alors $x \in V$, ce qui contredit le fait que $x \notin f_H(a)$. Ainsi nous obtenons l'élément x'_* recherché.

Nous pouvons prendre x'_* de sorte que $px'_* = 0$. De plus, x'_* est H'-propre, car si $h'(x'_* + z') > a$, et donc $h'z' = a$, alors

$$h'pz' \geqslant \min(h'p(x'_* + z'), h'px'_*) \gg a,$$

donc $z' \in f_{H'}(a)$, et $x'_* = -z'$ comme éléments de $f_{G'}(a)$, une contradiction.

1. **NdT.** L'élément x_1 doit être d'ordre p, et par exemple tout x d'ordre p^k peut être précédé par $p^{k-1}x, \dots, px$ dans l'énumération.

2. **NdT.** Ce résultat, appliqué aux H_n et H'_n successifs, permettra de construire par récurrence les isomorphismes φ_n.

On pose $\varphi x = x'_* + x'$, où $px' = \varphi px$ et $h'x' \geqslant a$, en notant que $x'_* + x'$ est H'-propre parce que x'_* l'est. □

Nous utilisons maintenant le théorème d'Ulm pour démontrer le théorème de Prüfer qui caractérise les sommes directes dénombrables de p-groupes cycliques finis.

Théorème 4.5 (Prüfer)**.** *Un p-groupe dénombrable discret G est une somme directe de p-groupes cycliques finis si, et seulement si, p^nG est détachable pour chaque $n \in N$ et $G \setminus \{0\} = \bigcup_{n\in\mathbb{N}} p^nG \setminus p^{n+1}G$.*

Démonstration. Comme les p-groupes cycliques finis G ont les propriétés demandées, il en va de même pour leurs sommes directes. Inversement, si les propriétés demandées sont satisfaites, nous pouvons définir une fonction de hauteur sur G en posant $hx = n$ si $x \in p^nG \setminus p^{n+1}G$, et $h0 = \infty$. Nous pouvons alors construire une somme directe dénombrable de p-groupes cycliques finis avec les mêmes invariants d'Ulm que G. D'après le théorème d'Ulm, G est isomorphe à ce groupe, donc est une somme directe de p-groupes cycliques finis. □

Un corolaire immédiat du théorème 4.5 est que les p-groupes finis sont des sommes directes de groupes cycliques.

Exercices

1. Une **forêt de torsion** est un ensemble discret X avec un sous-ensemble détachable R et une fonction $\pi\colon X \setminus R \to X$ telle que pour chaque $x \in X$ il existe un n tel que $\pi^n x \in R$. Définir ce qu'est une fonction de hauteur sur une forêt de torsion (X, R, π). Soit $S(X, R, \pi)$ (abrégé en $S(X)$) le groupe abélien libre sur X modulo les relations $px = 0$ si $x \in R$, et $px = \pi x$ si $x \notin R$. Montrer que $S(X)$ est un p-groupe discret, et que si X admet une fonction de hauteur, il en va de même pour $S(X)$. Quel est l'ensemble X dans la démonstration du théorème 4.1 ? Les groupes de la forme $S(X)$ pour des (X, R, π) qui admettent une fonction de hauteur sont appelés des **p-groupes simplement présentés**. Montrer que tout p-groupe fini est simplement présenté.
2. Soit e le générateur d'un groupe cyclique fini H d'ordre p^3, et soit v la valuation sur H telle que $ve = 0$, $vpe = 2$, et $vp^2e = 3$. Quels sont les invariants d'Ulm de H ? Plonger H dans un groupe G de façon à ce que la valuation sur H soit la restriction de la fonction de hauteur sur G, et que les invariants d'Ulm de H et G soient isomorphes.
3. Quels sont les invariants d'Ulm du groupe dans l'exemple 3.2 ?
4. Soit $\lambda = \{0, 1, 2, 3\}$. Quels sont les invariants d'Ulm du groupe d'Ulm de longueur λ construit dans la démonstration du théorème 4.1 ?

5. La formulation classique du théorème 4.5 met $\bigcap_{n\in\mathbb{N}} p^nG = 0$ à la place de $G \setminus \{0\} = \bigcup_{n\in\mathbb{N}} p^nG \setminus p^{n+1}G$. Montrer que cette version modifiée du théorème 4.5 est équivalente au principe de Markov.
6. Construire un exemple brouwerien d'un groupe d'Ulm de longueur $\lambda \subseteq \{0,1\}$ qui n'est pas une somme directe de groupes cycliques. Montrer qu'un groupe d'Ulm de longueur λ est une somme directe de groupes cycliques si, et seulement si, $\lambda \leqslant \omega$ (i.e. il existe un plongement de λ dans ω).
7. Un sous-groupe H d'un p-groupe G est **pur** si $p^nH = H \cap p^nG$ pour tout $n \in \mathbb{N}$. Utiliser le théorème 4.4 pour montrer qu'un sous-groupe pur d'un p-groupe fini est un facteur direct.
8. Soient G un groupe d'Ulm et $x, y \in G$ des éléments d'ordre p. Montrer que $hx = hy$ si, et seulement si, il y a un automorphisme de G qui envoie x sur y.

5 Construction de groupes d'Ulm

Cela simplifie grandement les choses d'imposer une condition modérée sur la longueur de G. Soit λ un ensemble bien ordonné. Si $a < b$ dans λ, nous disons que b est le **successeur** de a, et nous écrivons $b = a + 1$, s'il n'y a aucun $c \in \lambda$ tel que $a < c < b$. Pour un entier naturel n, nous définissons $b = a + n$ par récurrence sur n en posant $a + 0 = a$, et $a + (n + 1) = c$ si $b = a + n$ et $c = b + 1$ [1]. On dit qu'un ensemble bien ordonné λ **admet des successeurs** si chaque fois que l'on a a, b dans λ avec $b > a$, alors $a + 1$ existe [2].

Soit f une fonction qui assigne à tout élément d'un ordinal dénombrable avec successeurs un espace vectoriel dénombrable discret sur $\mathbb{F}_p$. Quand pouvons-nous construire un groupe d'Ulm G tel que $f_G = f$? Une condition nécessaire est donnée dans le théorème suivant.

Théorème 5.1. *Soient λ un ordinal avec successeurs et G un groupe d'Ulm de longueur λ. Si $a \in \lambda$, nous pouvons trouver un entier naturel n tel que $a + n$ existe et $f_G(a + n) \neq 0$.*

Démonstration. On prend un x tel que $hx = a$ et pour n le plus petit entier naturel tel que $hp^{n+1}x = \infty$ ou $hp^{n+1}x > hp^nx + 1$. Alors p^nx représente un élément non nul de $f_G(a + n)$. □

Soient λ un ordinal dénombrable avec successeurs et f une fonction qui assigne à tout élément d'un ordinal dénombrable avec successeurs un espace

1. **NdT.** On voit facilement que les deux définitions de l'égalité « $b = a + 1$ » coïncident.
2. **NdT.** L'énoncé « $a + n$ existe » est une abréviation pour « il existe un b dans λ tel que $b = a + n$ ».

vectoriel dénombrable discret sur $\mathbb{F}_p$. Nous disons que f est une **U-fonction** si, pour tout $a \in \lambda$, il existe un $n \in \mathbb{N}$ tel que $a+n$ existe et $f(a+n) \neq 0$. Le théorème 5.1 dit qu'une fonction d'Ulm d'un groupe d'Ulm dont la longueur est un ordinal avec successeurs, est une U-fonction. Nous allons montrer que, réciproquement, si f est une U-fonction sur λ, alors nous pouvons construire un groupe d'Ulm G de longueur λ tel que $f_G(a)$ est isomorphe à $f(a)$ pour chaque $a \in \lambda$. Ce résultat est connu sous le nom de **théorème de Zippin**.

Soit H un p-groupe réduit valué à valeurs dans un ordinal dénombrable avec successeurs λ. Soit f une U-fonction sur λ. Nous disons que H est **f-admissible** si nous pouvons immerger $f_H(a)$ comme sous-espace de $f(a)$ pour tout $a \in \lambda$. Cette condition est certainement nécessaire pour immerger H comme sous-groupe d'un groupe ayant une fonction d'Ulm f qui prolonge la valuation sur H. Il se trouve que c'est aussi suffisant lorsque H est fini ; le cas $H = 0$ est le théorème de Zippin. La construction clé consiste à agrandir un groupe fini valué f-admissible en un groupe fini valué f-admissible dans lequel une instance donnée de la propriété (iii) d'une fonction de hauteur est satisfaite.

Lemme 5.2. *Soit H un p-groupe fini valué réduit à valeurs dans λ_∞ pour un ordinal avec successeurs λ. Soient f une U-fonction sur λ et $\varphi^c\colon f_H(c) \to f(c)$ des fonctions injectives pour chaque $c \in \lambda$. Étant donnés $x \in H$ et $a < vx = b$, nous pouvons construire un p-groupe valué fini K qui contient H et tel que les propriétés suivantes soient satisfaites :*

(i) *la valuation sur K prolonge celle sur H ;*

(ii) *les fonctions φ^c se prolongent en des fonctions injectives de $f_K(c)$ vers $f(c)$;*

(iii) *il existe un $y \in K$ tel que $py = x$ et $vy \geqslant a$.*

Démonstration. En faisant croitre a, si nécessaire, nous pouvons supposer que $b = a+1$, ou que $f(a) \neq 0$ et il n'y a aucun élément $z \in H$ tel que $vz = a$. Nous pouvons également supposer que la valeur de x est maximale dans l'ensemble $\{\, x+pz : z \in H \text{ et } vz \geqslant a \,\}$, car si $py = x+pz$, alors $p(y-z) = x$. On ajoute un élément y à H, soumis à la seule relation $py = x$, et on pose

$$v(z+my) = \min(vz, a)$$

pour $z \in H$ et $0 < m < p$. On vérifie facilement que cela définit un p-groupe valué K qui contient H, dont la valuation prolonge celle sur H. Nous devons maintenant prolonger les fonctions φ^c.

Le plongement $H \subseteq K$ donne des fonctions injectives $f_H(c) \to f_K(c)$ pour chaque $c \in \lambda$. Supposons que $z+my$ représente un élément de $f_K(c)$, avec $z \in H$ et $0 < m < p$. Alors $c = \min(vz, a) \leqslant a$. Comme nous sommes intéressés uniquement par le sous-espace engendré par $z+my$, nous pouvons supposer que $m = 1$. Si $c < a$, alors $z+y = z$ dans $f_K(c)$, donc $z+y$ représente un

élément de $f_H(c)$. Si $c = a$ et $b = a+1$, alors $vp(z+y) > b$, donc $v(pz+x) > vx$, contrairement au choix que nous avons fait pour x. Donc si $c < a$ ou $b = a+1$, alors $f_H(c) = f_K(c)$ et il n'y a pas de problème pour étendre φ^c. Il reste à traiter le cas suivant : $c = a$, il n'y a aucun $z \in H$ tel que $vz = c$, et $f(c) \neq 0$. Alors $f_H(c) = 0$ et $f_K(c)$ est de dimension 1, et nous plongeons ce dernier dans $f(c)$ comme bon nous semble. □

Théorème 5.3. *Soient λ un ordinal dénombrable avec successeurs et f une U-fonction définie sur λ. Soit H un p-groupe fini valué à valeurs dans λ_∞. Si H est f-admissible, alors il peut être plongé dans un groupe d'Ulm G de longueur λ tel que la fonction de hauteur sur G induise la valuation sur H, et que $f_G(a) \simeq f(a)$ pour chaque $a \in \lambda$.*

Démonstration. Si μ est un sous-ensemble fini de λ et si $\varphi^a \colon f_H(a) \to f(a)$ est une fonction injective pour chaque $a \in \lambda$, alors par des applications répétées du lemme 5.2, nous pouvons plonger H dans un p-groupe fini valué $E(H, \mu)$ tel que

(i) la valuation sur $E(H, \mu)$ prolonge la valuation sur H ;

(ii) les fonctions φ^a se prolongent en des fonctions injectives de $f_K(a)$ vers $f(a)$;

(iii) si $a \in \mu$ et si $x \in H$ avec $a < vx$, alors il y a un $y \in E(H, \mu)$ tel que $py = x$ et $vy \geqslant a$.

Nous allons construire une chaine de groupes finis valués $H = H_0 \subseteq H_1 \subseteq \cdots$ avec une même valuation v, et des fonctions injectives

$$\varphi_i^a \colon f_{H_i}(a) \to f(a)$$

telles que φ_{i+1}^a prolonge φ_i^a pour chaque $i \in \mathbb{N}$ et $a \in \lambda$. Soit $x_1, x_2, \ldots$ une énumération de la réunion disjointe de la famille $\{f(a)\}_{a\in\lambda}$ et soit $a_1, a_2, \ldots$ une énumération de λ, et posons $\mu_n = \{a_1, \ldots, a_n\}$. Si $x_n \in f(b)$, on définit

$$H_{2n} = E(H_{2n-1}, \mu_n),$$

$$H_{2n-1} = \begin{cases} H_{2n-2} & \text{si } x_n \in \varphi_{2n-2}^b(f_{H_{2n-2}}(b)), \\ H_{2n-2} \oplus \langle y \rangle & \text{où } py = 0 \text{ et } vy = b \text{ sinon.} \end{cases}$$

Dans le dernier cas, prolongeons la fonction φ_{2n-2}^b en posant $\varphi_{2n-1}^b(y) = x_n$. Alors le groupe $G = \bigcup_j H_j$ est clairement un p-groupe valué dénombrable à valeurs dans λ. Le fait que v est une fonction de hauteur sur G résulte de la construction $H_{2n} = E(H_{2n-1}, \mu_n)$, pourvu que nous puissions montrer que v envoie G sur λ_∞. Cela résulte du fait que f est une U-fonction : si $a \in \lambda$, il existe $m \in \mathbb{N}$ tel que $f(a+m) \neq 0$. D'après la construction de H_{2n-1}, nous pouvons trouver un élément $y_1 \in G$ tel que $vy_1 = a + m$. Si $m = 0$, nous avons terminé. Sinon, d'après la construction de H_{2n}, nous pouvons trouver un élément y_2 de G tel que $a \leqslant vy_2 < vy_1$, et nous terminons par récurrence sur m.

L'isomorphisme de $f_G(a)$ sur $f(a)$ est fourni par les fonctions φ_j^a ; il est surjectif d'après la construction de H_{2n-1}. □

Exercices

1. Donner un exemple brouwerien d'un ordinal dénombrable qui n'admet pas de successeurs.
2. Montrer qu'un ordinal a des successeurs si, et seulement si, chaque fois que $a < b$, alors ou bien $a \ll b$, ou bien $b = a + 1$.
3. Soit λ un ordinal dénombrable avec successeurs, et f une U-fonction sur λ. En utilisant des arguments semblables à ceux donnés dans les démonstrations du lemme 5.2 et du théorème 5.3, montrer qu'il existe un groupe d'Ulm simplement présenté avec une fonction d'Ulm isomorphe à f.
4. Soit λ un ordinal dénombrable avec successeurs, et soit f une U-fonction sur λ. Si $f(b) \neq 0$, montrer qu'il existe une U-fonction g sur $[0, b]$ et une U-fonction f' sur λ telles que

   (i) $f(a) = g(a) \oplus f'(a)$ pour $a \leqslant b$;

   (ii) $f(a) = f'(a)$ pour $a > b$;

   (iii) $\dim g(b) = 1$.

   Conclure que tout élément d'ordre p et de hauteur a dans un groupe d'Ulm G de longueur λ est contenu dans un facteur direct H de G de longueur $[0, a]$ avec $\dim f_H(a) = 1$.
5. Utiliser l'exercice 4 pour montrer que si λ est un ensemble bien ordonné avec successeurs et si G est un groupe d'Ulm de longueur λ, alors G est une somme directe de groupes d'Ulm de longueurs $[0, a]$ pour des $a \in \lambda$.
6. Soit λ un ensemble bien ordonné avec successeurs tel que $\omega \leqslant \lambda$. Montrer que tout groupe d'Ulm de longueur λ contient un facteur direct qui est une somme directe non bornée de groupes cycliques. Pouvez-vous trouver un tel facteur direct dans l'exemple 3.2 ?

6 Notes

Notre construction d'une enveloppe divisible pour un groupe abélien dénombrable discret est due à Rick Smith (1981) qui travaillait dans le contexte de l'algèbre récursive. Dans le même article, il démontre que l'enveloppe divisible d'un p-groupe est unique si, et seulement si, pG est détachable dans G. La démonstration de la partie « seulement si » de ce théorème fournit une illustration dramatique de la différence entre mathématiques constructives et mathématiques récursives. Pour établir l'existence d'un algorithme qui décide pour n'importe quel élément de G s'il appartient à pG, il construit un algorithme qui ne fait pas

exactement la chose demandée pour chaque élément, mais qui ne peut pas se tromper une infinité de fois. D'un point de vue récursif, un tel algorithme peut être facilement modifié pour obtenir celui que l'on désire : il suffit de changer un nombre fini de réponses. D'un point de vue constructif, cet algorithme est essentiellement sans valeur : non seulement nous avons la mauvaise réponse dans un nombre fini de cas, mais nous n'avons aucune idée sur comment décider quelles réponses peuvent être considérées comme correctes.

Le traitement par Smith de l'unicité des enveloppes divisibles est calqué sur le traitement de l'unicité des clôtures algébriques dans [Metakides & Nerode 1979] où il est démontré, pour les corps discrets dénombrables de caractéristique nulle, que la clôture algébrique est unique si, et seulement si, le corps est factoriel. Pour plus de précisions sur cette question, voir le traitement de l'unicité des corps de décomposition dans [Bridges-Richman 1987].

Un contre-exemple en algèbre récursive pour le théorème d'Ulm est soi-disant construit dans [Lin 1981a], mais il s'appuie sur une démonstration fautive du théorème de Zippin.

Mal'cev (1971) contient une brève discussion des types des groupes abéliens sans torsion de rang 1 dans le contexte de l'algèbre récursive.

Le matériau présenté ici sur les théorèmes d'Ulm et de Zippin est une version simplifiée de [Richman 1973].

Rogers (1980) a étudié les p-groupes qui ne sont pas nécessairement discrets ou nécessairement dénombrables. Elle a examiné les p-groupes G tels que p^nG est un sous-groupe détachable de G pour tout n, et elle a démontré, pour les groupes avec des sous-ensembles dénombrables denses, que cette propriété est équivalente au fait d'avoir un sous-groupe basique [1]. En mathématiques classiques, tout p-groupe possède un sous-groupe basique ; mais constructivement c'est déjà un problème de construire un sous-ensemble dense discret. Tant que nous n'avons pas d'exemples à l'esprit, il semble inutile de spéculer sur les extensions de ce résultat.

1. **NdT.** Voir `https://fr.wikipedia.org/wiki/Sous-groupe_basique`.

XII. Théorie des valeurs absolues

Sommaire

1 Valeurs absolues

Soit k un corps de Heyting. Une **valeur absolue**[1] sur k est une fonction qui assigne à tout élément x de k un nombre réel $|x| \geqslant 0$ tel que

— $|x| > 0$ si, et seulement si, x est inversible ;

— $|xy| = |x||y|$;

1. **NdT.** (Rank one) valuation. Nous avons repris la terminologie « valeur absolue » de Bourbaki. La terminologie « valuation » serait ici en contradiction avec la terminologie française usuelle, de Bourbaki, qui correspond à celle de Krull. En mathématiques classiques, une valuation v sur un anneau A est une fonction v de A vers $\Gamma \cup \{\infty\}$, où Γ est un groupe abélien totalement ordonné, telle que : $v(1) = 0$, $v(0) = \infty$, $v(xy) = v(x) + v(y)$ et $v(x + y) \geqslant \inf(v(x), v(y))$. Lorsque Γ est (isomorphe à) un sous-groupe additif de $\mathbb{R}$, la valuation est dite de rang $\leqslant 1$. Si A est un corps de Heyting, la fonction $x \mapsto 2^{-v(x)}$ est alors une valeur absolue. En mathématiques constructives, comme $x = 0$ n'est pas testable, la définition classique ne fonctionne bien que dans le cas des corps discrets. Pour un corps de Heyting, pour que la fonction v soit bien définie, il faut munir $\mathbb{R} \cup \{\infty\}$ d'une topologie convenable.

— $|x+y| \leqslant |x| + |y|$.

L'ensemble $\{\, |x| : x \in k \text{ est inversible} \,\}$ forme un groupe appelé le **groupe de valeurs** de la valeur absolue. Un corps avec une valeur absolue est appelé un **corps valorisé** [1]. Un corps valorisé est un espace métrique pour la distance $|x-y|$.

Une **valeur absolue généralisée** [2] sur un corps de Heyting k est une fonction qui assigne à tout élément x de k un nombre réel $vx \geqslant 0$ qui satisfait les propriétés suivantes :

(i) $vx \neq 0$ si, et seulement si, x est inversible ;

(ii) $v(xy) = (vx)(vy)$;

(iii) il existe une constante B telle que $v(x+y) \leqslant B \cdot \sup(vx, vy)$ pour tous x et y.

La constante B de (iii) est appelée une **borne** [3] pour v. Notez que (i) et (ii) impliquent $v1 = 1$, donc en prenant $x = 1$ et $y = 0$ dans (iii) on obtient $B \geqslant 1$. Notez qu'une valeur absolue généralisée bornée par 1 est une valeur absolue et que toute valeur absolue est une valeur absolue généralisée bornée par 2.

Théorème 1.1. *Une valeur absolue généralisée est une valeur absolue si, et seulement si, elle est bornée par* 2.

Démonstration. Supposons que v est une valeur absolue généralisée avec 2 pour borne. Une récurrence facile montre que $v(a_1 + \cdots + a_m) \leqslant m \cdot \sup_{i=1}^m va_i$ si m est une puissance de 2. Comme m est toujours compris entre deux puissances de 2 consécutives, nous obtenons $v(a_1 + \cdots + a_m) \leqslant 2m \cdot \sup_{i=1}^m va_i$ pour tout m ; en particulier $v(m) \leqslant 2m$. Donc, pour tout $n > 1$,

$$v(x+y)^n = v\left(\sum\nolimits_{i=0}^n \binom{n}{i} x^i y^{n-i}\right) \leqslant 2(n+1) \sup\nolimits_{i=0}^n v\left(\binom{n}{i} x^i y^{n-i}\right)$$

$$\leqslant 2(n+1) \sum\nolimits_{i=0}^n 2\binom{n}{i} vx^i vy^{n-i} = 4(n+1)(vx+vy)^n.$$

En prenant les racines n-ièmes, pour n assez grand, on obtient $v(x+y) \leqslant vx + vy$. □

1. **NdT.** En anglais, le livre utilise la terminologie de *valued field*, en contradiction avec celle de Bourbaki, pour qui un corps valué est muni d'une valuation et non pas d'une valeur absolue. Nous utilisons dans notre traduction l'innovation terminologique de corps valorisé. Sinon, nous aurions dû utiliser à chaque fois « corps muni d'une valeur absolue », ce qui est un peu lourd.

2. **NdT.** General valuation. Même problème terminologique que précédemment concernant le mot valuation. Bourbaki ne donne pas de nom particulier à une valeur absolue généralisée, mais il note $\mathcal{V}(k)$ l'ensemble des valeurs absolues généralisées sur k. Le traitement des valeurs absolues généralisées de [CCA] est semblable à celui de Bourbaki, mais les auteurs prennent en compte la nécessité de démonstrations complètement constructives, notamment pour les corps de Heyting, inconnus en mathématiques classiques.

3. **NdT.** Bounding constant.

Un valeur absolue généralisée est **non triviale** si $vx > 1$ pour un $x \in k$, **non archimédienne** ou **ultramétrique** si $v(x+y) \leqslant \sup(vx, vy)$ pour tous x et $y \in k$, et **archimédienne** [1] si $vn > 1$ pour un entier n. Nous disons que deux valeurs absolues généralisées sont **équivalentes** si elles définissent la même structure uniforme, i.e. pour tout $\varepsilon > 0$ il existe un $\delta > 0$ tel que $v_1 x < \delta$ implique $v_2 x < \varepsilon$, et $v_2 x < \delta$ implique $v_1 x < \varepsilon$. Nous disons que v_1 et v_2 sont **inéquivalentes** s'il existe un x tel que $v_1 x < 1$ et $v_2 x \geqslant 1$, ou $v_2 x < 1$ et $v_1 x \geqslant 1$.

Théorème 1.2. *Soient v_1 et v_2 des valeurs absolues généralisées et considérons les trois propriétés suivantes.*

(i) *Il existe un nombre réel $r > 0$ tel que $v_1 x = (v_2 x)^r$ pour tout x inversible,*

(ii) *v_1 est équivalente à v_2,*

(iii) *$v_1 x < 1$ implique $v_2 x < 1$ pour tout x.*

On a (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii). *Et si v_1 est non triviale,* (iii) $\Rightarrow$ (i).

Démonstration. Supposons (i) et montrons (ii). Pour un $\varepsilon > 0$, on prend $\delta = \varepsilon^r$. On a $v_2 x < \varepsilon$ ou $v_2 x > 0$, et dans ce dernier cas x est inversible, donc si $v_1 x < \varepsilon^r$, $v_2 x < \varepsilon$. Le même argument fonctionne en échangeant les rôles de v_1 et v_2.

Supposons (ii) et montrons (iii). Si $v_1 x < 1$ on prend un δ tel que si $v_1 y < \delta$, alors $v_2 y < 1$. Nous avons $(v_1 x)^n < \delta$ pour un $n > 0$, donc $(v_2 x)^n < 1$, puis $v_2 x < 1$.

Supposons (iii) avec v_1 non triviale. Notez que si $v_1 y > 1$, alors $v_1 y^{-1} < 1$, donc $v_2 y > 1$. Comme v_1 est non triviale, nous avons un y tel que $v_1 y > 1$ et donc $v_2 y > 1$. Nous prenons $r = (\log v_1 y)/(\log v_2 y) > 0$. Il suffit de montrer, pour $x \neq 0$, que $\gamma_1 = (\log v_1 x)/(\log v_1 y)$ est égal à $\gamma_2 = (\log v_2 x)/(\log v_2 y)$. Notons $\sim$ pour $<$, ou pour $>$, et soient des entiers naturels m et n avec $n > 0$. Alors $m/n \sim \gamma_1$ implique $v_1(y^m x^{-n}) \sim 1$, qui implique $v_2(y^m x^{-n}) \sim 1$, qui implique $m/n \sim \gamma_2$. □

Théorème 1.3. *Soient v_1 et v_2 des valeurs absolues généralisées non triviales. Si v_1 et v_2 sont inéquivalentes, il existe un x tel que $v_1 x < 1$ et $v_2 x > 1$. Si v_1 et v_2 ne sont pas inéquivalentes, elles sont équivalentes.*

Démonstration. Premier point. Supposons v_1 et v_2 inéquivalentes. En remplaçant x par x^{-1} dans la conclusion, on voit que la propriété est symétrique. Supposons donc qu'il existe un y tel que $v_1 y < 1$ et $v_2 y \geqslant 1$. On prend un z tel que $v_2 z > 1$ et on pose $x = y^n z$. Alors $v_2 x > 1$, et, pour n assez grand, nous avons $v_1 x < 1$.

1. **NdT.** Une valeur absolue généralisée ultramétrique admet la borne 1 et c'est donc toujours une valeur absolue. Dans la suite, nous abandonnons valeur absolue généralisée ultramétrique au profit de valeur absolue ultramétrique. En mathématiques classiques, la notion de de valeur absolue ultramétrique correspond aux valuations de rang $\leqslant 1$: voir la note du traducteur 1 page 285.

Supposons maintenant que v_1 et v_2 ne sont pas inéquivalentes. D'après le théorème 1.2, il suffit de démontrer que si $v_1x < 1$, alors $v_2x < 1$. Soit y un élément tel que $v_2y > 1$. Alors $v_1(x^ny) < 1$ pour un $n \in \mathbb{N}$. Si nous avions $v_2(x^ny) > 1$, les deux valeurs absolues généralisées seraient inéquivalentes. Donc $v_2(x^ny) \leqslant 1$ (voir l'exercice II.3.1), donc $v_2x^n \leqslant v_2y^{-1} < 1$, et enfin $v_2x < 1$. □

L'hypothèse de non trivialité dans le théorème 1.2 est essentielle, même si l'on prend pour (iii) la propriété « $v_1x < 1$ si, et seulement si, $v_2x < 1$ ». En fait, sans l'hypothèse de non trivialité, on ne peut démontrer ni (iii) ⇒ (ii), ni (ii) ⇒ (i).

Pour voir qu'on ne peut pas démontrer (iii) ⇒ (ii), on considère un nombre réel $t \geqslant 0$ et on définit les valeurs absolues v_1 et v_2 sur les nombres rationnels en posant $v_1x = |x|^t$, et $v_2x = (v_1x)^t$ si $x \neq 0$. Ici $|x|$ est la valeur absolue usuelle de x. Alors $v_1x < 1$ si, et seulement si, $v_2x < 1$, mais si nous avions un $\delta > 0$ tel que $v_1x < \delta \Rightarrow v_2x < 1/2$, nous aurions $t > 0$ ou $\delta^t > 3/4$, et dans ce dernier cas $t = 0$, car si nous avions $t > 0$, nous aurions un x tel que le réel $v_1x < \delta$ soit aussi près que nous le voudrions de δ, donc v_2x serait aussi près que nous le voudrions de $\delta^t > 3/4$. Et nous aurions le moyen de décider si $t > 0$ ou $t = 0$, ce qui est LPO.

Pour voir qu'on ne peut pas démontrer (ii) ⇒ (i), on considère un nombre réel t et on définit les valeurs absolues généralisées v_1 et v_2 sur les nombres rationnels en posant $v_1x = |x|^{|t|}$ pour $x \neq 0$ et v_2x égal à v_1x si $t > 0$ et à v_1x^2 si $t < 0$. On prolonge ceci à tous les t par continuité. On vérifie facilement que v_2 est une valeur absolue généralisée et que v_1 et v_2 sont équivalentes. Mais si nous avions un r tel que $v_1x = (v_2x)^r$, nous pourrions décider si $t \geqslant 0$ ou $t \leqslant 0$, ce qui est LLPO, car $r < 1$ implique $t \leqslant 0$, et $r > 1/2$ implique $t \geqslant 0$.

Notons que si $v_1 = v_2^r$ $(r > 0)$ et si B est une borne pour v_2, alors B^r est une borne pour v_1. Donc toute valeur absolue généralisée est équivalente à une valeur absolue [1].

Théorème 1.4. *Soient v une valeur absolue généralisée sur k, x et y dans k, et m et n des entiers > 1. Alors*

(i) $vm \leqslant \sup(1, vn)^{\log m/\log n}$,

(ii) $\sup(1, v2)$ *est une borne pour* v.

Démonstration. Notons $\log = \log_2$ et remarquons que

$$v(x_1 + \cdots + x_j) \leqslant B^{1+\log j} \sup_{i=1}^{j} vx_i.$$

1. **NdT.** En effet, pour un choix convenable de r, on a $B^r \leqslant 2$, donc v_1^r est une valeur absolue (théorème 1.1).

Pour démontrer le point (i), on écrit $m^s = a_0 + a_1 n + \cdots + a_r n^r$, où $0 \leqslant a_i < n$ et $r \log n \leqslant s \log m$. Alors on a

$$vm^s \leqslant B^{1+\log((n-1)(r+1))} \sup(1, vn)^r.$$

En élevant les deux membres à la puissance $1/s$, et en faisant tendre s vers ∞, on obtient le résultat.
Pour démontrer le point (ii), on pose $q = \sup(vx, vy)$ et on considère

$$v(x+y)^s = v \sum\nolimits_{i=0}^{s} \binom{s}{i} x^i y^{s-i} \leqslant B^{1+\log(s+1)} \sup\nolimits_{i=0}^{s} q^s v \binom{s}{i}.$$

D'après le point (i), nous avons $v\binom{s}{i} \leqslant \sup(1, v2)^{\log\binom{s}{i}}$. Mais $\binom{s}{i} \leqslant \binom{s}{[s/2]}$, donc

$$v(x+y) \leqslant B^{(1+\log(s+1))/s} q \cdot \sup(1, v2)^{\left(\log\binom{s}{[s/2]}\right)/s}$$

et $(1 + \log(s+1))/s \to 0$ tandis que $\log\binom{s}{[s/2]}/s \to 1$ (utiliser la formule de Stirling), donc $v(x+y) \leqslant q \cdot \sup(1, v2) = \sup(1, v2) \cdot \sup(vx, vy)$. □

Comme corolaires nous obtenons les caractérisations suivantes des valeurs absolues non archimédiennes et archimédiennes.

Corolaire 1.5. *Soit v une valeur absolue généralisée sur k. Alors les propriétés suivantes sont équivalentes.*

(i) *v est non archimédienne (ultramétrique) ;*
(ii) *$v(1+x) \leqslant 1$ pour tout x tel que $vx \leqslant 1$;*
(iii) *$vm \leqslant 1$ pour tous les entiers m ;*
(iv) *$v2 \leqslant 1$;*
(v) *$vn \leqslant 1$ pour un entier $n > 1$.*

Démonstration. Clairement (i) ⇒ (ii) ⇒ (iii) ⇒ (iv) ⇒ (v).
Si l'on a (v), alors $v2 \leqslant 1$ d'après le théorème 1.4(i), donc on peut prendre $B = 1$ d'après le théorème 1.4(ii). □

Corolaire 1.6. *Soit v une valeur absolue généralisée sur un corps k. Les propriétés suivantes sont équivalentes.*

(i) *$v(x+y) > \sup(vx, vy)$ pour un couple (x, y) ;*
(ii) *on a un $q > 0$ tel que si B est une borne pour v, alors $B > 1 + q$;*
(iii) *$v2 > 1$;*
(iv) *$vm > 1$ pour un entier m (v est archimédienne) ;*
(v) *$vn > 1$ pour tous les entiers $n > 1$;*
(vi) *on a un x tel que $vx \leqslant 1$ et $v(1+x) > 1$.*

Démonstration. Clairement (i) implique (ii). Que (ii) implique (iii) se déduit du fait que $v2$ est une borne pour v (théorème 1.4(ii)). Clairement (iii) implique (iv). Que (iv) implique (v) résulte du théorème 1.4(i). Clairement (v) implique (vi) en prenant $x = 1$. Enfin (vi) implique (i) en prenant $y = 1$. □

Comme conséquence des corolaires 1.5(iv) et 1.6(iii), une valeur absolue généralisée de k est non archimédienne si, et seulement si, elle n'est pas archimédienne, car affirmer $v2 \leqslant 1$ est la même chose que nier $v2 > 1$.

Exemple 1.7 (*un exemple brouwerien d'une valeur absolue non triviale qui n'est ni archimédienne ni non archimédienne*)**.** Soit a une suite binaire fugitive. Soit $R = \mathbb{Z}[X]/I$, où I est l'idéal (premier détachable) engendré par l'ensemble $\{\, a_n(X - 2^n) : n \in \mathbb{N} \,\}$. Soit k le corps de fractions de R. Nous définissons une valeur absolue v sur R en faisant correspondre à un polynôme $f(X)$ la limite de la suite de Cauchy définie par

$$r_m = \begin{cases} |f(2^m)|^{1/m} & \text{si } a_n = 0 \text{ pour tout } n \leqslant m \\ |f(2^n)|^{1/n} & \text{si } a_n = 1 \text{ pour un } n \leqslant m. \end{cases}$$

Ici $|\ |$ est la valeur absolue usuelle. La valeur absolue v se prolonge de manière unique à k. Elle est non triviale parce que $vX = 2$. Cependant, décider si v est archimédienne revient à décider si $a_n = 1$ pour un n, ou non. □

Théorème 1.8. *Soit v une fonction sur un corps de Heyting k vers les réels $\geqslant 0$ qui satisfait les points* (i) *et* (ii) *de la définition d'une valeur absolue généralisée. Si $vx \leqslant 1$ implique $v(1 + x) \leqslant B$ pour un certain B, v est une valeur absolue généralisée de borne B.*

Démonstration. Il suffit de démontrer que l'on ne peut pas avoir $v(x + y) > B \cdot \sup(vx, vy)$.
Supposons que ce soit le cas. Si $vx > 0$ et $v(y/x) < 1$, alors

$$v(x + y) = vx \cdot v(1 + y/x) \leqslant B \cdot vx \leqslant B \cdot \sup(vx, vy),$$

une contradiction, donc $v(y/x) \geqslant 1$, puis $vy > 0$ et $v(x/y) \leqslant 1$. Mais alors

$$v(x + y) = vy \cdot v(1 + x/y) \leqslant B \cdot vy \leqslant B \cdot \sup(vx, vy),$$

une contradiction. Donc $vx = 0$ et par suite $x = 0$ car k est un corps de Heyting. Mais alors $v(x + y) = vy \leqslant B \cdot \sup(vx, vy)$. □

Exercices

1. Prenons pour k un anneau commutatif dans la définition d'une valeur absolue généralisée. Montrer que si k admet une valeur absolue généralisée,

c'est un anneau local. Vérifier que les théorèmes de 1.1 à 1.4, et les corolaires 1.5 et 1.6, sont valides dans ce contexte plus général. Montrer que le théorème 1.8 est satisfait si k est un anneau local, et construire un contre-exemple (classique) pour ce théorème lorsque k n'est pas supposé local.

2. *La valeur absolue triviale.* Montrer que tout corps discret admet la valeur absolue v définie par $v(x) = 1$ pour tout $x \neq 0$.
3. *Les valeurs absolues p-adiques de* $\mathbb{Q}$. Soit p un nombre premier. Tout nombre rationnel non nul s'écrit de manière unique sous la forme $r = \pm p^n a/b$, avec des entiers a et b premiers entre eux et non divisibles par p ; on définit $v_p r = p^{-n}$. Montrer que v_p est une valeur absolue ultramétrique sur $\mathbb{Q}$. Montrer que toute valeur absolue ultramétrique sur $\mathbb{Q}$ est équivalente à une valeur absolue v_p.
4. Soit v une valeur absolue ultramétrique. Montrer que si $vx < vy$, alors $v(x + y) = vy$.
5. Soit k un corps discret. On définit une fonction v sur le corps des fractions rationnelles $k(X)$ en posant $v(f) = 2^{-\deg f}$ pour $f \in k[X]$, et $v(f/g) = v(f)/v(g)$. Montrer que v est une valeur absolue ultramétrique sur $k(X)$.
6. Soit S l'ensemble des valeurs absolues non triviales sur un corps de Heyting k, avec pour égalité dans S l'équivalence des valeurs absolues. Montrer que l'inéquivalence est une relation de séparation étroite sur S.

2 Valeurs absolues localement précompactes

Un sous-ensemble B d'un espace métrique X est **borné** s'il existe un N tel que $d(x, y) \leqslant N$ pour tous $x, y \in B$. Un espace métrique est **localement précompact** si on peut approximer les sous-ensembles bornés par des ensembles finis, c'est-à-dire, si pour tout sous-ensemble borné B et tout $\varepsilon > 0$, il existe un sous-ensemble fini Y tel que si $x \in B$, alors $d(x, y) < \varepsilon$ pour un $y \in Y$. Un espace localement précompact est **localement compact** s'il est complet.

On voit facilement qu'un corps valorisé k est localement précompact si, pour tout entier $N > 0$ et tout nombre $\varepsilon > 0$, il existe un sous-ensemble fini Y de k tel que si $|x| \leqslant N$, alors $|x - y| < \varepsilon$ pour un $y \in Y$. Un tel sous-ensemble Y est appelé une **ε-approximation de la N-boule**. la valeur absolue usuelle et les valeurs absolues p-adiques sur $\mathbb{Q}$ ont cette propriété.

Théorème 2.1. *Une valeur absolue localement précompacte est archimédienne ou ultramétrique.*

Démonstration. Notons $|x|$ cette valeur absolue. On considère un sous-ensemble fini Y de k tel que si $|x| \leqslant 2$, alors $|x - y| < 1/3$ pour un $y \in Y$. On considère

les entiers $0, 1, \ldots,$ card Y. Vus dans k, ou bien l'un d'entre eux a une valeur absolue > 1, donc k est archimédienne, ou bien ils ont tous une valeur absolue < 2. Dans ce cas, deux d'entre eux doivent approcher à $1/3$ près un même y, donc leur distance est inférieure à $2/3$, i.e. leur différence a une valeur absolue plus petite que $2/3$; donc $|\ |$ est ultramétrique d'après le corolaire 1.5(v) : comme $|1| = 1$, la différence doit être > 1. □

Soit k un corps valorisé ultramétrique. Le **corps résiduel** de (la valeur absolue de) k est l'ensemble $\overline{k} = \{\, x \in k : |x| \leqslant 1 \,\}$ avec l'égalité définie par $x = y$ si $|x - y| < 1$. Notez que $x \in \overline{k}$ est inversible si, et seulement si, $|x| = 1$, et que $\overline{k}$ est un corps par négation. Le corps résiduel $\overline{k}$ n'est pas nécessairement un anneau local comme nous le verrons dans l'exemple qui suit le théorème 6.2. Cependant, si le groupe de valeurs de k est discret, $\overline{k}$ est un corps discret. Une valeur absolue ultramétrique non triviale sur k est dite **discrète** [1] si le groupe de valeurs de k est cyclique. Notez qu'une valeur absolue discrète a un groupe de valeurs discret et un corps résiduel discret.

Théorème 2.2. *Soit k un corps de Heyting avec une valeur absolue ultramétrique non triviale. Alors k est localement précompact si, et seulement si, la valeur absolue est discrète et le corps résiduel fini.*

Démonstration. Supposons k localement précompact. Comme la valeur absolue est non triviale, on a un $z \in k$ tel que $0 < |z| < 1$. On considère une $|z|$-approximation $x_1, \ldots, x_n$ de la N-boule pour $N \geqslant 1/|z|$ [2]. Montrons que le groupe de valeurs est un sous-ensemble discret de $\{\, x \in \mathbb{R} : x \geqslant 0 \,\}$. Pour $x \in k$, ou bien $|x^n| \neq 1$, auquel cas $|x| \neq 1$, ou bien $|z| < |x^n| < 1/|z|$, auquel cas $|z| < |x^t| < 1/|z|$ pour $t = 0, 1, \ldots, n$. Dans ce dernier cas, on doit avoir des entiers s, t et i avec $s \neq t$, $|x^s - x_i| \leqslant |z|$ et $|x^t - x_i| \leqslant |z|$. Comme $|x^s| > |z|$ et $|x^t| > |z|$, et comme la valeur absolue est ultramétrique, nous avons $|x^s| = |x_i| = |x^t|$, donc $|x| = 1$.

Ainsi, le groupe de valeurs est un sous-ensemble discret de $\{\, x \in \mathbb{R} : x \geqslant 0 \,\}$. Comme $|z| < 1 < N$, on a un i tel que $|z - x_i| < |z|$, donc $|x_i| \leqslant \sup(|z - x_i|, |z|) = |z| < 1$, $|z| \leqslant \sup(|z - x_i|, |x_i|) = |x_i|$, et finalement $|z| = |x_i|$. Prenons parmi $x_1, \ldots, x_n$ l'élément π de plus grande valeur absolue strictement plus petite que 1. Pour tout y inversible, on a un entier m tel que $|\pi| < |\pi^{-m} y| \leqslant 1$. On considère un indice j tel que $|x_j - \pi^{-m} y| < |z|$. Notons que $|z| = |x_i| \leqslant |\pi|$. Alors $|x_j| = |x_j - \pi^{-m} y + \pi^{-m} y| = |\pi^{-m} y|$, donc $|\pi^{-m} y|$ ne peut pas être plus

1. **NdT.** Dans la terminologie classique, un *anneau de valuation discrète* est un anneau de valuation dont le groupe de valuation est isomorphe à $(\mathbb{Z}, \geqslant)$. La valeur absolue correspondante s'écrit $|x| = a^{-vx}$ pour un réel $a > 0$. C'est cette situation que décrit ici une *valeur absolue discrète*. Ceci explique l'utilisation du mot discret dans un sens inhabituel pour les mathématiques constructives.

2. **NdT.** Ici, $1/|z|$ est introduit en tant qu'élément de valeur absolue > 1. Tout autre ferait aussi bien l'affaire.

petit que 1 d'après le choix de π. Donc $|\pi^{-m}y| = 1$, et $|y| = |\pi|^m$. Ceci montre que la valeur absolue est discrète.

Pour montrer que le corps résiduel est fini, on considère une 1-approximation finie Y de la 1-boule. Les éléments de Y représentent tous les éléments du corps résiduel, qui est donc fini puisqu'il est discret.

Inversement, si la valeur absolue est discrète et si le corps résiduel est fini, soit $|\pi| < 1$ un générateur du groupe de valeurs et soit A un système fini de représentants du corps résiduel. Étant donnés $N > 0$ et $\varepsilon > 0$, nous devons trouver un ensemble fini Y tel que si $|x| \leqslant N$, alors $|x - y| < \varepsilon$ pour un $y \in Y$. On considère un entier m tel que $|\pi|^m < \varepsilon$ et $|\pi|^{-m} \geqslant N$ et on définit

$$Y = \Big\{ \sum\nolimits_{i=-m}^{m} a_i \pi^i : a_i \in A \Big\}.$$

Si $|x| \leqslant N$, alors $|\pi^m x| \leqslant 1$ et l'on peut écrire [1]

$$\pi^m x = a_{-m} + a_{-m+1}\pi + \cdots + a_m \pi^{2m} + a_{m+1}\pi^{2m+1}.$$

En posant $b = a_{m+1}\pi^{m+1}$, on a $|b| < |\pi|^m$, donc $x = \sum_{i=-m}^{m} a_i \pi^i + b$ et $|b| < |\pi|^m < \varepsilon$. □

Dans le cas localement précompact, on peut décider si la valeur absolue est archimédienne ou ultramétrique, mais on ne peut pas nécessairement décider si la valeur absolue est triviale ou non triviale.

Exemple 2.3. Soient k un corps fini et X une indéterminée. Soit α une suite binaire fugitive, avec $\alpha_0 = \alpha_1 = 0$. Soit F le sous-corps de $k(X)$ engendré par k et $\{ \alpha_n X : n \in \mathbb{N} \}$. Nous définissons une valeur absolue ultramétrique sur F en posant $|X| = n$ si $\alpha_n = 1$. Donc $|f| = n^{\deg f}$ si f est un polynôme non nul dans F. Notez que si $\alpha_n = 0$, alors pour tout $x \in F$, ou bien $|x| > n$, ou bien $|x| \leqslant 1$. Dans ce dernier cas, $|x - t| < 1/n$ pour un $t \in k$. Comme $\alpha_0 = \alpha_1 = 0$, le corps résiduel de F est k. Pour obtenir une ε-approximation de la N-boule, on considère un $n > \sup(N, 1/\varepsilon)$. Si $\alpha_n = 1$, la valeur absolue est discrète et le théorème 2.2 montre que F est localement précompact. Si $\alpha_n = 0$, k est une ε-approximation de la N-boule selon l'argument précédent. □

Exercices

1. Montrer que la valeur absolue usuelle et les valeurs absolues p-adiques sur $\mathbb{Q}$ sont localement précompactes. Montrer que la valeur absolue triviale sur n'importe quel corps discret est localement compacte.

1. **NdT.** Puisque $|\pi^m x| \leqslant 1$, $\pi^m x$ est égal dans $\overline{k}$ à un $a_{-m} \in A$. Donc $|\pi^m x - a_m| < 1$; on écrit cet élément sous la forme πy avec $|y| \leqslant 1$ et on recommence.

2. Montrer que la valeur absolue sur le corps des fractions rationnelles $\mathbb{Q}(X)$ donnée par $v(f) = 2^{-\deg f}$ n'est pas localement précompacte (voir l'exercice 1.5).
3. Montrer que tout corps résiduel est un corps par négation.
4. Construire un exemple brouwerien d'une valeur absolue ultramétrique dont le groupe de valeurs est cyclique mais n'est pas discret.

3 Corps pseudofactoriels

Un corps k avec une valeur absolue $|\ |$ est **pseudofactoriel** si le nombre réel $\inf\{\, |f(a)| : a \in k \,\}$ existe pour tout polynôme $f \in k[T]$. L'explication de cette terminologie est que le test de racines (théorème VII.1.7) dit qu'un corps discret k est factoriel si, et seulement si, pour tout polynôme $f \in k[X]$, ou bien f a une racine dans k, ou bien $f(a) \neq 0$ pour tout $a \in k$. Donc un corps discret k est factoriel précisément lorsqu'il est pseudofactoriel pour la valeur absolue triviale. Un exemple d'un corps factoriel qui n'est pas pseudofactoriel est obtenu en prenant pour k le corps $\bigcup k_n$ où k_n est $\mathbb{Q}(\alpha_n Y)$ (ici, α est une suite binaire fugitive, et si $\alpha_n = 1$, le corps $\mathbb{Q}(Y) \simeq \mathbb{Q}(i\pi) \subseteq \mathbb{C}$ est muni de la valeur absolue induite par celle de $\mathbb{C}$: l'infimum de $|X^2 + 1|$ sur k ne peut pas être calculé.

Lorsque k est un corps valorisé, nous pouvons construire le **complété** $\hat{k}$ de k de la même manière que nous avons construit $\mathbb{R}$ à partir de $\mathbb{Q}$ en utilisant la valeur absolue usuelle sur $\mathbb{Q}$. La valeur absolue sur k se prolonge de manière naturelle à $\hat{k}$, et $\hat{k}$ est un corps de Heyting complet. Les nombres p-adiques sont construits de cette manière à partir de la valeur absolue p-adique sur les nombres rationnels. Si k est ultramétrique, et si E est un corps intermédiaire entre k et $\hat{k}$, alors k et E ont le même corps résiduel et le même groupe de valeurs.

Théorème 3.1 (méthode de Newton)**.** *Soient k un corps discret avec une valeur absolue et $\hat{k}$ le complété de k. Soit f un polynôme séparable de $k[X]$. Alors il existe un $\delta > 0$ tel que, étant donné un $a_0 \in k$ pour lequel $|f(a_0)| < \delta$, nous pouvons construire une racine de f dans $\hat{k}$.*

Démonstration. Si f est constant, on prend $\delta = f$ [1]. Supposons maintenant $\deg f > 0$. On considère un N tel que $|f(a)| \geqslant 1$ pour tout $|a| \geqslant N$, et donc $|a| \leqslant N$ lorsque $|f(a)| < 1$. On écrit

$$f(Y + Z) = f(Y) + Zf'(Y) + Z^2 g(Y, Z)$$

et l'on considère un M tel que $|g(a, b)| \leqslant M$ si $|a| \leqslant N$ et $|b| \leqslant 1$.

1. **NdT.** Si un polynôme séparable est constant, cette constante est inversible car le polynôme étranger à sa dérivée formelle.

Soient s et $t \in k[X]$ tels que $s(X)f(X) + t(X)f'(X) = 1$. Soit $0 < r \leqslant 1$ tel que $|t(a)| \leqslant r^{-1}$ et $|s(a)| \leqslant r^{-1}$ si $|a| \leqslant N$. Si $|f(a)| < 1$, $|a| \leqslant N$, donc

$$r^{-1}|f'(a)| \geqslant |t(a)f'(a)| \geqslant 1 - |s(a)||f(a)| \geqslant 1 - r^{-1}|f(a)|,$$

d'où

$$|f'(a)| \geqslant r - |f(a)|.$$

On considère un $\delta \leqslant r/2$ tel que si $u \geqslant 1/\delta$, on a

$$2M\left(\frac{1}{ru-1}\right)^2 \leqslant \frac{1}{u}.$$

Soit maintenant un a_0 tel que $|f(a_0)| < \delta$. Nous utilisons alors la **méthode de Newton** pour construire une racine de f, précisément comme suit. On définit a_n par récurrence en posant $a_{n+1} = a_n + h_n$, où $h_n = -f(a_n)/f'(a_n)$. Montrons que $|f(a_n)| \leqslant 2^{-n}\delta$. C'est vrai pour $n = 0$. Si $|f(a_n)| \leqslant 2^{-n}\delta < 1$, alors $|a_n| \leqslant N$ et $|f'(a_n)| \geqslant r - 2^{-n}\delta$, donc $|h_n| \leqslant (r2^n/\delta - 1)^{-1}$. Or

$$|f(a_{n+1})| = |f(a_n + h_n)| = |h_n^2| \cdot |g(a_n, h_n)| \leqslant |h_n|^2 M \leqslant 2^{-(n+1)}\delta$$

(prendre $u = 2^n/\delta$). Donc $\{a_n\}$ est une suite de Cauchy qui converge vers une racine de f dans $\hat{k}$. □

Corolaire 3.2. *Soient k un corps discret pseudofactoriel, $\hat{k}$ son complété et f un polynôme séparable de $k[X]$. Alors ou bien f a une racine dans $\hat{k}$, ou bien il existe un $r > 0$ tel que $|f(a)| > r$ pour tout $a \in k$.*

Démonstration. On prend un δ comme dans le théorème 3.1. Ou bien $\inf\{\,|f(a)| : a \in k\,\} \geqslant \delta/2$, auquel cas $|f(a)| > \delta/3$ pour tout $a \in k$, ou bien $\inf\{\,|f(a)| : a \in k\,\} < \delta$, auquel cas on a une racine de f dans $\hat{k}$ d'après le théorème 3.1. □

En utilisant la notion du *nombre de tours*, nous obtenons une nouvelle démonstration de la version discrète du théorème fondamental de l'algèbre.

Corolaire 3.3. *Soient k un sous-corps discret de $\mathbb{C}$ et K la clôture algébrique de k dans $\mathbb{C}$. Alors K est algébriquement clos.*

Démonstration. Soit f un polynôme unitaire de degré n à coefficients dans K, qui est un corps discret d'après le théorème VI.1.9. On prend un $r > 0$ tel que si z est un nombre complexe de module r, alors $|z^n - f(z)| < r^n$. Alors le nombre de tours autour de 0 du chemin obtenu en restreignant f au cercle de rayon r est n. Si on avait $\inf\{\,|f(x)| : |x| \leqslant r\,\} > 0$, ce nombre de tours serait nul. Donc $\inf\{\,|f(x)| : |x| \leqslant r\,\} = 0$. Comme f est un produit de polynômes séparables (théorème VI.6.3), nous pouvons trouver une racine de f dans $\mathbb{C}$ d'après le théorème 3.1. D'après le corolaire VI.1.5, une telle racine est dans K, et le corolaire est démontré. □

Nous donnons dans le théorème suivant des exemples de corps pseudofactoriels.

Théorème 3.4. *Soit k un corps discret avec une valeur absolue. Si k est localement précompact ou si la valeur absolue est ultramétrique discrète avec un corps résiduel factoriel, le corps k est pseudofactoriel.*

Démonstration. Soit f un polynôme dans $k[X]$. On doit montrer que $\inf\{\,|f(a)| : a \in k\,\}$ existe. Il suffit de traiter le cas où $\deg(f) > 0$ et $|f(0)| > 0$.

Si k est localement précompact, on considère un N tel que $|f(a)| \geqslant |f(0)|$ si $|a| \geqslant N$. Donc si $|f(a)| < |f(0)|$, on a $|a| \leqslant N$. Soit Y_n une $1/n$-approximation de la N-boule. Alors la suite $r_n = \inf\{\,|f(y)| : y \in Y_n\,\}$ est une suite de Cauchy et converge vers $\inf\{\,|f(a)| : a \in k\,\}$, donc k est pseudofactoriel.

Supposons la valeur absolue discrète avec un corps résiduel factoriel. En remplaçant $f(X)$ par $dc^{\deg f} f(X/c)$ nous pouvons supposer que f est unitaire et que les valeurs des autres coefficients de f sont < 1. Supposons le groupe de valeurs engendré par $r < 1$ et considérons un $\pi \in k$ tel que $|\pi| = r$. Nous allons construire une suite d'ensembles finis (possiblement vides)

$$B_m \subseteq \{\, b \in k : |b| \leqslant 1 \text{ et } |f(b)| \leqslant r^m \,\},$$

et des entiers $n_m > 0$ tels que si $|f(a)| \leqslant r^{n_m}$, alors $|a - b| \leqslant r^m$ pour un $b \in B_m$.

L'ensemble B_1 est formé par des représentants de chacune des racines de f vue dans le corps résiduel (qui est factoriel), et on prend $n_1 = 1$. Si $|f(a)| \leqslant r$, alors $|a| < 1$ parce que f est unitaire avec de petits coefficients, donc a représente une racine de f dans le corps résiduel. Alors $a \in B_1$ et donc $|a - b| \leqslant r$ pour un $b \in B_1$. Pour construire B_{m+1} à partir de B_m, nous procédons comme suit. Pour chaque $b \in B_m$, nous écrivons $f(b + \pi^m X)$ sous la forme $\pi^{e_b} g_b(X)$ avec $g_b \in k[X]$ et la valeur maximum des coefficients de g_b égale à 1. Comme $f(b + \pi^m X) - f(b)$ est divisible par $\pi^m X$, et comme $|f(b)| \leqslant r^m$, nous avons $e_b \geqslant m$. Soient $c_1^b, \ldots, c_s^b$ des représentants des racines de g_b vues dans le corps résiduel, et prenons pour B_{m+1} l'ensemble de tous les éléments de la forme

$$b + \pi^m c_i^b$$

pour $b \in B_m$. Soit n_{m+1} strictement plus grand que n_m et que les e_b pour b dans B_m. Supposons que $|f(a)| \leqslant r^{n_{m+1}}$. Alors $|a - b| \leqslant r^m$ pour un $b \in B_m$, donc $a = b + \pi^m c$ pour un $c \in k$ tel que $|c| \leqslant 1$. Comme $|f(a)| \leqslant r^{n_{m+1}}$ et $f(a) = \pi^{e_b} g_b(c)$, nous avons $|g_b(c)| \leqslant r$, donc c représente une racine de g_b vue dans le corps résiduel. Donc $|c - c_i^b| \leqslant r$ pour un i, et $|a - (b + \pi^m c_i^b)| = |\pi^m c - \pi^m c_i^b| \leqslant r^{m+1}$.

Si B_1 est vide, $1 = |f(0)| \leqslant |f(a)|$ pour tout $a \in k$. Sinon, on calcule $\inf\{\,|f(a)| : a \in k\,\}$ comme limite de la suite de Cauchy des valeurs absolues

$$d_n = \inf\{\,|f(b)| : b \in \bigcup\nolimits_{m \leqslant n} B_m\,\}. \qquad \square$$

Corolaire 3.5. *Soit k un corps discret pseudofactoriel. La clôture algébrique (séparable) de k dans son complété $\hat{k}$ est séparablement factorielle.*

Démonstration. La clôture algébrique (séparable) K de k dans $\hat{k}$ est un corps discret (théorème VI.1.9). En outre, K est pseudofactoriel parce que k est dense dans K. Donc, si f est un polynôme séparable de $K[X]$, ou bien f a une racine dans $\hat{K} = \hat{k}$, ou bien $|f(a)| > 0$ pour tout $a \in K$, d'après le corolaire 3.2. Mais toute racine de f dans $\hat{k}$ est dans K, donc K est séparablement factoriel (théorème VII.1.7). □

Exercices

1. Soit k un corps discret. On munit le corps des fractions rationnelles $K = k(X)$ de la valeur absolue de l'exercice 1.5. Le complété $\hat{K}$ de K est le **corps de séries formelles** sur k. Montrer que nous pouvons identifier les éléments de $\hat{K}$ avec des sommes formelles du type
$$f = \sum\nolimits_{i=m}^{\infty} a_i X^i,$$
où $m \in \mathbb{Z}$ et $a_i \in k$. Montrer que si $a_m \neq 0$, alors $v(f) = m$.
2. *L'hypothèse selon laquelle f est séparable ne peut pas être supprimée dans le théorème 3.1.* Soit $\{a_n\}$ une suite binaire fugitive. Soit K le corps des séries formelles en Y sur le corps $\mathbb{Z}_2$. Soit ζ un élément de K qui est transcendant sur $\mathbb{Z}_2(Y)$. Montrer que l'élément
$$\eta = \left(1 + \sum a_n Y^{2n+1}\right) \zeta^2$$
est transcendant sur $\mathbb{Z}_2(Y)$. Soient $k = \mathbb{Z}_2(Y, \eta)$ et $f(X) = X^2 - \eta$. Montrer que f a une racine dans $K = \hat{k}$ si, et seulement si, $a_n = 0$ pour tout n. Montrer que k est pseudofactoriel d'après le théorème 3.4. Le corolaire 3.2 nous permettrait donc de décider si f a ou n'a pas une racine dans K.
3. Décrire la valeur absolue sur le complété $\hat{k}$ d'un corps ultramétrique k. Montrer que le corps résiduel et le groupe de valeurs de k et $\hat{k}$ sont les mêmes.
4. Montrer que les suites r_n et d_n dans la démonstration du théorème 3.4 sont des suites de Cauchy.

4 Espaces vectoriels normés

Soit k un corps valorisé. Un **espace vectoriel normé** sur k est un espace vectoriel V sur k, avec une inégalité étroite, et une fonction, appelée **norme**, qui envoie chaque $x \in V$ sur un réel $|x| \geqslant 0$, satisfaisant les propriétés suivantes.

(i) $|x| \neq 0$ si, et seulement si, $x \neq 0$;

(ii) $|ax| = |a||x|$;

(iii) $|x + y| \leqslant |x| + |y|$.

Si V n'est pas muni d'une inégalité et si nous remplaçons (i) par « $|x| = 0$ seulement si $x = 0$ », nous pouvons utiliser (i) pour *définir* une inégalité étroite sur V. Un espace vectoriel normé est un espace métrique pour la distance $|x-y|$.

On définit l'**inégalité forte** sur k^n en posant $x \neq y$ si $x_i \neq y_i$ pour un i. Nous faisons de k^n un espace vectoriel normé en posant $|x| = \sup\{\, |x_i| : i = 1, \ldots, n\}$ (**norme du sup**). Si nous prenons la valeur absolue usuelle sur $\mathbb{Q}$ et sur $\mathbb{R}$, tout sous-corps de $\mathbb{R}$ est un espace vectoriel normé sur $\mathbb{Q}$.

Soit V un espace vectoriel normé sur un corps valorisé k. Nous disons que $v_1, \ldots, v_n \in V$ sont **métriquement indépendants** si pour tout $\varepsilon > 0$ on a un $\delta > 0$ tel que si $|\sum a_i v_i| < \delta$, alors $|a_i| < \varepsilon$ pour chaque i. Si, en outre, tout élément de V peut être écrit comme une combinaison linéaire des v_i, nous disons que les v_i forment une **base métrique** de V. Ainsi V admet un base métrique si, et seulement si, il y a un isomorphisme bicontinu de V vers k^n, ce dernier équipé de la norme du sup.

Le sous-corps $\mathbb{Q}(\sqrt{2})$ de $\mathbb{R}$ est un espace vectoriel normé de dimension finie sur un corps discret qui n'admet pas de base métrique. D'autre part, comme les applications linéaires entre espaces vectoriels de dimension finie sont continues, si un espace vectoriel normé sur un corps discret valorisé admet une base métrique, toute base est une base métrique.

Deux normes $|\ |_1$ et $|\ |_2$ sont **équivalentes** s'il existe un $\varepsilon > 0$ tel que $\varepsilon|x|_1 \leqslant |x|_2 \leqslant \varepsilon^{-1}|x|_2$ pour tout $x \in V$. On démontre facilement que les normes $|\ |_1$ et $|\ |_2$ sont équivalentes si, et seulement si, l'application identique de $(V, |\ |_1)$ sur $(V, |\ |_2)$ est bicontinue.

Soit V un espace vectoriel normé sur k. Un ensemble d'éléments $v_1, \ldots, v_n$ de V est appelé une **base** de V si l'application linéaire φ de k^n vers V définie par $\varphi(e_i) = v_i$ est un isomorphisme qui préserve l'inégalité. Nous allons voir que pour un corps localement compact k, toute base de V est une base métrique ; cela revient à dire que toutes les normes sur k^n sont équivalentes. Attention : un corps discret est localement compact pour la valeur absolue triviale, mais pas nécessairement pour d'autres valeurs absolues – par exemple, $\mathbb{Q}$ avec la valeur absolue usuelle n'est pas complet.

Lemme 4.1. *Soit k un corps valorisé, et soit $e_1, \ldots, e_n$ la base naturelle de k^n. Une norme sur k^n est équivalente à la norme du sup si, et seulement si, e_i est éloigné*[1] *de $k^{i-1} = ke_1 + \cdots + ke_{i-1}$ pour $i = 2, \ldots, n$.*

Démonstration. Le « seulement si » est clair d'après la définition de la norme du sup. Pour le « si », il suffit de démontrer que les fonctions coordonnées

1. **NdT.** Dans un espace métrique (S, d), un élément x est **éloigné** d'un sous-ensemble T s'il existe un $\delta > 0$ tel que $d(x, y) \geqslant \delta$ pour tout $y \in T$.

$\pi_i(x_1e_1 + \cdots + x_ne_n) = x_i$ sont continues. Supposons que $|e_n - \alpha| \geqslant \delta > 0$ pour tout $\alpha \in k^{n-1}$. Alors $|x_ne_n - \alpha| \geqslant \delta|x_n|$ pour $|x_n| > 0$ et $\alpha \in k^{n-1}$, et donc $\delta|x_n| \leqslant |x_1e_1 + \cdots + x_ne_n|$ pour tous $x_1, \ldots, x_n$. Ainsi, la projection de k^n sur sa dernière coordonnée, et donc aussi sur k^{n-1}, est continue. Nous terminons la démonstration par récurrence sur n. □

Un sous-ensemble A d'un espace métrique X est **situé** [1] si, pour tous $x \in X$ et $\varepsilon > 0$, il existe un $a_0 \in A$ tel que $d(x, a_0) < d(x, a) + \varepsilon$ pour tout $a \in A$; dans ce cas, la distance

$$d(x, A) = \inf\{\, d(x, a) : a \in A \,\}$$

existe. Tout sous-ensemble A localement précompact non vide est situé : considérer un N tel que l'ensemble borné $B = \{\, a \in A : d(x, a) < N \,\}$ soit non vide ; approximer B à $\varepsilon/2$ près par un ensemble fini $F \subseteq A$; prendre un $a_0 \in F$ tel que $d(x, a_0) - \inf\{\, d(x, a) : a \in F \,\} < \varepsilon/2$.

Théorème 4.2. *Si k est un corps valorisé localement compact, k^n est un espace normé localement compact pour la norme du sup, et toute norme sur k^n est équivalente à cette dernière.*

Démonstration. Clairement k^n est localement compact pour la norme du sup. Considérons une autre norme sur k^n. Par récurrence k^{n-1} est localement compact et donc situé dans k^n.
D'après le lemme 4.1, il suffit de montrer que $d(e_n, k^{n-1}) > 0$. En utilisant le fait que k^{n-1} est situé, on définit une suite d'éléments $\theta_i \in k^{n-1}$ de la manière suivante. Pour $i > 0$, on décide si $d(e_n, k^{n-1}) < 1/i$ ou $d(e_n, k^{n-1}) > 1/(i+1)$.

— Dans le premier cas, on prend pour θ_i dans k^{n-1} un élément qui vérifie $|\theta_i - e_n| < 1/i$. Dans ce cas, on a aussi $|\theta_{i-1} - e_n| < 1/(i-1)$ (si $i \geqslant 2$) car on est forcément dans le premier cas pour l'indice $i - 1$.
— Dans le second cas on pose $\theta_i = \theta_{i-1}$. La suite est alors constante à partir de l'indice $i - 1$.

Dans le premier cas pour l'indice i, on voit que si $j \geqslant i \geqslant 1$, $|\theta_j - e_n| < 1/i$ (faire une récurrence sur j) et par suite $|\theta_j - \theta_i| < 2/i$. Dans le deuxième cas pour l'indice i, si $j \geqslant i \geqslant 1$, on a $|\theta_j - \theta_i| = 0 < 2/i$. La suite des θ_i est donc une suite de Cauchy. Comme k^{n-1} est complet, la suite converge vers un $\theta \in k^{n-1}$ avec $|\theta - \theta_i| \leqslant 2/i$ pour tous $i \geqslant 2$. Comme e_n est distinct de tout élément de k^{n-1}, on obtient $\theta \neq e_n$, donc $|\theta - e_n| > 0$, et par suite $|\theta - e_n| > 1/\ell$ pour un ℓ. Or si l'on avait $d(e_n, k^{n-1}) < 1/(\ell+1)$, on serait dans le premier cas pour l'indice ℓ et donc $|\theta_j - e_n| < 1/\ell$ pour tout $j \geqslant \ell$, d'où $|\theta - e_n| \leqslant 1/\ell$. Donc $d(e_n, k^{n-1}) \geqslant 1/(\ell+1)$. □

1. **NdT.** Located subset.

L'hypothèse dans le théorème 4.2 selon laquelle le corps k est localement compact ne peut pas être affaiblie en disant seulement que k est complet, comme dans le contexte classique ; l'appel au fait que k^{n-1} est situé est essentiel dans la démonstration, comme le montre le contre-exemple brouwerien suivant.

Exemple 4.3. Soit $r \geqslant 0$ un nombre réel, et soit k le complété du sous-corps $\mathbb{R}(ri)$ de $\mathbb{C}$. Alors k est un sous-corps fermé de $\mathbb{C}$. Nous allons construire une norme sur k^2 telle qu'on ne puisse pas montrer que e_2 est éloigné de $k^1 = ke_1$.

Soit e_1, e_2 la base naturelle de $\mathbb{C}^2$, qui est aussi la base naturelle de $k^2 \subseteq \mathbb{C}^2$. Tout élément de $\mathbb{C}^2$ s'écrit de manière unique sous la forme $z = \alpha(e_1 - ie_2) + \beta(e_1 + ie_2)$ avec α et $\beta \in \mathbb{C}$. Si $z = \gamma_1 e_1 + \gamma_2 e_2 \in k^2$, on a $2\alpha = \gamma_1 + i\gamma_2$, $2\beta = \gamma_1 - i\gamma_2$ et $2(\alpha - \overline{\beta}) = (\gamma_1 + \overline{\gamma}_1) + i(\gamma_2 - \overline{\gamma}_2)$, de sorte que $\alpha - \overline{\beta} \neq 0$ implique $r > 0$.

Munissons $\mathbb{C}^2$ de la seminorme [1] $\|z\| = |\beta| + r|\alpha|$. Montrons que cela définit une norme sur k^2, i.e. que $z \neq 0$ et $z \in k^2$ impliquent $\|z\| > 0$. Supposons $z \neq 0$, donc $\alpha \neq 0$ ou $\beta \neq 0$. Si $\beta \neq 0$, $\|z\| > 0$. Supposons $|\alpha| > 0$. Ou bien $|\alpha - \overline{\beta}| < \sup(|\alpha|, |\beta|)/2$, auquel cas $|\beta| > 0$, donc $\|z\| > 0$; ou bien $|\alpha - \overline{\beta}| > 0$, auquel cas $r > 0$ et par suite $\|z\| \geqslant r|\alpha| > 0$.

Supposons maintenant que $d(e_2, k^1)$ existe. Notons que $r = \|e_1 - ie_2\| \geqslant d(e_2, k^1)$. Supposons $d(e_2, k^1) < 1/2$, alors $|\gamma_1 - i| < 1$ pour un $\gamma_1 \in k$, donc $r > 0$. Supposons $d(e_2, k^1) > 0$. On a $r > 0$ ou $r < d(e_2, k^1)$. Si $r < d(e_2, k^1)$, $r = 0$ parce que $r > 0$ est impossible. Ainsi dans tous les cas, ou bien $r > 0$, ou bien $r = 0$, ce qui est équivalent à LPO. □

Exercices

1. La **métrique triviale** sur un ensemble discret X est définie par $d(x, y) = 0$ si $x = y$, et $d(x, y) = 1$ sinon. Montrer qu'un sous-ensemble de X est détachable si, et seulement si, il est situé pour la métrique triviale.
2. Montrer que l'espace $\mathbb{Q}(\sqrt{2})$ est discret.
3. Définir une notion positive d'inéquivalence entre normes sur un espace vectoriel, et montrer que la norme du sup sur $\mathbb{Q}^2$ est inéquivalente à la norme sur $\mathbb{Q}^2$ induite par un isomorphisme avec $\mathbb{Q}(\sqrt{2})$.

5 Corps réels et complexes

Tout corps valorisé archimédien contient une copie du corps des nombres rationnels $\mathbb{Q}$, et il y a essentiellement une seule valeur absolue archimédienne sur $\mathbb{Q}$. Le théorème suivant décrit toutes les valeurs absolues non triviales sur $\mathbb{Q}$.

1. **NdT.** Une **seminorme** sur un k-espace vectoriel V, où k est un corps valorisé, est une fonction qui satisfait les mêmes propriétés qu'une norme, à l'exception de la propriété (i).

Théorème 5.1. *Toute valeur absolue non triviale sur $\mathbb{Q}$ est équivalente à la valeur absolue usuelle ou à la valeur absolue p-adique pour un nombre premier p.*

Démonstration. Si $|n/p| > 1$ pour des entiers strictement positifs n et p, alors $|n| > |p|$ et, par cotransitivité, $|n| > 1$ ou $|p| < 1$. Si $|n| > 1$, alors $|m| > 1$ pour tout entier $m > 1$ d'après le corolaire 1.6. De plus,

$$|m| \leqslant |n|^{\log m/\log n} \text{ et } |n| \leqslant |m|^{\log n/\log m}$$

d'après le théorème 1.4, donc $|m| = |n|^{\log m/\log n} = m^r$ pour un r ; donc la valeur absolue est équivalente à la valeur absolue usuelle. D'autre part si $|p| < 1$, la valeur absolue est ultramétrique (corolaire 1.5) et nous pouvons supposer que p est un nombre premier. Si $sm + tp = 1$, on a

$$1 = |sm + tp| \leqslant \sup(|sm|, |tp|),$$

mais $|tp| = |t||p| < 1$, donc $|sm| = 1$ et $|m| = 1$. Ainsi, la valeur d'un entier positif arbitraire mp^e est $|p|^e$ si $(m, p) = 1$; donc la valeur absolue est équivalente à la valeur absolue p-adique. □

Notez que toute valeur absolue non triviale sur $\mathbb{Q}$ est localement précompacte, et que la valeur absolue usuelle est la seule valeur absolue archimédienne sur $\mathbb{Q}$ telle que $|2| = 2$.

Il y a deux types importants de corps archimédiens.

Définition. Soit k un corps archimédien. S'il y a un $\delta > 0$ tel que $|a^2 + 1| \geqslant \delta$ pour tout $a \in k$, on dit que k est un **corps réel**. Si pour tout $\delta > 0$ il existe un $a \in k$ tel que $|a^2 + 1| < \delta$, on dit que k est un **corps complexe**.

En mathématiques classiques tout corps archimédien est réel ou complexe. Cependant, le corps k de l'exemple 4.3 ne peut pas être dit réel ou complexe.

La construction du corps valorisé $\mathbb{C}$ des nombres complexes à partir du corps valorisé $\mathbb{R}$ des nombres réels peut être utilisée pour construire un corps valorisé de décomposition pour $X^2 + 1$ (unique) sur n'importe quel corps réel.

Théorème 5.2. *Si k est un corps réel, il peut être plongé dans un corps valorisé K qui contient un élément i tel que $i^2 = -1$ et $K = k(i)$. De plus, si k est plongé dans un corps valorisé E qui contient un élément j tel que $j^2 = -1$, alors j est éloigné de k et $k(j)$ est isomorphe à K en tant que corps valorisé.*

Démonstration. Soit K l'anneau des sommes formelles $a + bi$ avec $a, b \in k$ et $i^2 = -1$. Nous définissons une inégalité sur K en posant $a + bi \neq 0$ si $a \neq 0$ ou $b \neq 0$, ce qui fait de K un corps de Heyting. Nous définissons une valeur absolue sur K en posant $|a + bi| = \sqrt{|a^2 + b^2|}$.

Pour montrer tout d'abord que l'on a bien une valeur absolue généralisée, il nous suffit de trouver une constante B telle que $|(1+a)^2+b^2| \leqslant B$ lorsque $|a^2+b^2| \leqslant 1$ (théorème 1.8). Or

$$|(1+a)^2+b^2| \leqslant 1+|a^2+b^2|+2|a| \leqslant 2+2|a| \text{ si } |a^2+b^2| \leqslant 1,$$

donc il suffit simplement de borner $|a|$. Or si $|a|>0$, on a $1 \geqslant |a^2+b^2| = |a|^2|1+b^2/a^2| \geqslant |a|^2\delta$.

Enfin, comme $|2| \leqslant 2$, on a bien une valeur absolue (théorèmes 1.1 et 1.4).

Pour démontrer la seconde affirmation, nous établissons d'abord que j est éloigné de k. Pour un $a \in k$ arbitraire, on a $|a|>2$ ou $|a|<3$. Si $|a|>2$, $|a-j| \geqslant |a|-|j|>1$; si $|a|<3$, $|a-j| = |a^2+1|/|a+j| > |a^2+1|/4$, et ce dernier est uniformément éloigné de 0 parce que k est réel.

On définit $\varphi\colon K \to k(j)$ en posant $\varphi(a+bi) = a+bj$: φ est un homomorphisme de K sur $k(j)$. Nous montrons d'abord que φ préserve l'inégalité. Si $a+bj \neq 0$, $a \neq 0$ ou $bj \neq 0$ car E est un corps de Heyting, donc $a \neq 0$ ou $b \neq 0$, et donc $a+bi \neq 0$. Inversement, si $a+bi \neq 0$, alors $a \neq 0$ ou $b \neq 0$, donc $0 \neq a^2+b^2 = (a+bj)(a-bj)$, d'où $a+bj \neq 0$. La valeur absolue sur $k(j)$ induit, *via* φ, une valeur absolue sur K. Le lemme 4.1 implique que cette valeur absolue est équivalente à la valeur absolue que nous avons construite sur K, donc chacune est une puissance strictement positive de l'autre (théorème 1.2). Comme elles coïncident sur k, elles sont égales. □

Corolaire 5.3. *Il y a une seule valeur absolue sur le corps $\mathbb{C}$ qui prolonge la valeur absolue usuelle sur $\mathbb{R}$.*

Démonstration. Immédiat d'après le théorème 5.2. □

Théorème 5.4 (Gelfand-Tornheim)**.** *Si k est un corps normé*[1] *sur $\mathbb{C}$, alors $k = \mathbb{C}$.*

Démonstration. Comme $\mathbb{C}$ est complet, il suffit de démontrer que $\mathbb{C}$ est dense dans k. Si nous cherchons un élément de $\mathbb{C}$ qui est proche d'un élément donné $a \in k$, alors comme 0 est proche de a ou $|a|>0$, nous pouvons toujours supposer être dans le dernier cas. Nous construisons un carré de largeur $|8a|$, centré en 0, découpé en $4n^2$ petit carrés de largeur $|4a|/n$, et nous considérons la ligne polygonale S formée par les côtés des petits carrés situés sur le périmètre du grand carré. Soit δ l'infimum des $|z-a|$ pour les z qui se trouvent au milieu des côtés ou au centre des petits carrés. Nous allons montrer que $\delta^3 \leqslant 3|4a|^3/n$, et donc on pourra trouver des nombres complexes arbitrairement proches de a en prenant n suffisamment grand. Par cotransitivité, nous pouvons supposer que $\delta > 0$.

1. **NdT.** On dit que k est un **corps normé** lorsque c'est un corps de Heyting et un espace vectoriel normé sur $\mathbb{C}$, et que la norme est une valeur absolue sur k.

Étant donnée une fonction $f\colon \mathbb{C} \to k$ et une ligne polygonale P avec les sommets successifs $z_0, \dots, z_n \in \mathbb{C}$, nous définissons l'« intégrale » $I_P(f)$ comme la somme

$$\sum\nolimits_{i=1}^{n} (z_i - z_{i-1}) f((z_i + z_{i-1})/2).$$

Clairement I_P est linéaire en f, et si $f(z) = cz + d$, alors

$$I_P(f) = (z_n - z_0)((z_n + z_0)c/2 + d).$$

En particulier, si P est une ligne polygonale fermée, c'est-à-dire si $z_0 = z_n$, l'intégrale I_P est nulle pour les polynômes de degré au plus 1.

Considérons la fonction $g(z) = 1/(z-a)$ de $\mathbb{C}$ vers k. Nous majorons tout d'abord $I_Q(g)$ lorsque Q est un carré de largeur ε. Soit $\delta > 0$ un minorant de l'infimum des distances de a aux milieux des côtés ou au centre de Q. Notre borne dépendra seulement de ε et δ ; nous pouvons supposer que 0 est le centre de Q. Comme

$$g(z) = \frac{1}{z-a} = \frac{z^2}{a^2(z-a)} - \frac{a+z}{a^2}$$

et comme I_Q est nul pour les polynômes de degré au plus 1, nous avons $|I_Q(g)| \leqslant 4\varepsilon(\varepsilon/2)^2/\delta^3 = \varepsilon^3/\delta^3$.

Comme $I_S(g)$ est égal à la somme des intégrales $I_Q(g)$, où Q parcourt les $4n^2$ petits carrés de largeur $\varepsilon = |4a|/n$, nous avons $|I_S(g)| \leqslant 4|4a|^3/\delta^3 n$. Nous utilisons ceci pour majorer $I_S(1/z)$. On a

$$\frac{1}{z} = \frac{1}{z-a} - \frac{a}{z(z-a)}\ ,$$

et donc

$$|I_S(1/z)| \leqslant \frac{4|4a|^3}{\delta^3 n} + \frac{|a|4|8a|}{|4a|(|4a| - |a|)} = \frac{4|4a|^3}{\delta^3 n} + \frac{8}{3}\ .$$

Nous calculons maintenant un minorant de $I_S(1/z)$ directement à partir de la définition. Chacun des quatre côtés du carré contribue pour

$$\frac{i}{n} \sum\nolimits_{k=1}^{n} \left(\frac{1}{1 + i(k-1/2)/n} + \frac{1}{1 - i(k-1/2)/n} \right)$$

dont la valeur absolue usuelle est égale à

$$\sum\nolimits_{k=1}^{n} \frac{2n}{n^2 + (k-1/2)^2} \geqslant \sum\nolimits_{k=1}^{n} \frac{2n}{2n^2} = 1.$$

En combinant ceci avec le majorant de $|I_S(1/z)|$, nous obtenons

$$4 \leqslant \frac{4|4a|^3}{\delta^3 n} + \frac{8}{3}\ .$$

Ainsi $\delta^3 \leqslant 3|4a|^3/n$. □

Corolaire 5.5. *Soit k un corps archimédien avec $|2| = 2$. Alors k est réel si, et seulement si, $\hat{k} \simeq \mathbb{R}$ comme corps valorisé.*

Démonstration. Clairement, tout sous-corps de $\mathbb{R}$ est réel. Inversement, si k est réel, $\hat{k}$ est réel et nous construisons $\hat{k}(i)$ (théorème 5.2). Le théorème 5.1 nous permet de supposer que $\mathbb{R} \subseteq \hat{k}$. Comme $\mathbb{R}(i) \simeq \mathbb{C}$ d'après le théorème 5.2, nous avons $\hat{k}(i) = \mathbb{R}(i)$ d'après le théorème 5.4. Mais i est éloigné de $\hat{k}$ car $\hat{k}$ est réel, donc $\hat{k} = \mathbb{R}$. □

Théorème 5.6. *Soit k un corps archimédien avec $|2| = 2$. Les propriétés suivantes sont équivalentes.*

(i) *k est complexe ;*

(ii) *$|a^2 + 1| < 3/4$ pour un $a \in k$;*

(iii) *il existe un $i \in \hat{k}$ tel que $i^2 = -1$;*

(iv) *$\hat{k} \simeq \mathbb{C}$.*

Démonstration. Clairement (i) implique (ii), et (iv) implique (i).

Supposons (ii). Si $|a^2 + 1| < 3/4$, $|a|^2 > 1/4$, donc si $b = (a - 1/a)/2$, on a

$$|b^2 + 1| = |(a^2 + 1)^2/4a^2| \leqslant |a^2 + 1|^2.$$

Définissons une suite en posant $a_0 = a$ et $a_{n+1} = (a_n - 1/a_n)/2$. Nous avons $a_n^2 \to -1$, et l'inégalité $|a_{n+1} - a_n| = |a_n^2 + 1|/2|a_n| < |a_n^2 + 1|$ montre que nous avons une suite de Cauchy.

Supposons maintenant (iii). D'après le théorème 5.1, nous pouvons supposer que $\mathbb{R} \subseteq \hat{k}$, et $\mathbb{R}(i) \simeq \mathbb{C}$ d'après le théorème 5.2, donc $\hat{k} \simeq \mathbb{R}(i)$ d'après le théorème 5.4. □

En utilisant la condition (ii) du théorème 5.6 et la cotransitivité, nous voyons qu'un corps archimédien est réel si, et seulement si, il n'est pas complexe.

Corolaire 5.7 (Ostrowski)**.** *Soit k est un corps valorisé localement précompact avec $|2| = 2$. Alors $\hat{k} \simeq \mathbb{R}$ ou $\hat{k} \simeq \mathbb{C}$.*

Démonstration. Comme k est localement précompact, nous pouvons calculer l'infimum de $|a^2 + 1|$ pour $a \in k$. Si cet infimum est $< 3/4$, k est complexe d'après le théorème 5.6. Si l'infimum est > 0, k est réel. □

Comme le complété $\hat{k}$ d'un corps discret n'est pas discret en général, il est souvent utile de travailler plutôt avec la clôture séparable $\tilde{k}$ de k dans $\hat{k}$. Comme dans le cas ultramétrique le corps $\tilde{k}$ est intimement relié avec le lemme de Hensel, nous appelons $\tilde{k}$ le **hensélisé** de k. Le théorème suivant caractérise pour un corps archimédien k le fait d'être réel ou complexe en termes de son hensélisé.

Théorème 5.8. *Soit k un corps discret archimédien. Alors $\tilde{k}$ est factoriel si, et seulement si, k est réel ou complexe. Si k est complexe, $\tilde{k}$ est algébriquement clos. Si k est réel, le hensélisé de $k(i)$ est $\tilde{k}(i)$, qui est algébriquement clos, et tout polynôme sur $\tilde{k}$ est un produit de polynômes irréductibles de degrés* 1 *ou* 2.

Démonstration. Si $\tilde{k}$ est factoriel, ou bien X^2+1 a une racine dans $\tilde{k}$, ou bien X^2+1 est irréductible sur $\tilde{k}$. Dans le premier cas, k est complexe d'après le théorème 5.6(iii) ; dans le second cas, k est réel parce que le point (iii) du théorème 5.6 est impossible, donc $|a^2+1| > 1/2$ pour tout $a \in k$. Si k est complexe, $\hat{k} \simeq \mathbb{C}$, donc $\tilde{k}$ est algébriquement clos, donc factoriel. Si k est réel, $\hat{k} \simeq \mathbb{R}$, et nous pouvons supposer que $\hat{k} = \mathbb{R}$. Soit f un polynôme de degré > 0 dans $\tilde{k}[X]$. Alors f a une racine complexe $a+bi$, et $a-bi$ est aussi une racine de f. Donc a et b sont algébriques sur $\tilde{k}$, et donc sont dans $\tilde{k}$ (ainsi le hensélisé de $k(i)$ est $\tilde{k}(i)$). Si $b=0$, $X-a$ est un facteur de f. Si $b \neq 0$, $X^2-2aX+a^2+b^2$ est un facteur irréductible de f dans $\tilde{k}[X]$. □

Exercices

1. Construire un exemple brouwerien d'une valeur absolue ultramétrique sur $\mathbb{Q}$ qui n'est ni triviale ni équivalente à une valeur absolue p-adique. Comparer avec le théorème 5.1.
2. Montrer que $I_S(1/z)$ dans la démonstration du théorème 5.4 tend vers $2\pi i$ lorsque $n \to \infty$, en utilisant que
$$\int_0^1 (1+x^2)^{-1} dx = \pi/4.$$
3. Montrer que si tout corps archimédien peut être plongé dans $\mathbb{C}$, alors l'axiome du choix le plus simple du monde est satisfait (utiliser la construction de l'exercice VI.3.1).

6 Le lemme de Hensel

Soient k un corps valorisé ultramétrique et $\overline{k}$ son corps résiduel. Soit f un polynôme unitaire de $k[X]$ dont la valeur des coefficients est $\leqslant 1$. Alors f définit un polynôme $\overline{f} \in \overline{k}[X]$. Une forme standard du lemme de Hensel est que si $\overline{f}$ a une racine simple dans $\overline{k}[X]$ et si k est complet, alors f a une racine dans k. Plus généralement, si $\overline{f}$ se décompose en facteurs deux à deux étrangers, cette factorisation provient d'une factorisation de f (voir l'exercice 6.2). Notre version du lemme de Hensel concerne la manière d'approximer des factorisations de f par des factorisations en facteurs deux à deux étrangers.

Tout d'abord, nous montrons comment étendre une valeur absolue ultramétrique sur k en une valeur absolue sur $k(X)$, en spécifiant (de manière arbitraire)

la valeur absolue de X. Le lemme suivant est nécessaire parce que nous n'avons pas moyen de déterminer un coefficient de valeur maximum.

Lemme 6.1. *Soient $s_1, \dots, s_\ell$ des nombres réels, σ leur supremum, et m un entier > 0. Alors, sauf pour au plus $(m+1)(\ell-1)$ entiers strictement positifs n, nous pouvons construire un sous-ensemble fini A de $\{1, \dots, \ell\}$ tel que*

$$s_i > \sigma - 2^{-(m+n)} \text{ si } i \in A, \text{ et } s_i < \sigma - 2^{-n} \text{ si } i \notin A.$$

Démonstration. Pour chaque entier $n > 0$, nous pouvons construire un sous-ensemble fini A_n de $\{1, \dots, \ell\}$ tel que

$$s_i > \sigma - 2^{-(n-1)} \text{ si } i \in A_n, \text{ et } s_i < \sigma - 2^{-n} \text{ si } i \notin A_n.$$

Les A_n forment une chaine descendante de sous-ensembles finis non vides de $\{1, \dots, \ell\}$. Comme $\#A_1 \leqslant \ell$, il y a au plus $\ell - 1$ valeurs de n pour lesquelles $A_{n+1} \neq A_n$, et donc au plus $(m+1)(\ell-1)$ valeurs de n telles que $A_{m+n+1} \neq A_n$. Pour une autre valeur de n nous posons $A = A_n = A_{m+n+1}$. □

Théorème 6.2. *Soient k un corps ultramétrique et λ un nombre réel > 0. Pour $f(X) = \sum a_i X^i \in k[X]$ on pose $|f| = \sup |a_i| \lambda^i$. Cela définit une valeur absolue sur $k(X)$.*

Démonstration. Il suffit de démontrer que l'on a défini une valeur absolue sur $k[X]$.
Soit $g(X) = \sum b_i X^i$. La seule difficulté est de montrer que $|fg| = |f||g|$. Clairement $|fg| \leqslant |f||g|$, donc il suffit de montrer que $|fg| + \varepsilon > |f||g|$ pour tout $\varepsilon > 0$. Si $|f||g| < \varepsilon$, nous avons terminé. Supposons donc $|f||g| > 0$, i.e. $|f| > 0$ et $|g| > 0$. On considère m et n tels que

$$2^{-m} \sup(1, |f| + |g|) < \inf(|f|, |g|) \text{ et } 2^{-n} \inf(|f|, |g|) < \varepsilon,$$

et on utilise le lemme 6.1 pour construire des sous-ensembles finis A et B des ensembles d'indices des coefficients de f et g, respectivement, tels que

$$\begin{array}{ll} |a_i| > |f| - 2^{-(n+m)} > 0 & \text{si } i \in A \\ |a_i| < |f| - 2^{-n} & \text{si } i \notin A \\ |b_j| > |g| - 2^{-(n+m)} > 0 & \text{si } j \in B \\ |b_j| < |g| - 2^{-n} & \text{si } j \notin B \end{array}$$

Soit $r = |f||g| - 2^{-n} \inf(|f|, |g|)$. Si $i \in A$ et $j \in B$, alors

$$\begin{aligned} |a_i X^i b_j X^j| &> (|f| - 2^{-(n+m)})(|g| - 2^{-(n+m)}) \\ &> |f|\,|g| - 2^{-(n+m)}(|f| + |g|) > r. \end{aligned}$$

Si $j \notin B$, $|a_i X^i b_j X^j| < |f|(|g| - 2^{-n}) = |f||g| - 2^{-n}|f| \leqslant r$. Même chose pour $i \notin A$.

On écrit $f = f_1 + f_2$ et $g = g_1 + g_2$ avec $f_1 = \sum_{i\in A} a_i X^i$ et $g_1 = \sum_{j\in B} b_j X^j$. Alors

$$fg = f_1g_1 + f_1g_2 + f_2g_1 + f_2g_2 \quad \text{et} \quad |f_1g_2 + f_2g_1 + f_2g_2| < r.$$

En considérant le monôme de plus haut degré dans f_1g_1, on voit que $|f_1g_1| > r$. Donc $|fg| = |f_1g_1| > r > |f||g| - \varepsilon$. □

Nous pouvons maintenant donner un exemple d'un corps résiduel qui n'est pas un anneau local. Soit k un corps avec une valeur absolue ultramétrique, et soient α et β des nombres réels > 0 tels que $\sup(\alpha, \beta) = 1$. En appliquant deux fois le théorème 6.2, nous obtenons une valeur absolue sur le corps des fractions rationnelles $k(X, Y)$ telle que $|X| = \alpha$ et $|Y| = \beta$ et $|X + Y| = \sup(\alpha, \beta) = 1$. Dans le corps résiduel $\overline{k(X, Y)}$, nous avons $X + Y$ inversible, mais nous ne pouvons pas affirmer que X ou Y est inversible (voir l'exercice II.3.5).

Le théorème suivant donne une borne sur la valeur du reste dans l'algorithme de division (théorème II.5.2) dans le cas d'un corps ultramétrique.

Théorème 6.3. *Soient k un corps ultramétrique,*

$$g(X) = b_0 + b_1X + \cdots + b_mX^m \quad et \quad \varphi(X) = a_0 + a_1X + \cdots + a_nX^n.$$

avec a_n inversible. On étend la valeur absolue à $k[X]$ selon le théorème 6.2. On pose $s = |\varphi(X)|/|a_nX^n|$ et $M = \max(m - n + 1, 0)$. Il existe des polynômes $q, r \in k[X]$ tels que

$$g(X) = q(X)\varphi(X) + r(X)$$

avec $\deg r(X) < \deg \varphi(X)$ et $|r(X)| \leqslant s^M|g(X)|$.

Démonstration. Nous procédons par récurrence sur m, que nous pouvons supposer $\geqslant n$. On écrit

$$g_1(X) = g(X) - \varphi(X)X^{m-n}b_m/a_n.$$

Alors $|\varphi(X)X^{m-n}b_m/a_n| = s|b_mX^m| \leqslant s|g(X)|$, donc $|g_1(X)| \leqslant s|g(X)|$ (parce que $s \geqslant 1$). Par récurrence, $g_1(X) = q_1(X)\varphi(X) + r(X)$ avec $\deg r(X) < \deg \varphi(X)$ et $|r(X)| \leqslant s^{M-1}|g_1(X)| \leqslant s^M|g(X)|$. On prend $q(X) = q_1(X) + X^{m-n}b_m/a_n$. □

L'objectif du lemme de Hensel est de construire une factorisation approchée d'un polynôme avec des facteurs approximativement étrangers.

Définition 6.4. Soit k un corps ultramétrique. On étend la valeur absolue à $k[X]$ selon le théorème 6.2. Un **contexte hensélien** est donné par

$$f, \varphi, \psi, h, A, B, C \in k[X], \qquad d \in k, \quad L, M \in \mathbb{N}, \quad \varepsilon \in \mathbb{Q}$$

tels que

(i) $f = \varphi\psi + h$;

(ii) $A\varphi + B\psi = d + C$;

(iii) $|\psi| \leqslant 1$ et $|B| \leqslant 1$;

(iv) $\varphi = \sum_{i=0}^{n} a_i X^i$ et $|a_n| \neq 0$;

(v) $\deg f$, $\deg h$, $n \leqslant L$;

(vi) $\deg A \leqslant M - L - 1$ et $\deg B \leqslant M - 2(L - n) - 1$;

(vii) $0 < |d| \leqslant 1$ et $\varepsilon < 1$;

(viii) $s^M |C/d| \leqslant \varepsilon$ et $s^{2M} |h/d^2\varphi| \leqslant \varepsilon$ où $s = |\varphi|/|a_n X^n| \geqslant 1$.

La condition (i) dit que $\varphi\psi$ approche f à h près, et (viii) dit que h est petit par rapport à φ. La condition (viii) dit également que $|C|$ est petit par rapport à $|d|$, donc (ii) dit φ et ψ sont approximativement étrangers [1].

Lemme 6.5. *Soit $f, \varphi, \psi, h, A, B, C, d, L, M, \varepsilon$ un contexte hensélien. Alors*

(i) $|A\varphi| \leqslant 1$,

(ii) $\deg \psi \leqslant L - n$,

(iii) $\deg C \leqslant M$,

(iv) $\deg Ch$, $\deg Bh \leqslant M + n - 1$.

Démonstration. La définition 6.4(ii) nous donne

$$|A\varphi| \leqslant \sup\{|B\psi|, |d|, |C|\} \leqslant 1$$

en utilisant les majorations sur $|B|, |\psi|, |d|$ et $|C|$ dans la définition. Comme $\deg \varphi\psi = \deg(f - h) \leqslant L$, et comme le coefficient dominant a_n de φ est inversible, nous avons $\deg \psi \leqslant L - n$. Donc

$$\deg C \leqslant \sup(\deg A + n,\ \deg B + L - n) \leqslant M - L - 1 + n$$

et $\deg Ch \leqslant M + n - 1$. Enfin,

$$\deg Bh \leqslant M - (L - n) + n - 1 \leqslant M + n - 1. \qquad \square$$

Le cœur du lemme de Hensel consiste en la possibilité de raffiner un contexte hensélien.

1. **NdT.** Un contexte hensélien pour un corps ultramétrique décrit donc d'une manière précise, contrôlée par ε, une factorisation approchée de $f \in k[X]$ en un produit $\varphi\psi$ de deux polynômes approximativement étrangers. Notez que si k n'est pas discret, seul le degré de φ est à priori bien défini. Par ailleurs, la valeur précise de s dépend du choix de $\lambda = |X|$ dans le théorème 6.2.

Théorème 6.6. *Il existe une fonction entre contextes henséliens qui, à partir du contexte*

$$f, \varphi, \psi, h, A, B, C, d, L, M, \varepsilon$$

produit un contexte

$$f, \varphi^*, \psi^*, h^*, A, B, C^*, d, L, M, \varepsilon$$

avec les propriétés suivantes[1].

(i) $|h^*| \leqslant \varepsilon |h|$;

(ii) φ^* *a le même degré et le même coefficient dominant que* φ ;

(iii) $|\varphi^* - \varphi| \leqslant s^M |h/d| \leqslant s^{-M}\varepsilon |d\varphi|$, *d'où* $|\varphi^*| = |\varphi|$;

(iv) $|\psi^* - \psi| \leqslant s^M |h/d\varphi| \leqslant s^{-M}\varepsilon |d|$.

Démonstration. Nous allons construire $\varphi^* = \varphi + \beta$ et $\psi^* = \psi + \alpha$ qui satisfont les conditions (ii), (iii) et (iv), et nous définirons

$$h^* = f - \varphi^*\psi^* \text{ et } C^* = A\varphi^* + B\psi^* - d.$$

Nous devons d'abord démontrer la condition (i), $\deg h^* \leqslant L$, et $s^M|C^*/d| \leqslant \varepsilon$. Le fait que $|\psi^*| \leqslant 1$ résulte de la condition (iv).

D'après le lemme 6.5(iv), nous pouvons appliquer le théorème 6.3 avec $g = Bh/d$ et $g = Ch/d$ ce qui donne

$$\begin{aligned} Bh/d &= q\varphi + \beta, \\ Ch/d &= p\varphi + r, \end{aligned}$$

où $\deg \beta < n$, $\deg r < n$ et

$$\begin{aligned} |\beta| &\leqslant s^M|Bh/d| \leqslant s^M|h/d|, \\ |r| &\leqslant s^M|Ch/d| \leqslant \varepsilon|h|. \end{aligned}$$

En définissant $\varphi^* = \varphi + \beta$, on obtient les conditions (ii) et (iii). On pose

$$\alpha = Ah/d + q\psi - p.$$

Alors en multipliant 6.4(ii) par h/d, on a

$$\alpha\varphi + \beta\psi = h + r,$$

1. **NdT.** D'après les égalités dans (ii) et (iii), la valeur de s dans le nouveau contexte est la même que celle dans le premier contexte ; et ceci explique qu'il n'y ait pas de s^* dans l'énoncé. Notez que seuls φ, ψ, h et C sont modifiés. Le point (i) indique dans quelle mesure la contexte a été amélioré.

donc $\deg \alpha\varphi \leqslant L$, puisque $\deg \beta\psi \leqslant n + (L-n)$ d'après le point 6.5(ii), donc $\deg \alpha \leqslant L - n$. Nous avons aussi

$$\begin{aligned} |\alpha\varphi| &\leqslant \sup\{|\beta\psi|, |h|, |r|\} \\ &\leqslant \sup\{|\beta|, |h|, |r|\} \\ &\leqslant \sup\{s^M \left|h/d\right|, |h|, \varepsilon\,|h|\} = s^M \left|h/d\right|, \end{aligned}$$

et donc

$$|\alpha| \leqslant s^M |h/d\varphi|.$$

Ainsi la condition (iv) est satisfaite pour $\psi^* = \psi + \alpha$.

Soit $h^* = f - \varphi^*\psi^*$. Alors

$$h^* = h - (h+r) - \alpha\beta = -r - \alpha\beta,$$

donc

$$\deg h^* \leqslant \sup(\deg r, \deg \alpha\beta) \leqslant L.$$

Nous avons aussi

$$\begin{aligned} |h^*| &\leqslant \sup(|r|, |\alpha\beta|) \\ &\leqslant \sup\{s^M \left|Ch/d\right|, \left(s^M \left|h\right| / \left|d\varphi\right|\right) s^M \left|h/d\right|\} \\ &\leqslant \varepsilon|h|, \end{aligned}$$

ce qui donne la condition (i). Nous définissons C^* par

$$A\varphi^* + B\psi^* = d + C^*$$

Il reste à vérifier la majoration pour $|C^*|$ dans la définition 6.4(viii). Nous avons

$$C^* = C + A\beta + B\alpha,$$

donc

$$\begin{aligned} s^M|C^*| \leqslant s^M \sup\{|C|, |A\beta|, |B\alpha|\} &= s^M \sup\{|C|, |A\varphi||\beta/\varphi|, |\alpha|\} \\ &= \sup\{s^M|C|, s^{2M}|h|/\left|d\varphi\right|, s^{2M}|h|/|d\varphi|\} \leqslant \varepsilon|d|. \end{aligned}$$ □

Définition 6.7. Soit k un corps ultramétrique. On prolonge la valeur absolue à $k[X]$ *via* le théorème 6.2. Nous disons que k est **hensélien** si chaque fois que

$$f, \varphi, \psi, h, A, B, C, d, L, M, \varepsilon$$

est un contexte hensélien, il existe un contexte hensélien

$$f, \hat{\varphi}, \hat{\psi}, 0, A, B, \hat{C}, d, L, M, \varepsilon$$

tel que $\hat{\varphi}$ a le même degré et le même coefficient dominant que φ [1].

1. **NdT.** Notez que l'on a maintenant la factorisation exacte $f = \hat{\varphi}\,\hat{\psi}$.

Notez que cette définition dépend de la valeur absolue $\lambda = |X|$ choisie dans le théorème 6.2. En fait, cette dépendance est seulement apparente, au moins pour les corps discrets, comme nous le verrons dans le théorème 6.11.

Théorème 6.8 (lemme de Hensel)**.** *Un corps ultramétrique complet est hensélien.*

Démonstration. Soit $f, \varphi, \psi, h, A, B, C, d, L, M, \varepsilon$ un contexte hensélien. D'après le théorème 6.6, nous pouvons construire des suites $\{\varphi_i\}$, $\{\psi_i\}$, $\{h_i\}$ et $\{C_i\}$ telles que $f, \varphi_i, \psi_i, h_i, A, B, C_i, d, L, M, \varepsilon$ est un contexte hensélien, $\varphi_0 = \varphi$, $\psi_0 = \psi$, $h_0 = h$, $C_0 = C$ et

(i) $|h_{i+1}| \leqslant \varepsilon |h_i|$;

(ii) φ_i a le même degré et le même coefficient dominant que φ ;

(iii) $|\varphi_{i+1} - \varphi_i| \leqslant s^M |h/d| \leqslant s^{-M} \varepsilon |d\varphi|$;

(iv) $|\psi_{i+1} - \psi_i| \leqslant s^M |h/d\varphi| \leqslant s^{-M} \varepsilon |d|$.

Les points (i), (iii) et (iv) impliquent que $h_i \to 0$, et que les autres suites sont de Cauchy. Comme tous les degrés sont bornés, et comme k est complet, nous avons $\varphi_i \to \hat{\varphi}$, $\psi_i \to \hat{\psi}$, et $C_i \to \hat{C}$, avec $\hat{\varphi}, \hat{\psi}, \hat{C} \in k[X]$. Comme toutes les conditions sur $\hat{\varphi}, \hat{\psi}$ et $\hat{C}$ sont des égalités et des inégalités larges satisfaites par φ_i, ψ_i et C_i, on obtient facilement le résultat [1]. □

Notez que si k est un corps discret, la clôture algébrique de k dans $\hat{k}$ est un corps hensélien d'après le corolaire VII.1.5, et un corps discret d'après le théorème VI.1.9. Ceci nous donne une grande quantité de corps henséliens discrets : par exemple, la clôture algébrique du corps des rationnels dans le corps des nombres p-adiques.

Corolaire 6.9. *Soit $f(X) = a_r X^r + \cdots + a_1 X + a_0$ un polynôme sur un corps hensélien k. Si pour un $n < r$ on a $a_n \neq 0$ et*

$$|(a_j X^j / a_n X^n)^{2(2(r-n)+1)} a_m X^m| < \sup\{\, |a_i X^i| : 0 \leqslant i \leqslant n \,\}$$

pour tout $j \leqslant n < m \leqslant r$, alors f a un facteur de degré n dans $k[X]$.

Démonstration. Nous définissons un contexte hensélien. On pose $\varphi = a_n X^n + \cdots + a_0$ et $\psi = 1$, donc $h = f - \varphi\psi = a_r X^r + \cdots + a_{n+1} X^{n+1}$. On prend $A = C = 0$, $B = d = 1$, $L = r$ et $M = 2(r-n)+1$. Les hypothèses impliquent qu'il y a un $\varepsilon < 1$ tel que $s^{2M}|h| \leqslant \varepsilon |\varphi|$. Ainsi, $f, \varphi, \psi, h, A, B, C, d, L, M, \varepsilon$ est un contexte hensélien. Comme k est hensélien, nous obtenons le facteur souhaité. □

1. **NdT.** De plus, $|\hat{\varphi} - \varphi| \leqslant s^M |h/d|$ et $|\hat{\varphi}| = |\varphi|$.

Corolaire 6.10. *Soit $f = a_r X^r + \cdots + a_1 X + a_0$ un polynôme sur un corps hensélien k. Si*

$$0 < |a_r X^r| < |f| = \sup\{\, |a_i X^i| : 0 < i < r \,\},$$

le polynôme f est réductible sur k.

Démonstration. D'après le lemme 6.1, nous pouvons construire un sous-ensemble fini A de $\{0, \ldots, r\}$ tel que

$$|a_i X^i| > |f| - 2^{-(m+t)} \text{ si } i \in A$$

et

$$|a_i X^i| < |f| - 2^{-t} \text{ si } i \notin A.$$

De plus, nous pouvons prendre m et t tels que $N = 4r + 2 < 2^m$ et $2^{-t} < |f|$. Alors

$$\begin{aligned} (|f| - 2^{-(m+t)})^N &> (|f| - 2^{-t}/N)^N \\ &> |f|^N - 2^{-t}|f|^{N-1} = |f|^{N-1}(|f| - 2^{-t}), \end{aligned}$$

donc

$$\left(\frac{|f|}{|f| - 2^{-(m+t)}}\right)^N (|f| - 2^{-t}) < |f|.$$

Nous pouvons aussi supposer que $|a_r X^r| + 2^{-(m+t)} < |f|$, donc que $r \notin A$. Soit n le plus grand élément de A. Comme $|f| = \sup\{\, |a_i X^i| : 0 < i < r \,\}$, nous avons $n > 0$. Les hypothèses du corolaire 6.9 sont satisfaites, donc f a un facteur de degré n dans $k[X]$. □

Théorème 6.11. *Soit k un corps hensélien discret avec une valeur absolue triviale ou non triviale, et soit f un polynôme séparable de $k[X]$. Alors il existe un $\delta > 0$ tel que si $|f - \varphi\psi| < \delta$ et si $\deg f = \deg \varphi\psi$, alors f a un facteur dans $k[X]$ de même degré que φ.*

Démonstration. Le cas de la valeur absolue triviale est trivial, donc nous pouvons supposer qu'il existe un $e \in k$ tel que $0 < |e| < 1$. Pour tout polynôme non nul $p \in k[X]$, notons $L(p)$ la valeur absolue du monôme dominant de p. Comme la fonction qui envoie le polynôme $F(X)$ sur $F(X/e^m)$ est un automorphisme de $k[X]$ uniformément bicontinu sur les polynômes de degré borné, nous pouvons supposer que $|f| = L(f)$. En utilisant l'algorithme d'Euclide, et en multipliant par une puissance convenable de e, nous trouvons a et $b \in k[X]$ tels que $|a| \leqslant 1$, $|b| \leqslant 1$ et

$$0 \neq af + bf' = d \in k$$

avec $|d| \leqslant 1$, et $|af| < |e|^2$ et $|bf| < |e|^2|X|$. On pose

$$\delta = |d|^2 \inf(|X|, |f|).$$

Supposons maintenant que $|f-\varphi\psi|<\delta$ et $\deg f=\deg\varphi\psi$. Comme $\delta\leqslant 2|f|=L(f)$, nous avons $|f|=|\varphi\psi|$ et $L(f)=L(\varphi\psi)$, donc $|\varphi|=L(\varphi)$, i.e. $s=1$ dans la définition 6.4. On prend $h=f-\varphi\psi$. En multipliant ψ par une puissance convenable de e, et en multipliant φ par la même puissance de e^{-1}, nous pouvons supposer que $|e|^2<|\psi|<1$, donc $|f|=|\varphi\psi|<|\varphi|<|f|/|e|^2$. Alors $|a\varphi|<|af|/|e|^2<1$ et $|b\varphi|<|bf|/|e|^2<|X|$. Il existe un $\varepsilon<1$ tel que $|h|\leqslant\varepsilon\delta\leqslant\varepsilon|d^2|\inf(|X|,|f|)\leqslant\varepsilon|d^2\varphi|$. Notez que si $F\in k[X]$, alors $|F'|\leqslant|F|/|X|$, donc $|f'-\varphi'\psi-\varphi\psi'|\leqslant\varepsilon|d|^2$ et $|b\varphi'|<1$. Donc

$$\varepsilon|d|^2\geqslant|ah+b(f'-\varphi'\psi-\varphi\psi')|=|d-[(a\varphi+b\varphi')\psi+b\psi'\varphi]|\,;$$

en posant

$$A=b\psi',$$
$$B=a\varphi+b\varphi',$$
$$C=A\varphi+B\psi-d,$$
$$L=\max(\deg f,\deg h,n),$$

et en prenant M aussi grand que nécessaire ($s=1$), nous obtenons un contexte hensélien. Comme le corps k est hensélien, le facteur souhaité peut être construit. □

Ce théorème reste-t-il vrai sans l'hypothèse que la valeur absolue sur k est triviale ou non triviale ?

Rappelons que lorsque k est un corps valorisé discret, nous définissons le hensélisé $\tilde{k}$ de k comme la clôture séparable de k dans $\hat{k}$. Cette terminologie est justifiée par le fait qu'un corps discret avec une valeur absolue ultramétrique est hensélien exactement quand il est séparablement clos dans son complété (théorème 6.13).

Lemme 6.12. *Soit $\varphi(X)=a_nX^n+\cdots+a_0$ un polynôme sur un corps ultramétrique k avec $|a_n|\neq 0$. Posons $s=|\varphi|/|a_nX^n|$. Soient $C\in k[X]$ et $d\in k$ tels que $s^M|C|<|d|$ et $\deg C\leqslant M$. Alors φ et $d+C$ sont premiers entre eux.*

Démonstration. Soit $\theta=\theta_0+\theta_1X+\cdots+\theta_rX^r$ un facteur commun de φ et $d+C$. Soit $d+C=\theta\sigma$ avec $\sigma=\sigma_0+\sigma_1X+\cdots+\sigma_tX^t$. Comme $|C|<|d|$, on a $|\theta_0\sigma_0|=|d|=|d+C|=|\theta||\sigma|$, donc $|\theta|=|\theta_0|$ et nous pouvons supposer que $\theta_0=1$. Supposons, par contradiction, que $r>0$ et $\theta_r\neq 0$. Comme θ est un facteur de φ et que $|\varphi/\theta|=|\varphi|$, on a $|\theta_rX^r|\geqslant|a_nX^n|/|\varphi|=1/s$. Donc $|\sigma_tX^t|\leqslant s|C|$. De la même manière $|\sigma_{t-1}X^{t-1}|\leqslant s^2|C|$ et de même jusqu'à $|\sigma_0|\leqslant s^{t+1}|C|$. Donc $t+1>M\geqslant\deg C$ et $\sigma_t=0$, et nous terminons par récurrence sur t, ce qui donne une contradiction pour $t=0$. □

Théorème 6.13. *Soit k un corps ultramétrique discret. Alors k est hensélien si, et seulement si, il est séparablement clos dans son complété.*

Démonstration. Supposons k séparablement clos dans son complété $\hat{k}$. Comme $\hat{k}$ est hensélien, nous pouvons construire les polynômes voulus $\hat{\varphi}$ et $\hat{\psi}$ à coefficients dans $\hat{k}$. Le coefficient dominant de $\hat{\varphi}$, et par suite le coefficient dominant de $\hat{\psi}$, sont dans k. D'après le théorème VII.1.4, tous les coefficients de $\hat{\varphi}$ et $\hat{\psi}$ sont algébriques sur k. Le lemme 6.12 dit que $\hat{\varphi}$ et $\hat{\psi}$ sont premiers entre eux, donc étrangers car leurs coefficients sont dans un sous-corps discret. Comme k est séparablement clos dans $\hat{k}$, les coefficients de $\hat{\varphi}$ et $\hat{\psi}$ sont dans k d'après le corolaire VII.1.6.

Supposons maintenant que k est hensélien et que $\theta \in \hat{k}$ est séparable sur k, i.e. θ annule un polynôme séparable f de $k[X]$. Si $\deg f = 1$, $\theta \in k$ et nous avons terminé. Sinon nous pouvons trouver un $\alpha \in k$ tel que $|f(\alpha)| < 1$. Comme k est discret, on sait si α annule f. Donc, ou bien f a une racine dans k, et nous obtenons un polynôme de degré plus petit annulé par θ, ou bien $|f(\alpha)| \neq 0$ et la valeur absolue sur k est non triviale. Dans ce cas, comme $f(\alpha) = f - (X - \alpha)\psi$ pour un $\psi \in k[X]$, le théorème 6.11 dit que nous pouvons trouver un facteur linéaire de f dans $k[X]$, et donc obtenir un polynôme de plus petit degré annulé par θ. □

Comme on l'avait signalé plus tôt, ce théorème montre que la définition d'un corps hensélien pour un corps discret est indépendante du choix de $|X|$.

Exercices

1. Soit $f \in \mathbb{Z}[X]$. Notons $\overline{f}$ l'image de f dans $\mathbb{Z}_p[X]$. Montrer que si $\overline{f}$ a une racine simple dans $\mathbb{Z}_p$, il existe un x dans le complété p-adique de $\mathbb{Q}$ qui annule f.
2. *Lemme de Hensel.* Soit k un corps hensélien et soit f un polynôme unitaire de $k[X]$ dont tous les coefficients ont une valeur absolue $\leqslant 1$. Si l'image $\overline{f}$ de f dans $\overline{k}[X]$ est un produit de deux polynômes unitaires étrangers λ et μ, f est un produit de polynômes unitaires φ et ψ tels que $\overline{\varphi} = \lambda$ et $\overline{\psi} = \mu$.

7 Extensions de valeurs absolues

Nous étudions maintenant la question du prolongement d'une valeur absolue de k à $k(\theta)$ lorsque θ est algébrique sur k. En général, nous devons nous restreindre au cas où $k(\theta)$ est de dimension finie sur k, i.e. où θ annule un polynôme irréductible (théorème VI.1.13). L'exemple suivant illustre à la fois les cas archimédien et ultramétrique.

Exemple. On munit le corps $\mathbb{Q}$ de la valeur absolue usuelle ou de la valeur absolue 7-adique. Soit $\sqrt{2}$ une racine carrée de 2, fixée, dans le complété $\hat{\mathbb{Q}}$ de $\mathbb{Q}$.

Soit a une suite binaire fugitive. Le corps

$$k = \bigcup\nolimits_n \mathbb{Q}(a_n\sqrt{2}) \subseteq \hat{\mathbb{Q}}$$

est discret, dénombrable, et localement précompact. On définit un corps $E = k(\theta)$ avec θ algébrique sur k en posant

$$E = \{\, s + t\theta : s, t \in k \,\}$$

où $\theta^2 = 2$ et l'égalité est définie en posant $s + t\theta = 0$ si $s = t = 0$, ou si $a_m = 1$ et $s = (-1)^m t\sqrt{2}$. Notez que E est un corps discret. Si nous arrivions à prolonger la valeur absolue à E, on aurait dans $\hat{E}$ la disjonction $|\theta - \sqrt{2}| \neq 0$ ou $|\theta + \sqrt{2}| \neq 0$. Et donc $a_m = 0$ pour tous les m impairs, ou $a_m = 0$ pour tous les m pairs, ce qui donne LLPO. □

Lemme 7.1. *Soient K un corps ultramétrique et k un sous-corps discret hensélien de K sur lequel la valeur absolue est triviale ou non triviale. Soit $\theta \in K$ une racine d'un polynôme séparable irréductible de degré n sur k. Alors il existe un $\varepsilon > 0$ tel que $|g(\theta)| \geqslant \varepsilon|g|$ pour tout $g \in k[X]$ de degré $\leqslant n$. Donc les éléments $1, \theta, \ldots, \theta^{n-1}$ forment une base métrique de $k(\theta)$ sur k.*

Démonstration. Nous construisons une suite $1 = \varepsilon_0 \geqslant \varepsilon_1 \geqslant \cdots \geqslant \varepsilon_{n-1} > 0$ telle que $|g(\theta)| \geqslant \varepsilon_m|g|$ si $\deg g = m$. Soit $g(X) = g_0 + g_1X + \cdots + g_mX^m$. Comme $|g| \leqslant \sup(1, |X|^n)\sup\{\, |g_i| : 0 \leqslant i \leqslant m \,\}$, nous pouvons supposer que $|X| = 1$. Nous pouvons supposer aussi que g est unitaire, donc $|g| \geqslant 1$.

Notons f le polynôme minimal de θ et supposons que nous avons construit ε_{m-1}. On pose $\mu = \sup(1, |\theta|^n)$ et

$$\varepsilon_m = \delta(\varepsilon_{m-1}/2\mu)^{n-m+2}|f|^{-1},$$

où $\delta \leqslant 1$ est obtenu par le théorème 6.11. On écrit $f = qg + r$ avec $\deg r < m$. D'après le théorème 6.3, on a $|r| \leqslant |g|^{n-m+1}|f|$, donc

$$|q| = |f - r|/|g| \leqslant |f||g|^{n-m},$$

d'où

$$|q(\theta)| \leqslant |q|\mu \leqslant |f||g|^{n-m}\mu.$$

On a $|g| > \mu/\varepsilon_{m-1}$ ou $|g| < 2\mu/\varepsilon_{m-1}$.
Si $|g| > \mu/\varepsilon_{m-1} \geqslant 1$, alors, par récurrence,

$$|g(\theta) - \theta^m| \geqslant \varepsilon_{m-1}|g(X) - X^m| = \varepsilon_{m-1}|g| > \mu \geqslant |\theta^m|,$$

et comme la valeur absolue est ultramétrique, on a

$$|g(\theta)| = |g(\theta) - \theta^m| \geqslant \varepsilon_{m-1}|g| \geqslant \varepsilon_m|g|.$$

Si $|g| < 2\mu/\varepsilon_{m-1}$, alors

$$|g(\theta)| = |r(\theta)|/|q(\theta)| \geqslant \varepsilon_{m-1}|r|/|f||g|^{n-m}\mu$$

car $\deg r < m$. Comme f est irréductible, le théorème 6.11 dit que $|r| \geqslant \delta$, d'où

$$\varepsilon_{m-1}|r|/|f||g|^{n-m}\mu > \varepsilon_{m-1}\delta|g|/|f|(2\mu/\varepsilon_{m-1})^{n-m+1}\mu = 2\varepsilon_m|g| > \varepsilon_m|g|. \quad \square$$

L'hypothèse que la valeur absolue est triviale ou non triviale dans ce lemme était nécessaire pour appliquer le théorème 6.11. Le lemme reste-t-il vrai sans cette hypothèse ?

Lemme 7.2. *Soient k un corps discret hensélien et K une extension séparable de dimension finie de k. Alors deux valeurs absolues sur K qui prolongent la valeur absolue sur k sont égales.*

Démonstration. On peut écrire $K = k(\theta)$ avec θ séparable de degré n (corollaire VI.5.5). Notons f le polynôme minimal de θ. Soient $|\ |_1$ et $|\ |_2$ des valeurs absolues sur K qui prolongent celle sur k.

Supposons que $|b|_1 > |b|_2$ pour un $b \in K$. Comme $f(\theta) = 0$, si on prend $|X| = 1$ (théorème 6.2), on a $|\theta|_i \leqslant |f(X)|$. Tout élément a de K peut être écrit de manière unique sous forme $a = g_a(\theta)$ avec $g_a \in k[X]$ de degré $< n$. Si la valeur absolue sur k est triviale ou non triviale, alors d'après le lemme 7.1, nous avons pour un $\varepsilon > 0$

$$|f(X)|^n|g_a(X)| \geqslant |a|_i \geqslant \varepsilon|g_a(X)|.$$

Mais alors il existe un m tel que $|b^m|_1 > (|f(X)|^n/\varepsilon)|b^m|_2$, ce qui est impossible. Donc si $|b|_1 > |b|_2$, il est impossible que la valeur absolue soit triviale ou non triviale ; mais une valeur absolue sur un corps discret est triviale si, et seulement si, elle n'est pas non triviale, donc $|b|_1 > |b|_2$ implique que la valeur absolue est à la fois triviale et non triviale. En bref $|b|_1 > |b|_2$ est impossible.

Donc $|b|_1 \leqslant |b|_2$ pour tout $b \in K$. $\square$

Soit E un corps extension de dimension finie d'un corps discret k. La **norme**[1] $\mathrm{N}_{E/k}$ **de l'extension** E/k est définie en posant, pour $x \in E$, $\mathrm{N}_{E/k}(x)$ égal au déterminant de la transformation k-linéaire de E définie par la multiplication par x.

Nous noterons V_k le groupe de valeurs d'un corps valorisé k.

Théorème 7.3. *Soient k un corps discret hensélien et E une extension de dimension finie de k. Alors la valeur absolue sur k se prolonge de manière unique à E, et $\mathrm{V}_E^\ell \subseteq \mathrm{V}_k$ pour un entier $\ell > 0$. Donc si le groupe de valeurs de k est discret, il en va de même pour le groupe de valeurs de E.*

1. **NdT.** The field norm of $\mathrm{N}_{E/k}$ from E to k.

Démonstration. Soit F la clôture séparable de k dans E. Comme $E^m \subseteq F$ pour un entier $m > 0$ (théorème VI.6.8), toute valeur absolue sur F se prolonge de manière unique à E, et nous pouvons supposer que E est séparable. Le lemme 7.2 donne l'unicité. Pour construire une valeur absolue sur E, on pose pour $\theta \in E$

$$|\theta| = |\mathrm{N}(\theta)|^{1/n},$$

où $\mathrm{N} = \mathrm{N}_{E/k}$ et $n = \dim_k E$. Pour montrer que cela définit une valeur absolue ultramétrique, il suffit de vérifier que $|\mathrm{N}(1+\theta)| \leqslant 1$ si $|\mathrm{N}(\theta)| \leqslant 1$ (corolaire 1.5). On suppose $|\mathrm{N}(\theta)| \leqslant 1$ et l'on note

$$f(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_0.$$

le polynôme minimal de θ.

Comme $\mathrm{N}(\theta)$ est une puissance de $|\mathrm{N}_{k(\theta)/k}(\theta)|$ [1], on a $|a_0| = |\mathrm{N}_{k(\theta)/k}(\theta)| \leqslant 1$. D'après le corolaire 6.10, on a $|a_i| \leqslant 1$ pour tout i, car $\sup |a_i| > 1$ implique que f est réductible, ce qui est impossible. Or $f(X-1)$ est le polynôme minimal de $1+\theta$ et son terme constant est $\pm(1 + \sum \pm a_i)$. Comme la valeur absolue est ultramétrique, on a $|1 + \sum \pm a_i| \leqslant 1$, et comme $\mathrm{N}(1+\theta)$ est une puissance de ce terme, on a $|\mathrm{N}(1+\theta)| \leqslant 1$.

Enfin, on prend $\ell = mn$. □

Théorème 7.4. *Soient k un corps discret hensélien avec une valeur absolue triviale ou non triviale, et E une extension séparable de dimension finie de k. Alors E est hensélien.*

Démonstration. D'après le théorème 6.13, il suffit de démontrer que E est séparablement clos dans son complété. Soit $E = k(\theta)$. Comme k est séparablement clos dans $\hat{k}$, le théorème VII.2.3 dit que E est séparablement clos dans $\hat{k}(\theta)$. Le lemme 7.1 montre que la norme sur $k(\theta)$ donnée par la valeur absolue est équivalente à la norme du sup sur k^n, donc $\hat{k}(\theta) = \hat{E}$. □

D'après le corolaire 3.5, le hensélisé d'un corps discret pseudofactoriel est séparablement factoriel. Il y a donc un grand nombre de situations où le théorème suivant s'applique.

Théorème 7.5. *Soit k un corps discret avec une valeur absolue non triviale qui est réelle, ou complexe, ou ultramétrique. On note $\tilde{k}$ le hensélisé de k, et on considère un corps $E = k(\theta)$ extension de dimension finie séparable de k. Si le polynôme minimal de θ sur k est un produit $g_1 g_2 \cdots g_s$ de facteurs irréductibles dans $\tilde{k}[X]$, il existe des valeurs absolues $|\ |_1, \ldots, |\ |_s$ distinctes sur E qui prolongent la valeur absolue $|\ |$ sur k, et telles que, en notant $\tilde{E}_i$ le hensélisé de E pour $|\ |_i$, les propriétés suivantes sont satisfaites.*

1. **NdT.** Si $e_1, \ldots, e_r$ est une base de E sur $k(\theta)$, E est la somme directe des k-espaces vectoriels $e_i k(\theta)$; alors la multiplication par θ opère sur chaque facteur direct avec pour déterminant $|\mathrm{N}_{k(\theta)/k}(\theta)|$.

(i) *Le polynôme g_i est le polynôme minimal de θ sur $\tilde{k}$ vu comme sous-corps de $\tilde{E}_i$.*

(ii) *Toute valeur absolue sur E qui prolonge $|\ |$ est égale à une $|\ |_i$.*

(iii) *Le degré $n_i = [\tilde{E}_i : \tilde{k}]$ est égal au degré de g_i, et l'on a $\sum_i n_i = n$.*

Démonstration. Soit α une racine de g_i dans un corps discret extension de $\tilde{k}$ (c'est possible parce que g_i est irréductible sur $\tilde{k}$). D'après le théorème 7.3 dans le cas ultramétrique, et d'après les théorèmes 5.2 et 5.8 dans le cas archimédien, nous pouvons prolonger $|\ |$ à $\tilde{k}(\alpha)$ de manière unique. Comme α annule le polynôme minimal de θ sur k, il y a un monomorphisme $\varphi\colon E \to \tilde{k}(\alpha)$ qui est l'identité sur k et qui envoie θ sur α. Pour $x \in E$, on pose $|x|_i = |\varphi(x)|$. Comme $\tilde{k}(\alpha)$ est le hensélisé de $k(\alpha)$ d'après les théorèmes 7.4 et 5.8, nous pouvons identifier $\tilde{E}_i$ avec $\tilde{k}(\alpha)$, donc (i) et (iii) sont clairs.

Démontrons (ii). On considère une valeur absolue sur E qui prolonge la valeur absolue sur k, et on note $\tilde{E}$ le hensélisé de E pour cette valeur absolue. Alors il y a un i tel que $g_i(\theta) = 0$, donc la valeur absolue sur $\tilde{E}$ doit être égale à $|\ |_i$ d'après le lemme 7.2 et le théorème 5.2.

Montrons que $|\ |_i \neq |\ |_j$ si $i \neq j$. Comme $g_i g_j$ est séparable, on a des polynômes s et t tels que $sg_i + tg_j = 1$. Donc $g_i(\theta) = 0$ dans $\tilde{E}_i$ et $g_i(\theta) \neq 0$ dans $\tilde{E}_j$. En prenant une approximation suffisamment précise $g_i^* \in k[X]$ de g_i, nous avons $|g_i^*(\theta)|_i$ aussi petit que nous voulons et nous avons $|g_i^*(\theta)|_j$ éloigné de 0, donc $|\ |_i \neq |\ |_j$. □

Exercices

1. Soit K un corps ultramétrique. Montrer que si $\theta \in K$ est une racine de $f \in K[X]$, alors $|\theta| \leqslant |f|$ si $|X| = 1$ (théorème 6.2).

2. Trouver toutes les valeurs absolues archimédiennes sur les corps suivants.

   (i) $\mathbb{Q}[X]/(X^2 - 2)$.

   (ii) $\mathbb{Q}[X]/(X^2 + 1)$.

   (iii) $\mathbb{Q}[X]/(X^3 - 2)$.

   Trouver toutes les extensions de la valeur absolue 5-adique sur $\mathbb{Q}$ pour les mêmes corps.

3. Soit K un corps extension de dimension finie de $\mathbb{Q}$. Montrer qu'un élément x de K est entier sur $\mathbb{Z}$ si, et seulement si, $|x| \leqslant 1$ pour toute valeur absolue ultramétrique sur K.

8 Indice de ramification et degré résiduel (e et f)

Soient k un corps discret avec une valeur absolue discrète et E une extension séparable de k de dimension finie avec une valeur absolue qui prolonge celle de k. Si le quotient $\mathrm{V}_E/\mathrm{V}_k$ des groupes de valeurs de E et k est fini, on définit l'**indice de ramification** $e = e(E/k)$ comme le nombre d'éléments de $\mathrm{V}_E/\mathrm{V}_k$. De la même manière, si le corps résiduel $\overline{E}$ est de dimension finie sur $\overline{k}$, on définit le **degré résiduel** $f = f(E/k)$ comme la dimension de $\overline{E}$ sur $\overline{k}$. Comme le passage aux hensélisés $\tilde{k} \subseteq \tilde{E}$ conserve le groupe de valeurs et le corps résiduel, nous pouvons supposer que k est hensélien.

La méthode en mathématiques classiques pour construire e consiste à choisir un $\pi \in k$ qui engendre le groupe de valeurs V_k de k. Alors (théorème 7.3) V_E est un sous-groupe du groupe cyclique engendré par $|\pi|^{1/\ell}$, donc il est cyclique et contient V_k comme sous-groupe d'indice fini e. Comme nous ne pouvons pas établir qu'un sous-groupe non trivial d'un groupe cyclique est cyclique, notre construction de e doit être plus élaborée. Le problème pour calculer f est qu'une extension algébrique de type fini d'un corps discret n'est pas nécessairement de dimension finie. Nous devons imposer la condition P de Seidenberg sur le corps résiduel.

Théorème 8.1. *Soit k un corps discret hensélien avec une valeur absolue discrète. Soit E une extension séparable de k, de dimension finie n. Supposons que le corps résiduel $\overline{k}$ satisfait la condition P de Seidenberg. Alors le groupe quotient $\mathrm{V}_E/\mathrm{V}_k$ est fini (de cardinalité notée e), le corps résiduel $\overline{E}$ est de dimension finie (notée f) sur $\overline{k}$, et $n = ef$. En particulier, la valeur absolue sur E est discrète, et $\overline{E}$ satisfait la condition P.*

Démonstration. D'après le théorème 7.3, la valeur absolue sur k s'étend de manière unique à E, et le groupe V_E est discret, donc $\overline{E}$ est discret. De plus $\mathrm{V}_E/\mathrm{V}_k$ est discret parce que V_k est cyclique et $\mathrm{V}_E^{\ell} \subseteq \mathrm{V}_k$.

Nous allons construire un sous-ensemble fini S de E qui s'envoie injectivement sur $\mathrm{V}_E/\mathrm{V}_k$, et un sous-ensemble fini W de $\{\, w \in E : |w| = 1 \,\}$ qui s'envoie injectivement sur une base de $\overline{E}$ sur $\overline{k}$, avec $SW = \{\, sw : s \in S \text{ et } w \in W \,\}$ une base de E sur k. Nous faisons une construction par récurrence en commençant avec $S = W = \{1\}$.

À chaque étape de notre construction, nous avons un ensemble fini S d'éléments non nuls de E qui contient 1 et qui s'envoie injectivement dans $\mathrm{V}_E/\mathrm{V}_k$, et un sous-ensemble fini W de $\{\, w \in E : |w| = 1 \,\}$ qui s'envoie sur une famille $\overline{k}$-linéairement indépendante $\overline{W} \in \overline{E}$. De plus, nous demandons que $\overline{kW}$, le sous-$\overline{k}$-espace vectoriel de $\overline{E}$ engendré par $\overline{W}$, soit un corps.

Si $b_w \in k$ pour $w \in W$, alors $|\sum_{w\in W} b_w w| = \max |b_w|$ car si $|\sum b_w w| < |b_{w'}| = \max |b_w|$, nous obtenons en divisant par $b_{w'}$ une relation de dépendance

linéaire dans $\overline{W}$. Donc si $a_{sw} \in k$ avec $s \in S$ et $w \in W$, alors

$$\left|\sum\nolimits_{S\times W} a_{sw} sw\right| = \max\nolimits_W \left|\sum\nolimits_S a_{sw} s\right| = \max\nolimits_{S\times W} |a_{sw} s|$$

parce que les valeurs des $a_{sw}s$ non nuls sont distinctes pour un w fixé. Ainsi SW est linéairement indépendant sur k. Notons kSW le sous-k-espace vectoriel de E engendré par SW. Si $|a_{sw}s| = 1$, $s = 1$, donc si $x \in kSW$ et $|x| \leqslant 1$, l'image $\overline{x}$ de x dans $\overline{E}$ est dans $\overline{kW}$.

Si $E = kSW$, nous avons terminé car S s'envoie sur $\mathrm{V}_E/\mathrm{V}_k$ et $\overline{E} = \overline{kW}$. Sinon il existe un $\alpha \in E \setminus kSW$. Comme k est hensélien, E a une base métrique sur k d'après le lemme 7.1, donc $\{\alpha\} \cup SW$ est métriquement indépendant, donc α est éloigné de kSW avec une distance > 0. Soit $\pi \in k$ tel que $|\pi| < 1$ engendre V_k. Nous pouvons supposer que si $s \in S \setminus \{1\}$, alors $|\pi| < |s| < 1$. Soit r le maximum des valeurs des éléments de $S \setminus \{1\}$, avec $r = |\pi|$ si $S = \{1\}$. Étant donné $b \in kSW$, nous allons construire l'un des objets suivants :

(i) $b' \in kSW$ tel que $|\alpha - b'| \leqslant r|\alpha - b|$;

(ii) $\beta \in E$ tel que $|\beta|/|s|$ n'est dans V_k pour aucun $s \in S$;

(iii) un corps $K \subseteq E$ extension de k de dimension $m > 1$ tel que $\overline{K}$ est de dimension m sur $\overline{k}$ (donc $\mathrm{V}_K = \mathrm{V}_k$) ;

(iv) un corps extension de $\overline{kW}$ de dimension finie contenu dans $\overline{E}$.

Comme le quotient $\mathrm{V}_E/\mathrm{V}_k$ est discret, ou bien $\beta = \alpha - b$ satisfait (ii), ou bien nous pouvons trouver $t \in k$ et $s \in S$ tels que $\theta = (\alpha - b)/st$ est de valeur absolue 1. Dans ce cas, nous allons voir que, ou bien $\overline{\theta} \in \overline{kW}$, ou bien (iii) est satisfait, ou bien (iv) est satisfait. Voyons d'abord ce qu'il faut faire si $\overline{\theta} \in \overline{kW}$. On a alors un $u \in kW$ tel que $\overline{\theta} = \overline{u}$ et donc $|\theta - u| < 1$. Ou bien $|\theta - u| \leqslant r$, ou bien $\beta = \theta - u$ satisfait (ii). Si $|\theta - u| \leqslant r$, nous posons $b' = b + stu$, et (i) est satisfait parce que $\alpha - b = st\theta$ et $|\theta| = 1$.

Nous retournons à la question si $\overline{\theta} \in \overline{kW}$.

Notons A_k le sous-anneau de k défini par $A_k = \{\, x \in k : |x| \leqslant 1 \,\}$. Alors A_k est un anneau intègre discret dans lequel a divise b si, et seulement si, $|a| \geqslant |b|$; ainsi a divise b ou b divise a, et le pgcd de deux éléments est l'un d'entre eux. Donc A_k est un anneau intègre à pgcd (voir page 108) [1].

Comme V_k est discret, et comme θ est algébrique sur k, nous pouvons diviser le polynôme minimal de θ par son coefficient de valeur absolue maximum pour montrer que $\overline{\theta}$ est algébrique sur $\overline{k}$. D'après le théorème VI.6.3, on a un polynôme unitaire g à coefficients dans k, tous de valeur absolue $\leqslant 1$, tel que $\overline{g}$ est séparable et $\overline{g}(\overline{\theta}^q) = 0$, où q est égal à 1 ou à une puissance de la caractéristique finie de $\overline{k}$. Comme E est hensélien (théorème 7.4), on a un $\omega \in E$ qui annule g avec $\overline{\omega} = \overline{\theta}^q$. Le polynôme minimal de ω, qui existe parce que E est

1. **NdT.** Pour tout $x \neq 0$ dans k, on a $x \in A_k$ ou $1/x \in A_k$; on dit dans ce cas que A_k est un **anneau de valuation du corps discret** k.

de dimension finie sur k, divise g et, par le lemme de Gauss (lemme IV.4.3), tous ses coefficients sont de valeur absolue $\leqslant 1$. Nous pouvons donc supposer que g est irréductible. Comme E est hensélien et $\overline{g}$ est séparable, $\overline{g}$ est irréductible. Ainsi $\overline{k}(\overline{\omega})$ est de dimension finie sur $\overline{k}$. Si $\deg g > 1$, on pose $K = k(\omega)$ et on obtient (iii). Si $\deg g = 1$, $\overline{\theta}$ est purement inséparable sur $\overline{k}$, et donc sur $\overline{kW}$. D'après la condition P, nous savons que $\overline{kW}(\overline{\theta})$ est de dimension finie sur $\overline{kW}$. Si cette dimension est égale à 1, $\overline{\theta} \in \overline{kW}$. Sinon $\overline{kW}(\overline{\theta})$ est le corps voulu dans le point (iv).

Si le point (ii) est satisfait, on peut agrandir S ; si (iv) est satisfait, on peut agrandir W. Comme α est éloigné de kSW, la situation (i) ne peut se produire qu'un nombre fini de fois. Enfin, si (iii) est satisfait, on a $\mathrm{V}_K = \mathrm{V}_k$ et K est hensélien (théorème 7.4) ; de plus, $\overline{K}$ satisfait la condition P parce que $\overline{K}/\overline{k}$ est de dimension finie (théorème VII.3.1(ii)) ; nous terminons par récurrence sur n. □

L'hypothèse dans le théorème 8.1 que $\overline{k}$ satisfait la condition P ne peut pas être supprimée, en tout cas pas complètement. Pour nous en convaincre, nous démontrons le théorème suivant.

Théorème 8.2. *Soit K un corps discret de caractéristique p. Il existe un corps discret hensélien k muni d'une valeur absolue discrète avec pour corps résiduel $\overline{k} = K$ et tel que pour chaque $y \in \overline{k}$ il y a une extension séparable de dimension finie E de k avec $y \in \overline{E}^p$.*

Démonstration. Lorsque k est un corps de caractéristique p, on note $k^{1/p}$ un corps qui contient k et tel que $(k^{1/p})^p = k$. Le fait qu'un tel corps existe est rendu évident par la contemplation de l'isomorphisme $k \simeq k^p \subseteq k$. Soit k le hensélisé du corps des fractions rationnelles $K(T)$ pour la valeur absolue T-adique (la valeur absolue de l'exercice 1.5). Si $y = 0$, on prend $E = k$. Si $y \neq 0$, on considère le polynôme séparable $f(X) = X^p + TX + y \in k[X]$. On voit facilement que $f(X)$ est irréductible (sur $k^{1/p}$) en considérant la substitution $X = Z - \lambda$, où λ est la racine p-ième de y dans $k^{1/p}$, et en utilisant le critère d'Eisenstein. Ainsi nous pouvons construire $E = k(\theta)$ avec $f(\theta) = 0$. Clairement $|\theta| = |y|^{1/p} = 1$ et $y = \overline{\theta}^p$. □

Un corps discret $\overline{k}$ de caractéristique p satisfait la condition P si, et seulement si, K^p est détachable dans K pour tout corps K extension de dimension finie de $\overline{k}$ (théorème VII.3.1(ii)), i.e. pour tout $y \in K$, $y \in K^p$ ou $y \notin K^p$. Le corolaire suivant montre donc que le corps $\overline{k}$ dans le théorème 8.1 doit au moins satisfaire une forme faible de la condition P.

Corolaire 8.3. *Soit K un corps discret. Supposons que pour tout corps discret hensélien k dont le corps résiduel $\overline{k}$ est isomorphe à K, et pour tout corps E extension séparable de dimension finie de k, le corps résiduel $\overline{E}$ soit de dimension finie sur $\overline{k}$. Alors K^p est détachable dans K.*

Démonstration. Soit $y \in \overline{k}$; on applique le théorème 8.2 pour construire k et E avec $y \in \overline{E}^p$. Alors $\overline{E}$ est de dimension finie sur $\overline{k}$. Donc $\overline{E}^p$ est de dimension finie sur $\overline{k}^p$. Donc y est ou n'est pas dans $\overline{k}^p$. □

L'hypothèse dans le théorème 8.1 selon laquelle l'extension est séparable ne peut pas être supprimée. On se reporte à l'exercice 3.2 avec $k = \mathbb{Z}_2(Y^2, \eta^2)$ et $E = \mathbb{Z}_2(Y^2, \eta)$ muni de la valeur absolue qui provient du corps des séries formelles en Y. Alors le groupe de valeurs de E est égal au groupe de valeurs de k si, et seulement si, $a_n = 0$ pour tout n. Le passage aux hensélisés ne change pas la situation.

Les valeurs absolues p-adiques sur $\mathbb{Q}$ satisfont les hypothèses du théorème suivant.

Théorème 8.4. *Soit k un corps discret avec une valeur absolue telle que*

(i) *la valeur absolue est discrète ;*

(ii) *le hensélisé est séparablement factoriel (c'est le cas par exemple si k est pseudofactoriel) ;*

(iii) *le corps résiduel satisfait la condition P.*

Si E est une extension finie séparable de k, toute valeur absolue sur E qui prolonge celle sur k satisfait les points (i), (ii) *et* (iii).

Démonstration. Soient $\tilde{E}$ le hensélisé de E et $\tilde{k}$ le hensélisé de k. Nous pouvons supposer que $\tilde{k} \subseteq \tilde{E}$. On prend un $\alpha \in E$ tel que $E = k(\alpha)$. Comme $\tilde{k}$ est séparablement factoriel, $\tilde{k}(\alpha)/\tilde{k}$ est de dimension finie, donc $\tilde{k}(\alpha)$ est hensélien d'après le théorème 7.4. Par suite $\tilde{k}(\alpha) = \tilde{E}$. Donc $\tilde{E}$ est séparablement factoriel d'après le théorème VII.2.4, donc (ii) est satisfait. Comme les groupes de valeurs et les corps résiduels de E et $\tilde{E}$ sont les mêmes, les points (i) et (iii) sont vérifiés d'après le théorème 8.1. □

Théorème 8.5. *Soit k un corps avec une valeur absolue qui satisfait les hypothèses du théorème 8.4. Soit E une extension séparable de dimension n de k. Alors il y a un nombre fini s de valeurs absolues sur E qui prolongent la valeur absolue sur k. Notons $E_1, \dots, E_s$ le corps E muni de ces valeurs absolues. Alors $e(E_i/k)$ et $f(E_i/k)$ sont définis et l'on a*

$$n = \sum\nolimits_{i=1}^{s} e(E_i/k) f(E_i/k).$$

Démonstration. Le théorème 7.5 construit les valeurs absolues sur E (en nombre fini égal à s). On a $e(\tilde{E}_i/\tilde{k}) f(\tilde{E}_i/\tilde{k}) = n_i = [\tilde{E}_i : \tilde{k}]$ d'après le théorème 8.1, et $n = \sum n_i$ d'après le théorème 7.5. Enfin le hensélisé ne change ni le groupe de valeurs ni le corps résiduel. □

Exercice

1. Calculer e et f pour les extensions de la valeur absolue 5-adique sur $\mathbb{Q}$ pour l'extension $\mathbb{Q}[X]/(X^3-2)$. Vérifier le théorème 8.5 dans ce cas.

9 Notes

Pour un traitement plus complet de la théorie constructive des nombres réels et des espaces métriques la lectrice peut consulter [Bishop 1967] et [Bishop-Bridges 1985].

La théorie des valeurs absolues joue un rôle central dans la théorie des corps d'un point de vue constructif. L'étude des corps munis d'une valeur absolue fournit un mélange intéressant de constructions discrètes, purement algébriques, combinées avec des constructions analytiques comme le complété d'un corps.

Bien que la théorie algébrique des nombres est généralement ressentie comme essentiellement constructive dans sa forme classique, même les auteurs qui attachent une attention particulière aux aspects constructifs de la théorie emploient des techniques hautement non constructives qui annulent leurs efforts. Par exemple, dans l'ouvrage [Borevich et Shafarevich 1966], les auteurs supposent que tout polynôme peut être décomposé en un produit de facteurs irréductibles (tout corps est factoriel), et qu'étant donné un sous-ensemble non vide des entiers naturels, on peut trouver son plus petit élément.

La définition d'une valeur absolue généralisée sur un corps a été adoptée par Staples (1971) dans son traitement constructif des valeurs absolues, et la démonstration du théorème 1.8 se trouve dans cet article. Le problème ici est que nous ne pouvons pas en général décider si $vx \leqslant vy$ ou $vy \leqslant vx$, ni si vx est nul. Notre démonstration du théorème 1.1 est prise dans [Weiss 1963, Proposition 1-1-8]. Les deux dernières affirmations de notre démonstration du théorème 1.2 viennent de [Weiss 1963, Theorem 1-1-4].

La notion d'un corps pseudofactoriel est purement constructive et n'a pas de contrepartie classique (tout corps muni d'une valeur absolue est pseudofactoriel en mathématiques classiques). Cependant, cette notion nous donne exactement l'information requise pour construire une racine d'un polynôme, ou (sinon) pour éloigner ce polynôme de 0, dans le complété du corps (corolaire 3.2). La démonstration du corolaire 3.3 qui utilise le nombre de tours provient de [Brouwer-de Loor 1924]. Le théorème 3.4 montre que nous avons beaucoup de corps pseudofactoriels. Le corolaire 3.5 montre comment factoriser des polynômes séparables dans la clôture séparable ou la clôture algébrique d'un corps pseudofactoriel dans son complété. Par exemple, nous pouvons factoriser les polynômes sur les nombres algébriques p-adiques.

Notre démonstration du théorème de Gelfand-Tornheim provient de [Artin 1967, page 24].

Le lemme de Hensel un peu compliqué de la section 4 est une modification de [Artin 1967]. Les hypothèses du lemme sont légèrement affaiblies en ne réclamant pas que le terme dominant de φ ait la même valeur absolue queφ (on ne réclame pas $s = 1$), ceci en vue de traiter les situations où nous ne pouvons pas déterminer quels coefficients d'un polynôme ont une valeur absolue maximale, et nous devons traiter quelques particularités d'un point de vue constructif. La définition de *hensélien*, quand $s = 1$, est la conclusion du lemme de Hensel donné dans [Artin 1967, theorem 5]. Le théorème essentiel est le théorème 6.13 qui affirme qu'un corps discret avec une valeur absolue ultramétrique satisfait la conclusion du lemme de Hensel exactement quand il est séparablement clos dans son complété.

La construction de la valeur absolue dans le théorème 7.3 provient de [O'Meara 1963, Theorem 14:1].

XIII. Domaines de Dedekind

Sommaire

1 Ensembles de Dedekind (de valeurs absolues discrètes)

Si S est un ensemble de valeurs absolues sur un corps de Heyting k, nous noterons un élément de S par $|\ |$ avec un indice. Au lieu d'écrire $|\ |_p \in S$, nous écrirons souvent $p \in S$.

Pour chaque nombre premier p, nous avons une valeur absolue discrète sur le corps $\mathbb{Q}$ des nombres rationnels définie par $|p|_p = 1/p$, et $|q|_p = 1$ si q est un nombre premier différent de p. Cette famille de valeurs absolues forme un ensemble de Dedekind au sens de la définition suivante.

Définition 1.1. Un ensemble discret non vide S de valeurs absolues discrètes non triviales (voir page 292) sur un corps de Heyting k est appelé un **ensemble de Dedekind** lorsque les propriétés suivantes sont satisfaites.

(i) Pour tout $x \in k$, il existe un sous-ensemble fini T de S tel que $|x|_p \leqslant 1$ pour les $p \in S \setminus T$ [1].

(ii) Si $|\ |_q$ et $|\ |_{q'}$ sont des valeurs absolues distinctes dans S, et si $\varepsilon > 0$, il existe un $x \in k$ tel que $|x|_p \leqslant 1$ pour toute $p \in S$, $|x-1|_q < \varepsilon$, et $|x|_{q'} < \varepsilon$. Par suite, des valeurs absolues distinctes dans S sont inéquivalentes.

1. **NdT.** Pour un $x \in k$ inversible, on en déduit que $|x|_p = 1$ pour toutes les valeurs absolues p en dehors d'un sous-ensemble fini T' de S. Mais comme on ne sait pas tester l'inversibilité dans un corps de Heyting, l'information donnée ici est plus précise.

Notez qu'un sous-ensemble non vide détachable d'un ensemble de Dedekind est un ensemble de Dedekind.

Soit S un ensemble de Dedekind de valeurs absolues sur un corps de Heyting k. Si $p \in S$, alors, comme p est ultramétrique, l'ensemble $R(p) = \{ x \in k : |x|_p \leqslant 1 \}$ est un anneau, qui est local parce que p est discrète. L'anneau $R(p)$ est appelé l'**anneau local en** p. Les éléments de l'anneau $\bigcap_{p\in S} R(p)$ sont appelés les éléments **entiers de** S. Un anneau est appelé un **domaine de Dedekind** si c'est l'anneau des entiers d'un ensemble de Dedekind de valeurs absolues sur un corps de Heyting.

Théorème 1.2. *L'anneau des entiers d'un ensemble de Dedekind S de valeurs absolues sur un corps de Heyting k est détachable dans k.*

Démonstration. Soit $x \in k$. On a un sous-ensemble fini T de S tel que $|x|_p \leqslant 1$ pour toute $p \in S \setminus T$. Alors x est un entier de S si, et seulement si, $|x|_p \leqslant 1$ pour les p dans l'ensemble fini T de valeurs absolues discrètes. □

Étant données des valeurs absolues inéquivalentes $|\ |_1, \ldots, |\ |_n$ sur k et des éléments $x_1, \ldots, x_n \in k$, nous sommes intéressés par la construction d'un élément de k qui approche simultanément chaque x_i pour la valeur absolue $|\ |_i$. Nous avons tout d'abord le lemme suivant.

Lemme 1.3. *Soient $|\ |_1, \ldots, |\ |_n$ des valeurs absolues inéquivalentes non triviales sur un corps de Heyting k. Alors il existe un $x \in k$ tel que $|x|_1 > 1$, et $|x|_i < 1$ pour $i \neq 1$.*

Démonstration. Si $n = 1$, alors, comme $|\ |_1$ est non triviale, il y a un $x \in k$ tel que de $|x|_1 > 1$. Si $n = 2$, alors, comme $|\ |_1$ et $|\ |_2$ sont des valeurs absolues inéquivalentes non triviales, il existe un $x \in k$ tel que $|x|_1 < 1$ et $|x|_2 > 1$. Pour $n > 2$, nous procédons par récurrence. Nous supposons que nous avons un $y \in k$ tel que $|y|_1 > 1$, et $|y|_i < 1$ pour $2 \leqslant i < n$. Nous prenons un $z \in k$, d'après le cas $n = 2$, tel que $|z|_1 > 1$ et $|z|_n < 1$, et nous prenons m assez grand pour que $|y^m|_i|z|_i < 1$ pour $2 \leqslant i < n$. Comme $|z|_n^{-1} > 1$, $|y^m|_n > 1$ ou $|y^m|_n < |z|_n^{-1}$. Dans ce dernier cas, $|y^m z|_n < 1$, donc $x = y^m z$ est l'élément voulu. Dans le premier cas, on pose $x_m = zy^m/(1 + y^m)$. La suite des $|x_m|_i$ converge vers $|z|_i$ si $i = 1$ ou n, et converge vers 0 sinon. On prend $x = x_m$ avec m suffisamment grand pour que $|x_m|_1 > 1$ et $|x_m|_i < 1$ pour $2 \leqslant i \leqslant n$. □

Nous notons k_p le corps k avec la métrique associée à la valeur absolue $|\ |_p$. Le théorème suivant dit que la diagonale est dense dans le produit $\prod_p k_p$.

Théorème 1.4 (théorème d'approximation faible)**.** *Soient $|\ |_1, \ldots, |\ |_n$ des valeurs absolues inéquivalentes non triviales sur un corps de Heyting k, $x_1, \ldots, x_n$ des éléments de k, et un $\varepsilon > 0$. Il existe $x \in k$ tel que $|x - x_i|_i < \varepsilon$ pour tout i.*

Démonstration. Le lemme 1.3 construit pour chaque i un $y_i \in k$ tel que $|y_i|_i > 1$ et $|y_i|_j < 1$ si $j \neq i$. Pour $m \in \mathbb{N}$, on définit

$$z_{i,m} = y_i^m x_i/(1 + y_i^m).$$

Alors $\lim_{m\to\infty} |z_{i,m} - x_i|_i = 0$, et $\lim_{m\to\infty} |z_{i,m}|_j = 0$ si $j \neq i$. On pose $z_m = \sum_{i=1}^n z_{i,m}$. Si m est suffisamment grand, $|z_m - x_i|_i < \varepsilon$ pour tout i. □

Le théorème d'approximation forte donne des approximations entières.

Théorème 1.5 (théorème d'approximation forte)**.** *Soit T un sous-ensemble fini d'un ensemble de Dedekind S sur un corps de Heyting k. Soit $\varepsilon > 0$, et pour tout $p \in T$ soit $x_p \in k$. Alors il existe un $y \in k$ tel que*

(i) $|y - x_p|_p < \varepsilon$ *pour tout* $p \in T$,

(ii) $|y|_q \leqslant 1$ *pour tout* $q \in S \setminus T$.

Démonstration. On peut supposer $\varepsilon \leqslant 1$. Pour chaque $p \in T$, il y a seulement un nombre fini de $q \in S$ tels que $|x_p|_q > 1$. Pour chaque $p \in T$ et $q \in S \setminus T$ tel que $|x_p|_q > 1$, on ajoute q à T et on définit $x_q = 0$. Nous pouvons alors supposer que $|x_p|_q \leqslant 1$ pour tous $p \in T$ et $q \in S \setminus T$.

Fixons $p \in T$. Pour chaque $q \in T \setminus \{p\}$, on a, d'après la définition 1.1(ii), un élément de k qui est un entier de S, qui est proche de 1 en p, et qui est proche de 0 en q. Soit y_p le produit de ces éléments (le produit vide est égal à 1). Les éléments y_p sont proches de 1 en p et proches de 0 en les valeurs absolues $q \in T \setminus \{p\}$. Enfin, on prend $y = \sum_{p\in T} y_p x_p$; donc $|y|_q \leqslant 1$ pour chaque $q \in S \setminus T$, et y est proche de x_p en p. □

Le théorème d'approximation forte nous permet d'écrire les éléments de k comme quotients d'entiers de S.

Théorème 1.6. *Soit S un ensemble de Dedekind de valeurs absolues sur un corps de Heyting k, et soit R l'ensemble des entiers de S. Alors tout élément de k est un quotient d'éléments de R, et R est intégralement clos dans k.*

Démonstration. Soit $x \in k$. D'après la définition 1.1(i), on a un sous-ensemble fini T de S tel que $|x|_q \leqslant 1$ pour chaque $q \in S \setminus T$. Si $|x|_p \leqslant 1$ pour toute p dans l'ensemble fini T, alors $x \in R$, donc nous pouvons supposer que $x \neq 0$. Comme les valeurs absolues dans l'ensemble fini T sont discrètes, nous pouvons supposer que $|x|_p > 1$ pour toute $p \in T$.

D'après le théorème 1.5, on a un $y \in k$ tel que

$$|y - x^{-1}|_p < \min\{\, |x^{-1}|_p : p \in T \,\} < 1$$

pour toute $p \in T$, et $|y|_q \leqslant 1$ pour toute $q \in S \setminus T$. Comme $|y - x^{-1}|_p < |x^{-1}|_p$ pour toute $p \in T$, et comme $|\ |_p$ est ultramétrique, on a $|y|_p = |x^{-1}|_p < 1$

pour toute $p \in T$. En particulier, $y \in R$. Si $p \in T$, alors $|xy|_p = |x|_p|y|_p = |x|_p|x^{-1}|_p = 1$, et si $q \in S \setminus T$, alors $|xy|_q \leqslant 1$. Donc $xy \in R$, et $x = (xy)y^{-1}$ est un quotient d'éléments de R.

Enfin, comme les valeurs absolues dans S sont ultramétriques, tout élément de k qui annule un polynôme unitaire de $R[X]$ est dans R. □

Exercices

1. Soit S l'ensemble des valeurs absolues p-adiques sur $\mathbb{Q}$. Montrer que l'anneau des entiers de S est $\mathbb{Z}$. Quel est l'anneau des entiers si $S = \{3\}$?
2. Vérifier que si $|\ |$ est une valeur absolue discrète, alors $\{\, x : |x| \leqslant 1 \,\}$ est un anneau local.
3. Compléter $\mathbb{Q}$ pour la valeur absolue p-adique pour démontrer qu'un domaine de Dedekind n'est pas nécessairement discret.
4. *Théorème des restes chinois.* Utiliser le théorème d'approximation forte pour démontrer que si a_1 et $a_2 \in \mathbb{Z}$ sont étrangers, et b_1 et $b_2 \in \mathbb{Z}$, alors il existe $x \in \mathbb{Z}$ congruent à b_i modulo a_i pour $i = 1, 2$.

2 Théorie des idéaux

Dans cette section, k est un corps de Heyting, S un ensemble de Dedekind de valeurs absolues sur k, et R le domaine de Dedekind correspondant.

Un **idéal fractionnaire** est un sous-R-module non nul A de k tel que $|A|_p = \max\{\, |x|_p : x \in A \,\}$ existe pour toute valeur absolue $p \in S$, et est égal à 1 pour toutes les $p \in S$ sauf peut-être pour un nombre fini d'entre elles. Autrement dit, pour chaque $p \in S$, il existe un $x(p) \in A$ tel que $|y|_p \leqslant |x(p)|_p$ pour tout $y \in A$, et $|x(p)| = 1$ pour p en dehors d'un sous-ensemble fini de S.

Théorème 2.1. *Un sous-R-module non nul de type fini de k est un idéal fractionnaire.*

Démonstration. Soit A un sous-R-module non nul de k engendré par $a_1, \ldots, a_n$. Comme k est un corps de Heyting, l'un des a_i est non nul, et si $a_i \neq 0$, alors ou bien $a_j \neq 0$, ou bien $a_i + a_j \neq 0$; nous pouvons donc supposer que les a_i sont tous non nuls. Supposons que $a = \sum_{i=1}^n r_i a_i$ est un élément de A, et que $p \in S$. Comme $|\ |_p$ est ultramétrique, $|a|_p = |\sum_{i=1}^n r_i a_i|_p \leqslant \max |r_i a_i|_p \leqslant \max |a_i|_p$. Comme chaque $|\ |_p$ est discrète, l'élément $|A|_p = \max\{\, |a_i|_p : i = 1, \ldots, n \,\}$ existe. On prend un sous-ensemble fini T de S tel que $|a_i|_p = 1$ pour $p \in S \setminus T$ et $i = 1, \ldots, n$. Alors $|A|_p = 1$ si $p \in S \setminus T$. □

Nous montrerons plus loin qu'inversement, tout idéal fractionnaire non nul est engendré comme R-module par deux éléments.

Soient A et B des idéaux fractionnaires. On définit la **somme** de A et B par $A+B=\{\,a+b : a\in A \text{ et } b\in B\,\}$, et le **produit** de A et B comme l'ensemble AB des sommes finies d'éléments de la forme ab, avec $a\in A$ et $b\in B$.

Théorème 2.2. *Soient A et B des idéaux fractionnaires. Alors $A+B$, AB et $A\cap B$ sont des idéaux fractionnaires avec les propriétés suivantes :*

(i) $|A+B|_p=\max(|A|_p,|B|_p)$,

(ii) $|AB|_p=|A|_p|B|_p$ *et*

(iii) $|A\cap B|_p=\min(|A|_p,|B|_p)$

pour toute valeur absolue $p\in S$.

Démonstration. Comme $\max(1,1)=\min(1,1)=1\times 1$, si l'on démontre les égalités voulues pour toute $p\in S$, on voit que la seconde propriété définissant les idéaux fractionnaires est bien satisfaite par les R-modules considérés.

On a un $a\in A$ et un $b\in B$ tels que $|A|_p=|a|_p$ et $|B|_p=|b|_p$. Comme $|\ |_p$ est discrète, les valeurs absolues $|a|_p$ et $|b|_p$ sont comparables, et nous pouvons supposer que $|A|_p\leqslant|B|_p$.

Tout d'abord $|x|_p\leqslant\max(|a'|_p,|b'|_p)\leqslant\max(|A|_p,|B|_p)=|b|_p$ pour tout $x=a'+b'\in A+B$. Par ailleurs $b\in A+B$, donc $|b|_p$ est atteint pour un $x\in A+B$. Donc $A+B$ est un idéal fractionnaire avec $|A+B|_p=\max(|A|_p,|B|_p)$.

Pour $x\in AB$, on a $|x|_p\leqslant|ab|_p=|A|_p|B|_p$ parce que la valeur absolue $|\ |_p$ est multiplicative et ultramétrique, donc (ii) est valide et AB est un idéal fractionnaire avec $|AB|_p=|A|_p|B|_p$.

Si $x\in A\cap B$, alors clairement $|x|_p\leqslant\min(|A|_p,|B|_p)$, donc il suffit de construire un élément x de $A\cap B$ tel que $|x|_p=\min(|A|_p,|B|_p)$. Or l'ensemble

$$T=\{p\}\cup\{\,q\in S : |a/b|_q<1\,\}$$

est fini ; donc, d'après le théorème 1.5, il existe un $y\in k$ tel que $|y|_p=|a/b|_p\leqslant 1$, et $|y|_q\leqslant\min(1,|a/b|_q)$ pour toute $q\in S$. Cette dernière inégalité implique $yb/a\in R$, donc $yb\in A$, et aussi $y\in R$, donc $yb\in B$. Mais $\min(|A|_p,|B|_p)=|A|_p=|a|_p=|yb|_p$, donc $x=yb$ est l'élément cherché. □

Un idéal fractionnaire A est complètement déterminé par les valeurs absolues $|A|_p$.

Théorème 2.3. *Soient A et B des idéaux fractionnaires.*

(i) *On a $A=\{\,x\in k : |x|_p\leqslant|A|_p$ pour toute $p\in S\,\}$.*

(ii) *On a $A\subseteq B$ si, et seulement si, $|A|_p\leqslant|B|_p$ pour toute $p\in S$.*

Démonstration. Il suffit de démontrer (i). Soit $x\in k$ tel que $|x|_p\leqslant|A|_p$ pour toute $p\in S$. On prend un élément non nul $z\in A$ et on considère xz^{-1}. Comme $|xz^{-1}|_p\leqslant 1$ en dehors d'un ensemble fini et comme $|\ |_p$ est discrète, ou bien

$xz^{-1} \in R$, et alors $x = (xz^{-1})z \in A$, ou bien $xz^{-1} \neq 0$, et alors $x \neq 0$. Nous pouvons donc supposer que $x \neq 0$.

En remplaçant A par $x^{-1}A$, il suffit de démontrer que $1 \in A$ si A est un idéal fractionnaire tel que $|A|_p \geqslant 1$ pour toute $p \in S$. En remplaçant A par $R \cap A$, et en utilisant le théorème 2.2, il revient au même de démontrer que $1 \in A$ si A est un idéal fractionnaire contenu dans R avec $|A|_p = 1$ pour toute $p \in S$.

Soit z un élément non nul de A. D'après la définition 1.1(i), on a un sous-ensemble fini T de S tel que $|z^{-1}|_q \leqslant 1$ pour $q \in S \setminus T$. Comme $z \in A \subseteq R$, on a $|z|_q = 1$ pour tout $q \in S \setminus T$. Si $|z|_p = 1$ pour tout $p \in T$, alors $z^{-1} \in R$, donc $1 \in A$. Ainsi, comme T est fini et comme les valeurs absolues $|\ |_p$ sont discrètes, nous pouvons supposer que T est non vide et que $|z|_p < 1$ pour toute $p \in T$.

Pour chaque $p \in T$, on prend un $x_p \in A$ tel que $|x_p|_p = 1$. Comme $|z|_q = 1$ en dehors d'un ensemble fini, le théorème 1.5 dit qu'il existe un $y_p \in k$ tel que $|y_p - x_p^{-1}|_p \leqslant |z|_p < 1$, et $|y_p|_q \leqslant |z|_q \leqslant 1$ pour toute $q \in S \setminus \{p\}$. Comme $|x_p^{-1}|_p = 1$, et comme $|\ |_p$ est ultramétrique, on a $y_p \in R$. Si $q \in T$, alors

$$\begin{aligned}\Big|1 - \sum\nolimits_{p\in T} x_p y_p\Big|_q &= \Big|(1 - x_q y_q) - \sum\nolimits_{p\in T\setminus\{q\}} x_p y_p\Big|_q \\ &\leqslant \max(|1 - x_q y_q|_q, \max\{\, |y_p|_q : p \in T \setminus \{q\}\,\}) \\ &\leqslant \max(|x_q(x_q^{-1} - y_q)|_q, |z|_q) = |z|_q,\end{aligned}$$

et si $q \in S \setminus T$, alors

$$\Big|1 - \sum\nolimits_{p\in T} x_p y_p\Big|_q \leqslant 1 = |z|_q.$$

Ainsi $(1 - \sum_{p\in T} x_p y_p)z^{-1} \in R$, donc $1 - \sum_{p\in T} x_p y_p \in zR \subseteq A$. Mais $x_p y_p \in A$, donc $1 \in A$. □

Corolaire 2.4. *Si $A \subseteq B$ sont des idéaux fractionnaires, A est détachable dans B. Donc tout domaine de Dedekind discret est fortement discret.*

Démonstration. Si $x \in B$, alors le théorème 2.3 dit que $x \in A$ si, et seulement si, $|x|_p \leqslant |A|_p$ pour toute $p \in S$. On a un sous-ensemble fini T de S tel que $|A|_p = |B|_p = 1$ pour $p \in S \setminus T$. Donc $x \in A$ si, et seulement si, $|x|_p \leqslant |A|_p$ pour toute $p \in T$, ce qui est décidable.

En prenant $B = R$, on voit que R est fortement discret. □

Nous pouvons maintenant démontrer que les idéaux fractionnaires sont de type fini.

Théorème 2.5. *Pour toute $p \in S$, choisissons un élément d_p du groupe de valeurs de $|\ |_p$, avec la condition que $d_p = 1$ en dehors d'un sous-ensemble fini de S. Soit $A = \{\, x \in k : |x|_p \leqslant d_p$ pour toute $p \in S \,\}$. Alors $A \neq 0$, et si y est un élément non nul de A, il existe un $x \in A$ non nul tel que A est engendré par x et y comme R-module. De plus, $|A|_p = d_p$ pour chaque $p \in S$.*

Démonstration. D'après le théorème 1.5, il y a un y non nul dans A. Soit T un sous-ensemble fini de S tel que $|y|_p = d_p = 1$ pour les $p \in S \setminus T$. D'après le théorème 1.5, il existe un $x \in k$ tel que

(i) $|x|_p = d_p$ pour toute $p \in T$;

(ii) $|x|_q \leqslant 1$ pour toute $q \in S \setminus T$.

Soit B le sous-module de A engendré par x et y. Alors

$$|B|_p = \max(|x|_p, |y|_p) = d_p \text{ pour toute } p \in S,$$

donc $|A|_p = |B|_p$ pour toute $p \in S$, puis $A = B$ d'après le théorème 2.3. □

Soit I l'ensemble des fonctions $a\colon S \to \mathbb{Z}$ telles que $a(p) = 0$ en dehors d'un ensemble fini (qui dépend de a). Alors I est le groupe abélien libre sur l'ensemble S. Soit g_p le générateur du groupe de valeurs de $|\ |_p$ dont la valeur absolue est < 1. On considère l'application φ depuis le monoïde des idéaux fractionnaires (pour la multiplication) vers I, définie en envoyant A sur la fonction a telle que $|A|_p = g_p^{a(p)}$. Le théorème 2.2(ii) dit que φ est un homomorphisme, le théorème 2.3 dit qu'il est injectif, et le théorème 2.5 dit qu'il est surjectif. De plus, si $\varphi(A) \neq \varphi(B)$, alors $A \neq B$ comme sous-ensembles de k ; i.e. ou bien il existe un élément $x \in A$ tel que $x \neq y$ pour tout $y \in B$, ou bien il existe un élément $y \in B$ tel que $y \neq x$ pour tout $x \in A$.

La base naturelle du groupe abélien libre I sur S est donnée par les fonctions δ_p qui vérifient $\delta_p(p) = 1$ et $\delta_p(q) = 0$ pour $q \neq p$. Les idéaux fractionnaires correspondants M_p sont des idéaux maximaux de R, car si $x \in R$ avec $|x|_p < 1$, alors on a $x \in M_p$, tandis que si $|x|_p = 1$, alors l'idéal A de R engendré par x et M_p vérifie $|A|_q = 1$ pour tout $q \in S$, donc est égal à R [1].

Exercices

1. Montrer que tout idéal fractionnaire est détachable dans k. Construire un exemple brouwerien d'un sous-module de type fini de la complétion p-adique de $\mathbb{Q}$ qui n'est pas détachable.

1. **NdT.** La structure du groupe multiplicatif des idéaux fractionnaires de k est donc l'analogue exact de celle du groupe multiplicatif des nombres rationnels > 0. Et pour le sous-monoïde des idéaux entiers, le théorème de décomposition unique en facteurs premiers est vérifié, comme pour un anneau principal à factorisation unique. Cependant, comme un anneau principal n'est pas nécessairement à factorisation unique, ce n'est pas non plus nécessairement un domaine de Dedekind.

2. Montrer qu'un domaine de Dedekind discret est un anneau de Lasker-Noether intégralement clos dans lequel tout idéal premier propre non nul est maximal.

3 Extensions finies

Nous sommes intéressés par les valeurs absolues discrètes p sur un corps discret k qui satisfont la propriété suivante, triviale en mathématiques classiques.

Propriété 3.1. *Le hensélisé $\tilde{k}_p$ est séparablement factoriel, et le corps résiduel $\overline{k}_p$ satisfait la condition P.*

Soit p une valeur absolue discrète sur k qui satisfait la propriété 3.1, et soit E une extension finie séparable de k. Alors les théorèmes XII.8.4 et XII.8.5 disent que toute valeur absolue sur E qui prolonge p est discrète, et que l'ensemble de ces valeurs absolues est fini.

Les valeurs absolues p-adiques sur $\mathbb{Q}$ satisfont la propriété 3.1. Les corps de nombres de la théorie des nombres algébriques sont des extensions de dimension finie de $\mathbb{Q}$, et ils sont munis d'ensembles de Dedekind de valeurs absolues de la manière suivante.

Théorème 3.2. *Soit k un corps discret et S un ensemble de Dedekind de valeurs absolues sur k, chacune d'entre elles satisfaisant la propriété 3.1. Soit E une extension séparable de dimension finie de k, et soit S' l'ensemble des valeurs absolues sur E qui prolongent une valeur absolue de S. Alors S' est un ensemble de Dedekind de valeurs absolues sur E.*

Démonstration. Nous montrons d'abord que l'ensemble S' est discret. Soient P et $Q \in S'$. Si P et Q prolongent des valeurs absolues distinctes de S, alors elles sont distinctes. Supposons maintenant que P et Q prolongent la même valeur absolue $p \in S$. D'après le théorème XII.7.5, l'ensemble des valeurs absolues de S' qui prolongent p est fini, donc $P = Q$ ou $P \neq Q$.

Le fait que toute valeur absolue de S' est discrète se trouve dans le théorème XII.8.4.

Étant donné $x \in E$, nous devons construire un sous-ensemble fini T' de S' tel que $|x|_p \leqslant 1$ pour toute $P \in S' \setminus T'$. Comme E est une extension de dimension finie de k, le théorème VI.1.13 dit qu'il existe un polynôme irréductible $f(X) = X^n + a_1X^{n-1} + \cdots + a_n \in k[X]$ tel que $f(x) = 0$. Soit T un sous-ensemble fini de S tel que $|a_i|_p \leqslant 1$ pour chaque i et chaque $p \in S \setminus T$. Soit T' le sous-ensemble fini de S' formé par les valeurs absolues sur E qui prolongent les éléments de T. Si $P \in S' \setminus T'$, alors $|a_i|_P \leqslant 1$, donc $|x|_P \leqslant 1$ car P est ultramétrique.

Enfin, nous montrons que si P et P' sont des valeurs absolues distinctes dans S' et si $\varepsilon > 0$, il existe un $x \in E$ tel que $|1 - x|_P$ et $|x|_{P'}$ sont $< \varepsilon$

et $|x|_Q \leqslant 1$ pour les $Q \in S' \setminus \{P, P'\}$. Soient P et P' qui prolongent p et $p' \in S$ respectivement. Si $p \neq p'$, alors, comme S est un ensemble de Dedekind, on a un $x \in k$ qui satisfait les propriétés requises. Supposons maintenant que $p = p'$. Nous pouvons supposer $\varepsilon \leqslant 1$. Soit S'_p l'ensemble fini des valeurs absolues sur E qui prolongent p. D'après le théorème 1.4, il existe un $y \in E$ tel que $|y|_Q < \varepsilon$ pour toute $Q \in S'_p \setminus \{P\}$ et $|y-1|_P < \varepsilon$; par conséquent, $|y|_Q \leqslant 1$ pour toute $Q \in S'_p$. D'après le paragraphe précédent, on a un sous-ensemble fini T' de S', disjoint de S'_p, tel que $|y|_Q \leqslant 1$ pour toute $Q \in S' \setminus T'$. Soit T le sous-ensemble fini de S des valeurs absolues qui ont un prolongement dans T'. Alors $p \notin T$, et, d'après le théorème 1.5, on a un $x \in k$ tel que $|x|_q \leqslant |y|_Q^{-1}$ pour toute Q qui prolonge $q \in T$, $|1-x|_p < \varepsilon$, et $|x|_q \leqslant 1$ pour toute $q \in S \setminus T$. Alors $|xy|_Q = |x|_Q|y|_Q \leqslant 1$ pour toute $Q \in S'$, $|1-xy|_P = |1-y+(1-x)y|_P < \varepsilon$ et $|xy|_{P'} < \varepsilon$. □

Soit R un domaine de Dedekind discret et k son corps de fractions. Soit E une extension séparable de dimension finie de k. Si les valeurs absolues qui définissent R satisfont la propriété 3.1, le théorème 3.2 montre comment construire un domaine de Dedekind avec E pour corps de fractions. Nous donnons maintenant une caractérisation purement algébrique de ce domaine de Dedekind.

Théorème 3.3. *Soit E une extension séparable de dimension finie d'un corps discret k. Soit S un ensemble de Dedekind de valeurs absolues sur k qui satisfont la propriété 3.1. Soit S' l'ensemble de Dedekind sur E formé par les valeurs absolues qui prolongent une valeur absolue de S. Pour tout élément $x \in E$, les propriétés suivantes sont équivalentes.*

(i) *x est un entier de S'.*

(ii) *x annule un polynôme irréductible unitaire à coefficients dans R.*

(iii) *x est entier sur R.*

Démonstration. Clairement (ii) implique (iii), tandis que (iii) implique (i) parce que toute valeur absolue de S' est ultramétrique et prolonge une valeur absolue de S.

Montrons que (i) implique (ii). Soit $\alpha \in E$ un entier de S'. Comme E est de dimension finie, le théorème VI.1.13 dit que α annule un polynôme irréductible $f(X) = X^n + a_1X^{n-1} + \cdots + a_n \in k[X]$. Ainsi $k[\alpha]$ est une extension de dimension finie de k, et nous pouvons supposer que $k[\alpha] = E$. Il suffit de démontrer que $|a_i|_p \leqslant 1$ pour toute $p \in S$ et tout i. Soit $p \in S$, et soit $\tilde{k}_p$ le hensélisé de k en p. Comme E est séparable, le polynôme f est séparable. Comme p satisfait la propriété 3.1, le corps $\tilde{k}_p$ est séparablement factoriel, donc le corolaire VII.2.5 dit qu'on a un corps de décomposition K_p pour f sur $\tilde{k}_p$. Soient $r_1, \ldots, r_n$ les racines de $f \in K_p$, et soit P l'unique extension de la valeur absolue p à K_p obtenue par le théorème XII.7.3. On définit des monomorphismes

$\sigma_i \colon E \to K_p$ pour $i = 1, \ldots, n$, en posant $\sigma_i x = r_i$. D'après le théorème XII.7.5, chaque valeur absolue $|\ |$ sur E qui prolonge p est de la forme $|y| = |\sigma_i y|_P$ pour un i. Comme $|x|_Q \leqslant 1$ pour toute $Q \in S'$, on obtient $|r_i|_P \leqslant 1$ pour $i = 1, \ldots, n$. Les coefficients de $f(X)$ sont des polynômes symétriques en les racines r_j, et comme P est ultramétrique, on a $|r_i|_P \leqslant 1$ pour tout i. Or $r_i \in k$, donc $|r_i|_p = |r_i|_P \leqslant 1$. □

Références

Artin, E.

1967 *Algebraic numbers and algebraic functions*, Gordon and Breach.

Baumslag, G., F. B. Cannonito et C. F. Miller, III

1981 Computable algebra and group embeddings, *J. Algebra* **69**, 186-212.

Bishop, E.

1967 *Foundations of constructive analysis*, McGraw-Hill.

1973 *Schizophrenia in contemporary mathematics*, AMS Colloquium Lectures, Missoula, Montana.

Bishop, E. et D. S. Bridges

1985 *Constructive analysis*, Grundlehren der mathematischen Wissenschaften n° 279, Springer-Verlag

Borevich, Z. I. et I. R. Shafarevich

1966 *Number theory*, Academic Press, New York.

Bourbaki, N.

1961 *Algèbre commutative : I. Modules plats*, Hermann, Paris.

Bridges, D. S.

1979 *Constructive functional analysis*, Research Notes in Mathematics n° 28, Pitman, London.

Bridges, D. S. et F. Richman

1987 *Varieties of constructive mathematics*, London Math. Soc. Lecture Notes n° 97, Cambridge Univ. Press.

Brouwer, L. E. J.

1981 *Cambridge lectures on intuitionism*, édité par D. van Dalen, Cambridge Univ. Press.

Brouwer, L. E. J. et B. de Loor

1924 Intuitionistischer Beweis des Fundamentalsatzes der Algebra, *Proc. Acad. Amsterdam* **27**, 186-188.

Diaconescu, R.

1975 Axiom of choice and complementation, *Proc. Amer. Math. Soc.* **51**, 176-178.

Feferman, S.

1975 Impredicativity of the existence of the largest divisible subgroup of an abelian p-group, *Model theory and algebra*, Springer Lecture Notes in Math. n° 498, 117-130.

Fourman, M. P. et A. Scedrov

1982 The "world's simplest axiom of choice" fails, *Manuscripta Math.* **38**, 325-332.

Greenleaf, N.

1981 Liberal constructive set theory, *Constructive mathematics*, Springer Lecture Notes in Math. n° 873, 213-240.

Heyting, A.

1941 Untersuchungen über intuitionistische Algebra, *Verhandelingen Akad. Amsterdam (Eerste Sectie)* **18**, n° 2.

1971 *Intuitionism, an introduction*, North-Holland.

Julian, W., R. Mines et F. Richman

1978 Algebraic numbers, a constructive development, *Pac. J. Math.* **74**, 91-102.

1983 Alexander duality, *Pac. J. Math.* **106**, 115-127.

Kaplansky, I.

1949 Elementary divisors and modules, *Trans. Amer. Math. Soc.* **66**, 478-479.

1969 *Infinite abelian groups*, University of Michigan Press.

Kronecker, L.

1882 Grundzüge einer arithmetischen Theorie der algebraischen Größen (section 4), *Journal für die reine und angewandte Mathematik* **92**, 1-122.

Lin, C.

1981 Recursively presented abelian groups : effective p-group theory I, *Journal of Symbolic Computation* **46**, 617-624.

1981a The effective content of Ulm's theorem, *Aspects of effective algebra*, J. Crossley (ed), Upside down A book company, Yarra Glen, Victoria, Australia.

Magnus, W., A. Karrass et D. Solitar

1966 *Combinatorial group theory*, Interscience, New York.

Mal′cev, A. I.

1971 Recursive abelian groups, *The metamathematics of algebraic systems*, North-Holland, Amsterdam, 282-286.

Metakides, G. et A. Nerode

1979 Effective content of field theory, *Annals of Math. Logic* **17**, 289-320.

Mines, R. et F. Richman

1981 Dedekind domains, *Constructive mathematics*, Springer Lecture Notes in Math n° 873, 16-30.

1982 Separability and factoring polynomials, *Rocky Mountain J. Math.* **12**, 43-54.

1984 Valuation theory : a constructive view, *J. Number Theory* **19**, 40-62.

1986 Archimedean valuations, *J. London Math. Soc.* **34**, 403-410.

Myhill, J. et N. D. Goodman

1978 Choice implies excluded middle, *Zeit. Math. Log.* **24**, 461.

Nagata, M.

1962 *Local rings*, Interscience, New York

Olson, P. L.

1977 *Difference relations and algebra* : a *constructive study*, Thèse de doctorat, Univ. of Texas at Austin.

O'Meara, O. T.

1963 *Introduction to quadratic forms*, Springer-Verlag, Berlin.

Richman, F.

1973 The constructive theory of countable abelian p-groups, *Pac. J. Math.* **45**, 621-637.

1974 Constructive aspects of Noetherian rings, *Proc. Amer. Math. Soc.* **44**, 436-441.

1975 The constructive theory of KT-modules, *Pac. J. Math.* **61**, 263-274.

1977 A guide to valuated groups, *Abelian group theory (Proc. Second New Mexico State Univ. Conf., Las Cruces, N.M., 1976)*, Springer Lecture Notes in Math. n° 616, 73-86.

1977a Computing heights in Tor, *Houston J. Math.* **3**, 267-270.

1981 Seidenberg's condition P, *Constructive mathematics*, Springer Lecture Notes in Math. n° 873, 1-11.

1982 Finite-dimensional algebras over discrete fields, *The L. E. J. Brouwer centenary symposium*, A.S. Troelstra and D. van Dalen (editors), Stud. Logic Foundations Math. n° 111, North-Holland Pub. Co., 397-411.

1988 Nontrivial uses of trivial rings, *Proc. Amer. Math. Soc.* **103**, 1012-1014.

Rogers, L.

1980 Basic subgroups from a constructive viewpoint, *Communications in algebra* **8**, 1903-1925.

Rootselaar, B. van

1960 On intuitionistic difference relations, *Indag. math.* **22**, 316-322. Corrections : *Indag. math.* **25**, 132-133.

Rudin, W.

1985 Unique right inverses are two-sided, *Amer. Math. Monthly* **92**, 489-490.

Scedrov, A.

1986 Diagonalization of continuous matrices as a representation of intuitionistic reals, *Ann. Pure Appl. Logic.* **30**, 201-206.

Scott, D.

1979 Identity and existence in intuitionistic logic, *Applications of sheaves (Proc. Res. Sympos. Appl. Sheaf Theory to Logic, Algebra and Anal., Univ. Durham, Durham, 1977)* Springer Lecture Notes in Math. n° 753, 660-696.

Seidenberg, A.

1970 Construction of the integral closure of a finite integral domain, *Rend. Sem. Mat. e Fis. Milano* **40**, 100-120.

1971 On the length of a Hilbert ascending chain, *Proc. Amer. Math. Soc.* **29**, 443-450.

1972 Constructive proof of Hilbert's theorem on ascending chains, *Trans. Amer. Math. Soc.* **174**, 305-312.

1973 On the impossibility of some constructions in polynomial rings, *Proc. Int. Cong. Geom.* (Milano 1971), 77-85

1974 Constructions in algebra, *Trans. Amer. Math. Soc.* **197**, 273-313.

1974a What is Noetherian ?, *Rend. Sem. Mat. e Fis. Milano*, **44**, 55-61.

1975 Construction of the integral closure of a finite integral domain. II, *Proc. Amer. Math. Soc.* **52**, 368-372.

1978 Constructions in a polynomial ring over the ring of integers, *Amer. J. Math.* **100**, 685-703.

1984 On the Lasker-Noether decomposition theorem, *Amer. J. Math.* **106**, 611-638.

1985 Survey of constructions in Noetherian rings, *Proc. Symp. Pure Math.* n° 42, 377-386.

Smith, H. J. S.

1861 On systems of linear indeterminate equations and congruences, *Phil. Trans. of the Royal Society of London* **151**, 293-326.

Smith, Rick L.

1981 Two theorems on autostability in p-groups, *Logic year 1979-1980 (Proc. Seminars and Conf. Math. Logic, Univ. Connecticut, Storrs, Conn., 1979/80)*, Springer Lecture Notes in Math. n° 859, 302-311.

Soublin, J.-P.

1970 Anneaux et modules cohérents, *J. Algebra* **15**, 455-472.

Staples, J.

1971 On constructive fields, *Proc. London Math. Soc.* (3) **23**, 753-768.

Stolzenberg, G.

1968 Constructive normalization of an algebraic variety, *Bull. Amer. Math. Soc.* **74**, 595-599.

Uspenskii, V. A. et A. L. Semenov

1981 What are the gains of the theory of algorithms : basic developments connected with the concept of algorithm and with its application in mathematics, *Algorithms in modern mathematics and computer science (Urgench, 1979)*, Springer Lecture Notes in Computer Science n° 122, 100–234

Waerden, B. L. van der

1930 Eine Bemerkung über die Unzerlegbarkeit von Polynomen, *Math. Annalen* **102**, 738-739.

1953 *Modern Algebra*, Ungar, New York.

Wang, H.

1974 *From mathematics to philosophy*, Routledge & Kegan Paul, London.

Weiss, E.

1963 *Algebraic number theory*, McGraw-Hill, New York.

Postface du traducteur

L'algèbre dans le style de Bishop : quelques points essentiels du livre *A course in constructive algebra*

Introduction

Le livre qui précède, que nous citerons sous la forme [CCA], est une mise à jour des bases de l'algèbre classique dans un style proche des mathématiques constructives à la Bishop. Les versions constructives des théorèmes classiques leur donnent une nouvelle saveur et sont beaucoup plus précises. D'une manière qui peut sembler à priori étonnante, les démonstrations sont souvent plus simples et plus élégantes que celles que l'on trouve dans les textes usuels en mathématiques classiques. Cela tient au fait que, n'ayant plus aucune baguette magique du style « principe du tiers exclu » à sa disposition, on est forcé d'aller plus au fond des choses, et de mieux comprendre les mathématiques. Les raccourcis apparents qu'autorisent les mathématiques classiques introduisent ainsi souvent des détours inutiles : il n'est pas toujours bon d'être très (trop ?) savant pour traiter les problèmes de nature élémentaire, ou difficiles.

1 La réception de l'ouvrage

Après la postface se trouve un chapitre final sur la réception de [CCA]. La lectrice y trouvera une liste bibliographique des travaux qui ont cité le livre depuis sa parution. Cette liste est conséquente, mais la réception de l'ouvrage par la communauté mathématique est plutôt décevante eu égard à son caractère profondément novateur.

La réception de l'ouvrage en France est encore plus confidentielle que celle du livre de Bishop [2]. Je n'ai pratiquement jamais rencontré un ou une mathématicienne française qui ait seulement entendu parler de l'existence de l'ouvrage.

On pourrait s'attendre à ce que la communauté du Calcul Formel soit un peu plus au fait puisque les théorèmes du livre ont tous un contenu calculatoire direct qui leur permet, en principe, d'être implémentés dans les logiciels de calcul formel usuel.

Il m'est arrivé de soumettre un article d'algèbre constructive à la section « Computer Algebra » du *Journal of Algebra*, section dont les recommandations aux auteurs indiquent explicitement l'intérêt de la revue pour les mathématiques constructives. Quelle ne fut pas ma surprise lorsque le rapporteur me demanda d'expliquer ce que signifiait « ou » en mathématiques constructives, car il était dérouté et ne comprenait pas certains arguments. L'article fut finalement rejeté de cette section du *Journal of Algebra*, apparemment par impossibilité de trouver un rapporteur compétent.

J'ai cependant découvert récemment l'article *A constructive approach to Freyd categories* de Sebastian Posur, `https://arxiv.org/abs/1712.03492v1`. J'extrais un morceau de la section 2, « Constructive category theory ». Cet article me semble opérer un tournant salutaire et espéré.

> To present our algorithmic approach to Freyd categories, we chose the language of constructive mathematics (see, e.g., [MRR88]). We did that for the following reasons : the language of constructive mathematics
>
> 1. reveals the algorithmic content of the theory of Freyd categories,
> 2. is perfectly suited for describing generic algorithms, i.e., constructions not depending on particular choices of data structures,
> 3. allows us to express our algorithmic ideas without choosing some particular model of computation (like Turing machines),
> 4. encompasses classical mathematics, i.e., all results stated in constructive mathematics are also valid classically,
> 5. does not differ very much from the classical language in our particular setup.
>
> In constructive mathematics the notions of data types and algorithms (or operations) are taken as primitives and every property must have an algorithmic interpretation. For example, given an additive category **A** we interpret the property
>
> **A** has kernels
>
> as follows : we have algorithms that compute for given

- $A, B \in \mathrm{Obj}_{\mathbf{A}}$, $\alpha \in \mathrm{Hom}_{\mathbf{A}}(A, B)$, an object $\ker(\alpha) \in \mathrm{Obj}_{\mathbf{A}}$ and a morphism

$$\mathrm{KernelEmbedding}(\alpha) \in \mathrm{Hom}_{\mathbf{A}}(\ker(\alpha), A)$$

  for which $\mathrm{KernelEmbedding}(\alpha) \cdot \alpha = 0$,
- $A, B, T \in \mathrm{Obj}_{\mathbf{A}}$, $\alpha \in \mathrm{Hom}_{\mathbf{A}}(A, B)$, $\tau \in \mathrm{Hom}_{\mathbf{A}}(T, A)$ such that $\tau \cdot \alpha = 0$, a morphism $u \in \mathrm{Hom}_{\mathbf{A}}(T, \ker(\alpha))$ such that

$$u \cdot \mathrm{KernelEmbedding}(\alpha) = \tau,$$

  where u is uniquely determined (up to $=$) by this property.

Another important example is given by *decidable equality*, where we interpret the property that for all objects $A, B \in \mathbf{A}$, we have

$$\forall \alpha, \beta \in \mathrm{Hom}_{\mathbf{A}}(A, B) : (\alpha = \beta) \vee (\alpha \neq \beta)$$

as follows : we are given an algorithm that decides or disproves equality of a given pair of morphisms...

On the other hand, we allow ourselves to work classically whenever we interpret Freyd categories in terms of finitely presented functors. The reason for this is pragmatic : we want to demonstrate the usefulness of having Freyd categories computationally available, and we believe that this can be done by interpreting Freyd categories in terms of other categories that classical mathematicians care about.

2 Une théorie des ensembles revisitée

Dans [CCA], les auteurs introduisent une philosophie des mathématiques qui diffère légèrement de celle de [2, Bishop, 1967]. Ce point de vue se trouve sans doute exprimé de manière plus directe dans les articles [9, 10] et dans le livre [3].

Tout d'abord, comme chez Bishop, le point de vue n'est pas celui d'une mathématique formalisée, mais celui d'une mathématique ouverte à des développements imprévisibles, et pour laquelle le seul critère de vérité est la conviction qu'emporte une démonstration. L'univers mathématique n'est donc pas préexistant, il est bien au contraire une construction proprement humaine, à l'usage de la communauté humaine.

Un point original est cependant le suivant. L'attitude générale dans [CCA] est de considérer que toutes les mathématiques, aussi bien classiques que constructives, explorent un même univers d'objets idéaux, mais avec des outils différents.

Les mathématiques constructives sont une généralisation des mathématiques classiques en ce qu'elles ne supposent ni le principe du tiers exclu ni l'axiome du choix, exactement comme la théorie des groupes est une généralisation de la théorie des groupes commutatifs en ce qu'elle ne suppose plus valide la règle de commutativité.

Commençons par un premier extrait de [CCA].

> Notre notion de ce qu'est un **ensemble** est une notion plutôt libérale.
>
> **Définition I.2.1.** Un ensemble S est défini lorsque nous décrivons comment construire ses éléments à partir d'objets qui peuvent avoir été déjà construits, ou peut-être pas, avant S lui-même, et lorsque nous expliquons ce que signifie pour deux éléments de S qu'ils sont égaux.
>
> À la suite de Bishop nous regardons la **relation d'égalité** sur un ensemble comme conventionnelle : quelque chose à préciser lorsque l'ensemble est défini, et qui est soumis à la seule contrainte d'être une relation d'équivalence.
>
> . . . . . .
>
> Une relation unaire P sur S définit un **sous-ensemble** $A = \{\, x \in S : P(x) \,\}$ de S : un élément de A est un élément de S qui satisfait la propriété P, et deux éléments de A sont égaux si, et seulement si, ils sont égaux comme éléments de S. Si A et B sont des sous-ensembles de S, et si chaque élément de A est un élément de B, nous disons que A est **contenu** dans B, et nous écrivons $A \subseteq B$. Deux sous-ensembles A et B d'un ensemble S sont **égaux** si $A \subseteq B$ et $B \subseteq A$; ceci est clairement une relation d'équivalence sur les sous-ensembles de S. Nous avons décrit comment construire un sous-ensemble de S, et ce que cela signifie d'être égaux pour deux sous-ensembles de S. Donc nous avons défini l'ensemble de tous les sous-ensembles, encore appelé l'**ensemble des parties** de S.

Les lecteurs de Bishop sont ici très étonnés. Les auteurs pensent en effet que la notion de « relation unaire sur un ensemble donné » est suffisamment claire pour que l'on puisse considérer l'ensemble de toutes ces relations unaires. C'est-à-dire considérer que l'on sait les construire, comme par exemple on sait construire un entier naturel, un nombre réel ou une fonction réelle. Or cela semble problématique car nul ne prétend connaitre un langage universel pour les mathématiques, dans lequel on pourrait codifier ces relations unaires. En particulier, si l'ensemble Ω des parties du singleton $\{0\}$ existe, cela signifie que les valeurs de vérité forment un ensemble et non pas une classe. La difficulté est que l'on semble faire ici comme si l'on savait d'avance comment on pourra reconnaitre ce que seront les valeurs de vérité possibles dans l'avenir.

En fait, il semble que chaque fois qu'un « ensemble des parties de . . . » est

implicite ou explicite dans le livre, c'est dans un cadre où n'interviennent pas *toutes* les parties, mais seulement certaines parties, qui peuvent être regroupées dans un ensemble au sens plus strict adopté par Bishop ; ou alors la quantification sur l'ensemble des parties n'est pas nécessaire à la clarté du texte [1].

J'illustre ceci par un théorème assez extraordinaire, à la démonstration incroyablement simple et élégante [2].

La décomposition obtenue dans le théorème V.2.3 est essentiellement unique sur n'importe quel anneau commutatif.

Théorème V.2.4. *Soient R un anneau commutatif, $m \leqslant n$ des entiers > 0, et $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_m$ et $J_1 \supseteq J_2 \supseteq \cdots \supseteq J_n$ des idéaux de R. Supposons qu'un R-module M soit isomorphe à $\bigoplus_{i=1}^{m} R/I_i$ et à $\bigoplus_{j=1}^{n} R/J_j$. Alors*

(a) $J_1 = J_2 = \cdots = J_{n-m} = R$.

(b) $I_i = J_{n-m+i}$ pour $i = 1, \ldots, m$.

Ici, on ne fait aucune hypothèse sur les idéaux I_i et J_j. D'un point de vue d'une formalisation du discours, il semble donc qu'il faudrait quantifier sur l'ensemble de tous les idéaux de l'anneau R, ensemble tout aussi problématique que l'ensemble des parties de R. Mais on voit bien que c'est uniquement dans le cadre d'une formalisation mal maitrisée du discours que la nécessité de « l'ensemble des idéaux de R » se fait sentir. Pareillement, on n'a pas besoin de quantifier sur la classe des anneaux commutatifs lorsque l'on écrit : « Soit R un anneau commutatif ». Voir à ce sujet l'article [7, Dependent sums and dependent products in Bishop's set theory] de Iosif Petrakis pour un système formel utilisant la quantification sur des classes.

Signalons cependant le passage suivant qui traite de la catégorie des ensembles, et où l'ensemble Ω des parties de $\{0\}$ joue bien un rôle crucial. Notons que le joli théorème démontré ici ne semble pas avoir d'autre utilité qu'esthétique, dans le cadre de la théorie des catégories. Voir [18] pour une analyse de ce théorème dans le cadre de la théorie des types de Martin-Löf.

[...] La propriété catégorique qui correspond au fait qu'une fonction f est injective est la suivante : si g et h sont des flèches depuis n'importe quel

1. L'exception la plus importante se trouve dans la définition des ensembles bien fondés et des ordinaux, voir plus loin page 347.

2. On ne trouve pas ce théorème dans les grands traités d'algèbre en mathématiques classiques actuels. Par exemple Bourbaki (*Algèbre*, Chapitre VII, paragraphe 4, section 1), qui est un des meilleurs pour ce problème, ne donne le théorème que pour le cas où $m = n$, $I_1 \neq R$ et $J_1 \neq R$. Et la démonstration est moins belle que celle de [CCA].

ensemble C vers A et si $fg = fh$, alors $g = h$; c'est-à-dire f est **simplifiable à gauche** (on dit aussi **régulier à gauche**). Le fait qu'une fonction f est injective si, et seulement si, elle est simplifiable à gauche, est une démonstration purement routinière.

Une fonction f de A vers B est surjective si pour chaque $b \in B$ il existe un $a \in A$ tel que $f(a) = b$. La propriété catégorique correspondante est que f est **simplifiable à droite**, c'est-à-dire que si g et h sont des flèches de B vers n'importe quel ensemble C et si $gf = hf$, alors $g = h$. Le fait qu'une fonction f est surjective si, et seulement si, elle est simplifiable à droite, est une démonstration moins routinière que la démonstration du résultat correspondant pour les flèches simplifiables à la gauche.

Théorème I.4.1. *Une fonction est simplifiable à droite dans la catégorie des ensembles si, et seulement si, elle est surjective.*

Démonstration. Supposons que $f\colon A \to B$ est surjective et que $gf = hf$. Pour tout $b \in B$ il existe un $a \in A$ tel que $f(a) = b$. Donc $g(b) = g(f(a)) = h(f(a)) = h(b)$, et $g = h$. Réciproquement supposons que $f\colon A \to B$ est simplifiable à droite, et soit Ω l'ensemble des sous-ensembles de $\{0\}$. Définissons $g\colon B \to \Omega$ par $g(b) = \{0\}$ pour tout b, et définissons $h\colon B \to \Omega$ par

$$h(b) = \{\, x \in \{0\} : b = f(a) \text{ pour un } a \,\}.$$

Donc $h(b)$ est le sous-ensemble de $\{0\}$ tel que $0 \in h(b)$ si, et seulement si, il existe un a tel que $b = f(a)$. Clairement $gf = hf$ est la fonction qui fait correspondre à tout élément de A le sous-ensemble $\{0\}$. Donc $g = h$, et par suite $0 \in h(b)$, ce qui signifie que $b = f(a)$ pour un a. □

En fait, un trait original de [CCA] est la considération d'une notion de catégories en tant qu'objets mathématiques à part entière et non comme une simple « manière de parler » :

Nous travaillons avec deux types de collections d'objets mathématiques, les ensembles et les catégories.

. . . . . .

Étant donnés deux groupes, ou deux ensembles, il est en général incorrect de demander s'ils sont égaux ; la question pertinente est de savoir s'ils sont ou ne sont pas isomorphes, ou plus généralement quels sont les morphismes entre eux.

Une **catégorie** est une collection d'objets (comme l'est un ensemble).

Une relation d'égalité sur un ensemble construit, pour deux objets a et b de cet ensemble, une *proposition* « $a = b$ ». Pour spécifier une catégorie $\mathcal{C}$, nous devons montrer comment construire, pour deux objets A et B de $\mathcal{C}$, un *ensemble* $\mathcal{C}(A, B)$.

Un intérêt primordial des catégories est de permettre de généraliser la notion de famille d'objets (indexée par un ensemble). Pour la catégorie des ensembles, Bishop ne considère dans [2] que des familles de sous-ensembles d'un même ensemble. Mais dans les mathématiques usuelles, et particulièrement en algèbre, on a parfois besoin d'une notion plus générale, qui correspond à la notion de types dépendants en théorie constructive des types.

En utilisant la notion de foncteur nous pouvons étendre notre définition d'une famille d'éléments dans un ensemble à celle d'une famille d'objets dans une catégorie $\mathcal{C}$. Soit I un ensemble. Une **famille A d'objets de $\mathcal{C}$ indexée par I** est un foncteur depuis I, vu comme une catégorie, vers la catégorie $\mathcal{C}$. Nous notons souvent une telle famille par $\{A_i\}_{i\in I}$. Si $i = j$, la flèche de A_i vers A_j est notée A^i_j, et c'est un isomorphisme.

Avec cela comme outil, il est possible de construire certains objets cruciaux, comme

— les limites et colimites (en particulier les produits et les sommes directes de familles) dans certaines catégories,
— certaines structures algébriques librement engendrées par un ensemble S qui n'est pas nécessairement discret,
— de nombreuses opérations usuelles en mathématiques classiques sur les ordinaux (voir la définition des ordinaux dans [CCA] plus loin).

Par exemple on démontre qu'un module librement engendré par un ensemble S est plat ; mais il n'est pas nécessairement projectif (exercice IV.4.9). Le théorème classique selon lequel tout module est quotient d'un module libre reste valable ; la conséquence efficace n'est pas qu'il est quotient d'un module projectif, mais plutôt quotient d'un module plat. Ainsi, en forçant les ensembles à être discrets (selon le principe du tiers exclu), les mathématiques classiques simplifient à outrance la notion de module libre et aboutissent à des conclusions impossibles à satisfaire de manière algorithmique.

Une notion naturelle d'ordinal [1] est également introduite dans le chapitre I de [CCA], et elle est utilisée dans les problèmes de classification des groupes abéliens (au chapitre XI).

1. Cette notion est différente de celle que l'on peut trouver chez Brouwer ou Martin-Löf. Voir aussi [4, A constructive theory of ordinals].

Remarquons que la notion d'ensemble bien fondé définie ci-dessous utilise la quantification sur toutes les parties de W.

Soit W un ensemble muni d'une relation $a < b$. Un sous-ensemble S de W est dit **héréditaire** si $w \in S$ chaque fois que $w' \in S$ pour tout $w' < w$. L'ensemble W, ou la relation $a < b$, est dite **bien fondée** si tout sous-ensemble héréditaire de W est égal à W. Un ensemble ordonné discret est dit bien fondé si la relation $a < b$ (i.e. $a \leqslant b$ et $a \neq b$) est bien fondée. Un **ordinal**, ou **ensemble bien ordonné**, est un ensemble totalement ordonné discret et bien fondé.

Les ensembles bien ordonnés fournissent l'environnement pour les arguments par induction généraux.

. . . . . .

Pour des ordinaux λ et μ on définit un **plongement** de λ dans μ comme une fonction ρ de λ vers μ telle que si $a < b$ alors $\rho a < \rho b$, et si $c < \rho b$, alors on a un $a \in \lambda$ tel que $\rho a = c$. [. . .]

Théorème I.6.5. *Si λ et μ sont des ordinaux et si ρ et σ sont des plongements de λ dans μ, alors $\rho = \sigma$.*

. . . . . .

Lorsque l'on a un plongement de l'ordinal λ dans l'ordinal μ, nous écrivons $\lambda \leqslant \mu$. Clairement, une composition de plongements est un plongement, donc cette relation est transitive. Le théorème 6.5 implique que si $\lambda \leqslant \mu$ et $\mu \leqslant \lambda$, alors λ et μ sont isomorphes, i.e. il y a une bijection de λ vers μ qui préserve et réfléchit l'ordre. Il est naturel de dire que deux ordinaux isomorphes sont **égaux**. [. . .]

On se retrouve ainsi dans un cadre voisin de la théorie constructive des types dépendants, où tous les types sont créés par des définitions inductives généralisées.

Dans les sections suivantes, nous donnons quelques exemples significatifs de théorèmes classiques auxquels la reformulation constructive apporte un éclairage nouveau et des renseignements supplémentaires précis.

Nous indiquons aussi quelques exemples de théorèmes triviaux en mathématiques classiques et pourtant très importants du point de vue algorithmique.

3 L'exemple des anneaux principaux et des modules de type fini sur ces anneaux

Un anneau principal est en mathématiques classiques un anneau intègre dans lequel tout idéal est de type fini. D'un point de vue constructif, même le corps à deux éléments ne satisfait pas cette définition : on considère l'idéal engendré par une suite binaire ; fournir un générateur de cet idéal revient à décider si la suite est identiquement nulle, ce qui est LPO (voir page 4).

Une définition algorithmiquement pertinente, et classiquement équivalente à la définition classique, est celle d'un anneau de Bézout intègre discret qui satisfait une condition de noethérianité convenablement formulée.

Un **monoïde à pgcd** est un monoïde commutatif régulier dans lequel toute paire d'éléments possède un plus grand commun diviseur. Un **anneau intègre à pgcd** est un anneau intègre discret dont les éléments non nuls forment un monoïde à pgcd.

. . . . . .

Un **idéal principal** d'un monoïde commutatif M est un sous-ensemble I de M tel que $I = Ma = \{\, ma : m \in M \,\}$ pour un $a \in M$. Nous disons que le monoïde M **satisfait la condition de chaine des diviseurs** si pour chaque chaine ascendante $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ d'idéaux principaux, il y a un n tel que $I_n = I_{n+1}$.

On dit qu'un anneau intègre discret satisfait la condition de chaine des diviseurs si le monoïde des éléments non nuls la satisfait.

Définition IV.2.7. Un **anneau de Bézout intègre**, ou **domaine de Bézout** est un anneau intègre discret tel que pour tous éléments a, b on a deux éléments s, t tels que $sa + tb$ divise a et b. Un **anneau principal** est un domaine de Bézout qui satisfait la condition de chaine des diviseurs.

Le théorème de structure classique dit qu'un module de type fini sur un anneau principal est la somme directe d'un sous-module libre de rang fini et du sous-module de torsion, lui même égal à une somme directe de modules $R/(a_i)$ avec les a_i non nuls mis dans un ordre où chaque a_i divise le suivant.

La forme algorithmique la plus pure de ce théorème est le théorème de réduction d'une matrice en forme normale de Smith.

Une matrice $A = (a_{ij})$ est en **forme normale de Smith** si elle est diagonale et si $a_{ii} | a_{i+1,i+1}$ pour tout i.

Théorème V.1.2. *Toute matrice sur un anneau principal est équivalente à une matrice en forme normale de Smith.*

Théorème V.1.4. *Deux matrices en forme normale de Smith sur un anneau intègre à pgcd sont équivalentes si, et seulement si, les éléments diagonaux correspondants sont associés.*

Le théorème de structure pour les modules de présentation finie est une conséquence directe du théorème V.1.2.

Théorème V.2.3 (théorème de structure)**.** *Soit M un module de présentation finie sur un anneau principal R. Alors il existe des idéaux principaux $I_1 \supseteq I_2 \supseteq \cdots \supseteq I_n$ tels que M est isomorphe à la somme directe $R/I_1 \oplus R/I_2 \oplus \cdots \oplus R/I_n$.*

Puisque l'anneau est discret par définition, on peut séparer la somme en deux morceaux : le début, pour les indices de 1 à k disons, est alors le sous-module de torsion, avec $I_k = (a_k) \neq 0$, et le deuxième morceau, pour les $j > k$ avec les a_j nuls, est un module libre de rang $n - k$. Par contre, pour savoir quels I_j (pour les premiers indices j) sont égaux à R (et donc pourraient être supprimés sans dommage), il faut disposer d'un test pour l'inversibilité d'un élément, ce qui est la même chose ici que disposer d'un test de divisibilité entre deux éléments.

En mathématiques classiques, le théorème V.2.3 est énoncé pour les modules de type fini. D'un point de vue classique, les modules de type fini sur un anneau principal sont de présentation finie, tandis que d'un point de vue constructif il est clairement impossible d'avoir un algorithme pour réaliser cette implication, même dans le cas simple d'un $\mathbb{Z}$-module $\mathbb{Z}/I$ avec I de type dénombrable (par exemple engendré par une suite binaire).

La manière dont Bourbaki (*Algèbre*, chapitre VII) traite ces théorèmes mérite la comparaison. Le théorème de structure est donné avant le théorème de réduction de Smith pour les matrices. Et les démonstrations, qui utilisent trop le principe du tiers exclu, échouent à produire des algorithmes pour expliciter les théorèmes.

4 Les problèmes de factorisation

Le théorème IV.4.7(i) ci-après est usuellement démontré pour les anneaux factoriels, mais la condition noethérienne sous-jacente est en fait inutile.

Théorème IV.4.7. *Soit R un anneau intègre discret.*
(i) *Si R est un anneau à pgcd, alors il en va de même pour $R[X]$.*

On invite le lecteur à apprécier l'élégance de la démonstration que l'on trouve dans [CCA].

Le théorème classique de décomposition en facteurs premiers dans un monoïde à pgcd qui satisfait la condition de chaine des diviseurs est inaccessible d'un point de vue algorithmique. Il est remplacé en mathématiques constructives par un théorème un peu plus subtil qui rend en pratique les mêmes services que le théorème classique.

Théorème IV.1.8 (factorisation partielle)**.** *Soient $x_1, \ldots, x_k$ des éléments d'un monoïde à pgcd M qui satisfait la condition de chaine des diviseurs. Alors on peut construire une famille P d'éléments de M deux à deux premiers entre eux telle que chaque x_i est associé à un produit d'éléments de P.*

Soit M un monoïde régulier. Un élément $a \in M$ est dit **borné par l'entier naturel** n si chaque fois que $a = a_0 \cdots a_n$ avec des $a_i \in M$, alors l'un des a_i est inversible. Un élément de M est **borné** s'il est borné par un entier naturel ; le monoïde M est **à décomposition bornée** si tous ses éléments sont bornés. Un anneau intègre discret est **à factorisation bornée** si ses éléments non nuls forment un monoïde à décomposition bornée.

Un anneau intègre à pgcd qui satisfait la condition de chaine des diviseurs est appelé un **quasi-AFU**, où AFU est un acronyme pour « anneau à factorisation unique (en facteurs premiers) ».

Les anneaux quasi-AFU et les anneaux à pgcd à factorisation bornée sont deux versions constructives non équivalentes (constructivement) de la notion classique d'anneau factoriel. En fait, on trouve dans [CCA] encore trois autres versions constructives de cette notion classique.

Définition IV.2.1. Un anneau intègre discret R est appelé un **anneau à factorisation unique**, ou un **AFU**, si tout élément r non nul de l'anneau est inversible ou admet une factorisation essentiellement unique en produit d'éléments irréductibles, i.e. si $r = p_1 \cdots p_m$ et $r = q_1 \cdots q_n$ sont deux factorisations de r en produit d'éléments irréductibles, alors $m = n$ et on

peut réindexer les facteurs de façon à ce que $p_i \sim q_i$ pour chaque i. Nous disons que R est **factoriel** si $R[X]$ est un anneau à factorisation unique.

Un corps discret k est dit **pleinement factoriel** si tout corps extension de dimension finie de k est factoriel.

Les cinq versions constructives sont en mathématiques classiques équivalentes à la notion classique, mais elles introduisent des distinctions pertinentes du point de vue algorithmique, totalement invisibles en mathématiques classiques, par la faute de l'utilisation du principe du tiers exclu, qui écrase ces distinctions pertinentes. Dans le théorème IV.4.7 les points (ii) (joint au point (i)) et (vi) (i.e. (i) et (v)) sont deux versions distinctes, inéquivalentes, d'un même théorème de mathématiques classiques sur les anneaux factoriels.

Théorème IV.4.7. *Soit R un anneau intègre discret.*

(i) *Si R est un anneau à pgcd, alors il en va de même pour $R[X]$.*

(ii) *Si R est à factorisation bornée, alors il en va de même pour $R[X]$.*

(iii) *Si R a ses unités détachables, alors il en va de même pour $R[X]$.*

(iv) *Si la divisibilité est décidable dans R, alors il en va de même pour $R[X]$.*

(v) *Si R satisfait la condition de chaine des diviseurs, alors il en va de même pour $R[X]$.*

(vi) *Si R est un quasi-AFU, alors il en va de même pour $R[X]$.*

Concernant les problèmes de factorisation des polynômes sur un corps discret, la situation algorithmique n'est pas décrite correctement par les mathématiques classiques. Par exemple, le problème de factorisation dans $k[X]$ n'est pas trivial, contrairement à ce qu'affirme le théorème des mathématiques classiques.

Le chapitre VII de [CCA] explore cette situation en grands détails.

Le théorème constructif de base sur ce sujet est donné dans le chapitre VI. Comme il arrive que la caractéristique d'un corps ou d'un anneau ne soit pas connue d'avance, mais puisse être révélée au cours d'une construction, certaines précautions sont nécessaires dans les énoncés, comme ci-dessous dans le point (i). Notez que si l'on découvre un nombre premier p non nul dans un anneau k, il est nécessairement unique (sauf si l'anneau est trivial).

Lorsque k est un corps discret, on laisse simplement tomber l'alternative « k contient un élément non nul non inversible » dans le théorème. Mais il arrive que dans [CCA] le théorème soit utilisé sous la forme précise donnée ici, par exemple dans le chapitre IX sur la structure des algèbres de dimension finie.

Théorème VI.6.3. *Soient k un anneau commutatif discret avec unités détachables, et S un ensemble fini de polynômes unitaires de $k[X]$. Alors, ou bien k contient un élément non nul non inversible, ou bien nous pouvons construire un ensemble fini T de polynômes unitaires de $k[X]$ tel que :*

(i) *tout élément de T est de la forme $f(X^q)$ avec f séparable et q égal à 1 ou à une puissance d'un nombre premier nul dans k,*

(ii) *les éléments de T sont deux à deux étrangers,*

(iii) *tout polynôme de S est un produit de polynômes de T.*

Lorsque k est un corps discret, on obtient ainsi, en partant d'une famille donnée de polynômes univariés, une famille de polynômes unitaires séparables deux à deux étrangers qui fournit une version plus précise du théorème général de factorisation partielle IV.1.8 (lequel s'applique aux anneaux intègres à pgcd qui satisfont la condition de chaine des diviseurs).

5 Les anneaux noethériens, les décompositions primaires et le théorème de l'idéal principal de Krull

Un R-module est dit **fortement discret** si tout sous-module de type fini est détachable. Il est dit **cohérent** si tout sous-module de type fini est de présentation finie. La notion d'anneau cohérent fortement discret est fondamentale du point de vue algorithmique en algèbre commutative, en particulier pour la raison suivante : sur un anneau cohérent fortement discret, les systèmes linéaires sont parfaitement compris et maitrisés [1].

Dans les traités usuels en mathématiques classiques, cette notion est rarement mise en avant parce que l'on préfère la notion d'anneau *noethérien*. En mathématiques classiques, tout anneau noethérien A est cohérent parce que tous les sous-modules de A^n sont de type fini, et tout module de type fini est cohérent pour la même raison. En outre, on a le théorème de Hilbert qui dit que *si A est noethérien, toute A-algèbre de présentation finie est également un anneau noethérien*, tandis que la même affirmation est en défaut si l'on remplace « noethérien » par « cohérent » (voir [17, Soublin, 1970]).

D'un point de vue algorithmique cependant, il semble impossible de trouver une formulation constructive satisfaisante de la noethérianité qui implique la cohérence. Et la cohérence est souvent la propriété la plus importante du point de vue algorithmique. Comme conséquence, la cohérence doit être ajoutée (d'un

1. Dans l'article de Posur cité précédemment, ces anneaux sont appelés « calculables ».

point de vue constructif) lorsque l'on utilise la notion d'anneau ou de module noethérien.

La définition adoptée pour **module noethérien** dans [CCA] est : module dans lequel toute suite croissante de sous-modules de type fini admet deux termes consécutifs égaux. Il s'agit d'une définition constructivement acceptable, équivalente en mathématiques classiques à la définition usuelle.

Le théorème classique disant que sur un anneau noethérien tout A-module de type fini est noethérien est avantageusement remplacé par les théorèmes constructifs suivants (voir dans [CCA] le corolaire III.2.6, le théorème III.2.7 et le corolaire III.2.8).

Sur un anneau cohérent (resp. cohérent fortement discret), tout A-module de présentation finie est cohérent (resp. cohérent fortement discret).

Sur un anneau cohérent noethérien (resp. cohérent noethérien fortement discret), tout A-module de présentation finie est cohérent noethérien (resp. cohérent noethérien fortement discret).

Deux résultats classiques importants sur les anneaux noethériens ont des démonstrations constructives dans le cadre fixé par [CCA].

Théorème VIII.2.7 (Artin-Rees)**.** *Soit I un idéal de type fini d'un anneau commutatif cohérent noethérien R. Soit N un sous-module de type fini d'un R-module de présentation finie M. Alors il existe un entier k tel que pour tout $n \geqslant k$ on a*

$$I^{n-k}(I^k M \cap N) = I^n M \cap N.$$

Théorème VIII.2.8 (théorème d'intersection de Krull)**.** *Soient M un module de présentation finie sur un anneau commutatif cohérent noethérien R et I un idéal de type fini de R. Notons $A = \bigcap_n I^n M$. Alors $a \in Ia$ pour tout $a \in A$, et donc $IA = A$.*

Le théorème de la base de Hilbert

Quels sont les anneaux cohérents R pour lesquels les anneaux $R[X_1, \ldots, X_n]$ sont également cohérents ? D'un point de vue constructif, on connait deux classes d'anneaux qui satisfont cette propriété : les anneaux cohérents noethériens (voir ci-après) et les domaines de Prüfer (voir [19, Yengui, 2015, Chapter 4]).

Le théorème de la base de Hilbert pour la définition de noethérianité donnée dans [CCA] est le suivant. Les démonstrations remontent à 1974 ([8, Richman, 1974] et [13, Seidenberg, 1974], voir aussi [11, Seidenberg, 1971] et [12, Seidenberg,

1973] pour le cas des anneaux de polynômes sur un corps discret). Elles sont exposées de manière limpide dans [CCA].

Théorème VIII.1.5 (théorème de la base de Hilbert)**.** *Si R est un anneau cohérent noethérien (à gauche), alors il en va de même pour $R[X]$. Si en outre R est fortement discret (à gauche), alors il en va de même pour $R[X]$.*

Une version de ce théorème en calcul formel (voir [1, 1994, Théorème 4.2.8]) dit que pour un anneau cohérent noethérien fortement discret R, on peut donner un algorithme du type « base de Gröbner » pour calculer l'idéal de tête d'un idéal de type fini dans $R[\underline{X}] = R[X_1, \ldots, X_n]$ pour un ordre monomial donné. On en déduit assez facilement le théorème VIII.1.5. De la sorte, les deux théorèmes peuvent être considérés comme essentiellement équivalents.

Cependant, les algorithmes sous-jacents aux deux démonstrations sont assez différents. On doit aussi remarquer d'une part que les auteurs de 1994 semblent ignorer que le problème a été essentiellement résolu en 1974, et d'autre part que les algorithmes dans [1] ne sont pas certifiés de manière constructive (en particulier, en se basant sur la démonstration classique, aucune borne ne peut être calculée pour le nombre d'étapes de l'algorithme en fonction des données).

Le théorème de décomposition primaire

L'exposé de [CCA] sur le cadre constructif convenable pour les décompositions primaires est fondé sur les travaux de Seidenberg [14, 1978] et [15, 1984]. Il s'agit dans [CCA] d'une réélaboration de ce travail, de manière simplifiée et synthétique.

Soit R un anneau commutatif. Un idéal Q de R est dit **primaire** si $xy \in Q$ implique $x \in Q$ ou $y^n \in Q$ pour un n. On voit alors que $\sqrt{Q}$ est un idéal premier P.

Voici maintenant une légère variation par rapport à la terminologie classique, sans réelle importance dans le cas noethérien : les idéaux concernés sont tous de type fini [1].

Une **décomposition primaire** d'un idéal I d'un anneau commutatif est une famille finie d'idéaux primaires de type fini $Q_1, \ldots, Q_n$ telle que $I = \bigcap_i Q_i$ avec les $\sqrt{Q_i}$ de type fini. On dit aussi dans ce cas que l'idéal I est **décomposable**. En mathématiques classiques, tout idéal d'un anneau noethérien admet une décomposition primaire.

Dans le cadre constructif, pour un anneau cohérent noethérien fortement discret, que doit-on ajouter comme hypothèses constructivement acceptables pour avoir les décompositions primaires ?

1. Sauf I lui-même, mais dans le cadre des anneaux cohérents noethériens, I est nécessairement de type fini.

Voici une réponse possible, donnée dans [CCA].

> Un **anneau de Lasker-Noether** est un anneau commutatif cohérent noethérien fortement discret tel que le radical de tout idéal de type fini est l'intersection d'un nombre fini d'idéaux premiers de type fini.

Cette définition est constructivement acceptable parce que les anneaux $\mathbb{Z}$, $\mathbb{Q}[X]$, et $k[X]$ lorsque k est corps discret algébriquement clos, satisfont ces hypothèses de manière immédiate. De nombreux anneaux usuels, noethériens en mathématiques classiques, satisfont également ces hypothèses, comme expliqué plus loin.

En fait, on voit facilement que lorsque k est un corps discret, $k[X]$ est un anneau de Lasker-Noether si, et seulement si, le corps k est factoriel. Cette équivalence précise est impossible à énoncer en mathématiques classiques car tous les corps sont factoriels. On pourrait cependant énoncer un résultat analogue en se restreignant au cadre des algorithmes mécanisables à la Turing.

Les premières propriétés importantes des anneaux de Lasker-Noether sont résumées dans les trois théorèmes qui suivent. Le premier énoncé semble presque trop précis, par souci de généralité, voir le commentaire qui suit.

> **Théorème VIII.8.1.** *Soit S un sous-monoïde multiplicatif d'un anneau de Lasker-Noether R tel que $I \cap S$ est vide ou non vide pour tout idéal de type fini I de R. Alors $S^{-1}R$ est un anneau de Lasker-Noether.*

Si $S = R \setminus P$ pour un idéal premier P, la condition « $I \cap S$ est vide ou non vide » signifie « I est ou n'est pas contenu dans P ». Comme I est de type fini, le test est effectif si, et seulement si, P est détachable. Une conséquence du théorème VIII.8.1 est donc que pour tout idéal premier détachable, et en particulier pour tout idéal premier de type fini, le localisé R_P est un anneau de Lasker-Noether.

> **Théorème VIII.8.2.** *Soient R un anneau de Lasker-Noether et I un idéal de type fini de R. Alors R/I est un anneau de Lasker-Noether.*
>
> **Théorème VIII.8.5** (théorème de décomposition primaire)**.** *Soit R un anneau de Lasker-Noether. Alors tout idéal de type fini de R est décomposable.*

Le théorème de l'idéal principal de Krull

Une propriété plus élaborée des anneaux de Lasker-Noether est le fameux théorème de l'idéal principal de Krull, et le fait que tout idéal premier de type fini a une hauteur bien définie.

Théorème VIII.10.4 (théorème de l'idéal principal généralisé)**.** *Soient R un anneau de Lasker-Noether et $I = (a_1, \ldots, a_n)$. Alors tout idéal premier minimal au-dessus de I est de hauteur au plus n.*

Théorème VIII.10.5. *Soit P un idéal premier de type fini propre d'un anneau de Lasker-Noether R. Alors il existe un m tel que P est de hauteur m et est un idéal premier minimal au-dessus d'un idéal engendré par m éléments.*

Anneaux pleinement Lasker-Noether

Enfin, il faut répondre à la question : quelles hypothèses supplémentaires faut-il ajouter à la définition d'un anneau de Lasker-Noether R pour que les anneaux $R[X_1, \ldots, X_n]$ soient également de Lasker-Noether ? Voici une réponse donnée dans [CCA] :

On dit qu'un anneau R est **pleinement Lasker-Noether** si c'est un anneau de Lasker-Noether et si pour chaque idéal premier de type fini P de R, le corps de fractions de R/P est pleinement factoriel. Notez que l'anneau des entiers $\mathbb{Z}$ est pleinement Lasker-Noether, de même que tout corps pleinement factoriel.

Les trois théorèmes suivants (avec les théorèmes précédents sur les anneaux de Lasker-Noether) montrent alors que dans ce cadre (c'est-à-dire avec cette définition constructivement acceptable, équivalente en mathématiques classiques à la définition d'anneau noethérien), un très grand nombre de théorèmes classiques concernant les anneaux noethériens ont désormais une démonstration constructive et une signification claire. Cela semble un « miracle » de la même sorte que celui qu'a représenté la parution du livre de Bishop.

Théorème VIII.9.1. *Soit I un idéal de type fini d'un anneau pleinement Lasker-Noether R. Alors R/I est un anneau pleinement Lasker-Noether.*

Théorème VIII.9.2. *Si P est un idéal premier détachable d'un anneau pleinement Lasker-Noether R, le localisé R_P est un anneau pleinement*

Lasker-Noether.

Théorème VIII.9.6. *Si R est un anneau pleinement Lasker-Noether, il en va de même pour $R[X]$.*

Note. L'article [6, Perdry, 2004] définit une notion de noethérianité constructivement plus forte que celle de [CCA]. Les exemples usuels d'anneaux noethériens sont noethériens en ce sens. Avec cette notion, la définition d'un anneau de Lasker-Noether devient plus naturelle : c'est un anneau noethérien cohérent fortement discret qui possède un test de primalité pour les idéaux de type fini. L'article développe une théorie agréable des anneaux pleinement Lasker-Noether dans ce contexte.

Note. Le calcul de la décomposition primaire dans les anneaux de polynômes sur un corps discret ou sur $\mathbb{Z}$ est un sujet de recherche actif en Calcul Formel. L'article fondateur de Seidenberg est parfois cité, mais, à ma connaissance, le livre [CCA] ne l'est jamais.

6 Le théorème de structure de Wedderburn pour les k-algèbres de dimension finie

On parle ici de k-algèbres unitaires et associatives qui sont des k-espaces vectoriels de dimension finie sur un corps discret k. Autrement dit, ce sont des algèbres isomorphes à une sous-algèbre de type fini d'une algèbre de matrices $\mathrm{E}_k(k^n)$ (algèbre des k-endomorphismes de l'espace vectoriel k^n). On abrège la terminologie en parlant de « k-algèbre de dimension finie ».

Dans un anneau A non nécessairement commutatif, le **radical de Jacobson** de A est l'ensemble I des éléments x tels que $1 + xA \subseteq A^\times$. C'est un idéal (bilatère), et le quotient A/I a son radical de Jacobson nul.

Lorsque A est une k-algèbre de dimension finie, ce radical peut aussi être défini comme « radical nilpotent » : $\mathrm{rad}(A)$ est l'ensemble des éléments x tels que l'idéal (à gauche) xA est nilpotent, i.e. il existe un entier n tel que tout produit $xa_1 \cdots xa_n$ est nul.

Soit A une k-algèbre de dimension finie. On peut calculer une base du centre de A ainsi que le polynôme minimal sur k d'un élément arbitraire de A. On peut aussi calculer une base de l'idéal à gauche et une autre de l'idéal bilatère engendrés par une partie finie de A. Mais il peut être difficile de calculer une base du radical, et l'on ne peut pas affirmer en général que le radical est de dimension finie (sur k).

Néanmoins, on sait calculer des objets qui sont triviaux en mathématiques classiques (à condition qu'on ne cherche pas à les calculer !). Par exemple, comme

alternative au calcul du radical, on a le théorème suivant.

Théorème IX.3.3. *Soit A une k-algèbre de dimension finie et soit L un idéal (à gauche) de A de dimension finie. Alors, ou bien $L \cap \operatorname{rad} A \neq 0$, ou bien $A = L \oplus N$ pour un idéal (à gauche) N.*

Un module M est dit **réductible** s'il a un sous-module propre non nul ; sinon, il est dit **simple**.

Une k-algèbre est dite **simple** si tout idéal bilatère est trivial. Lorsque l'anneau est discret, comme dans le cas présent, la définition revient à dire que si un élément est non nul, l'idéal (bilatère) qu'il engendre contient 1.

La première partie du théorème de Wedderburn affirme qu'une k-algèbre de dimension finie de radical nul est un produit de k-algèbres simples. Voici la reformulation constructive que l'on trouve dans [CCA]. Un corps k est dit **séparablement factoriel** si les polynômes séparables dans $k[X]$ sont décomposables en facteurs premiers.

Nous caractérisons maintenant les corps séparablement factoriels en termes de décomposition d'algèbres en produit d'algèbres simples. Cela constitue la première partie du théorème de Wedderburn.

Théorème IX.4.3 (théorème de Wedderburn, première partie)**.** *Un corps discret k est séparablement factoriel si, et seulement si, toute k-algèbre de dimension finie de radical nul est un produit d'algèbres simples.*

Une précision concernant la capacité à calculer une base du radical est donnée dans le corolaire suivant.

Corolaire IX.4.5. *Un corps discret k est pleinement factoriel si, et seulement si, toute k-algèbre de dimension finie contient un idéal nilpotent de dimension finie I tel que A/I est un produit de k-algèbres simples.*

La seconde partie du **théorème de structure de Wedderburn** pour les algèbres semi-simples dit qu'une algèbre simple de dimension finie est isomorphe à un anneau total de matrices carrées sur une algèbre à division (un corps gauche).

La version constructive de ce théorème donnée dans [CCA] élucide d'une manière surprenante le contenu calculatoire de ce théorème classique.

Théorème IX.5.1 (théorème de structure de Wedderburn)**.**
Soit A une k-algèbre de dimension finie qui contient un idéal à gauche non trivial. L'une des propriétés suivantes est satisfaite.

(i) *Le radical de A est non nul.*

(ii) *A est un produit de k-algèbres de dimension finie (de dimensions plus petites que A).*

(iii) *Il existe un entier $n > 1$ tel que A est isomorphe à l'anneau des matrices carrées $n \times n$ sur une k-algèbre de dimension inférieure à celle de A.*

. . . . . .

Le problème fondamental et de savoir reconnaitre si une k-algèbre de dimension finie est une algèbre à division ou pas, à savoir, être capable d'affirmer que c'est une algèbre à division ou alors de construire un idéal à gauche non trivial. Si nous sommes capables de faire cela, alors le théorème 5.1 implique que toute k-algèbre de dimension finie a un radical de dimension finie, et que modulo ce radical elle est un produit d'anneaux de matrices carrées $n \times n$ sur des algèbres à division. Cette condition est équivalente à la capacité de reconnaitre si une représentation de dimension finie arbitraire d'une k-algèbre de dimension finie est réductible.

Théorème IX.5.2. *Les propriétés suivantes pour un corps discret k sont équivalentes.*

(i) *Toute k-algèbre de dimension finie est une algèbre à division ou sinon contient un idéal à gauche non trivial.*

(ii) *Tout k-module à gauche de dimension finie M sur une k-algèbre de dimension finie A est réductible ou irréductible.*

(iii) *Toute k-algèbre de dimension finie A a un radical de dimension finie, et $A/\operatorname{rad} A$ est un produit d'anneaux complets de matrices sur des algèbres à division.*

Et nous restons un peu sur notre faim avec ces interrogations à la fin du chapitre IX.

Pour quels corps k les conditions du théorème 5.2 sont-elles satisfaites ? Les corps finis et les corps algébriquement clos fournissent des exemples faciles. Le corps des nombres réels algébriques $\mathbb{R}^a$ admet seulement trois algèbres à division, et une démonstration constructive de cette assertion montre que ce corps satisfait les conditions du théorème 5.2.

Théorème IX.5.3. *Soient k un sous-corps discret du corps des nombres réels $\mathbb{R}$, algébriquement clos dans $\mathbb{R}$, $H = k(i, j)$ l'algèbre des quaternions sur k, et A une k-algèbre de dimension finie. Ou bien A contient un diviseur de zéro, ou bien A est isomorphe à l'une des algèbres k, $k(i)$, ou H.*

Est-ce que le corps $\mathbb{Q}$ des nombres rationnels satisfait les conditions du théorème 5.2 ? Nous n'allons certainement pas produire un contre-exemple brouwerien avec $k = \mathbb{Q}$. Une analyse détaillée de la théorie classique des algèbres à division sur $\mathbb{Q}$, en analogie avec le théorème 5.3, donnera probablement une démonstration.

7 Les domaines de Dedekind

Bien que la théorie algébrique des nombres est généralement ressentie comme essentiellement constructive dans sa forme classique, même les auteurs qui attachent une attention particulière aux aspects constructifs de la théorie emploient des techniques hautement non constructives qui annulent leurs efforts. Par exemple, dans l'ouvrage [Borevich et Shafarevich 1966], les auteurs supposent que tout polynôme peut être décomposé en un produit de facteurs irréductibles (tout corps est factoriel), et qu'étant donné un sous-ensemble non vide des entiers naturels, on peut trouver son plus petit élément.

La théorie constructive des domaines de Dedekind dans [CCA] permet de donner une version explicite des exposés classiques de théorie des nombres et de géométrie algébrique concernant les corps locaux, par exemple le livre de J.-P. Serre [16]. Elle donne aussi les hypothèses convenables pour rendre compte des résultats classiques de la théorie des anneaux de Dedekind telle qu'on la trouve par exemple dans Bourbaki.

Cela nécessite de donner des définitions suffisamment précises et contraignantes, en commençant par celles de la théorie des valeurs absolues.

Citons à titre d'exemple les définitions concernant les domaines de Dedekind.

Définition XIII.1.1. Un ensemble discret non vide S de valeurs absolues discrètes non triviales (voir page 292) sur un corps de Heyting k est appelé un **ensemble de Dedekind** lorsque les propriétés suivantes sont satisfaites.

(i) Pour tout $x \in k$, il existe un sous-ensemble fini T de S tel que $|x|_p \leqslant 1$ pour les $p \in S \setminus T$.

(ii) Si $|\ \ |_q$ et $|\ \ |_{q'}$ sont des valeurs absolues distinctes dans S, et si $\varepsilon > 0$, il existe un $x \in k$ tel que $|x|_p \leqslant 1$ pour toute $p \in S$, $|x-1|_q < \varepsilon$, et $|x|_{q'} < \varepsilon$. Par suite, des valeurs absolues distinctes dans S sont inéquivalentes.

Soit S un ensemble de Dedekind de valeurs absolues sur un corps de Heyting k. Si $p \in S$, alors, comme p est ultramétrique, l'ensemble $R(p) = \{\, x \in k : |x|_p \leqslant 1 \,\}$ est un anneau, qui est local parce que p est discrète. L'anneau $R(p)$ est appelé l'**anneau local en** p. Les éléments de l'anneau $\bigcap_{p\in S} R(p)$ sont appelés les éléments **entiers de** S. Un anneau est appelé un **domaine de Dedekind** si c'est l'anneau des entiers d'un ensemble de Dedekind de valeurs absolues sur un corps de Heyting.

Si le point fort est de rendre compte constructivement de l'essentiel des théorèmes classiques, un point faible est que par exemple un anneau principal intègre n'est un domaine de Dedekind que dans le cas où l'on dispose d'algorithmes de factorisation des idéaux principaux en produit d'idéaux premiers. On pourra comparer par exemple avec l'exposé dans l'ouvrage [5], avec une définition constructivement plus faible mais plus proche de la définition classique usuelle (voir la définition XII-7.7 et le théorème XII-7.9). Dans [5], les domaines de Dedekind admettent une factorisation partielle pour les ensembles finis d'idéaux de type fini, et les domaines de Dedekind à factorisation totale correspondent aux domaines de Dedekind de [CCA].

Références

[1] William W. Adams et Philippe Loustaunau : *An introduction to Gröbner bases.* American Mathematical Society, Providence, 1994.

[2] Errett Bishop : *Foundations of constructive analysis.* McGraw-Hill, New York, 1967.

[3] Douglas Bridges et Fred Richman : *Varieties of constructive mathematics.* London Mathematical Society Lecture Note Series, 97. Cambridge university press, Cambridge, 1987.

[4] Thierry Coquand, Henri Lombardi et Stefan Neuwirth : A constructive theory of ordinals. En préparation, `http://hlombardi.free.fr/ConstructiveOrdinals.pdf`, 2017.

[5] Henri Lombardi et Claude Quitté : *Algèbre commutative. Méthodes constructives. Modules projectifs de type fini. Cours et exercices.* Calvage & Mounet, Paris, 2011. Traduction en anglais (version révisée et étendue par les auteurs) par Tania K. Roblot : *Commutative algebra : constructive methods. Finite projective modules.* Springer, Dordrecht, 2015.

[6] Hervé Perdry : Strongly Noetherian rings and constructive ideal theory. *J. Symbolic Comput.*, 37(4):511–535, 2004.

[7] Iosif Petrakis : Dependent sums and dependent products in Bishop's set theory. Rapport technique, Hausdorff Research Institute for Mathematics, 2018. `http://www.hcm.uni-bonn.de/fileadmin/him/Preprints/Types18.pdf`.

[8] Fred Richman : Constructive aspects of Noetherian rings. *Proc. Amer. Math. Soc.*, 44:436–441, 1974.

[9] Fred Richman : Confessions of a formalist, Platonist intuitionist. `http://math.fau.edu/Richman/html/Confess.htm`, 1994.

[10] Fred Richman : Interview with a constructive mathematician. *Modern Logic*, 6(3):247–271, 1996.

[11] A. Seidenberg : On the length of a Hilbert ascending chain. *Proc. Amer. Math. Soc.*, 29:443–450, 1971.

[12] A. Seidenberg : Constructive proof of Hilbert's theorem on ascending chains. *Trans. Amer. Math. Soc.*, 174:305–312, 1973.

[13] A. Seidenberg : What is Noetherian ? *Rend. Semin. Mat. Fis. Milano*, 44:55–61, 1975.

[14] A. Seidenberg : Constructions in a polynomial ring over the ring of integers. *Amer. J. Math.*, 100:685–706, 1978.

[15] A. Seidenberg : On the Lasker-Noether decomposition theorem. *Amer. J. Math.*, 106:611–638, 1984.

[16] Jean-Pierre Serre : *Corps locaux*. Hermann, Paris, 1968. Deuxième édition, Publications de l'Université de Nancago, VIII.

[17] Jean-Pierre Soublin : Anneaux et modules cohérents. *J. Algebra*, 15:455–472, 1970.

[18] Olov Wilander : Setoids and universes. *Math. Structures Comput. Sci.*, 20(4): 563–576, 2010.

[19] Ihsen Yengui : *Constructive commutative algebra : projective modules over polynomial rings and dynamical Gröbner bases*. Lecture Notes in Mathematics, 2138. Springer, Cham, 2015.

Réception de l'ouvrage

Voici l'histoire chronologique de la réception de [CCA], réalisée à partir de plusieurs bases de données. Elle n'est certainement pas exhaustive.

1985

Bishop, E. et D. S. Bridges. *Constructive analysis*. Grundlehren der mathematischen Wissenschaften 279. Springer.

1987

Ruitenburg, W. B. G. « Constructions of finitely generated submodules of constructively Noetherian modules ». *Compositio Math.* 62, p. 47-52.

1989

Bridges, D. S. « *A course in constructive algebra* by Ray Mines, Fred Richman, and Wim Ruitenburg ». *Bull. Amer. Math. Soc. (N.S.)* 20, p. 127-132.

Calude, C. et D. Vaida. « Ehrenfeucht test set theorem and Hilbert basis theorem : a constructive glimpse ». *Mathematical foundations of computer science 1989*. Lecture Notes in Comput. Sci. 379. Springer, p. 177-184.

Feferman, S. « *A course in constructive algebra*. Ray Mines, Fred Richman, Wim Ruitenburg ». *American Scientist* 77, p. 402.

Freedman, H. « *A course in constructive algebra*, by R. Mines, F. Richman and W. Ruitenburg ». *Math. Gaz.* 73, p. 272-273.

Lombardi, H. « Algèbre élémentaire en temps polynomial ». *Publ. Math. Fac. Sci. Besançon. Théorie des nombres* 1989. Fascicule 2. Rassemble « Calculabilité dans les structures algébriques dénombrables », « Sous-résultants, suite de Sturm, spécialisation », « Nombres algébriques et approximations ».

— « Nombres algébriques présentés comme solutions de systèmes d'équations en cascade ». Présenté aux journées de calcul formel CALSYF 89.

— « Théorème des zéros réel effectif et variantes ». *Publ. Math. Fac. Sci. Besançon. Théorie des nombres* 1989. Fascicule 1, article n° 5.

Richman, F. « Letter to the editor ». *Math. Mag.* 62, p. 285-286.

1990

Beeson, M. J. « *A course in constructive algebra*. By R. Mines, F. Richman, and W. Ruitenburg ». *Amer. Math. Monthly* 97, p. 357-362.

Haskell, D. « Topics in constructive p-adic algebra ». Thèse de doct. Stanford University.

Ishihara, H. « An omniscience principle, the Kőnig lemma and the Hahn-Banach theorem ». *Z. Math. Logik Grundlag. Math.* 36, p. 237-240.

Oliveira, A. J. F. *O advento da matemática não-standard*. Monografias da Sociedade Paranaense de Matematica 8. Universidade Nova de Lisboa.

Richman, F. « Intuitionism as generalization ». *Philos. Math. (2)* 5, p. 124-128.

— « Polynomials and linear transformations ». *Linear Algebra Appl.* 131, p. 131-137.

— « The constructive theory of torsion-free abelian groups ». *Comm. Algebra* 18, p. 3913-3922.

Scowcroft, P. « Ray Mines, Fred Richman, and Wim Ruitenburg. *A course in constructive algebra* ». *J. Symbolic Logic* 55, p. 883-886.

1991

Dalen, D. van. « Douglas Bridges and Fred Richman. *Varieties of constructive mathematics* ». *The Journal of Symbolic Logic* 56, p. 750-751.

Drucker, T. « *Zermelo's axiom of choice : its origins, development and influence*. By Gregory H. Moore ». *Historia Mathematica* 18, p. 364-369.

Jacobsson, C. et C. Löfwall. « Standard bases for general coefficient rings and a new constructive proof of Hilbert's basis theorem ». *J. Symbolic Comput.* 12, p. 337-371.

Lombardi, H. « Effective real Nullstellensatz and variants ». *Effective methods in algebraic geometry*. Progr. Math. 94. Birkhäuser, p. 263-288.

Lombardi, H. et M.-F. Roy. « Elementary constructive theory of ordered fields ». *Effective methods in algebraic geometry*. Progr. Math. 94. Birkhäuser, p. 249-262. Version anglaise moins détaillée du suivant.

— « Théorie constructive élémentaire des corps ordonnés ». *Publ. Math. Fac. Sci. Besançon. Théorie des nombres* 1991. Article n° 3.

Ruitenburg, W. B. G. « Constructing roots of polynomials over the complex numbers ». *Computational aspects of Lie group representations and related topics*. CWI Tract 84. Math. Centrum, Centrum Wisk. Inform., p. 107-128.

— « Constructive logic and the paradoxes ». *Modern Logic* 1, p. 271-301.

— « Inequality in constructive mathematics ». *Notre Dame J. Formal Logic* 32, p. 533-553.

1992

Cox, D., J. Little et D. O'Shea. *Ideals, varieties, and algorithms : an introduction to computational algebraic geometry and commutative algebra*. Undergraduate Texts in Mathematics. Springer.

Feferman, S. « A new approach to abstract data types. I. Informal development ». *Math. Structures Comput. Sci.* 2, p. 193-229.

Fellows, M. R. et N. Koblitz. « Self-witnessing polynomial-time complexity and prime factorization ». *Proceedings of the seventh annual structure in complexity theory conference*. IEEE Comput. Soc. Press, p. 107-110. Version préliminaire du suivant.

— « Self-witnessing polynomial-time complexity and prime factorization ». *Des. Codes Cryptogr.* 2, p. 231-235. Version finale du précédent.

Forsman, K. *Elementary aspects of constructive commutative algebra*. Rapp. tech. Linköpings universitet.

Haskell, D. « A transfer theorem in constructive p-adic algebra ». *Ann. Pure Appl. Logic* 58, p. 29-55.

Labhalla, S., H. Lombardi et R. Marlin. *Algorithmes modulaires de calcul des réductions de Hermite et de Smith*. Rapp. tech. Équipe de mathématiques de Besançon, Université de Franche-Comté.

Lombardi, H. « Une borne sur les degrés pour le théorème des zéros réel effectif ». *Real algebraic geometry*. Lecture Notes in Mathematics 1524. Springer, p. 323-345.

Mines, R. et C. Vinsonhaler. « Butler groups and Bext : a constructive view ». *Abelian groups and noncommutative rings*. Contemp. Math. 130. Amer. Math. Soc., p. 289-299.

Richman, F. « The constructive theory of countably generated Warfield modules ». *Abelian groups and noncommutative rings*. Contemp. Math. 130. Amer. Math. Soc., p. 371-383.

Romano, D. A. « a-coideals of sets ». *Zb. Rad.* 6, p. 253-258.

— « Some theorems about constructions of a-coideals on the Cartesian product of sets ». *Zb. Rad. Prirod.-Mat. Fak. Ser. Mat.* 22, p. 111-118.

1993

Dalen, D. van. « Brouwer en het intuïtionisme in de wiskunde ». *Diligentia jaarboek*. Nieuwe reeks 71. Koninklijke maatschappij voor natuurkunde, p. 15-21.

Delzell, C. N., L. González-Vega et H. Lombardi. « A continuous and rational solution to Hilbert's 17th problem and several cases of the Positivstellensatz ». *Computational algebraic geometry*. Progr. Math. 109. Birkhäuser, p. 61-75.

Feferman, S. « Working foundations—'91 ». *Bridging the gap*. Boston Stud. Philos. Sci. 140. Kluwer, p. 99-124.

González-Vega, L. et H. Lombardi. « A real Nullstellensatz and Positivstellensatz for the semipolynomials over an ordered field ». *J. Pure Appl. Algebra* 90, p. 167-188.

Ishihara, H. *A note on Richman's principle*. Rapp. tech. '93-81. Mathematical Sciences Institute, Cornell University.

Merrin, S. « Constructing bases for radicals and nilradicals of Lie algebras ». *Proc. Amer. Math. Soc.* 119, p. 681-690.

Mishra, B. *Algorithmic algebra*. Texts and Monographs in Computer Science. Springer.

1994

Aczel, P. *Notes towards a formalisation of constructive Galois theory*. Rapp. tech. Departments of Mathematics and Computer Science, Manchester University.

Bach, E. « Tensor products and computability ». *J. Symbolic Comput.* 18, p. 585-593.
Jackson, P. B. « Exploring abstract algebra in constructive type theory ». *Automated deduction—CADE-12*. Lecture Notes in Comput. Sci. 814. Springer, p. 590-604.
Lombardi, H. *Mathématiques constructives*. Rassemble « Hier et demain », « À propos du théorème des accroissements finis », « De la difficulté d'être omniscient », « Notes sur le formalisme en mathématiques », « Quelques principes de travail ». IREM de Besançon.
Merrin, S. « A strong constructive version of Engel's theorem ». *Comm. Algebra* 22, p. 1115-1125.

1995

Cigler, J. *Körper – Ringe – Gleichungen*. Spektrum.
Jackson, P. B. « Can we resolve the tension between constructive type theorists and classical mathematicians ? » Notes d'un exposé au 2^{nd} *QED workshop*.
— « Enhancing the Nuprl proof development system and applying it to computational abstract algebra ». Thèse de doct. Cornell University.
Romano, D. A. « A theorem on residual ideal of a commutative ring with apartness ». *Zb. Rad. Prirod.-Mat. Fak. Ser. Mat.* 25, p. 99-100.
— « Decomposition of coequality relation on the Cartesian product of sets with apartnesses ». *Filomat* 9, p. 915-924.
— « Some theorems about primary coideals ». *Filomat* 9, p. 73-75.

1996

Arvind, V. « A note on the self-witnessing property of computational problems ». *Computing and combinatorics*. Lecture Notes in Comput. Sci. 1090. Springer, p. 241-249.
Gianni, P. et B. Trager. « Square-free algorithms in positive characteristic ». *Appl. Algebra Engrg. Comm. Comput.* 7, p. 1-14.
Lombardi, H. « Le contenu constructif d'un principe local-global avec une application à la structure d'un module projectif de type fini ». *Publ. Math. Fac. Sci. Besançon. Théorie des nombres* 1996. Article n° 6.
Romano, D. A. « Coequality relations : a survey ». *Bull. Soc. Math. Banja Luka* 3, p. 1-35.
Veldman, W. et F. Waaldijk. « Some elementary results in intuitionistic model theory ». *J. Symbolic Logic* 61, p. 745-767.

1997

Arvind, V. « Constructivizing membership proofs in complexity classes. » *Int. J. Found. Comput. Sci.* 8, p. 433-442.
Bridges, D. S. et L. S. Dediu. « Paradise lost, or paradise regained ? » *Bull. Eur. Assoc. Theor. Comput. Sci. EATCS*, p. 141-155.
Bridges, D. S., F. Richman et P. Schuster. *Linear independence and choice*. Rapp. tech. CDMTCS-037. Centre for Discrete Mathematics and Theoretical Computer Science, University of Auckland.

González-Vega, L. et H. Lombardi. « Smooth parametrizations for several cases of the Positivstellensatz ». *Math. Z.* 225, p. 427-451.

Ishihara, H. « 構成的数学とその周辺-解析学を中心として- ». *Expositions of current mathematics* 1997, p. 18-33.

Milošević, R. R., D. A. Romano et M. Vinčić. « A basic separation on a set with apartness ». *Univ. Beograd. Publ. Elektrotehn. Fak. Ser. Mat.* 8, p. 36-43.

Palmgren, E. « Constructive mathematics ». Note.

Richman, F. « Flat dimension, constructivity, and the Hilbert syzygy theorem ». *New Zealand J. Math.* 26, p. 263-273.

1998

Bridges, D. S. et H. Ishihara. « A definitive constructive open mapping theorem ? » *MLQ Math. Log. Q.* 44, p. 545-552.

Constable, R. L. et P. B. Jackson. « Towards integrated systems for symbolic algebra and formal constructive mathematics ». Note.

Coquand, T. et H. Persson. « Integrated development of algebra in type theory ». Présenté au *Calculemus and Types '98 workshop*.

Drago, A. « Apartness and group theory in constructive algebra ». *Logical colloquium '98*.

Feferman, S. *In the light of logic*. Logic and Computation in Philosophy. Oxford University Press.

Kalantari, I. « A bibliography of recursive algebra and recursive model theory ». *Handbook of recursive mathematics, 1*. Stud. Logic Found. Math. 138. North-Holland, p. 515-581.

Kalkbrener, M. « Algorithmic properties of polynomial rings ». *J. Symbolic Comput.* 26, p. 525-581.

Lombardi, H. « Relecture constructive de la théorie d'Artin-Schreier ». *Ann. Pure Appl. Logic* 91, p. 59-92.

— *Un nouvel algorithme de calcul d'une base de Gröbner*. Rapp. tech. Laboratoire de mathématiques de Besançon, Université de Franche-Comté. Version broken english : « A new algorithm for computing Gröbner bases ».

Lombardi, H. et H. Perdry. « The Buchberger algorithm as a tool for ideal theory of polynomial rings in constructive mathematics ». *Gröbner bases and applications*. London Math. Soc. Lecture Note Ser. 251. Cambridge Univ. Press, p. 393-407.

Richman, F. « The regular element property ». *Proc. Amer. Math. Soc.* 126, p. 2123-2129.

1999

Bridges, D. S. « Can constructive mathematics be applied in physics ? » *J. Philos. Logic* 28, p. 439-453.

Bridges, D. S. et S. Reeves. « Constructive mathematics in theory and programming practice ». *Philos. Math. (3)* 7, p. 65-104.

Coquand, T. et H. Persson. « Gröbner bases in type theory ». *Types for proofs and programs*. Lecture Notes in Comput. Sci. 1657. Springer, p. 33-46.

DeMarco, M. « Intuitionistic semantics for hereditarily Harrop logic programming ». Thèse de doct. Wesleyan University.

Fortuna, E. et P. Gianni. « Square-free decomposition in finite characteristic : an application to Jordan form computation ». *SIGSAM Bull.* 33, p. 14-32.

Persson, H. « Certified computer algebra ». *Types summer school '99 : Theory and practice of formal proofs*. INRIA.

Richman, F. « Existence proofs ». *Amer. Math. Monthly* 106, p. 303-308.

Ruys, M. P. J. « Studies in mechanical verification of mathematical proofs ». Thèse de doct. Katholieke Universiteit Nijmegen.

Schuster, P. « A very weak Nullstellensatz over Heyting fields ». *Indag. Math. (N.S.)* 10, p. 117-122.

Simpson, S. G. *Subsystems of second order arithmetic*. Perspectives in Mathematical Logic. Springer.

2000

Beall, J. C. et G. Restall. « Logical pluralism ». *Australasian Journal of Philosophy* 78, p. 475-493.

Bridges, D. S., F. Richman et P. Schuster. « A weak countable choice principle ». *Proc. Amer. Math. Soc.* 128, p. 2749-2752.

— « Linear independence without choice ». *Ann. Pure Appl. Logic* 101, p. 95-102.

Feferman, S. « Relationships between constructive, predicative and classical systems of analysis ». *Proof theory*. Synthese Lib. 292. Kluwer, p. 221-236.

Geuvers, H., R. Pollack, F. Wiedijk et J. Zwanenburg. « Skeleton for the proof development leading to the fundamental theorem of algebra ». Note.

Restall, G. « Constructive logic for all : formal issues ». Australasian Association for Logic 2000 Annual Conference.

Richman, F. « The fundamental theorem of algebra : a constructive development without choice ». *Pacific J. Math.* 196, p. 213-230.

Romano, D. A. « A maximal right zero band compatible coequality relation on semigroup with apartness ». *Novi Sad J. Math.* 30, p. 131-139.

Schuster, P. « A constructive look at generalised Cauchy reals ». *MLQ Math. Log. Q.* 46, p. 125-134.

2001

Bridges, D. S. « Prime and maximal ideals in constructive ring theory ». *Comm. Algebra* 29, p. 2787-2803.

Carlström, J. *Wheels – on division by zero*. Rapp. tech. Stockholms universitet.

Coquand, T. et H. Lombardi. *Constructions cachées en algèbre abstraite : dimension de Krull, going up, going down*. Rapp. tech. Laboratoire de Mathématiques de Besançon, Université de Franche-Comté. Version anglaise : *Hidden constructions in abstract algebra, Krull dimension, going up, going down*, arXiv:1712.04725.

Coste, M., H. Lombardi et M.-F. Roy. « Dynamical method in algebra : effective Nullstellensätze ». *Ann. Pure Appl. Logic* 111, p. 203-256.

Fortuna, E., P. Gianni et B. Trager. « Computation of the radical of polynomial ideals over fields of arbitrary characteristic ». *Proceedings of the 2001 international*

symposium on symbolic and algebraic computation. Association for Computing Machinery, p. 116-120.

Labhalla, S., H. Lombardi et E. M. Moutai. « Espaces métriques rationnellement présentés et complexité : le cas de l'espace des fonctions réelles uniformément continues sur un intervalle compact ». *Theoret. Comput. Sci.* 250, p. 265-332.

Lombardi, H. « Constructions cachées en algèbre abstraite. IV. La solution du 17ème problème de Hilbert par la théorie d'Artin-Schreier ». *Publ. Math. UFR Sci. Tech. Besançon. Théorie des nombres* 2001. Article n° 3.

— « Platitude, localisation et anneaux de Prüfer : une approche constructive ». *Publ. Math. UFR Sci. Tech. Besançon. Théorie des nombres* 2001. Article n° 2.

Lombardi, H. et C. Quitté. *Théorie constructive élémentaire des modules projectifs de type fini*. Rapp. tech. Laboratoire de mathématiques de Besançon, Université de Franche-Comté.

Richman, F. « Constructive mathematics without choice ». *Reuniting the antipodes—constructive and nonstandard views of the continuum*. Synthese Lib. 306. Kluwer, p. 199-205.

Rosemeier, F. « A constructive approach to Conway's theory of games ». *Seminarberichte aus dem Fachbereich Mathematik der FernUniversität Hagen* 70.

Salthe, S. N. « Theoretical biology as an anticipatory text : The relevance of Uexküll to current issues in evolutionary systems ». *Semiotica* 134, p. 359-380.

Schuster, P. M. « Too simple solutions of hard problems ». *Nord. J. Philos. Log.* 6, p. 138-146.

2002

Fortuna, E., P. Gianni et B. Trager. « Derivations and radicals of polynomial ideals over fields of arbitrary characteristic ». *J. Symbolic Comput.* 33, p. 609-625.

Greuel, G.-M. et G. Pfister. *A **Singular** introduction to commutative algebra*. Springer.

Lombardi, H. « About Merckel's lemma ». *Valuation theory and its applications, I*. Fields Inst. Commun. 32. Amer. Math. Soc., p. 247-251.

— « Dimension de Krull, Nullstellensätze et évaluation dynamique ». *Math. Z.* 242, p. 23-46.

Romano, D. A. « Some relations and subsets generated by principal consistent subset of semigroup with apartness ». *Univ. Beograd. Publ. Elektrotehn. Fak. Ser. Mat.* 13, p. 7-25.

Rosemeier, F. « Semiquadratische Algebren ». Thèse de doct. FernUniversität Gesamthochschule in Hagen.

Schuster, P. « Real numbers as black boxes ». *New Zealand J. Math.* 31, p. 189-202.

2003

Coquand, T., L. Ducos, H. Lombardi et C. Quitté. « L'idéal des coefficients du produit de deux polynômes ». *Revue des Mathématiques de l'Enseignement Supérieur* 113, p. 25-39.

Coquand, T. et H. Lombardi. « Hidden constructions in abstract algebra [III] : Krull dimension of distributive lattices and commutative rings ». *Commutative*

ring theory and applications. Lecture Notes in Pure and Appl. Math. 231. Dekker, p. 477-499.

Galligo, A., L. González-Vega et H. Lombardi. « Continuity properties for flat families of polynomials. I. Continuous parametrizations ». *J. Pure Appl. Algebra* 184, p. 77-103.

Grabmeier, J., E. Kaltofen et V. Weispfenning. *Computer algebra handbook : foundations, applications, systems*. Springer.

Lombardi, H. « Le programme de Hilbert et les mathématiques constructives ». *Repères-IREM* 50, p. 85-104.

Lombardi, H. et C. Quitté. « Constructions cachées en algèbre abstraite [II] : le principe local-global ». *Commutative ring theory and applications*. Lecture Notes in Pure and Appl. Math. 231. Dekker, p. 461-476.

Richman, F. « The ascending tree condition : constructive algebra without countable choice ». *Comm. Algebra* 31, p. 1993-2002.

Spitters, B. « Constructive and intuitionistic integration theory and functional analysis ». Thèse de doct. Katholieke Universiteit Nijmegen.

2004

Abdeljaoued, J. et H. Lombardi. *Méthodes matricielles : introduction à la complexité algébrique*. Mathématiques & Applications 42. Springer.

Bridges, D. S. « First steps in constructive game theory ». *MLQ Math. Log. Q.* 50, p. 501-506.

Ducos, L., H. Lombardi, C. Quitté et M. Salou. « Théorie algorithmique des anneaux arithmétiques, des anneaux de Prüfer et des anneaux de Dedekind ». *J. Algebra* 281, p. 604-650.

Palmgren, E. « Constructive logic and type theory ». Notes de cours.

Perdry, H. « Strongly Noetherian rings and constructive ideal theory ». *J. Symbolic Comput.* 37, p. 511-535.

Romano, D. A. « A review of some coequality relations on semigroups with apartness ». *Bull. Soc. Math. Banja Luka* 11, p. 17-24.

Yengui, I. « Computing a Gröbner basis of a polynomial ideal over a principal domain ». Prépubl.

2005

Berger, J. et H. Ishihara. « Brouwer's fan theorem and unique existence in constructive analysis ». *MLQ Math. Log. Q.* 51, p. 360-364.

Carlström, J. « Interpreting descriptions in intensional type theory ». *J. Symbolic Logic* 70, p. 488-514.

Clark, J. « Constructive analysis of iterated rational functions ». *J.UCS* 11, p. 1904-1931.

Coquand, T., H. Lombardi et P. Schuster. « A nilregular element property ». *Arch. Math. (Basel)* 85, p. 49-54.

Crosilla, L. et P. Schuster. « Introduction ». *From sets and types to topology and analysis*. Oxford Logic Guides 48. Oxford Univ. Press, p. 1-20.

Havea, R. S. « On firmness of the state space and positive elements of a Banach algebra ». *J.UCS* 11, p. 1963-1969.
Ishihara, H. « Constructive reverse mathematics : compactness properties ». *From sets and types to topology and analysis*. Oxford Logic Guides 48. Oxford Univ. Press, p. 245-267.
Palmgren, E. « Constructive completions of ordered sets, groups, and fields ». *Ann. Pure Appl. Logic* 135, p. 243-262.
Perdry, H. « Henselian valued fields : a constructive point of view ». *MLQ Math. Log. Q.* 51, p. 400-416.
Richman, F. « A division algorithm ». *J. Algebra Appl.* 4, p. 441-449.
Romano, D. A. « A note of a family of quasi-antiorders on semigroup ». *Kragujevac J. Math.* 27, p. 11-18.
Taschner, R. *The continuum : a constructive approach to basic concepts of real analysis*. Vieweg.

2006

Beall, J. C. et G. Restall. *Logical pluralism*. The Clarendon Press.
Bridges, D. S., R. Havea et P. Schuster. « Ideals in constructive Banach algebra theory ». *J. Complexity* 22, p. 729-737.
Bridges, D. S. et L. S. Vîţă. *Techniques of constructive analysis*. Universitext. Springer.
Coquand, T. « On seminormality ». *J. Algebra* 305, p. 577-584.
Coquand, T. et H. Lombardi. « A logical approach to abstract algebra ». *Math. Structures Comput. Sci.* 16, p. 885-900.
Díaz-Toca, G. M. « Dynamic construction of the splitting field of a polynomial ». Mathematics, algorithms, proofs (MAP) 2006.
Díaz-Toca, G. M., L. González-Vega, H. Lombardi et C. Quitté. « Modules projectifs de type fini, applications linéaires croisées et inverses généralisés ». *J. Algebra* 303, p. 450-475.
Díaz-Toca, G. M., H. Lombardi et C. Quitté. « L'algèbre de décomposition universelle ». *Transgressive computing 2006. A conference in honor of Jean Della Dora*. Universidad de Granada, p. 169-184.
Ishihara, H. « Reverse mathematics in Bishop's constructive mathematics ». *Philos. Sci. (Paris)* cahier spécial 6, p. 43-59.
Ishihara, H. et E. Palmgren. « Quotient topologies in constructive set theory and type theory ». *Ann. Pure Appl. Logic* 141, p. 257-265.
Lombardi, H. « Constructions cachées en algèbre abstraite. V. Principe local-global de Pfister et variantes ». *Focus on commutative rings research*. Nova Sci., p. 157-175.
— « Structures algébriques dynamiques, espaces topologiques sans points et programme de Hilbert ». *Ann. Pure Appl. Logic* 137, p. 256-290.
Richman, F. « Van der Waerden's construction of a splitting field ». *Comm. Algebra* 34, p. 2351-2356.
Schuster, P. « Formal Zariski topology : positivity and points ». *Ann. Pure Appl. Logic* 137, p. 317-359.

Schuster, P. et J. Zappe. « Do Noetherian modules have Noetherian basis functions ? » *Logical approaches to computational barriers. Second conference on computability in Europe, CiE 2006*. Springer, p. 481-489.

Yengui, I. « A dynamical solution of Kronecker's problem ». *Mathematics, algorithms, proofs*. Dagstuhl Seminar Proceedings 05021. Internationales Begegnungs- und Forschungszentrum für Informatik (IBFI) Schloss Dagstuhl.

— « Dynamical Gröbner bases ». *J. Algebra* 301, p. 447-458.

2007

Coquand, T. et A. Spiwack. « Towards constructive homological algebra in type theory. » *Towards mechanized mathematical assistants. 14th symposium, Calculemus 2007, 6th international conference, MKM 2007*. Springer, p. 40-54.

Crvenković, S. et D. A. Romano. « A theorem on anti-ordered factor-semigroups ». *Publ. Inst. Math. (Beograd) (N.S.)* 82(96), p. 119-128.

Ishihara, H. « 構成的数学とその動向 ». *Kagaku tetsugaku* 40, p. 1-12.

Lombardi, H. *Questions about algebraic properties of real numbers*. Rapp. tech. Laboratoire de mathématiques de Besançon, Université de Franche-Comté.

Mandelkern, M. « Constructive coordinatization of Desarguesian planes ». *Beiträge Algebra Geom.* 48, p. 547-589.

Romano, D. A. « A construction of lower-potent quasi-antiorders in semigroup with apartness ». *Int. Math. Forum* 2, p. 3293-3301.

— « A note on the quasi-antiorder in a semigroup ». *Novi Sad J. Math.* 37, p. 3-8.

— « On regular anti-congruence in anti-ordered semigroups ». *Publ. Inst. Math. (Beograd) (N.S.)* 81(95), p. 95-102.

— « The second isomorphism theorem on ordered set under antiorders ». *Kragujevac J. Math.* 30, p. 235-242.

2008

Alonso, M. E., H. Lombardi et H. Perdry. « Elementary constructive theory of Henselian local rings ». *MLQ Math. Log. Q.* 54, p. 253-271.

Barhoumi, S. et H. Lombardi. « An algorithm for the Traverso-Swan theorem on seminormal rings ». *J. Algebra* 320, p. 1531-1542.

Bogdanić, D., D. A. Romano et M. Vinčić. « A connection between quasi-antiorders and pairs of coequalities ». *Bull. Soc. Math. Banja Luka* 15, p. 9-14.

Bridges, D. S. et R. S. Havea. « Constructive notions of maximality for ideals ». *J.UCS* 14, p. 3648-3657.

Coquand, T. *Constructive logic in algebra*. Rapp. tech. Summer school and conference *Mathematics, algorithms and proofs*. The Abdus Salam international centre for theoretical physics.

Crvenković, S., D. A. Romano et M. Vinčić. « A note on band anticongruence of ordered semigroups ». *Int. J. Algebra* 2, p. 1-11.

Ellouz, A., H. Lombardi et I. Yengui. « A constructive comparison of the rings $R(X)$ and $R\langle X\rangle$ and application to the Lequain-Simis induction theorem ». *J. Algebra* 320, p. 521-533.

Jojić, D. et D. A. Romano. « Quasi-antiorder relational system ». *Int. J. Contemp. Math. Sci.* 3, p. 1307-1315.

Lecerf, G. « Fast separable factorization and applications ». *Appl. Algebra Engrg. Comm. Comput.* 19, p. 135-160.

Lombardi, H. *Budan-Fourier count and constructive real algebra.* Summer school and conference *Mathematics, algorithms and proofs.*

Lombardi, H. et C. Quitté. « Comparison of Picard groups in dimension 1 ». *MLQ Math. Log. Q.* 54, p. 247-252. Version anglaise de « Comparaison de groupes de Picard en dimension 1 ».

— « Seminormal rings (following Thierry Coquand) ». *Theoret. Comput. Sci.* 392, p. 113-127. Version anglaise de « Anneaux seminormaux (d'après Thierry Coquand) ».

Lombardi, H., C. Quitté et I. Yengui. « Hidden constructions in abstract algebra. VI. The theorem of Maroscia and Brewer & Costa ». *J. Pure Appl. Algebra* 212, p. 1575-1582.

Perdry, H. « Lazy bases : a minimalist constructive theory of Noetherian rings ». *MLQ Math. Log. Q.* 54, p. 70-82.

Romano, D. A. « A construction of the maximal matrix anticongruence ». *Int. J. Algebra* 2, p. 621-631.

— « A remark on coequality relation in anti-ordered set ». *Int. J. Contemp. Math. Sci.* 3, p. 43-48.

— « A remark on mappings between quasi-antiordered sets ». *Proceedings of the 12th Serbian Mathematical Congress.* Univerzitet u Novom Sadu.

— « A theorem on band anticongruence on ordered semigroup ». *Int. J. Algebra* 2, p. 339-347.

— « An isomorphism theorem for anti-ordered sets ». *Filomat* 22, p. 145-160.

— « Consistent positive and linear positive quasi-antiorders ». *Int. Math. Forum* 3, p. 883-891.

— « Isomorphism theorems for QA-mappings ». *Int. J. Contemp. Math. Sci.* 3, p. 695-701.

— « Quotient of a consistent subset by an element—constructive point of view ». *Int. Math. Forum* 3, p. 1547-1561.

Sacerdoti Coen, C. et S. Zacchiroli. « Spurious disambiguation errors and how to get rid of them ». *Math. Comput. Sci.* 2, p. 355-378.

Schuster, P. « The Zariski spectrum as a formal geometry ». *Theoret. Comput. Sci.* 405, p. 101-115.

Schuster, P. et J. Zappe. « Über das Kripke-Schema und abzählbare Teilmengen ». *Logique et Anal. (N.S.)* 51, p. 317-329.

Yengui, I. « Making the use of maximal ideals constructive ». *Theoret. Comput. Sci.* 392, p. 174-178.

— *Projective modules over polynomial rings and dynamical Gröbner bases.* Rapp. tech. Summer school and conference *Mathematics, algorithms and proofs.* The Abdus Salam international centre for theoretical physics.

— « The Hermite ring conjecture in dimension one ». *J. Algebra* 320, p. 437-441.

2009

Akharraz, I. et M. E. Charkani. « Induced modules by an endomorphism of finitely generated modules ». *Int. J. Algebra* 3, p. 589-597.

Barhoumi, S., H. Lombardi et I. Yengui. « Projective modules over polynomial rings : a constructive approach ». *Math. Nachr.* 282, p. 792-799.

Bogdanić, D., S. Crvenković et D. A. Romano. « Another isomorphism theorem on anti-ordered semigroups ». *Int. J. Contemp. Math. Sci.* 4, p. 241-245.

Constable, R. L. « Building mathematics-based software systems to advance science and create knowledge. » *Efficient algorithms. Essays dedicated to Kurt Mehlhorn on the occasion of his 60th birthday.* Springer, p. 3-17.

Coquand, T. « Space of valuations ». *Ann. Pure Appl. Logic* 157, p. 97-109.

Coquand, T., L. Ducos, H. Lombardi et C. Quitté. « Constructive Krull dimension. I. Integral extensions ». *J. Algebra Appl.* 8, p. 129-138.

Coquand, T., H. Lombardi et P. Schuster. « Spectral schemes as ringed lattices ». *Ann. Math. Artif. Intell.* 56, p. 339-360.

Lombardi, H. « Algèbre commutative effective : une introduction ». Cours à l'École du CIMPA.

— « Mathématiques constructives ». *Bulletin de l'APMEP* 483, p. 449-466.

Lombardi, H. et C. Quitté. « Complément 2 : "Principe local-global". Complément 3 : "Vision des mathématiques constructives sur les modules" ». *Mathématiques L3 : algèbre.* Pearson Education. Chap. 11 : « Modules », p. 679-708.

Mitrović, M., D. A. Romano et M. Vinčić. « A theorem on semilattice-ordered semigroup ». *Int. Math. Forum* 4, p. 227-232.

Nordvall Forsberg, F. « Constructive aspects of models for non-standard analysis ». Mém. de mast. Uppsala universitet.

Romano, D. A. « A complete anti-order is the intersection of family of all anti-orders containing it ». *J. Pure Appl. Math. Adv. Appl.* 1, p. 121-128.

— « A complete quasi-antiorder is the intersection of a collection of quasi-antiorders ». *J. Math. Sci. Adv. Appl.* 2, p. 215-220.

— « A construction of anti-ordered group by an anti-ordered semigroup with apartness ». *Bull. Soc. Math. Banja Luka* 16, p. 5-9.

— « A theorem on QA-homomorphisms ». *JP J. Algebra Number Theory Appl.* 13, p. 7-15.

Sukara-Ćelić, B., D. A. Romano et V. Telebak. « A theorem on weakly regular coequality relation ». *Int. J. Contemp. Math. Sci.* 4, p. 115-120.

2010

Beeson, M. « Foreword ». Retirage de *Foundations of Constructive Analysis* par Errett Bishop. Ishi Press International.

Coquand, T., H. Lombardi et C. Quitté. « Curves and coherent Prüfer rings ». *J. Symbolic Comput.* 45, p. 1378-1390.

Crvenković, S., M. Mitrović et D. A. Romano. « Complementary pair of quasi-antiorders ». *Rep. Math. Logic*, p. 135-142.

Hadj Kacem, A. et I. Yengui. « Dynamical Gröbner bases over Dedekind rings ». *J. Algebra* 324, p. 12-24.

Ishihara, H. et P. Schuster. « Kronecker's density theorem and irrational numbers in constructive reverse mathematics ». *Math. Semesterber.* 57, p. 57-72.
Lombardi, H. « Un anneau de Prüfer ». *Actes Rencontres C.I.R.M.* 2, p. 59-69.
Mannaa, B. « Dynamic construction of algebraic closure and a coinductive proof of Hensel's lemma ». Mém. de mast. Chalmers tekniska högskola.
Morrison, F. et N. L. Morrison. « Variable precision floating-point computations ». Note.
Mörtberg, A. « Constructive algebra in functional programming and type theory ». Mém. de mast. Chalmers tekniska högskola et Göteborgs universitet.
Palmgren, E. *Remarks on the relation between families of setoids and identity in type theory.* Rapp. tech. 36. Institut Mittag-Leffler.
Romano, D. A. « Extensions of rectangular band anti-congruence in semigroup with apartness ». *Int. J. Algebra* 4, p. 809-818.
— « Some characterizations of filed product of quasi-antiorders ». *Acta Univ. Apulensis Math. Inform.*, p. 133-138.
— « The lattice of regular coequalities ». *Miskolc Math. Notes* 11, p. 175-181.
Romano, D. A. et M. Vinčić. « On commuting property of filed product of coequality relations ». *J. Math. Sci. Adv. Appl.* 6, p. 113-124.
Wilander, O. « Setoids and universes ». *Math. Structures Comput. Sci.* 20, p. 563-576.

2011

Bridges, D. S. « Characterising weak-operator continuous linear functionals on $\mathcal{B}(H)$ constructively ». *Doc. Math.* 16, p. 597-617.
Droste, M. et R. Göbel. « Countable random p-groups with prescribed Ulm-invariants ». *Proc. Amer. Math. Soc.* 139, p. 3203-3216.
Finau, T. « An investigation of ideals in constructive Banach algebra theory ». Mém. de mast. University of the South Pacific.
Lombardi, H. et C. Quitté. *Algèbre commutative : méthodes constructives. Modules projectifs de type fini.* Calvage et Mounet.
Neukirchen, C. « The concept of set in constructive analysis ». Mém. de lic. Ludwig-Maximilians-Universität München.
O'Connor, R. « Classical mathematics for a constructive world ». *Math. Structures Comput. Sci.* 21, p. 861-882.
Perdry, H. et P. Schuster. « Noetherian orders ». *Math. Structures Comput. Sci.* 21, p. 111-124.
Romano, D. A. « A review of isomorphism theorems of anti-ordered semigroups with apartness ». *Research J. Pure Alg.* 1, p. 52-57.
— « An anti-order relation in factor-semigroup induced by a consistent subset ». Споменица академика Веселина Перића. Споменица 8. ANURS.
— « Dedekind partial groupoids for anti-ordered sets ». *Bull. Int. Math. Virtual Inst.* 1, p. 21-26.
— « Extensions of ordered sets – constructive point of view ». *International Journal of Mathematical Archive* 2, p. 969-981.
— « On a particular condition for regular coequality relations. » *Gen. Math. Notes* 2, p. 32-39.

Romano, D. A. « On retract extension of ordered set—a constructive point of view ». *International Journal of Mathematical Archive* 2, p. 944-948.
— « On semilattice-ordered semigroups : a constructive point of view ». *Sci. Stud. Res. Ser. Math. Inform.* 21, p. 117-134.
Yengui, I. « Stably free modules over $\mathbf{R}[X]$ of rank $>$ dim $\mathbf{R}$ are free ». *Math. Comp.* 80, p. 1093-1098.

2012

Berger, J., D. S. Bridges et E. Palmgren. « Double sequences, almost Cauchyness and BD-N ». *Log. J. IGPL* 20, p. 349-354.
Berger, J., H. Ishihara et P. Schuster. « The weak Kőnig lemma, Brouwer's fan theorem, de Morgan's law, and dependent choice ». *Rep. Math. Logic*, p. 63-86.
Cohen, C. « Construction of real algebraic numbers in Coq ». *Interactive theorem proving*. Lecture Notes in Comput. Sci. 7406. Springer, p. 67-82. Version française : « Construction des nombres algébriques réels en Coq », *JFLA – Journées francophones des langages applicatifs 2012*.
— « Formalisation des nombres algébriques : construction et théorie du premier ordre ». Thèse de doct. École polytechnique.
Coquand, T., A. Mörtberg et V. Siles. « Coherent and strongly discrete rings in type theory. » *Certified programs and proofs. Second international conference, CPP 2012*. Springer, p. 273-288.
Coquand, T. et C. Quitté. « Constructive finite free resolutions ». *Manuscripta Math.* 137, p. 331-345.
Dénès, M., A. Mörtberg et V. Siles. « A refinement-based approach to computational algebra in Coq ». *Interactive theorem proving*. Lecture Notes in Comput. Sci. 7406. Springer, p. 83-98.
Kawai, T. « On basic structures of general topology in constructive mathematics ». Mém. de mast. Japan Advanced Institute of Science et Technology.
Lambek, J. « The radical approach to infinitesimals in historical perspective ». *C. R. Math. Acad. Sci. Soc. R. Can.* 34, p. 9-22.
Lombardi, H. « Constructive semantics for classical formal proofs ». *Bull. Symb. Log.* 18, p. 423-424.
Lombardi, H., P. Schuster et I. Yengui. « The Gröbner ring conjecture in one variable ». *Math. Z.* 270, p. 1181-1185.
Lubarsky, R., F. Richman et P. Schuster. « The Kripke schema in metric topology ». *MLQ Math. Log. Q.* 58, p. 498-501.
Milovanović, M. et D. A. Romano. « A construction of quasi-antiorders on semigroups generated by coradicals of principal consistent subsets ». *Int. J. Algebra* 6, p. 517-529.
Mörtberg, A. *Constructive algebra in type theory*. Rapp. tech. 96L. Mém. de lic. Department of computer science and engineering, Chalmers tekniska högskola et Göteborgs universitet.
Palmgren, E. « Proof-relevance of families of setoids and identity in type theory ». *Arch. Math. Logic* 51, p. 35-47.
Rinaldi, D. « A formal proof of the projective Eisenbud-Evans-Storch theorem ». *Arch. Math. (Basel)* 99, p. 9-24.

Romano, D. A. « A construction of a quasi-antiorder by anti-congruence on semigroup with apartness ». *Bull. Int. Math. Virtual Inst.* 2, p. 163-166.
— « On quasi-antiorder in semigroups ». *Mat. Vesnik* 64, p. 190-199.
— « Semilattice-ordered semigroups with apartness representation problem ». *J. Adv. Math. Stud.* 5, p. 13-19.
Rubio, J. et F. Sergeraert. « Constructive homological algebra and applications ». arXiv:1208.3816.

2013

Aczel, P., B. Ahrens, T. Altenkirch, S. Awodey, B. Barras, A. Bauer, Y. Bertot, M. Bezem, T. Coquand, E. Finster, D. Grayson, H. Herbelin, A. Joyal, D. Licata, P. Lumsdaine, A. Mahboubi, P. Martin-Löf, S. Melikhov, A. Pelayo, A. Polonsky, M. Shulman, M. Sozeau, B. Spitters, B. van den Berg, V. Voevodsky, M. Warren, C. Angiuli, A. Bordg, G. Brunerie, C. Kapulkin, E. Rijke, K. Sojakova, J. Avigad, C. Cohen, R. Constable, P.-L. Curien, P. Dybjer, M. H. Escardó, K.-B. Hou, N. Gambino, R. Garner, G. Gonthier, T. Hales, R. Harper, M. Hofmann, P. Hofstra, J. Koch, N. Kraus, N. Li, Z. Luo, M. Nahas, E. Palmgren, E. Riehl, D. Scott, P. Scott et S. Soloviev. *Homotopy type theory—univalent foundations of mathematics*. The Univalent Foundations Program.
Aczel, P., B. van den Berg, J. Granström et P. Schuster. « Are there enough injective sets ? » *Studia Logica* 101, p. 467-482.
Barendregt, H. « Foundations of mathematics from the perspective of computer verification ». *Mathematics, computer science and logic—a never ending story*. Springer, p. 1-49.
Bura, V. B. « Reverse mathematics of divisibility in integral domains ». Mém. de mast. Victoria University of Wellington.
Cohen, C. et T. Coquand. « A constructive version of Laplace's proof on the existence of complex roots ». *J. Algebra* 381, p. 110-115.
Coquand, T. et H. Lombardi. « Álgebra constructiva ». *La Gaceta de la RSME* 16, p. 293-312. Version espagnole du plaidoyer *L'algèbre constructive*.
Crvenković, S., M. Mitrović et D. A. Romano. « Semigroups with apartness ». *MLQ Math. Log. Q.* 59, p. 407-414.
Gonthier, G., A. Asperti, J. Avigad, Y. Bertot, C. Cohen, F. Garillot, S. L. Roux, A. Mahboubi, R. O'Connor, S. O. Biha, I. Pasca, L. Rideau, A. Solovyev, E. Tassi et L. Théry. « A machine-checked proof of the odd order theorem ». *Interactive theorem proving*. Lecture Notes in Comput. Sci. 7998. Springer, p. 163-179.
Hendtlass, M. « Constructing fixed points and economic equilibria ». Thèse de doct. University of Leeds.
Kaltofen, E. et G. Lecerf. « Factorization of multivariate polynomials ». *Handbook of finite fields*. Discrete Mathematics and its Applications (Boca Raton). CRC Press.
Kraus, N., M. H. Escardó, T. Coquand et T. Altenkirch. « Generalizations of Hedberg's theorem ». *Typed lambda calculi and applications*. Lecture Notes in Comput. Sci. 7941. Springer, p. 173-188.

Lecerf, G. « Factorisation des polynômes à plusieurs variables ». *Les cours du CIRM* 3.

Lombardi, H. « Les nombres réels calculables selon Alan Turing (un exemple de définition constructive) ». *Quadrature* 90, p. 18-23.

— « Three lectures on constructive algebra ». *Constructive mathematics : foundations and practice*.

Mannaa, B. et T. Coquand. « Dynamic Newton-Puiseux theorem ». *J. Log. Anal.* 5. Article n° 5.

Palmgren, E. « Bishop-style constructive mathematics in type theory—a tutorial ». *Constructive mathematics : foundations and practice*.

Richman, F. « A constructive theory of minimal zero-dimensional extensions ». *J. Commut. Algebra* 5, p. 545-566.

Rinaldi, D. « A constructive notion of codimension ». *J. Algebra* 383, p. 178-196.

Schuster, P. « Induction in algebra : a first case study ». *Log. Methods Comput. Sci.* 9.

Vinčić, M. et D. A. Romano. « A note on coradical of consistent subset of σ-reflexive semigroups with apartness ». *Bull. Int. Math. Virtual Inst.* 3, p. 123-126.

2014

Alonso, M. E., T. Coquand et H. Lombardi. « Revisiting Zariski main theorem from a constructive point of view ». *J. Algebra* 406, p. 46-68.

Cohen, C. et A. Mörtberg. « A Coq formalization of finitely presented modules ». *Interactive theorem proving. 5th international conference, ITP 2014*. Springer, p. 193-208.

Coquand, T. « Recursive functions and constructive mathematics ». *Constructivity and computability in historical and philosophical perspective*. Log. Epistemol. Unity Sci. 34. Springer, p. 159-167.

Crosilla, L. et P. Schuster. « Finite methods in mathematical practice ». *Formalism and beyond*. Logos 23. De Gruyter, p. 351-410.

Díaz-Toca, G. M., H. Lombardi et C. Quitté. *Modules sur les anneaux commutatifs*. Calvage et Mounet.

Ilik, D. « Axioms and decidability for type isomorphism in the presence of sums ». *Proceedings of the joint meeting of the twenty-third EACSL annual conference on computer science logic (CSL) and the twenty-ninth annual ACM/IEEE symposium on logic in computer science (LICS)*. Article n° 53. Association for Computing Machinery.

Lombardi, H. « Algèbre constructive ». *Les cours du CIRM* 4.

Lombardi, H., C. Quitté et I. Yengui. « Un algorithme pour le calcul des syzygies sur $\mathbf{V}[X]$ dans le cas où $\mathbf{V}$ est un domaine de valuation ». *Comm. Algebra* 42, p. 3768-3781.

Mannaa, B. « Constructive Newton-Puiseux Theorem : sheaf model of the separable closure and dynamic evaluation ». Mém. de lic. Göteborgs universitet.

Mannaa, B. et T. Coquand. « A sheaf model of the algebraic closure ». *Proceedings fifth international workshop on classical logic and computation*. Electron. Proc. Theor. Comput. Sci. 164. EPTCS, p. 18-32.

Mörtberg, A. « Formalizing refinements and constructive algebra in type theory ». Thèse de doct. Göteborgs universitet.

Palmgren, E. « Lecture notes on type theory ». Notes de cours.

Perdry, H. et P. Schuster. « Constructing Gröbner bases for Noetherian rings ». *Math. Structures Comput. Sci.* 24. e240206.

Richman, F. « A theorem of Gilmer and the canonical universal splitting ring ». *J. Commut. Algebra* 6, p. 101-108.

Rinaldi, D. « Formal methods in the theories of rings and domains ». Thèse de doct. Ludwig-Maximilians-Universität München.

Rodriguez Caballero, J. M. « L'approximation diophantienne simultanée et l'optimisation discrète ». Mém. de mast. Université de Montréal.

Tête, C. « Profondeur, dimension et résolutions en algèbre commutative : quelques aspects effectifs ». Thèse de doct. Université de Poitiers.

2015

Aczel, P., H. Ishihara, T. Nemoto et Y. Sangu. « Generalized geometric theories and set-generated classes ». *Math. Structures Comput. Sci.* 25, p. 1466-1483.

Barras, B., T. Coquand et S. Huber. « A generalization of the Takeuti-Gandy interpretation ». *Math. Structures Comput. Sci.* 25, p. 1071-1099.

Ducos, L., A. Valibouze et I. Yengui. « Computing syzygies over $\mathbf{V}[X_1, \ldots, X_k]$, $\mathbf{V}$ a valuation domain ». *J. Algebra* 425, p. 133-145.

Gálvez Verdugo, W. E. « Algoritmos en línea para problemas de balanceamiento robusto ». Mém. de mast. Universidad de Chile.

Lombardi, H. et C. Quitté. *Commutative algebra : constructive methods : finite projective modules*. Traduction augmentée de l'ouvrage paru en 2011. Algebra and Applications 20. Springer.

Madore, D. A. et F. Orgogozo. « Calculabilité de la cohomologie étale modulo ℓ ». *Algebra Number Theory* 9, p. 1647-1739.

Mitrović, M., S. Crvenković et D. A. Romano. « Semigroups with apartness : constructive versions of some classical theorems ». *46th annual Iranian mathematics conference*, p. 64-67.

Pelayo, Á., V. Voevodsky et M. A. Warren. « A univalent formalization of the p-adic numbers ». *Math. Structures Comput. Sci.* 25, p. 1147-1171.

Rijke, E. et B. Spitters. « Sets in homotopy type theory ». *Math. Structures Comput. Sci.* 25, p. 1172-1202.

Yengui, I. *Constructive commutative algebra : projective modules over polynomial rings and dynamical Gröbner bases*. Lecture Notes in Mathematics 2138. Springer.

2016

Bridges, D., H. Diener, B. Kearfott, V. Kreinovich, P. Melin, R. Sainudiin et H. Schwichtenberg. *16w5099—Interval analysis and constructive mathematics*. Rapp. final. Banff international research station.

Cano, G., C. Cohen, M. Dénès, A. Mörtberg et V. Siles. « Formalized linear algebra over elementary divisor rings in Coq ». *Log. Methods Comput. Sci.* 12. Article n° 7.

Coquand, T. et H. Lombardi. « Anneaux à diviseurs et anneaux de Krull (une approche constructive) ». *Comm. Algebra* 44, p. 515-567.

— « Some remarks about normal rings ». *Concepts of proof in mathematics, philosophy, and computer science*. Ontos Math. Log. 6. De Gruyter, p. 141-149.

Crosilla, L. « Matematica costruttiva ». *APhEx (Analytical and Philosophical Explanation)* 14.

Crvenković, S., M. Mitrović et D. A. Romano. « Basic notions of (constructive) semigroups with apartness ». *Semigroup Forum* 92, p. 659-674.

Ducos, L., S. Monceur et I. Yengui. « Computing the $\mathbf{V}$-saturation of finitely-generated submodules of $\mathbf{V}[X]^m$ where $\mathbf{V}$ is a valuation domain ». *J. Symbolic Comput.* 72, p. 196-205.

Ilik, D. « Perspectives for proof unwinding by programming languages techniques ». arXiv:1605.09177.

Mannaa, B. « Sheaf semantics in constructive algebra and type theory ». Thèse de doct. Göteborgs universitet.

Osinenko, P., G. Devadze et S. Streif. « A note on constructive treatment of eigenvectors ». arXiv:1607.04108.

Romano, D. A. « A new analysis of regular coequality relation ». *Bull. Int. Math. Virtual Inst.* 6, p. 259-267.

— « A note on regular coequality relation ». « On coequality relation and its copartition on set with apartness ». « Some important classes of subsets in sets with apartness ». Prépubl.

Shitov, Y. « A matrix ring with commuting graph of maximal diameter ». *J. Combin. Theory Ser. A* 141, p. 127-135.

Wahdan, Z. A. A. H. « Codes over rings ». Mém. de mast. جَامعة بِيرزيت.

Zhang, Y. et L. Liao. « An algebraic specification language for organizational behavior of OOMAS ». *Proceedings of the 1st international workshop on specification, comprehension, testing, and debugging of concurrent programs*. Association for Computing Machinery, p. 1-6.

2017

Barhoumi, S. « Computing syzygies over $\mathbf{R}[X_1^{\pm 1}, \ldots, X_n^{\pm 1}]$, $\mathbf{R}$ a valuation ring ». *JP J. Algebra Number Theory Appl.* 39, p. 661-670.

Coquand, T., H. Lombardi et S. Neuwirth. « A constructive theory of ordinals ». En préparation.

Crvenković, S., M. Mitrović et B. M. Randjelović. « Constructive semigroups with apartness : foundations of the order theory ». *6th international conference* Logic and applications LAP 2017, p. 34-36.

Ekhlass, A. A. A. A. « On Coherent Modules ». Mém. de lic. جَامعة القَادسية.

Evseev, A. et S. Tsuchioka. « On graded Cartan invariants of symmetric groups and Hecke algebras ». *Math. Z.* 285, p. 177-213.

Kraus, N., M. H. Escardó, T. Coquand et T. Altenkirch. « Notions of anonymous existence in Martin-Löf type theory ». *Log. Methods Comput. Sci.* 13. Article n° 15.

Ouwehand, D. « Local rigid cohomology of weighted homogeneous hypersurface singularities ». Thèse de doct. Humboldt-Universität zu Berlin.

Posur, S. « A constructive approach to Freyd categories ». arXiv:1712.03492.
Rinaldi, D., P. Schuster et D. Wessel. « Eliminating disjunctions by disjunction elimination ». *Bull. Symb. Log.* 23, p. 181-200.
Romano, D. A. « A result on the lattice of all co-ideals and the lattice of all co-filters of ordered sets under co-quasiorder ». Prépubl.
— « On some mappings between co-quasiordered relational systems ». *Bull. Int. Math. Virtual Inst.* 7, p. 279-291.
— « Weakly isotone and strongly reverse isotone mappings of relational systems ». *Bull. Int. Math. Virtual Inst.* 7, p. 293-303.

2018

Bartels, T., U. Schreiber, M. Shulman et B. Spitters. *Bishop's constructive mathematics. n*Lab.
Blechschmidt, I. « Flabby and injective objects in toposes ». arXiv:1810.12708.
— « Using the internal language of toposes in algebraic geometry ». Thèse de doct. Universität Augsburg.
Bridges, D. S. et E. Palmgren. « Constructive mathematics ». *The Stanford Encyclopedia of Philosophy.* Metaphysics Research Lab.
Coquand, T. « Combinatorial topology and constructive mathematics ». *Indag. Math. (N.S.)* 29, p. 1637-1648.
Coquand, T., H. Lombardi, C. Quitté et C. Tête. « Résolutions libres finies : méthodes constructives ». arXiv:1811.01873.
Ishihara, H. « Constructive functional analysis : an introduction ». *Proof and computation : digitization in mathematics, computer science, and philosophy.* World Scientific. Chap. 4, p. 109-165.
Joseph, J. S. « Axioms for the real numbers : a constructive approach ». arXiv: 1808.00906.
— « On generalized ordered sets : a constructive development ». arXiv:1809.05230.
— « The surreal numbers as an ordered commutative ring with an apartness : a development in univalent foundations ». arXiv:1812.00051.
Lemos, A. et P. H. A. de Oliveira. « Suggested corrections for "A principal ideal domain that is not a Euclidean domain" ». *Amer. Math. Monthly* 125, p. 425.
Mitrović, M. et S. Silvestrov. « On basic constructive algebraic structures with apartness ». *7th international conference* Logic and applications LAP 2018, p. 34-36.
Petrakis, I. « Mathematical logic ». Notes de cours.
Rinaldi, D., P. Schuster et D. Wessel. « Eliminating disjunctions by disjunction elimination ». *Indag. Math. (N.S.)* 29, p. 226-259.
Romano, D. A. « Co-filters in semilattice-ordered semigroup with apartness ». *J. Adv. Math. Stud.* 11, p. 124-131.
— « Co-ideals and co-filters in ordered set under co-quasiorder ». *Bull. Int. Math. Virtual Inst.* 8, p. 177-188.
— « Semilattice ordered semi-rings with apartness ». *J. Adv. Math. Stud.* 11, p. 496-502.
— « Up-algebra with apartness ». Prépubl.
Shulman, M. « Linear logic for constructive mathematics ». arXiv:1805.07518.

Taschner, R. *Vom Kontinuum zum Integral. Eine Einführung in die intuitionistische Mathematik.* Springer.

Wessel, D. « Choice, extension, conservation : from transfinite to finite proof methods in abstract algebra ». Thèse de doct. Università degli studi di Trento et Università degli studi di Verona.

2019

Chan, Y.-K. « Foundations of constructive probability theory ». arXiv:1906.01803.

Cherubini, A. et A. Frigeri. « Inverse semigroups with apartness ». *Semigroup Forum* 98, p. 571-588.

Coquand, T., H. Lombardi et S. Neuwirth. « Lattice-ordered groups generated by an ordered group and regular systems of ideals ». *Rocky Mountain J. Math.* 49, p. 1449-1489.

Fellin, G., P. Schuster et D. Wessel. « The Jacobson radical of a propositional theory ». *5th international workshop on structures and deduction.*

Grinberg, D. « λ-rings : definitions and basic properties ». Note.

Joseph, J. S. « A problem involving polynomials over a finite ring : a solution in a quantum system ». Prépubl.

Mitrović, M., S. Silvestrov, S. Crvenković et D. A. Romano. « Constructive semigroups with apartness : towards a new algebraic theory ». *J. Phys. Conf. Ser.* 1194.

Neunhäuserer, J. *Einführung in die Philosophie der Mathematik.* Springer.

Petrakis, I. « Dependent sums and dependent products in Bishop's set theory ». *24th international conference on types for proofs and programs (TYPES 2018).* Leibniz International Proceedings in Informatics (LIPIcs) 130. Schloss Dagstuhl Leibniz-Zentrum für Informatik, 3:1-3:21.

— « Direct spectra of Bishop spaces and their limits ». arXiv:1907.03273.

Posur, S. « Closing the category of finitely presented functors under images made constructive ». arXiv:1911.11469.

— « Methods of constructive category theory ». arXiv:1908.04132.

Romano, D. A. « A remark on co-ideals in implicative semigroups with apartness ». « BCK-algebras with apartness ». « Co-filters in Γ-semigroups ordered under co-order ». « Co-filters in Γ-semigroups ordered under co-quasiorder ». « Co-ideals and quotients of co-quasiordered residuated systems ». « Ordered Γ-semirings with apartness under co-order ». « Ordered sets under co-quasiorder, a survey ». « Perception of Hilbert algebras in a non-classical principled-logical framework : Hilbert algebras with apartness ». « Semilattice co-congruence in Γ-semigroups ». Prépubl.

— « Co-quasiordered residuated systems : an introduction ». *Asian-Eur. J. Math.* 12.

— « Γ-semigroups with apartness ». *Bull. Allahabad Math. Soc.* 34, p. 71-83.

— « Γ-semirings with apartness ». *Rom. J. Math. Comput. Sci.* À paraitre.

— « On co-filters in co-quasiordered residuated systems ». *Ikonion J. Math.* 1, p. 27-33.

— « On co-ideals of implicative semigroups with apartness ». *Turk. J. Math. Comput. Sci.* 11, p. 101-106.

— « On coequality relations on set with apartness ». *Bull. Int. Math. Virtual Inst.* 9, p. 1-9.
— « Perception of BCC-algebras under the Bishop's principled-philosophical orientation : BCC-algebra with apartness ». *Filomat* 33, p. 6369-6380.
— « Some algebraic structures with apartness, a review ». *J. Int. Math. Virtual Inst.* 9, p. 361-395.
Wessel, D. « Ordering groups constructively ». *Comm. Algebra* 47, p. 4853-4873.

2020

Bonacina, R. et D. Wessel. « Ribenboim's order extension theorem from a constructive point of view ». *Algebra Universalis* 81. Article n° 5.
Díaz-Toca, G. M. et H. Lombardi. « Calcul matriciel généralisé sur les domaines de Prüfer ». *Bull. Sci. Math.* 159. Version préliminaire en anglais : « A pseudo-matrix approach to Prüfer domains », *XV encuentro de álgebra computacional y aplicaciones, EACA 2016*, Universidad de La Rioja, 2016.
Gamanda, M., H. Lombardi, S. Neuwirth et I. Yengui. « The syzygy theorem for Bézout rings ». *Math. Comp.* 89, p. 941-964.
Lombardi, H. « Spectral spaces versus distributive lattices : a dictionary ». *Proceedings of the conference on rings and factorizations*. Springer. À paraitre. Version française : « Treillis distributifs et espaces spectraux, un petit dictionnaire », arXiv:1812.06277.
Richman, F. « Laurent series over $\mathbb{R}$ ». *Comm. Algebra*. À paraitre.
Romano, D. A. « On co-filters in semigroups with apartness ». *Kragujevac J. Math.* 45, p. 607-613.
— « Quotient structures of implicative semigroup with apartness ». Prépubl.

Ce livre est la traduction française du classique *A Course in Constructive Algebra* (1988). Il présente les notions de base de l'algèbre moderne d'un point de vue constructif.

Dans l'univers mathématique constructif, le mathématicien idéal peut seulement réaliser des constructions finies par nature. Comme le dit Errett Bishop dans son *Constructive Manifesto* (1967), « la seule manière de démontrer qu'un objet existe est de donner une procédure finie pour le trouver ». En conséquence, les théorèmes d'existence dans ce livre ont tous un contenu algorithmique implicite qui permet de construire l'objet voulu lorsque les hypothèses sont satisfaites.

L'algèbre constructive peut aussi être vue comme une généralisation de l'algèbre classique en ce qu'elle ne suppose pas la loi du tiers exclu. Tout théorème dans ce livre peut donc également être compris comme se référant à l'univers conventionnel classique du discours mathématique, et les démonstrations du livre sont correctes dans cet univers. L'agréable surprise est que la démonstration constructive, normalement plus précise, est dans bien des cas plus simple.

Ouvrage publié avec le soutien du
Laboratoire de mathématiques de Besançon (UMR 6623).

Presses universitaires de Franche-Comté
http://presses-ufc.univ-fcomte.fr

UFC
UNIVERSITÉ
DE FRANCHE-COMTÉ

Prix : 20 euros
ISBN 978-2-84867-782-8