Algèbre approfondie

Joel Briançon
Département de Mathématiques
Université de Nice
Master

1990-1991

ALGEBRE APPROFONDIE 90-91

Joël Briançon

Je tiens à remercier tous les étudiants et tous les chers collègues qui tiennent si bien leur rôle dans les scènes qui suivent ; une mention spéciale pour G. Ebercwajg (j'ai utilisé les notes de son cours de 87-88 pour le chapitre V) , et pour P. Le Barz et M. Miniconi (j'ai largement repris les énoncés donnés en travaux dirigés). Le but poursuivi ... heu ... j'ai oublié ... excusez moi ...

Court résumé du cours d'

ALGEBRE APPROFONDIE 90-91

Chap. I : GENERATEURS ET RELATIONS

Pendant toute l'année, sauf mention expresse du contraire, un anneau est un anneau commutatif et unitaire.

§ I.1. Présentation de Mod.

La catégorie[1] A-Mod. {
- Objets : les A-modules
- Morphismes (= Flèches) : $\mathrm{Hom}_A(E,F)$ ensemble des applications A-linéaires de E dans F.

C'est le moment ou jamais de vérifier que les définitions et notions de bases sont bien connues ! Après, on enlève le filet.

[1] J.P LAFON : Les formalismes fondamentaux de l'algèbre commutative - Hermann 1974 pour une présentation fonctorielle et catégorique.

Conserverez vous le moindre doute sur ces objets ?

Un sous module N de M.

Un module quotient $\frac{M}{N}$

$\mathrm{Hom}_A(E,F)$

$\mathrm{Ker} f$

$\mathrm{Im} f$

$\mathrm{Coker} f$.

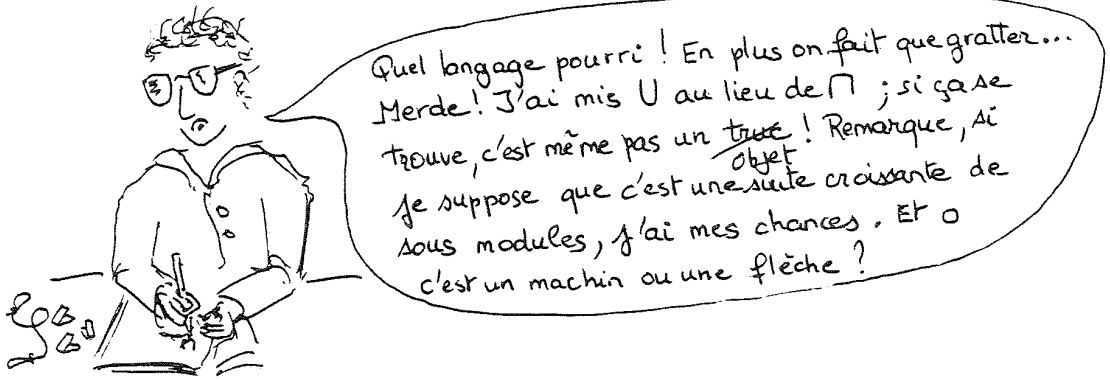
$\bigoplus_{i\in I} M_i$

A^I

$A^{(I)} = \bigoplus_{i\in I} A x_i$

$\bigcap_{i\in I} N_i$

et sur ces catégories ? K-Mod , $\mathbb{Z}$-Mod ?



(C'est vraiment pénible de commencer en haut à gauche)

Je leur dis qu'une famille c'est une application ? Zut ! J'en aurai pour 2 heures.

Définition I.1.1 : Soit M un A-module, $(e_i)_{i\in I}$ une famille d'éléments de M.
On dit que $(e_i)_{i\in I}$ est :
- un système de générateurs de M : si tout élément de M est combinaison linéaire finie d'éléments de la famille. (ou encore que l'application canonique $\Phi : A^{(I)} \longrightarrow M$ est surjective).
- un système libre de M : si la seule relation entre les éléments de la famille est la relation triviale (ou encore Φ est injective).
- une base de M : système libre et générateur (Φ isomorphisme).

Si je ne me trompe pas, une relation entre les $(e_i)_{i\in I}$, c'est $\sum_{\text{finie}} \lambda_i e_i = 0$ avec les λ_i dans A. Et elle est triviale si les λ_i sont tous nuls. "Dans une famille libre les relations sont triviales" : quel langage ! Finalement, les relations, c'est $\operatorname{Ker}\Phi$! Qu'est-ce que je suis bonne ! Je ne comprends pas ; il faut que je trouve tout moi même et c'est lui qui est payé !

Ah ! Parce que : $\Phi((\lambda_i)_{i\in I}) = \sum \lambda_i e_i$ et les λ_i sont tous nuls sauf un nombre fini. Bravo ! Il faut tout deviner ; on nous dit rien !

VIENS DANS MON MODULE NOUS AURONS DES RELATIONS NON TRIVIALES !!

Définition I.1.2 : On dit qu'un A-module M est :
- libre : s'il admet une base.
- de type fini : s'il admet un système fini de générateurs.

Que pouvez vous dire de ces A-modules ?

$M = \mathcal{A}$ idéal de A ; $M = A/\mathcal{A}$; $A = k[x,y]$, $M = Ax + Ay$, $\frac{A}{M}$;

$\mathbb{Q}$ objet de $\mathbb{Z}$-Mod ; $A = \mathbb{Z}$, $M = \mathbb{Z}[x]$, $M = \mathbb{Z}[\sqrt{2}]$.

Digression vers des problèmes existenciels

Les trois axiomes suivants sont équivalents(*) :

I.1.3. Axiome du choix : Tout ensemble E possède une fonction de choix, c'est à dire une application $\theta : \mathcal{P}(E) - \{\phi\} \longrightarrow E$ qui à toute partie non vide A de E associe un de ses éléments $\theta(A) \in A$.

Formulation équivalente : soit $(E_i)_{i \in I}$ une famille de parties de E, $\prod_{i \in I} E_i = \{x : I \to E / \forall i \in I \; x(i) \in E_i\} \subset E^I$; si pour tout $i \in I$ E_i est non vide, alors $\prod_{i \in I} E_i \neq \phi$.

I.1.4. Axiome de Zorn : Etant donné un ensemble ordonné $(E, \leqslant)$, on appelle chaîne de E une partie totalement ordonnée non vide ; et on dit que $(E, \leqslant)$ est inductif si toute chaîne de E est majorée. L'axiome de Zorn affirme que si $(E, \leqslant)$ est inductif, tout élément x_0 de E admet un majorant maximal.

I.1.5. Axiome de Zermelo : Un ensemble $(E, \leqslant)$ est bien ordonné si toute partie non vide de E admet un plus petit élément.

Ernst Zermelo affirme en 1904 que tout ensemble peut être bien ordonné.

(*) Les équivalences sont admises sans démonstration, et les axiomes aussi !

I.1.6 Théorème de la base incomplète

Soit E un espace vectoriel sur un corps K, L une partie libre de E ; il existe une base B de E contenant L

I.1.7 Corollaire :

Tout sous espace vectoriel d'un espace vectoriel E sur un corps K admet un supplémentaire.

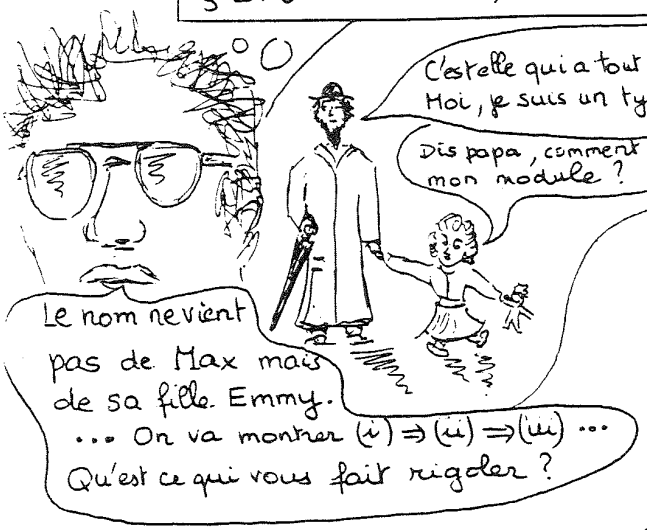
I.1.8 Théorème (Krull) :

Dans un anneau A, tout idéal propre est contenu dans un idéal maximal

(*) Apprécier dans S. Lang "Algebra" p. la manière d'évoquer le problème.

(**) Pour une preuve : N. Bourbaki . Algèbre . livre II . chap 2 . §1 n°13 . prop. 23 .

§ I.2 Anneaux Noetheriens



I.2.1 Proposition et définition :
Un anneau A est noethérien s'il satisfait aux conditions équivalentes :

(i) Tout idéal de A est de type fini.

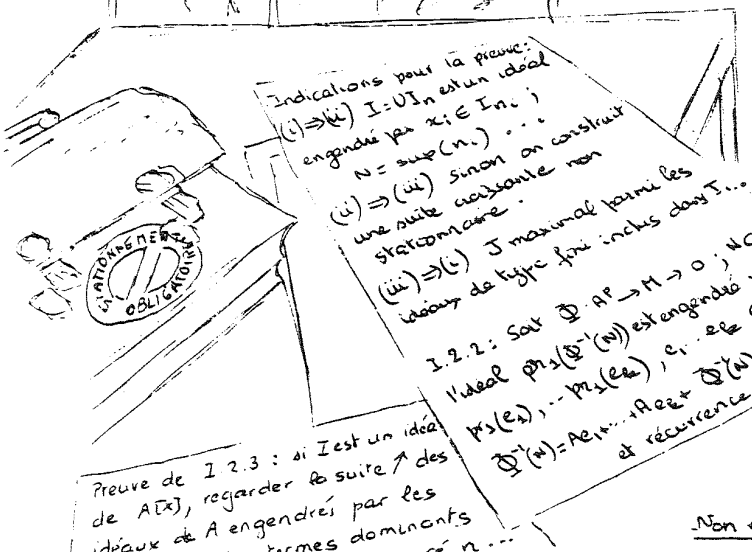
(ii) Toute suite croissante d'idéaux de A est stationnaire.

(iii) Toute famille non vide d'idéaux de A admet un élément maximal.

exemples :

- A principal ⇒ noethérien.
- A noethérien ⇒ $\frac{A}{I}$ noethérien.
- Une k-algèbre de type fini (d'après I.2.3)

I.2.2 Proposition : Sur A Noethérien, tout sous module d'un module de type fini est de type fini.



Preuve de I.2.3 : si I est un idéal de A[x], regarder la suite ↗ des idéaux de A engendrés par les coefficients des termes dominants des éléments de I de degré n ...

I.2.3 Théorème : (de transfert)

A noethérien

⇓

A[x] noethérien.

Non exemples :

- $k[(x_i)_{i\in\mathbb{N}}]$. $I_n = \langle x_1, \dots, x_n \rangle$
- $\mathcal{C}^\infty(\mathbb{C})$. $I_n = \{ f \,/\, f(z) = 0 \text{ pour } z = n, n+1, \dots \}$
  $\frac{\sin 2\pi z}{z(z-1)\cdots(z-n+1)} \in I_n - I_{n-1}$.
- $\mathcal{C}^\infty_{\mathbb{R}}(\mathbb{R})$. $I_n = \{ f \,/\, f(z) = 0 \text{ pour } z \in]0, \frac{1}{n}[\}$

Remarque : Un module M de type fini sur un anneau noethérien admet une <u>présentation finie</u> : $A^q \xrightarrow{u} A^p \xrightarrow{v} M \to 0$
v surjective et Im u = Ker v.

I.2.4 Théorème (décomposition des idéaux réduits)

Soit A un anneau noethérien, $I = \sqrt{I}$ un idéal réduit de A ; il existe des idéaux premiers $P_1, \dots, P_r$ uniques à permutation près tels que : $I = P_1 \cap P_2 \dots \cap P_r$; $P_i \not\subset P_j$ pour $i \neq j$.

En théorie des schémas, comme en géométrie algébrique hyperclassique, il n'y a pas besoin de supposer l'anneau noethérien pour montrer que le nil radical est intersection des idéaux premiers MINIMAUX ! (a)

J'ai mis très longtemps à comprendre ça...

J'insiste ! L'hypothèse A noethérien sert à montrer qu'il y en a un nombre FINI ! (b) Il reste du THE si tu veux ... (c)

Pour la décomposition primaire, c'est plus cher ! Je vous le fais en heures sup. si la fac débloque... Sinon : J.P. LAFON ALGEBRE COMMUTATIVE Hermann 1977 Chap 3

A faire à la maison :

(a) Applique le théorème I.1.8 (de Krull) à l'anneau de fraction A_f où f est un élément non nilpotent. Si tu ne sais pas ce que c'est, prends un idéal maximal parmi les idéaux de A ne coupant pas $\{(f^k)_{k \in \mathbb{N}}\}$ (grâce à Zorn), et montre que cet idéal est premier. Tu peux prendre un BISCUIT.

(b) Supposons l'existence d'un idéal I de A, réduit, ne s'écrivant pas comme intersection finie d'idéaux premiers ; d'après la définition I.2.1 (iii), on peut supposer I maximal pour cette propriété. I n'est donc pas premier, $\exists\, g, h$ n'appartenant pas à I tels que $gh \in I$, $\sqrt{I + Ag} = Q_1 \cap Q_2 \dots \cap Q_\ell$, $\sqrt{I + Ah} = R_1 \cap \dots \cap R_m$ et il reste à vérifier que $I = \sqrt{I} = Q_1 \cap \dots \cap Q_\ell \cap R_1 \cap \dots \cap R_m$ ...

Tu peux prendre deux BISCUITS.

(c) Se mettre devant la glace, dire la tirade à haute voix en appuyant très FORT sur les mots en majuscule.

§ I.3 . Les idéaux de Fitting.

Soit M un A-module de présentation finie (si A est noethérien, M = un A-module de type fini) et $A^q \xrightarrow{u} A^p \xrightarrow{v} M \to 0$ une présentation ; on lui associe la suite $F^0(M) \subset F^1(M) \subset \dots \subset F^p(M) = A = \dots$ d'idéaux de A :

$F^j(M)$ = l'idéal engendré par les $(p-j)\times(p-j)$ mineurs extraits de la matrice de u dans les bases canoniques, pour $j = 0, 1 \dots p-1$; avec la convention $F^j(M) = 0$ si $q < p-j$.

$F^j(M) = A$ pour $j \geq p$.

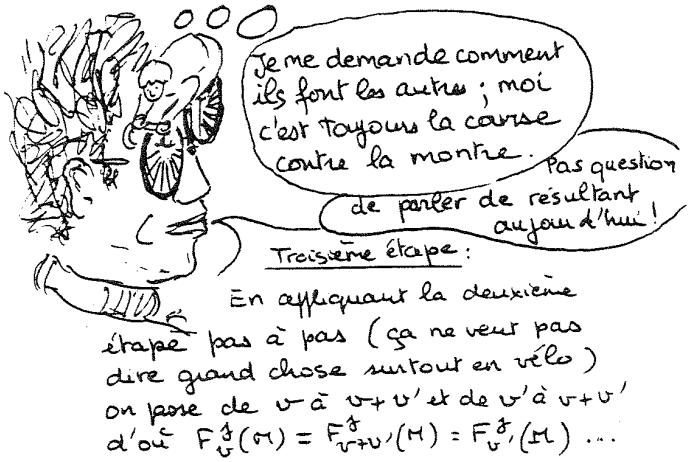
I.3.1 Proposition et définition : Etant donné un A-module de présentation finie M, et $j \in \mathbb{N}$, l'idéal $F^j(M)$ ne dépend pas de la présentation choisie ; on l'appelle le j-ième idéal de Fitting de M.

Première étape : $F^j(M)$ ne dépend pas de u. Si on choisit un autre système de générateurs $A^{q'} \xrightarrow{u'} \text{Im } u \to 0$ de $\text{Im } u = \text{Ker } v$, les vecteurs colonnes de la matrice P' de u' (dans les bases canoniques) s'expriment linéairement en fonction des vecteurs colonnes de la matrice P de u ; d'où $F^j_{u'}(M) \subset F^j_u(M)$ et par symétrie, l'égalité.

Deuxième étape : on ajoute un générateur à M : $F^j_{v'}(M) = F^j_v(M)$ où $v' : A^{q+1} \to M \to 0$, $v'(x,\lambda) = v(x) + \lambda\xi$

ξ donné dans M : $\xi = \sum a_i v(e_i)$

$$P' = \left(\begin{array}{c|c} P & \begin{matrix} -a_1 \\ \vdots \\ -a_q \end{matrix} \\ \hline \begin{matrix} 0 \dots 0 \end{matrix} & 1 \end{array}\right)$$



Troisième étape : En appliquant la deuxième étape pas à pas (ça ne veut pas dire grand chose surtout en vélo) on pose de v à v+v' et de v' à v+v' d'où $F^j_v(M) = F^j_{v+v'}(M) = F^j_{v'}(M)$ ...

Réfléchissez chez vous et posez des questions la prochaine fois.

Chap II : ANNEAUX PRINCIPAUX, ANNEAUX FACTORIELS

§ II.1 : Anneaux factoriels

Soit A un anneau commutatif, unitaire, INTEGRE.
U le groupe multiplicatif des unités (= éléments inversibles) de A.

Définition II.1.1 : $a \in A$ est irréductible si $a \notin U$ et si $a = bc$ implique $b \in U$ ou $c \in U$.

Définition II.1.2 : A est factoriel si tout élément de A s'écrit de manière unique, à unité près, et à permutation près comme produit d'éléments irréductibles. C'est à dire :

(F_1) $\forall a \in A - U$, $\exists (a_1, \dots, a_p)$ irréductibles, tels que $a = a_1 a_2 \cdots a_p$.

(F_2) Si $a_1, \dots, a_p$; $b_1, \dots b_q$ sont irréductibles et $a_1 \cdots a_p = b_1 \cdots b_q$, alors $q = p$, et à permutation près $b_i = u_i a_i$ avec $u_i \in U$.

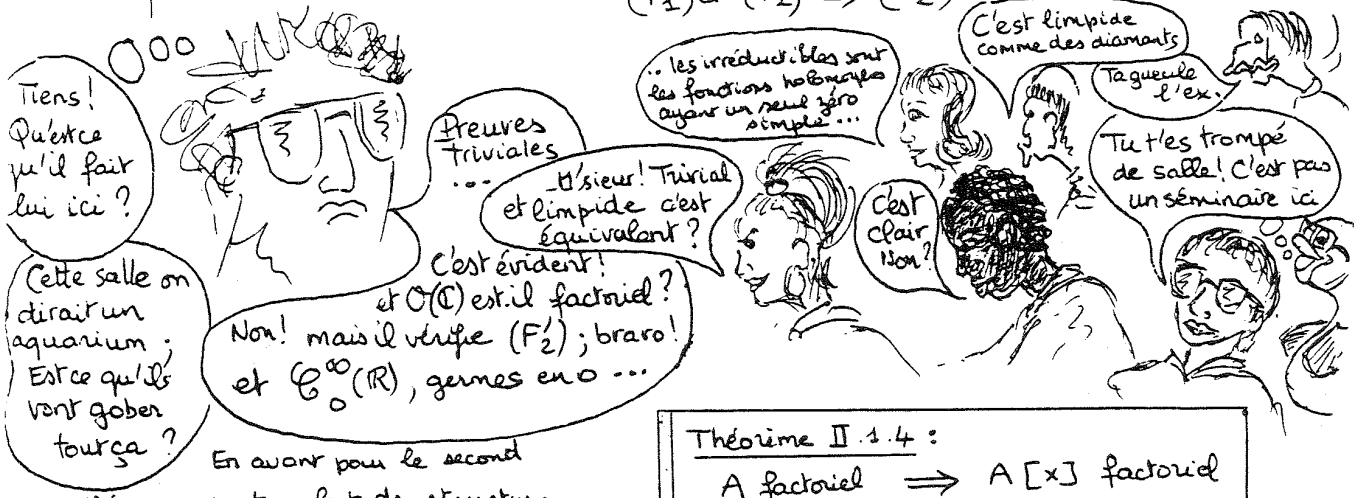
II.1.3 Proposition :

Soit A un anneau intègre ; soit la propriété :

(F_2') $a \in A$ irréductible divise $bc \Rightarrow$ a divise b ou c.

On a les implications : $(F_2') \Rightarrow (F_2)$

(F_1) et $(F_2) \Rightarrow (F_2')$



En avant pour le second théorème de transfert de structure ...

Théorème II.1.4 :

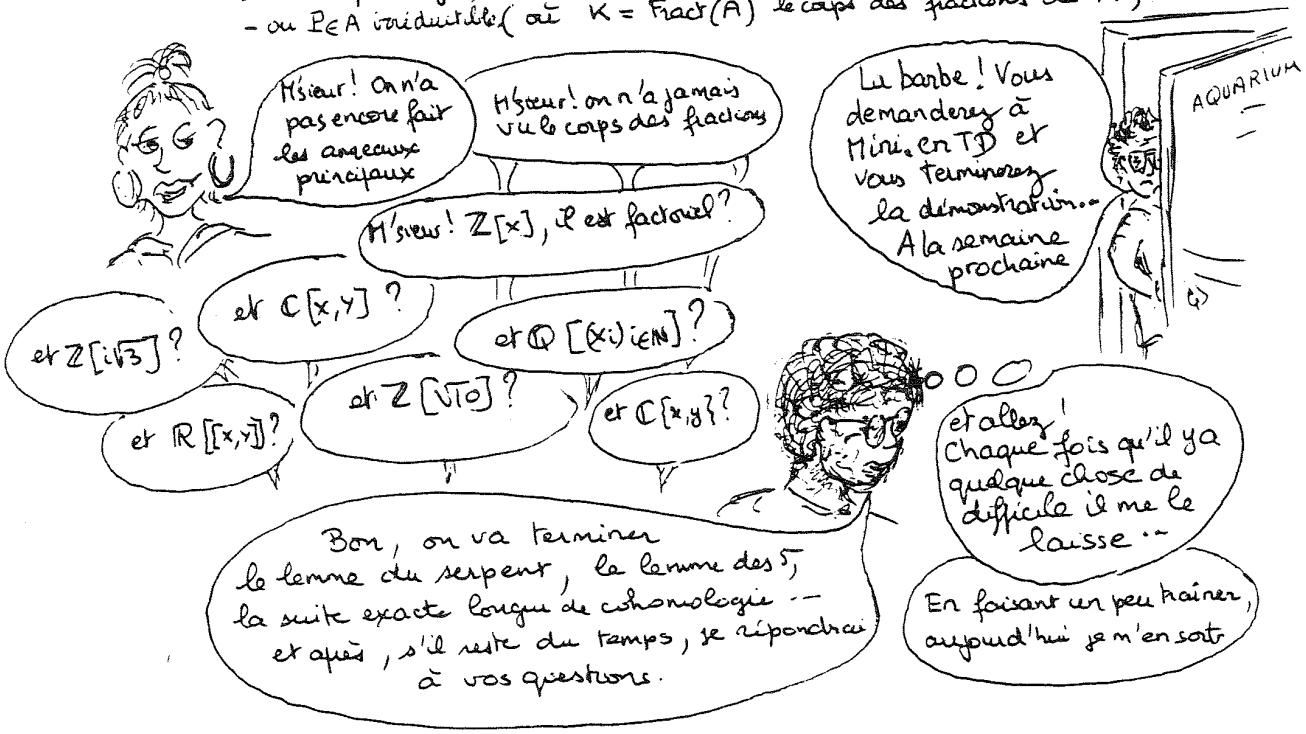
A factoriel $\Rightarrow$ A[x] factoriel

Dans un anneau factoriel on peut donc définir le PGCD (ou le PPCM) de plusieurs éléments ; pour un polynôme $P \in A[x]$ non nul on définit son <u>contenu</u> $c(P)$ comme le PGCD des coefficients et on dit que P est <u>primitif</u> si $c(P) = 1$ (tout ça c'est à une unité près !).

<u>Lemme II.1.5</u> : Le produit de deux polynômes primitifs est primitif.

Preuve : classique ! ... On en déduit facilement :

<u>Lemme II.1.6</u> : $P \in A[x]$ est irréductible si et seulement si :
- il est primitif, et irréductible dans l'anneau principal $K[x]$.
- ou $P \in A$ irréductible (où $K = \mathrm{Fract}(A)$ le corps des fractions de A)



§II.2 : Anneaux principaux

Définition II.2.1 : on appelle anneau principal un anneau (commutatif, unitaire) INTEGRE, dans lequel tout idéal est monogène.

Proposition II.2.2 : un anneau principal est noethérien.

Proposition II.2.3 : un anneau principal est factoriel

Proposition II.2.4 (Identité de Bezout) : dans un anneau principal A, on a : $Ad = Aa + Ab$ où $d = PGCD(a, b)$.
En particulier $A = Aa + Ab$ si a et b sont premiers entre eux.

Théorème II.2.5 (du chinois) : A principal, a et b premiers entre eux ;
L'application canonique $\frac{A}{Aab} \longrightarrow \frac{A}{Aa} \times \frac{A}{Ab}$ est un isomorphisme d'anneaux.

Plus généralement, dans un anneau A quelconque, si I et J sont étrangers, c'est à dire si $I+J = A$, on a $I.J = I \cap J$ et l'isomorphisme $\frac{A}{I \cap J} \longrightarrow \frac{A}{I} \times \frac{A}{J}$.
Généraliser à une famille finie d'idéaux deux à deux étrangers.

Théorème II.8.6 : Un sous-module M d'un module libre L sur un anneau principal est libre.

Soit $(e_i)_{i\in I}$ une base de L, $(p_i)_{i\in I}$ les coordonnées relatives à cette base. Grâce à Zornelo, nous supposons I bien ordonné. Pour $i\in I$, soit L_i le sous module (libre !) engendré par les $(e_j)_{j\leq i}$ et $M_i = M\cap L_i$. Posons $p_i(M_i) = A\alpha_i$ et choisissons pour tout i $a_i\in M_i$ tel que $p_i(a_i)=\alpha_i$. On prend $a_i=0$ pour $\alpha_i=0$.

La famille des $(a_j)_{j\leq i}$ engendre M_i : en effet c'est vrai pour $i=i_0=\min(I)$; supposons vrai pour tout $j<i$ et soit $x\in M\cap L_i$; $x-p_i(x)a_i \in M\cap L_i$ est combinaison linéaire finie de $e_{j_1},\dots,e_{j_k}$ donc appartient à M_j pour $j=\sup(j_1,\dots,j_k)<i$. D'où x est combinaison des $(a_j)_{j\leq i}$; et c'est donc vrai pour tout i. (la famille des indices pour les quels ce n'est pas vrai est vide sinon elle aurait un plus petit élément).

La famille des $(a_j)_{j\in I^*}$ est libre (I^* est l'ensemble des j avec $a_j\neq 0$). En effet si $\sum \lambda_j a_j = 0$ est une relation, et si i est le plus grand indice tel que $\lambda_j a_j \neq 0$, alors $p_i\left(\sum \lambda_j a_j\right) = \lambda_i\alpha_i = 0$ et donc $\lambda_i = 0$ ...

Enfin, comme M est réunion des $M_i = M\cap L_i$, $(a_j)_{j\in I^*}$ est une base de M.

Exemple : $\mathbb{R}$ n'est pas libre sur $\mathbb{Z}$ sinon $\mathbb{Q}$ le serait lui aussi.

§ II.3 Modules de type fini sur les anneaux principaux

Soit L un A-module libre de type fini, de base $(e_1, \cdots e_n)$. On remarque que tout autre base a même nombre n d'éléments, rang de L ; j'aurais d'ailleurs dû le dire plutôt : vous le démontrerez en exercice en prenant par exemple le produit des matrices de passages (remarquer que $I = \left(S\right)\overbrace{T}$ est impossible si S a n lignes et m colonnes, T a m lignes et n colonnes avec $n > m$ — prendre le déterminant après avoir ajouter des zéros). Le groupe des automorphismes de L s'identifie donc à $GL(n, A)$ groupe des matrices carrées inversibles (c'est à dire à déterminant inversible dans A).

Théorème II.3.1 : soit A un anneau principal, L un A-module libre de rang n, $M \subset L$ un sous A-module non réduit à 0.

a) M est libre de rang $r \leq n$.

b) Il existe une base $(e'_1, \cdots, e'_n)$ de L, des éléments $(\alpha_1, \cdots, \alpha_r)$ de A non nuls tels que α_i divise α_{i+1} pour $i = 1, \cdots, r-1$ et tels que $(\alpha_1 e'_1, \cdots, \alpha_r e'_r)$ soit une base de M.

c) La suite $(\alpha_1, \cdots, \alpha_r)$ satisfaisant aux conditions (b) est unique à unités près.

Définition II.3.2 : la suite $(\alpha_1, \cdots, \alpha_r)$ s'appelle la suite des facteurs invariants de M dans L. On devrait dire la suite $A\alpha_1 \supset A\alpha_2 \supset \cdots \supset A\alpha_r$.

[PS] **Preuve** : soit $\varphi \in L^*$ et $I_\varphi = \varphi(M)$; I_φ est une famille d'idéaux de A qui admet un élément maximal $I_{\varphi_1} = A\alpha_1$; on choisit $a_1 \in M$ tel que $\varphi_1(a_1) = \alpha_1$. Dans la base de départ $(e_1, \cdots, e_n)$ de L, $a_1 = x_1 e_1 + \cdots x_n e_n$ donc $\alpha_1 = x_1 \varphi_1(e_1) + \cdots x_n \varphi_1(e_n)$.

Soit d le pgcd de $\alpha_1 = \varphi_1(a_1)$ et $\varphi(a_1)$ pour un $\varphi \in L^*$; on peut écrire $d = u\alpha_1 + v\varphi(a_1) = (u\varphi_1 + v\varphi)(a_1) \in I_{u\varphi_1 + v\varphi}$:

$$I_{\varphi_1} = A\alpha_1 \subset Ad \subset I_{u\varphi_1 + v\varphi}$$

et comme I_{φ_1} est maximal, il y a égalité, $d = \alpha_1$ divise $\varphi_a(a_1)$ pour tout $\varphi \in L^*$; en particulier toutes les coordonnées x_i de a_1.

d'où $a_1 = \alpha_1 e'_1$ avec $e'_1 = \frac{x_1}{\alpha_1} e_1 + \cdots + \frac{x_n}{\alpha_1} e_n$.

[PS] Pierre SAMUEL - Théorie algébrique des nombres - chez Hermann - page 26

On a : $L = Ae'_1 \oplus \operatorname{Ker}\varphi_1$ (*) et $M = A\alpha_1 e'_1 \oplus (M \cap \operatorname{Ker}\varphi_1)$. (**)

En effet $y \in L$ s'écrit $y = \varphi_1(y)\,e'_1 + (y - \varphi_1(y))e'_1$ et unicité non moins évidente ...

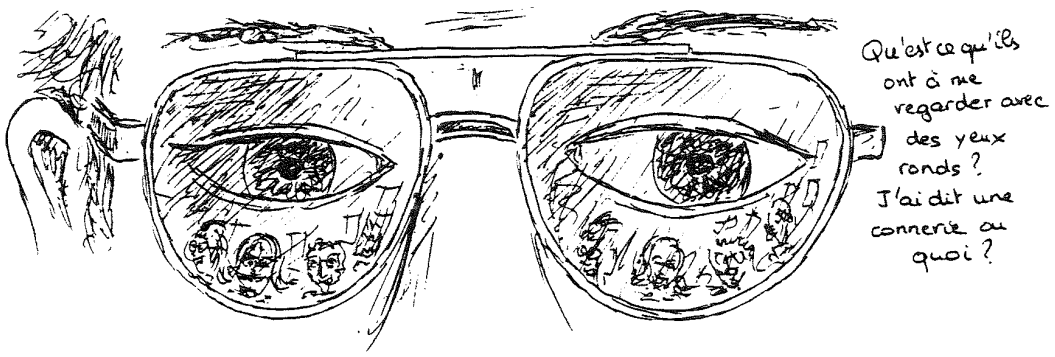
On démontre d'abord a) par récurrence sur le rang de M : $M \cap \operatorname{Ker}\varphi_1$ est un sous module de rang $r-1$ de L d'après (**) donc libre. A condition d'avoir donné une définition correcte du rang puisque nous ne savons pas encore que M est libre : on pose $\operatorname{rg}(M) = \dim_K(K \otimes_A M)$.

Ayant ainsi démontré a) (tu parles !) nous savons que $\operatorname{Ker}\varphi_1$ est libre de rang $n-1$. Par récurrence sur n, $M \cap \operatorname{Ker}\varphi_1 \subset \operatorname{Ker}\varphi_1$ possède une base $(\alpha_2 e'_2, \dots, \alpha_r e'_r)$ où $(e'_2 \dots e'_r)$ est une base de $\operatorname{Ker}\varphi_1$, et $(\alpha_2, \dots, \alpha_r)$ sont les facteurs invariants de $M \cap \operatorname{Ker}\varphi_1$ dans $\operatorname{Ker}\varphi_1$. D'où, d'après (*) et (**) tout est fini à condition de voir que α_1 divise α_2 ; or si φ est la somme des deux premières coordonnées dans la base $(e_1, e'_2) \dots e'_n)$, on a $\varphi(\alpha_1 e'_1) = \alpha_1$ et $\varphi(\alpha_2 e'_2) = \alpha_2$, donc $I_\varphi \supset I_{\varphi_1} = A\alpha_1$; et comme I_{φ_1} est maximal, $I_\varphi = A\alpha_1$ contient α_2.

Enfin, pour l'unicité, c), voir plus haut (à propos des idéaux de Fitting). Plus précisément :

<u>Lemme II.3.2</u> : pour $1 \leq k \leq r$, $A\alpha_1 \dots \alpha_k$ est l'idéal engendré par les $(k \times k)$ mineurs extraits de la matrice des composantes d'un système de générateurs de M dans une base de L.

Puisque c'est le $(n-k)$ ième idéal de Fitting du A-module L/M d'après I.3.



Corollaire II.3.3 ; soit A un anneau principal, $L' \xrightarrow{u} L$ une application linéaire entre deux modules libres de type fini de rang n' et n.

a) Il existe une suite $(\alpha_1, \dots \alpha_r)$ d'éléments non nuls de A tels que α_i divise α_{i+1} pour $i = 1, \dots, r-1$; il existe une base $(e'_1, \dots, e'_{n'})$ de L', une base $(e_1, \dots e_n)$ de L dans les quelles la matrice de u est diagonale : $u(e'_i) = \alpha_i e_i$ pour $i = 1, \dots r$ et $u(e'_i) = 0$ pour $i = r+1, \dots, n'$.

b) pour $i = 1, \dots, r$ $\alpha_1 \times \dots \times \alpha_i$ est le pg.c.d des $i \times i$ déterminants extraits de la matrice de u dans des bases quelconques.

Preuve : soit r le rang de $\mathrm{Im}\, u$, $(\alpha_1, \dots \alpha_r)$ ses facteurs invariants dans L, $(e_1 \dots e_n)$ une base de L telle que $(\alpha_1 e_1, \dots \alpha_r e_r)$ soit une base de $\mathrm{Im}\, u$; choisissons $(e'_1, \dots, e'_r)$ dans L' tels que $u(e'_i) = \alpha_i e_i$; $(e'_1 \dots e'_r)$ sont indépendants (car les images $(\alpha_1 e_1, \dots \alpha_r e_r)$ sont indépendantes) et $L' = (Ae'_1 \oplus \dots \oplus Ae'_r) \oplus \mathrm{Ker}\, u$ car si $u(x) = \sum_{i=1}^{r} \lambda_i \alpha_i e_i$, $x - \sum \lambda_i e'_i \in \mathrm{Ker}\, u$. D'après le théorème $\mathrm{Ker}\, u$ est libre et on peut en prendre une base $(e'_{r+1}, \dots, e'_{n'})$.

Corollaire II.3.4 : Soit A un anneau principal, N un A-module de type fini. Il existe $k \geq 0$; il existe $s \geq 0$, des éléments non inversibles et non nuls de A, $(\beta_1, \dots, \beta_s)$, tels que β_i divise β_{i+1} pour $i = 1, \dots, s-1$ et :

$$N \approx \left(\frac{A}{A\beta_1} \oplus \dots \oplus \frac{A}{A\beta_s} \right) \oplus A^k$$

les entiers k, s et les éléments $(\beta_1 \dots \beta_s)$ à unité près sont uniques, satisfaisant les conditions précédentes.

Nous obtenons donc la classification des modules de type fini sur un anneau principal. L'existence découle du théorème II.3.1 appliqués aux relations d'un système de générateurs ; et l'unicité de la définition - unicité (I.3.1) des idéaux de Fitting de N.

Le chinois va encore plus loin !

$$\mathbb{Z}/12\mathbb{Z} \approx \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$$

$$\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{6\mathbb{Z}} \approx \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}}$$

Conséquences : un module de type fini sur un anneau principal est libre si et seulement si il est sans torsions ; un module de type fini est somme directe de son sous module de torsion et d'un sous module libre.

§ II.4. Unités de $\mathbb{Z}/n\mathbb{Z}$ et indicatrice d'Euler

On note U_n le groupe multiplicatif des unités de $\mathbb{Z}/n\mathbb{Z}$,

$$\varphi(n) = \#\{k \;/\; 1 \leq k \leq n \;\; (k,n) = 1\}$$

on a $\varphi(1) = 1$ et $\varphi(n) = \# U_n$ pour $n \geq 2$.

Proposition II.4.1 : soit $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ la décomposition de n en produit de nombres premiers ; on a :

$$\boxed{\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_s}\right)}$$

preuve : si $n = p^\alpha$ où p est un nombre premier, $\mathbb{Z}/n\mathbb{Z} - U_n$ sont les multiples de p, et il y en a $p^{\alpha-1}$ $(0, p, 2p \cdots, (p^{\alpha-1}-1)\cdot p)$.
Si n est le produit de deux entiers premiers entre eux, $n = a.b$, alors $\varphi(n) = \varphi(a).\varphi(b)$ d'après le théorème chinois.

Proposition II.4.2 : $\boxed{n = \sum_{\substack{1 \leq d \leq n \\ d \mid n}} \varphi(d).}$

Il suffit de montrer que $\mathbb{Z}/n\mathbb{Z}$ possède exactement $\varphi(d)$ éléments d'ordre d pour d divisant n. Si k est d'ordre $d > 1$, d est le plus petit entier tel que $kd \in n\mathbb{Z}$, soit $kd \in n'd\,\mathbb{Z}$. $(n = n'd)$.
Posons $k = n'k'$; $1 \leq k = n'k' \leq n-1 = n'd - 1$; donc $1 \leq k' \leq d$ et $(k', d) = 1$ sinon son ordre serait strictement inférieur à d. Donc k' prend $\varphi(d)$ valeurs.

Proposition II.4.3 : soit p premier ; le groupe $U_p = \mathbb{F}_p^*$ est cyclique.

Comme vous l'avez deviné, $\mathbb{F}_p$ n'est rien d'autre que $\mathbb{Z}/p\mathbb{Z}$. Soit $\Psi(d)$ le nombre des éléments d'ordre d de U_p (multiplicatif !). Comme U_p est de cardinal $p-1$, on a :

$$p-1 = \sum_{\substack{d \mid p-1 \\ 1 \le d \le p-1}} \Psi(d).$$

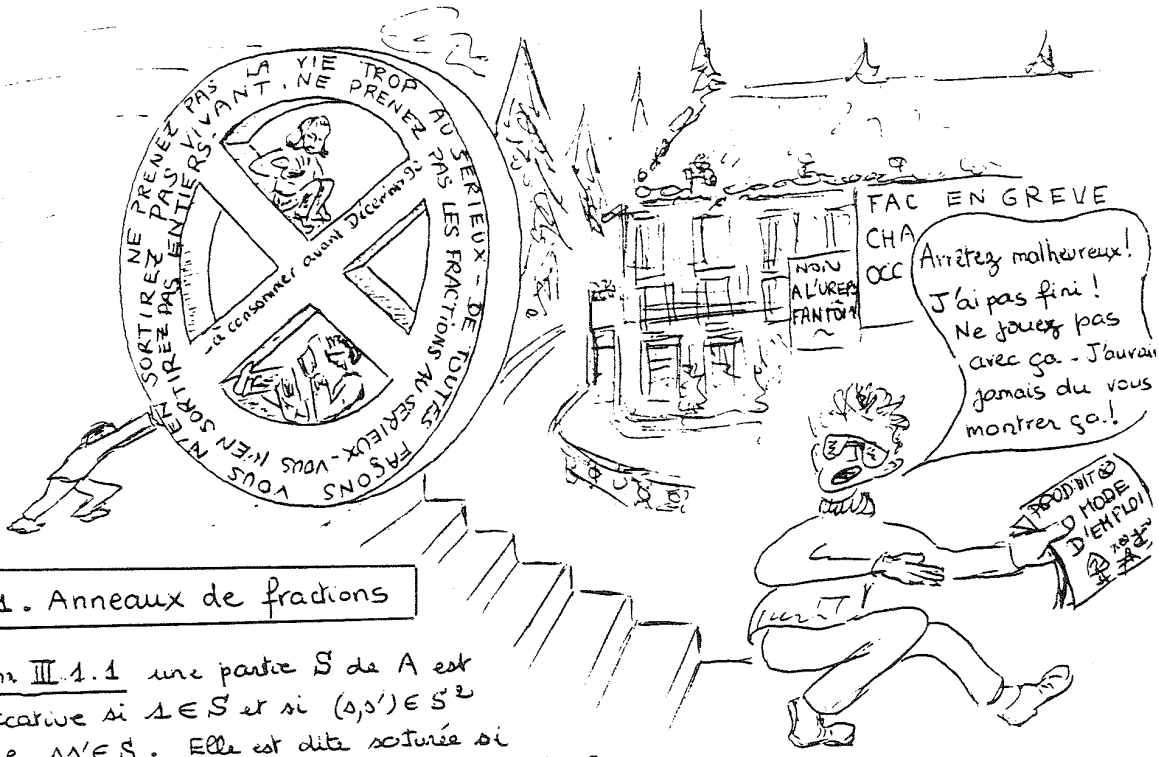
Tout élément d'ordre d'ordre d de U_p est racine (dans $\mathbb{F}_p$) du polynôme $X^d - 1 \in \mathbb{F}_p[X]$; comme il y a au plus d racines de ce polynôme, ou bien $\Psi(d) = 0$, ou bien si $\Psi(d) \neq 0$, il existe $a \in U_p$ d'ordre d donc $\{1, a, \dots, a^{d-1}\}$ sont d éléments distincts de U_p = toutes les racines du polynôme $X^d - 1$; donc tout élément d'ordre d de U_p appartient au sous groupe $\{1, a, \dots, a^{d-1}\}$: ce sont les a^k, $(k,d) = 1$, $1 \le k \le d-1$ et il y en a exactement $\varphi(d)$; dans ce cas $\varphi(d) = \Psi(d)$.

Conclusion : $p-1 = \sum_{\substack{d \mid p-1 \\ 1 \le d \le p-1}} \Psi(d) = \sum_{\substack{d \mid p-1 \\ 1 \le d \le p-1}} \varphi(d)$ d'après la proposition précédente, avec $\forall d$, $\Psi(d) = 0$ ou $\Psi(d) = \varphi(d)$. D'où $\forall d$, $\Psi(d) = \varphi(d)$ et en particulier $\Psi(p-1) = \varphi(p-1) \geq 1$.

Remarque : on ne s'est pas servi du fait que le corps est $\mathbb{F}_p$; donc pour tout corps fini K, K^* est cyclique.

[M.P.M] Malliavin - Algèbre commutative. p37

Chap. III : ANNEAUX DE FRACTIONS ET PRODUITS TENSORIELS DE MODULES



§ III.1. Anneaux de fractions

Définition III.1.1 une partie S de A est multiplicative si $1 \in S$ et si $(s,s') \in S^2$ implique $ss' \in S$. Elle est dite saturée si de plus $(s,s') \in A^2$, $ss' \in S \Rightarrow s \in S$ et $s' \in S$.

On considère sur $S \times A$ la relation d'équivalence $(s,a) \sim (s',a')$ si $\exists t \in S$ tel que $t(sa' - s'a) = 0$; on note $\frac{a}{s}$ la classe d'équivalence, $S^{-1}A$ le quotient.

Proposition III.1.2 : $S^{-1}A$ est un anneau (unitaire pour $0 \notin S$), muni d'un homomorphisme naturel $\theta_A : A \longrightarrow S^{-1}A$ $\left(\theta_A(1) = \frac{a}{1}\right)$. Ce couple est solution du problème universel suivant : $\forall f : A \to B$ homomorphisme d'anneaux tel que $\forall s \in S$, $f(s)$ soit inversible dans B, $\exists\, \overline{f} : S^{-1}A \to B$ homomorphisme d'anneaux tel que $\overline{f} \circ \theta_A = f$. C'est l'ANNEAU DE FRACTIONS DE A A DENOMINATEURS DANS S.

Sujets de réflexion :
∃ une plus petite partie multiplicative contenant $\pi \subset S$: que devient le problème universel ?

Comparer : idéaux premiers de $S^{-1}A$ et idéaux premiers de A ne coupant pas S.

Il existe une plus petite partie multiplicative saturée contenant S, soit $\mathcal{S}$. Comparer $S^{-1}A$ et $\mathcal{S}^{-1}A$.

Changement de partie multiplicative $S \subset T$

$\mathcal{S} = \bigcap_{i \in I} (A - \mathcal{P}_i)$

$\mathcal{P}_i$ premier, $\mathcal{P}_i \cap S = \emptyset$

Utiliser un idéal maximal parmi les idéaux de A ne coupant pas S.

Et $\ker \theta_A$?

A intègre
$S = A - \{0\}$; $S^{-1}A = \mathrm{Frac}(A)$
corps des fractions de A

$f \in A$, $S = \{1, f, f^2 \cdots\}$
$S^{-1}A = A_f$
Par exemple les nombres décimaux, les nombres dialiques.

Exercice : comparer $\frac{A[x]}{(xf-1)}$ et A_f.

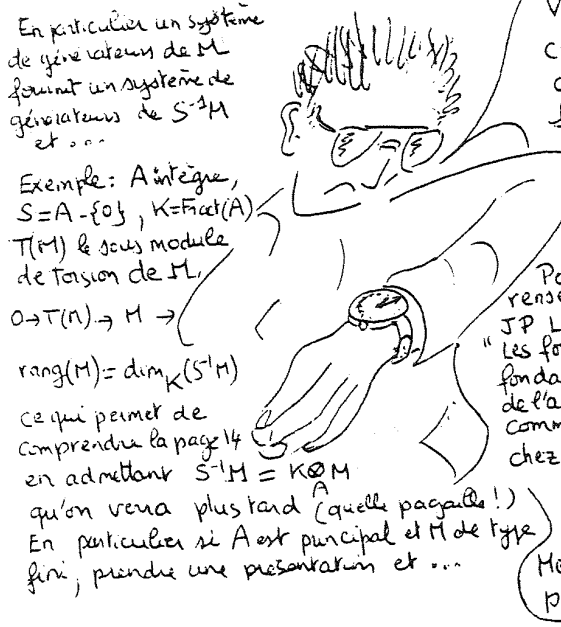
S = les éléments non diviseur de 0 dans A ;
$S^{-1}A = \mathrm{Tot}(A)$ "anneau total" de fractions de A

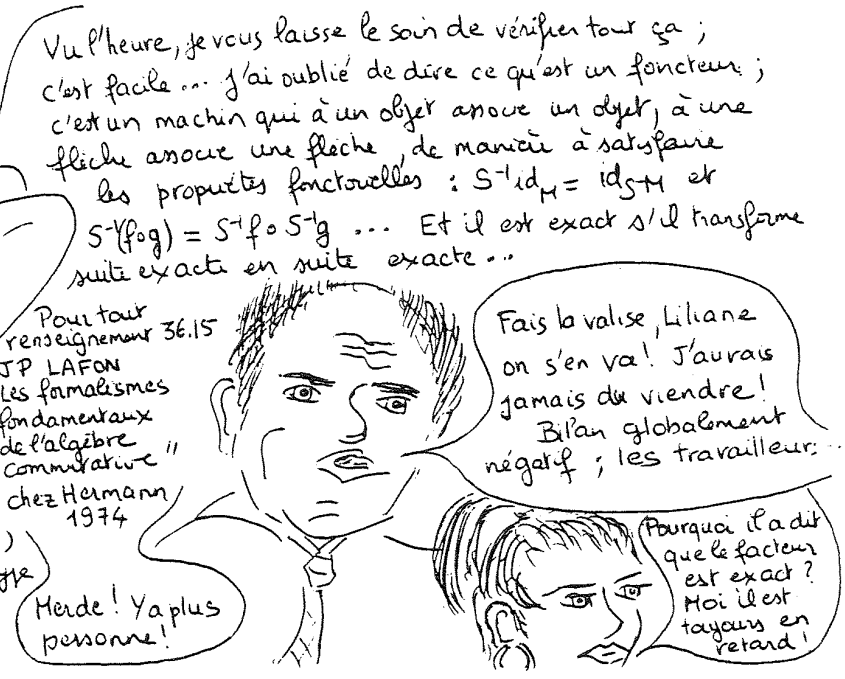
$S = A - \mathfrak{P}$ où $\mathfrak{P}$ est un idéal premier de A ;
$S^{-1}A = A_{\mathfrak{P}}$ localisé de A en $\mathfrak{P}$. C'est un anneau local d'idéal maximal $\mathfrak{P}A_{\mathfrak{P}}$, de corps "résiduel" $K(\mathfrak{P}) = \frac{A_{\mathfrak{P}}}{\mathfrak{P}A_{\mathfrak{P}}}$; comparer $\mathrm{Frac}(\frac{A}{\mathfrak{P}})$ et $K(\mathfrak{P})$.

Module de fractions : si S est une partie multiplicative de A, M un A-module, on considère sur $S \times M$ la relation d'équivalence $(s,m) \sim (s',m')$ si il existe $t \in S$ tel que $t(sm' - s'm) = 0$. On note $S^{-1}M$ le quotient et $\frac{m}{s}$ la classe d'équivalence : c'est le module de fractions de M à dénominateurs dans S.

Proposition III.1.3 : $S^{-1}M$ est naturellement muni d'une structure de $S^{-1}A$-module et d'un morphisme naturel $\theta_M : M \longrightarrow S^{-1}M$ $(\theta_M(m) = \frac{m}{1})$. Pour toute application A-linéaire $f : M \to N$, il existe une application $S^{-1}A$-linéaire unique $S^{-1}f$ de $S^{-1}M$ dans $S^{-1}N$ telle que $S^{-1}f \circ \theta_M = \theta_N \circ f$.

Théorème III.1.4 : Le foncteur S^{-1} de la catégorie A-Mod vers la catégorie $S^{-1}A$-Mod est exact.





§ III.2 Produit tensoriel

Donnons nous M, M', P trois A-modules ; $Bil_A(M, M'; P)$ ensemble des applications bilinéaires de $M \times M'$ dans P s'identifie, comme A-module, et en se forçant un peu, à $Hom_A(M, Hom_A(M', P))$.

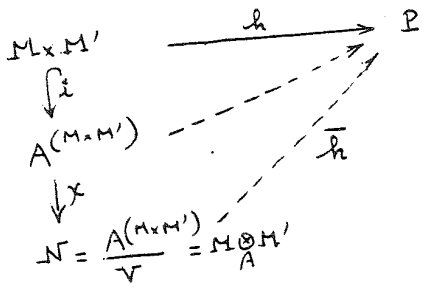
On se pose le problème universel suivant : trouver un A-module N et une application bilinéaire $\varphi : M \times M' \longrightarrow N$ telle que pour toute application bilinéaire $h : M \times M' \longrightarrow P$, il existe une unique $\overline{h} : N \to P$ linéaire satisfaisant $h = \overline{h} \circ \varphi$.

Unicité : deux solutions de ce problème sont isomorphes - Classique ; faites le vous même, car ce n'est pas en me regardant faire, ni en utilisant Nuluo Yoneda (J P LAFON page 14) que vous apprendrez quelque chose.

Existence : soit $A^{(M \times M')}$ le A-module libre construit sur $M \times M'$ muni de sa base canonique $(e_{m,m'})_{(m,m') \in M \times M'}$; et soit V le sous A-module de $A^{(M \times M')}$ engendré par les éléments : $\{ e_{m_1+m_2, m'} - e_{m_1,m'} - e_{m_2,m'}$; $e_{am,m'} - a e_{m,m'}$; $e_{m,m'_1+m'_2} - e_{m,m'_1} - e_{m,m'_2}$; $e_{m,am'} - a e_{m,m'} \}$.

On note $N = \dfrac{A^{(M \times M')}}{V} = M \underset{A}{\otimes} M'$ le quotient, $\varphi : M \times M' \longrightarrow M \underset{A}{\otimes} M'$ l'application canonique, $\varphi(m,m') = m \otimes m'$: c'est lui le produit tensoriel de M et M' sur A.

A vous de vérifier l'existence et l'unicité de $\overline{h}$ A-linéaire qui fait commuter le diagramme.



$\varphi = \gamma \circ i$ bilinéaire
$i(m,m') = e_{m,m'}$
$\gamma(m,m') = m \otimes m'$.

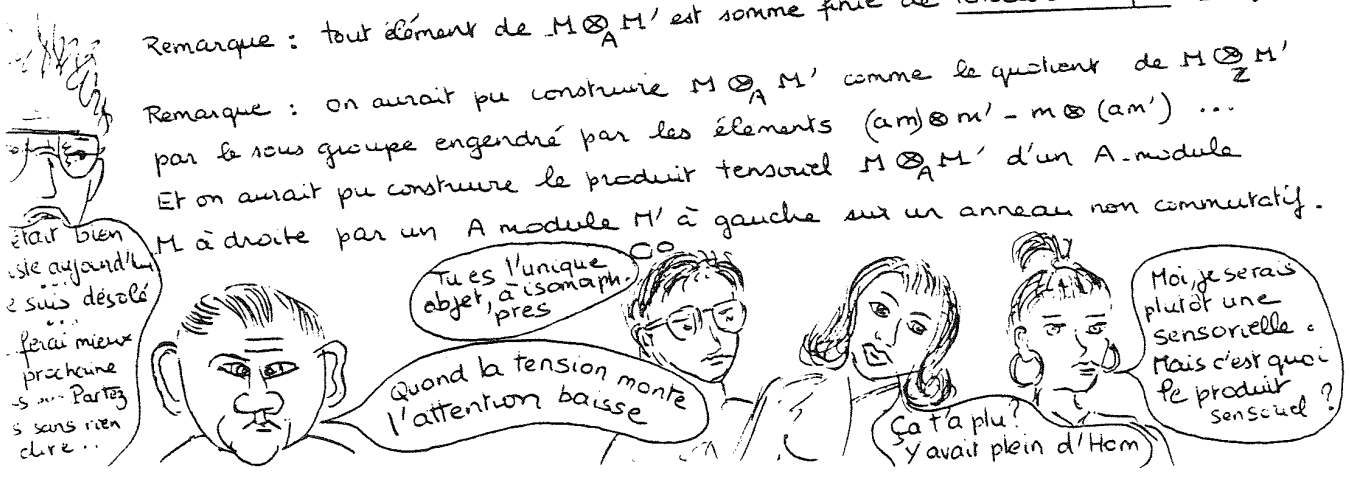
Proposition III.2.1

a) Soit $h : M \times M' \longrightarrow P$ bilinéaire ; $\exists ! \ \overline{h} : M \underset{A}{\otimes} M' \longrightarrow P$ linéaire telle que $\overline{h} \circ \varphi = h$.

b) Soit $\varphi_1 : M \times M' \longrightarrow N_1$ bilinéaire solution du problème universel précédent ; il existe un isomorphisme unique $\lambda : M \underset{A}{\otimes} M' \longrightarrow N_1$ tel que $\lambda \circ \varphi = \varphi_1$.

Remarque : tout élément de $M \underset{A}{\otimes} M'$ est somme finie de tenseurs simples $\sum m_i \otimes m'_i$.

Remarque : on aurait pu construire $M \underset{A}{\otimes} M'$ comme le quotient de $M \underset{\mathbb{Z}}{\otimes} M'$ par le sous groupe engendré par les éléments $(am) \otimes m' - m \otimes (am')$ ... Et on aurait pu construire le produit tensoriel $M \underset{A}{\otimes} M'$ d'un A-module M à droite par un A module M' à gauche sur un anneau non commutatif.



Une page de pub. pour une équipe originale et singulière ...

.. et, les jeunes, si vous apprenez bien votre produit tensoriel, on vous prendra peut-être dans notre équipe !

Proposition III.2.2 : il existe des isomorphismes canoniques :

(a) $M \otimes_A M' \xrightarrow{\sim} M' \otimes_A M$

(b) $(M \otimes_A M') \otimes_A M'' \xrightarrow{\sim} M \otimes_A (M' \otimes_A M'')$

(c) $A \otimes_A M \xrightarrow{\sim} M$.

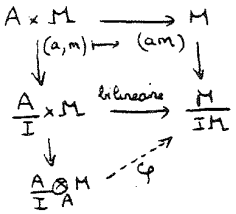
(d) $\left(\bigoplus_{i \in I} M_i\right) \otimes_A M' \xrightarrow{\sim} \bigoplus_{i \in I} (M_i \otimes_A M')$

On vérifie que pour $m \in M$ fixé, l'application $(m', m'') \longmapsto (m \otimes m') \otimes m''$ de $M' \times M''$ dans $(M \otimes_A M') \otimes_A M''$ est bilinéaire, donc définit une application linéaire $h_m : M' \otimes_A M''$ dans $(M \otimes_A M') \otimes_A M''$. Il faut voir maintenant que $(m, u) \longmapsto h_m(u)$ est bilinéaire de $M \times (M' \otimes_A M'')$ dans $(M \otimes_A M') \otimes_A M''$ pour montrer l'existence de h linéaire unique satisfaisant $h(m \otimes (m' \otimes m'')) = (m \otimes m') \otimes m''$ sur les tenseurs simples ....

Pour le (d) : soit $h : \left(\bigoplus_{i \in I} M_i\right) \times M' \longrightarrow \bigoplus_{i \in I} (M_i \otimes M')$ définie par $h(\Sigma x_i, m') = \Sigma (x_i \otimes m')$; elle est bilinéaire donc détermine $\tilde{h}$ unique ... Dans l'autre sens on détermine $M_i \otimes_A M' \longrightarrow \left(\bigoplus_{i \in I} M_i\right) \otimes M'$, d'où, en faisant la somme ...

Proposition III.2.3 :
Si M et M' ont respectivement $(e_i)_{i\in I}$ et $(e'_j)_{j\in J}$ pour systèmes de générateurs (resp. bases), $M\otimes_A M'$ admet $(e_i\otimes e'_j)_{(i,j)\in I\times J}$ pour système de générateurs (resp. base).

Proposition III.2.4 :
Soit I un idéal de A ; il existe un isomorphisme canonique : $\frac{A}{I}\otimes_A M \xrightarrow{\sim} \frac{M}{IM}$



φ est surjective, évident. Supposons $\varphi(\Sigma a_i\otimes m_i) = \Sigma a_i m_i = 0$; alors $\Sigma a_i m_i = \Sigma b_j n_j$ avec $b_j\in I$ et $n_j\in M$ donc
$\Sigma a_i\otimes m_i = 1\otimes\Sigma a_i m_i = 1\otimes\Sigma b_j n_j = \Sigma b_j\otimes n_j = 0$

Lemme de Nakayama - III.2.5
Soit A un anneau local, d'idéal maximal $\mathfrak{m}$; M un A-module de type fini.
Alors $M = 0 \iff M = \mathfrak{m}M$.

(celui là je vous l'encadre pour rompre la monotonie du cours, et parcequ'un japonais y a laissé son nom ; il n'en était pas fier pour autant - Il n'y a d'ailleurs pas de quoi (en être fier) et je vous laisse la démonstration en exercice (voir TD).
Vous en déduirez sous les mêmes hypothèses :

$(e_1,\dots,e_n)$ système minimal de générateurs de M sur A $\iff$ $(\dot e_1,\dots,\dot e_n)$ base de $\frac{M}{\mathfrak{m}M}$ sur $k = \frac{A}{\mathfrak{m}}$.

Définition III.2.5 : Soit $E\xrightarrow{u}E'$, $F\xrightarrow{v}F'$ deux applications linéaires ; il existe une unique application linéaire $u\otimes v : E\otimes_A F \longrightarrow E'\otimes_A F'$ satisfaisant à $u\otimes v(x\otimes y) = u(x)\otimes v(y)$.

Théorème III.2.6 : Le foncteur $M\otimes_A \cdot$ est exact à droite.

On commence par vérifier les propriétés fonctorielles de tout ça, et on peut alors passer à la preuve du théorème : soit $E\xrightarrow{\alpha}F\xrightarrow{\beta}G\to 0$ une suite exacte ; nous devons montrer que $M\otimes_A E\xrightarrow{1_M\otimes\alpha} M\otimes_A F\xrightarrow{1_M\otimes\beta} M\otimes_A G\to 0$

est encore exacte. On voit d'abord que $(1_M \otimes \beta) \circ (1_M \otimes \alpha) = 1_M \otimes (\beta \circ \alpha) = 0$ et donc que $H = (1_M \otimes \alpha)(M \underset{A}{\otimes} E)$ est contenu dans le noyau de $1_M \otimes \beta$; d'où par passage au quotient : $\dfrac{M \underset{A}{\otimes} F}{H} \xrightarrow{\overline{\beta}} M \underset{A}{\otimes} G$. Construisons une application $\overline{\gamma}$ en sens inverse : pour $(x, y) \in M \times G$, soit $z \in F$ tel que $\beta(z) = y$ et regardons la classe de $x \otimes z$ dans $\dfrac{M \underset{A}{\otimes} F}{H}$; elle ne dépend pas du choix de z ... facile... et l'application $(x, y) \longmapsto x \otimes z$ bilinéaire de $M \times G$ dans $\dfrac{M \underset{A}{\otimes} F}{H}$ induit $\overline{\gamma}$ unique de $M \underset{A}{\otimes} G$ dans $\dfrac{M \underset{A}{\otimes} F}{H}$ vérifiant $\overline{\gamma}(x \otimes y) = x \otimes z$ pour $\beta(z) = y$.
On vérifie alors que $\overline{\beta} \circ \overline{\gamma}$ et $\overline{\gamma} \circ \overline{\beta}$ sont les identités des modules correspondants.

Remarque : si la suite exacte courte $0 \longrightarrow E \xrightarrow{\alpha} F \xrightarrow{\beta} G \longrightarrow 0$ est scindée (ce qui est le cas, en particulier, lorsque G est libre) alors la suite $0 \longrightarrow M \underset{A}{\otimes} E \longrightarrow M \underset{A}{\otimes} F \longrightarrow M \underset{A}{\otimes} G \longrightarrow 0$ reste exacte.
Lorsque A est un corps, autrement dit dans la catégorie des espaces vectoriels sur un corps K, $M \underset{K}{\otimes} \cdot$ est exact.
En T.D vous avez même vu que G projectif équivaut à G facteur direct d'un libre et qu'alors la suite exacte est scindée.

Exemple : tensorisez $0 \to \mathbb{Z} \xrightarrow{\times p} \mathbb{Z} \to \dfrac{\mathbb{Z}}{p\mathbb{Z}} \to 0$ par $\dfrac{\mathbb{Z}}{q\mathbb{Z}}$; si $p = p'\delta$, $q = q'\delta$ $(p', q') = 1$ on obtient : $0 \to q'\dfrac{\mathbb{Z}}{q\mathbb{Z}} \to \dfrac{\mathbb{Z}}{q\mathbb{Z}} \xrightarrow{\times p} \dfrac{\mathbb{Z}}{q\mathbb{Z}} \to \dfrac{\mathbb{Z}}{p\mathbb{Z}} \underset{\mathbb{Z}}{\otimes} \dfrac{\mathbb{Z}}{q\mathbb{Z}} \to 0$
$\dfrac{\mathbb{Z}}{\delta\mathbb{Z}}$

§ III.3 Extension des scalaires

Soit $\rho : A \longrightarrow B$ un homomorphisme d'anneaux (commutatifs et unitaires).
B est donc un A-module "via ρ" : $a \cdot b = \rho(a) b$ pour $a \in A$ et $b \in B$.

Définition III.3.1 : si M est un A-module, $M \underset{A}{\otimes} B$ est naturellement muni d'une structure de B-module, et d'un morphisme (au dessus de ρ) canonique de M dans $M \underset{A}{\otimes} B$ = on dit que $M \underset{A}{\otimes} B$ est obtenu à partir de M par extension des scalaires de A à B.

A titre d'exercice, vérifier :

Lorsque M admet $(e_i)_{i\in I}$ comme système de générateurs (resp. base), la famille $(e_i\otimes 1)_{i\in I}$ est un système de générateurs (resp. base) de $M\otimes_A B$ sur B.

Proposition III.3.2 : Si $A\longrightarrow B\longrightarrow C$ sont des homomorphismes d'anneaux, il existe un C-isomorphisme naturel : $(M\otimes_A B)\otimes_B C \xrightarrow{\sim} M\otimes_A C$.

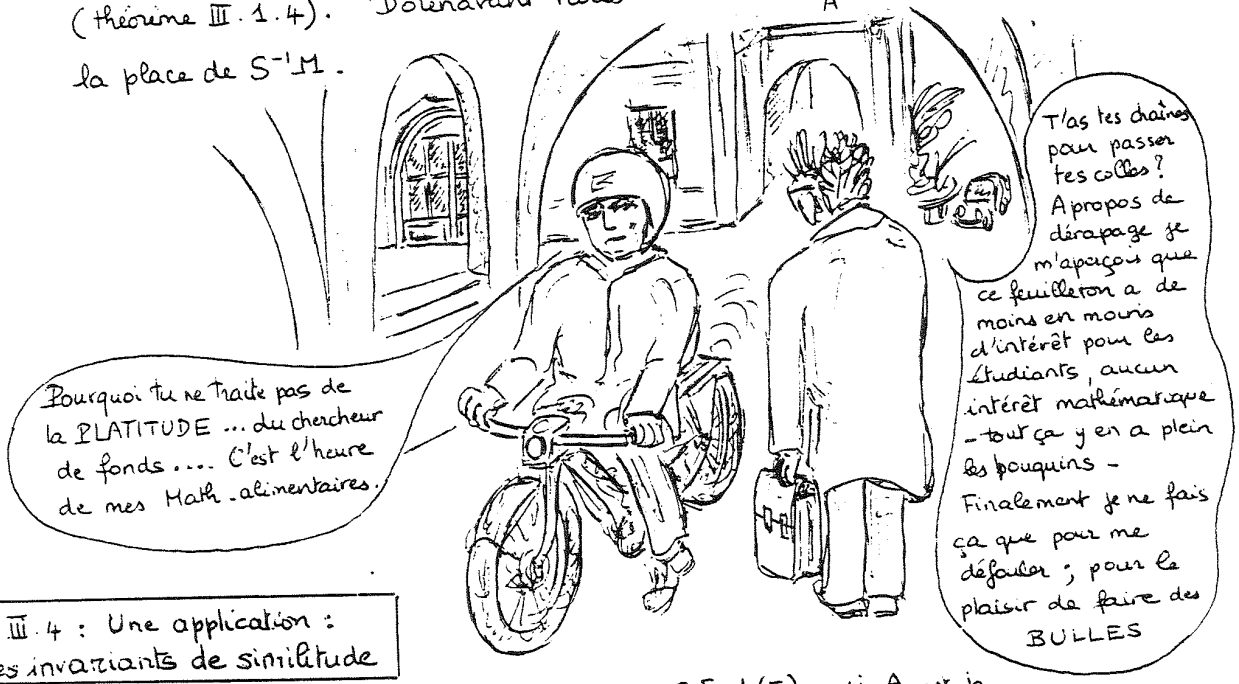
Cas particuliers d'extension de scalaires :

a) $A\longrightarrow \frac{A}{I}$ où I est un idéal de A : voir proposition III.2.4

b) $A\xrightarrow{\theta_A} S^{-1}A$ où S est une partie multiplicative de A.

Si M est un A-module : $\boxed{M\otimes_A S^{-1}A \xrightarrow{\sim} S^{-1}M}$.

Le foncteur $\cdot\otimes_A S^{-1}A$ s'identifie au foncteur S^{-1}. et est donc exact (théorème III.1.4). Dorénavant nous écrirons $M\otimes_A B$ si $B=S^{-1}A$, à la place de $S^{-1}M$.



§ III.4 : Une application : les invariants de similitude

E un espace vectoriel sur un corps k, de dimension n, $u\in \mathrm{End}(E)$; si A est la matrice de u dans une base, on note $d_j(x)$ le PGCD des $j\times j$ mineurs extraits de $A-xI$. $(d_1,\cdots,d_n)$ ne dépend pas du choix de la base, et ne dépend que de la classe de similitude de u (voir proposition I.3.1 - 1ère étape). E est un $k[x]$ module en "faisant" $x=u$ et on a la suite exacte de $k[x]$-modules : $E[x]=E\otimes_k k[x] \xrightarrow{\varphi} E[x] \xrightarrow{\psi} E\longrightarrow 0$ en posant : $\varphi(\sum m_j x^j)=\sum u(m_j)x^j - m_j x^{j+1}$ et $\psi(\sum m_i x^i)=\sum u^i(m_i)$.

Il résulte de § II.3 que $E\approx \bigoplus_{j=1}^{\hat{n}} \frac{k[x]}{(\alpha_j(x))}$ comme $k[x]$-module où $\alpha_1\cdots\alpha_j=d_j$.

Dans la base correspondante à la base canonique, la matrice de u est la matrice de blocs diagonaux = {matrice compagnon de α_j}$_{j=1\cdots n}$

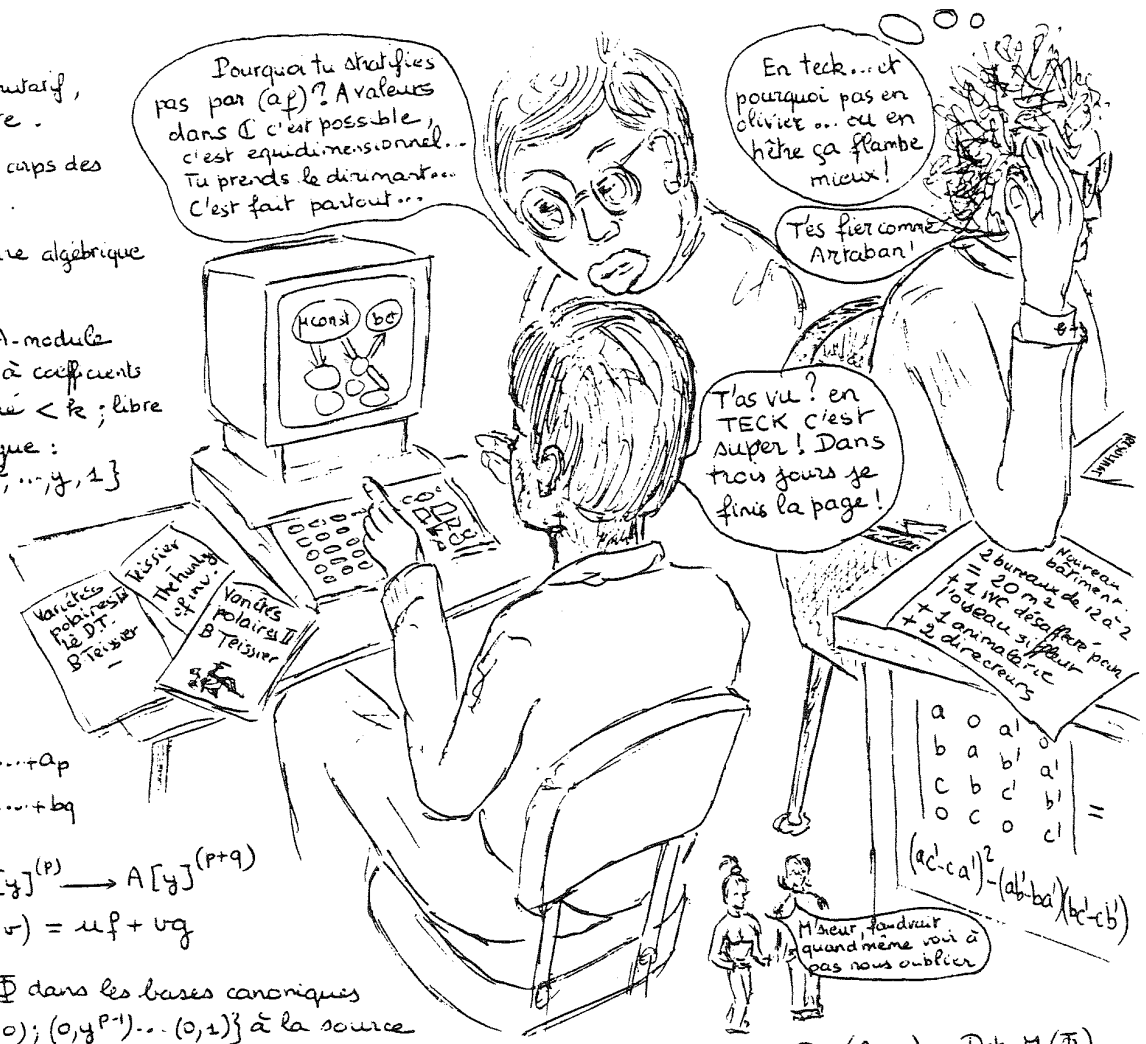
On peut conclure : deux endomorphismes sont semblables si et seulement si ils ont la même suite d'invariants $(d_1,d_2,\cdots,d_n)$ dans $k[x]$

Je leur fourre ici ce complément pour l'agreg. uniquement pour terminer la page. On va bien voir s'ils s'aperçoivent de quelque chose.

Source : R. GODEMENT - Cours d'Algèbre - Hermann - Paris - 1963 - Exercice p 629 ex 10

§III.5 : Le résultant de deux polynômes

Comme ce paragraphe n'a pas grand-chose à voir avec ce qui précède, je leur fais un dessin qui n'a rien à voir avec le contexte : "LA VIE DE CHATEAU"



A : anneau commutatif, unitaire, intègre.

$K = \mathrm{Frac}(A)$ le corps des fractions de A.

Ω = une clôture algébrique de K.

$A[y]^{(k)}$ = le A-module des polynômes à coefficients dans A de degré $< k$; libre de base canonique : $\{y^{k-1}, y^{k-2}, \dots, y, 1\}$

$f = a_0 y^p + a_1 y^{p-1} + \dots + a_p$

$g = b_0 y^q + b_1 y^{q-1} + \dots + b_q$

$$\Phi : A[y]^{(q)} \times A[y]^{(p)} \longrightarrow A[y]^{(p+q)}$$
$$\Phi(u,v) = uf + vg$$

La matrice de Φ dans les bases canoniques $\{(y^{q-1},0) \dots (1,0); (0,y^{p-1}) \dots (0,1)\}$ à la source et $(y^{p+q-1}, \dots, 1)$ à l'arrivée est :

$$M(\Phi) = \begin{pmatrix} a_0 & & & b_0 & & \\ a_1 & a_0 & & b_1 & \ddots & \\ \vdots & \ddots & a_0 & \vdots & \ddots & b_0 \\ a_p & \ddots & a_1 & b_q & \ddots & b_1 \\ & \ddots & \vdots & & \ddots & \vdots \\ & & a_p & & & b_q \end{pmatrix}$$

Par définition : $\mathrm{Res}(f,g) = \mathrm{Det}\, M(\Phi)$

Propriétés du résultant :

(a) $\mathrm{Res}(g,f) = (-1)^{pq}\, \mathrm{Res}(f,g)$

(b) $\mathrm{Res}(f,g) \in A \subset K \subset \Omega$ ne change pas lorsque f et g sont considérés comme des polynômes à coefficients dans A, K, Ω (renseigner par K et par Ω).

(c) Φ injective $\Leftrightarrow \mathrm{Res}(f,g) \neq 0 \Leftrightarrow (f,g)$ premiers entre eux dans $K[y]$ $\Leftrightarrow (f,g)$ sans racine commune dans Ω.

(d) $\mathrm{Res}(f,g)$ appartient à l'idéal de $A[y]$ engendré par f et g.

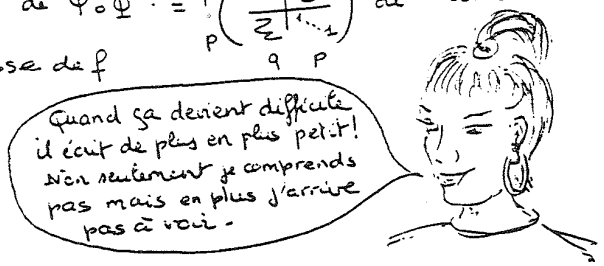
$$ {}^t M(\Phi)^* \cdot M(\Phi) = \mathrm{Res}(f,g)\, I $$

où ${}^t M(\Phi)^*$ est la transposée de la matrice des cofacteurs de $M(\Phi)$

(e) Si g est un polynôme unitaire ($b_0 = 1$) et $\mathrm{Res}(f,g) \neq 0$, on a la suite exacte : $0 \longrightarrow A^{p+q} \xrightarrow{\Phi} A^{p+q} \longrightarrow \frac{A[y]}{(f,g)} \longrightarrow 0$ résolution libre du A-module $\frac{A[y]}{(f,g)}$. A utiliser en particulier lorsque A est principal.

(f) On suppose g unitaire ; $B = \frac{A[y]}{(g)}$ est un A-module libre de rang q (par division euclidienne). Alors $(-1)^{pq}\,\mathrm{Res}(f,g)$ est égal au déterminant de la multiplication dans B par la classe de f.

Preuve : considérer $\Psi : A[y]^{p+q} \longrightarrow A[y]^q \times A[y]^p$ qui à h associe le couple formé par son reste et son quotient par g. La matrice de Ψ dans les bases canoniques est $M(\Psi) = {}^{q}_{p}\left(\begin{array}{c|c} \Sigma & * \\ \hline 0 & \Sigma \end{array}\right)$ et la matrice de $\Psi \circ \Phi = {}^{q}_{p}\left(\begin{array}{c|c} N & C \\ \hline \Sigma & * \end{array}\right)$ où N est la matrice de la multiplication dans B par la classe de f (dans la base canonique de B).



(g) $\mathrm{Res}(f_1 f_2, g) = \mathrm{Res}(f_1, g)\cdot \mathrm{Res}(f_2, g)$

(h) $f = a_0 \prod_{i=1}^{p} (y - \xi_i) \qquad g = b_0 \prod_{j=1}^{q} (y - \eta_j)$ dans Ω.

$$\mathrm{Res}(f,g) = a_0^q \prod_{i=1}^{p} g(\xi_i) = a_0^q\, b_0^p \prod_{i=1}^{p}\prod_{j=1}^{q} (\xi_i - \eta_j)$$

(i) Si l'on accorde à a_i (resp. b_j) le poids i (resp. j) le résultant des polynômes unitaires $f = y^p + a_1 y^{p-1} + \dots + a_p$ et $g = y^q + b_1 y^{q-1} + \dots + b_q$ est un polynôme quasi-homogène par rapport aux variables (a_i) et (b_j) de poids total pq.

Discriminant d'un polynôme

Traduire toute les propriétés du resultant dans le cas particulier $\mathrm{Res}(f, f')$. On prend :

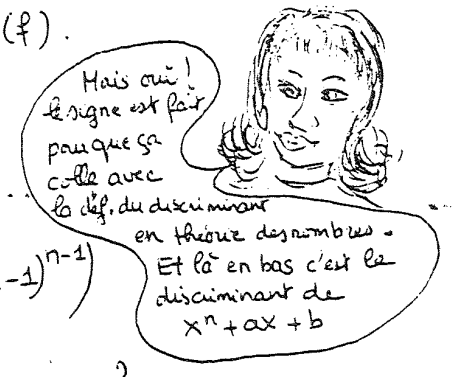
$$\boxed{\mathrm{Disc}(f) = \prod_{1 \leq i < j \leq p} (\xi_i - \xi_j)^2}$$

On a en particulier : $\prod_{i=1}^{p} f'(\xi_i) = (-1)^{\frac{p(p-1)}{2}}\,\mathrm{Disc}(f)$.

$b^2 - 4ac$

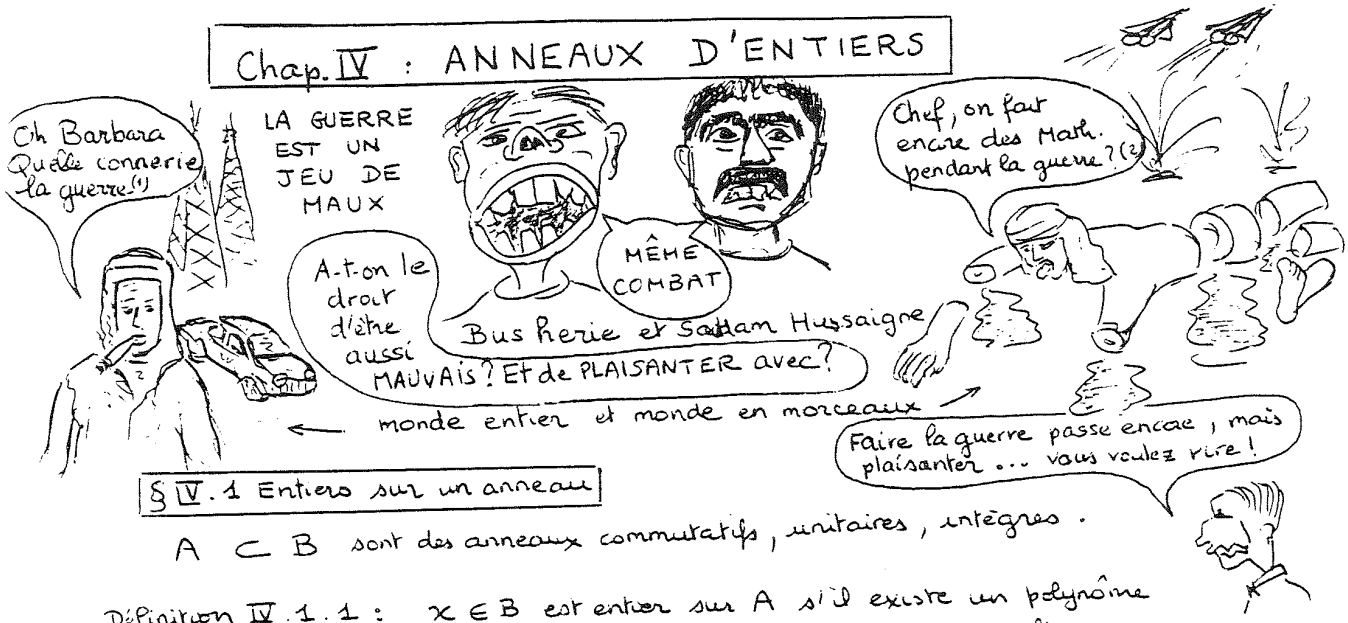
$-(4p^3 + 27q^2)$

$(-1)^{\frac{n(n-1)}{2}} \left(n^n b^{n-1} + (-1)^{n-1} a^n (n-1)^{n-1}\right)$



et pour $f = X^{p-1} + X^{p-2} + \dots + 1$ avec p premier ?

Chap. IV : ANNEAUX D'ENTIERS



§ IV.1 Entiers sur un anneau

$A \subset B$ sont des anneaux commutatifs, unitaires, intègres.

Définition IV.1.1 : $x \in B$ est entier sur A s'il existe un polynôme unitaire $P(X) \in A[X]$ tel que $P(x) = 0$. $P(X) = 0$ s'appelle une équation de dépendance intégrale de x sur A ; et le polynôme unitaire de plus petit degré qui annule x s'appelle le polynôme minimal de x sur A - lorsqu'il est unique (par exemple pour A factoriel) (4) -

Remarque IV.1.2 : le polynôme minimal P de x sur A est irréductible dans $A[X]$. Si l'on suppose de plus que A est factoriel, il résulte du lemme II.1.6 que P est irréductible dans $K[X]$ où K est le corps des fractions de A.

J'ouvre une parenthèse qui pourra faire l'objet d'un exercice : (si le polynôme minimal de x est $P(X) = X^n + a_1 X^{n-1} + \dots + a_n$, si B est fini sur A, et si $\sqrt{B \cdot x}$ est un idéal premier, D. Mumford (3) montre que $\sqrt{B \cdot x} \cap A = \sqrt{(a_n)}$ - page 60 - Il utilise que P est irréductible dans $K[X]$ - pour lui $A = k[z_1, \dots, z_p]$ - mais donne une démonstration de ce fait en raisonnant sur les conjugués de x dans une extension normale de $\mathrm{Frac}(B)$, qui semble marcher avec la seule hypothèse A normal.

Voir § IV.4.

(1) J. Prévert - PAROLES.

(2) La légende veut que J Leray ait inventé la théorie des FAISCEAUX dans un camp de prisonnier en Autriche.

(3) D. Mumford - The Red Book -

(4) Ex : $\mathbb{C}[t^{10}, t^6] \subset \mathbb{C}[t^{10}, t^6, t^{15}] \subset \mathbb{C}[t]$

Lemme IV.1.3 : soit $x \in B$; les conditions suivantes sont équivalentes :

(i) x est entier sur A

(ii) $A[x]$ est un A-module de type fini.

(iii) Il existe un sous A-module M de type fini de A tel que $xM \subset M$.

Preuve : seul point non évident : (iii) $\Rightarrow$ (i). Soit $(e_i)_{1 \le i \le p}$ un système de générateurs de M sur A, $xe_i = \sum_{j=1}^{p} \lambda_{ij} e_j$, Λ la matrice $(\lambda_{ij}) \in \mathcal{M}_p(A)$

Dans B^p on a : $\Lambda \begin{pmatrix} e_1 \\ \vdots \\ e_p \end{pmatrix} = \begin{pmatrix} xe_1 \\ \vdots \\ xe_p \end{pmatrix}$ donc $(xI - \Lambda) \begin{pmatrix} e_1 \\ \vdots \\ e_p \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$; et en multipliant par la matrice des cofacteurs transposée : $\mathrm{Det}(xI - \Lambda) \begin{pmatrix} e_1 \\ \vdots \\ e_p \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$.

Comme B est intègre et M non nul, $\mathrm{Det}(xI - \Lambda) = 0$ et, miracle, c'est une équation de dépendance intégrale de x sur A.

Proposition IV.1.4 :

L'ensemble $\overline{A}$ des éléments de B entiers sur A forment un anneau appelé la fermeture intégrale de A dans B.

Soit x_1 et x_2 deux éléments de $\overline{A}$ de polynôme minimal P_1 et P_2 de degré respectivement d_1 et d_2. Par division euclidienne, il est clair que le A-module $A[x_1, x_2]$ est de type fini engendré par les monômes $x_1^{i_1} x_2^{i_2}$: $0 \le i_1 \le d_1 - 1$ $0 \le i_2 \le d_2 - 1$. On peut donc appliquer le lemme et en déduire que $x_1 + x_2$ et $x_1 x_2$ sont entiers.

Pourquoi faire simple lorsqu'on peut faire compliqué ? ... parce que ça peut rapporter gros ! Par exemple si $s = x_1 + x_2$, il s'agit "d'éliminer" x_1 entre $P_1(x_1)$ et $P_2(s - x_1)$ ... et le résultant de ces deux polynômes en x_1 fournit une équation de dépendance intégrale de s sur A. La preuve ? Vous n'avez qu'à le faire avec $A = \mathbb{Z}$, $B = \mathbb{R}$, $x_1 = \sqrt[3]{2}$, $x_2 = \sqrt{3}$.

Proposition IV.1.5 : $\overline{\overline{A}} = \overline{A}$

Si $y \in \overline{\overline{A}}$, il vérifie l'équation de dépendance intégrale $y^d + b_1 y^{d-1} + \dots + b_d = 0$ où $b_1, \dots, b_d$ sont dans $\overline{A}$; donc $A[y, b_1, \dots, b_d]$ est un A-module de type fini stable par multiplication par y : $y \in \overline{A}$.

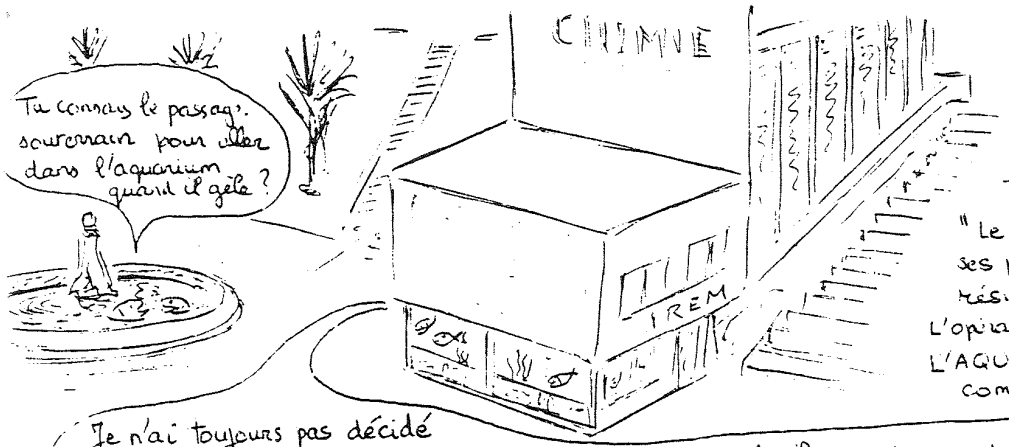
Definition IV.1.6 : Un anneau A est intégralement clos dans B si $\overline{A} = B$.

Un anneau A est NORMAL s'il est intégralement clos dans son corps de fractions.

(*) le Burkina Faso

Proposition IV.1.7 : Un anneau factoriel est NORMAL

Preuve : pas la place ...



De notre correspondant de guerre en direct de Valrose
Vendredi 1er Février 91
"Le capitaine bombarde ses propres troupes qui résistent vaillamment ! L'opération TEMPÊTE DANS L'AQUARIUM vient de commencer .."

Je n'ai toujours pas décidé d'orienter le cours vers la géométrie algébrique ou la théorie des nombres ... Vous préférez la théorie des nombres ? ... Bon ! Alors on fera peut être les deux ... Je vais commencer par un truc VACHEMENT INTERESSANT orienté plutôt vers la géométrie ...

§ IV.2 - Le lemme de normalisation de Noether et le "going-up théorem" de Cohen - Seidenberg.

Pour ce paragraphe, je me suis inspiré de D. Humford - The red-book - page 3 et 4 - qui s'était lui même inspiré de Nagata qui s'était lui même inspiré de ... Bref ! si quelque chose vous embête allez consulter M.P. Malliavin - Algèbre commutative - Masson - 1985 chap. 5 - § 5 -

C'est quand même complètement idiot de recopier les bouquins à la main alors qu'on a des photo-copieurs ... Jospinque et et Rantanplan ont raison : remplaçons les prof. par des méthodes audio-visuelles ...

IV.2.1 Lemme de normalisation de Noether :

Soit B une k-algèbre de type fini de degré de transcendance n sur k, intègre. Il existe $(x_1, \cdots x_n)$ de B algébriquement indépendants sur k tels que B soit fini sur $A = k[x_1, \cdots, x_n]$.

Preuve : $B = k[Y_1, \cdots, Y_m]/I$ où I est un idéal premier - Si $m=n$, les images de $Y_1, \cdots Y_n$ sont algébriquement indépendantes et donc $I=0$, $A=B$. Si $m>n$, les générateurs $(y_1, \cdots y_m)$ ($de\ B$ comme k-algèbre) sont algébriquement dépendants = il existe un polynôme non nul $f \in k[Y_1, \cdots, Y_m]$ tel que $f(y_1 \cdots, y_m) = 0$. Soit $r_2, \cdots, r_m$ des entiers positifs, $z_2 = y_2 - y_1^{r_2}$, $\cdots$ $z_m = y_m - y_1^{r_m}$; $(y_1, z_2 \cdots z_m)$ sont racines du polynôme $f(Y_1, Z_2 + Y_1^{r_2}, \cdots, Z_m + Y_1^{r_m})$ et un moment de réflexion (SIC) permet au lecteur de se convaincre que pour $r_2 \ll r_3 \ll r_m$ assez grand, bien choisis on a affaire à un polynôme unitaire en Y_1, et qu'alors B est fini sur $k[z_2, \cdots z_m]$ ... la récurrence s'impose ■

Remarquons que si le corps est de caractéristique 0, un changement linéaire générique de coordonnées convient, ce qui fournit une interprétation géométrique plus agréable.

(*) PÉTILLON : Jack Palmer - UN DETECTIVE DANS LE YUCCA.

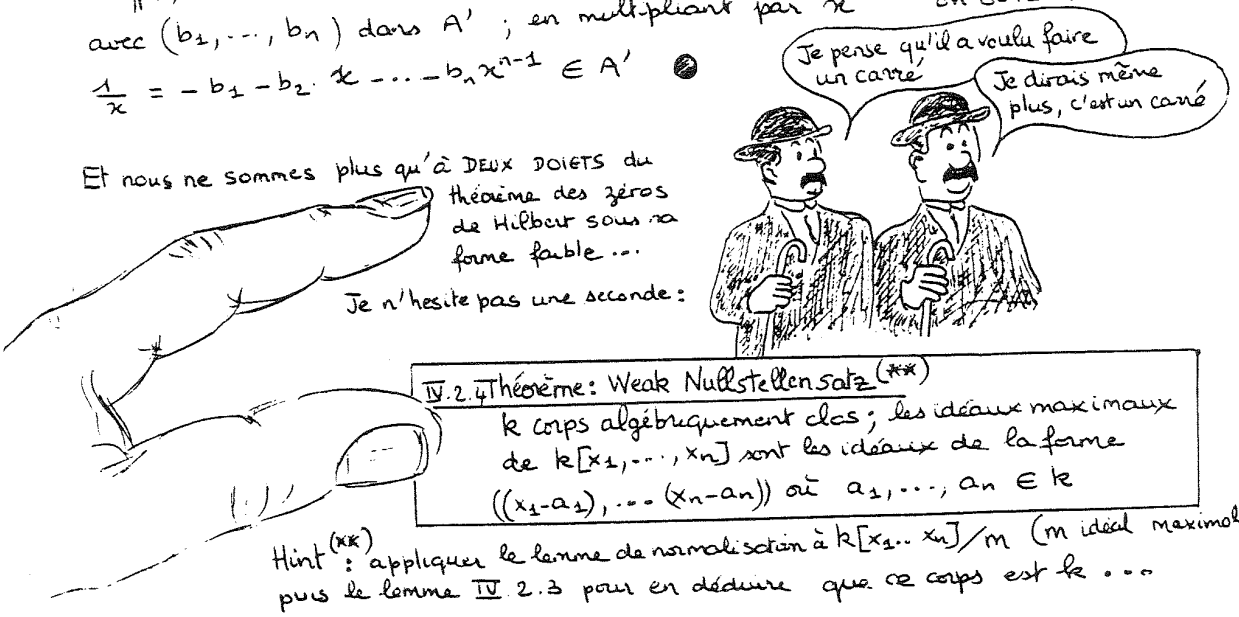
IV.2.2 - Going-up théoum of Cohen-Seidenberg

Soit $A \subset B$ deux anneaux (commutatifs, unitaires, intègres), B entier sur A ; pour tout idéal premier I de A, il existe J idéal premier de B tel que $J \cap A = I$.

B entier sur A signifie : $\forall x \in B$ entier sur A.
Preuve : on localise par rapport à la partie multiplicative $S = A - I$ (voir page 19) et on se ramène ainsi à la situation où A est local et I est son idéal maximal. Soit alors J un idéal maximal de B ; on a bien sûr $A \cap J \subset I$ et $\frac{A}{A\cap J} \subset \frac{B}{J}$ avec $\frac{B}{J}$ entier sur $\frac{A}{A\cap J}$. Pour montrer le théorème il suffit de prouver que $A \cap J$ est maximal, c'est à dire $\frac{A}{A\cap J}$ est un corps (d'où $A \cap J = I$), ce qui résulte du lemme :

lemme IV.2.3 : $A' \subset B'$, B' corps entier sur A' $\Rightarrow$ A' est un corps.

En effet, si $x \in A'$, $\frac{1}{x} \in B'$ et vérifie l'équation : $\left(\frac{1}{x}\right)^n + b_1\left(\frac{1}{x}\right)^{n-1} + \dots + b_n = 0$ avec $(b_1, \dots, b_n)$ dans A' ; en multipliant par x^{n-1} on obtient $\frac{1}{x} = -b_1 - b_2 x - \dots - b_n x^{n-1} \in A'$ ●



IV.2.4 Théorème : Weak Nullstellensatz (**)

k corps algébriquement clos ; les idéaux maximaux de $k[x_1, \dots, x_n]$ sont les idéaux de la forme $((x_1 - a_1), \dots (x_n - a_n))$ où $a_1, \dots, a_n \in k$

Hint (**) : appliquer le lemme de normalisation à $k[x_1 \dots x_n]/m$ (m idéal maximal) puis le lemme IV.2.3 pour en déduire que ce corps est k ...

(*) En l'honneur de Michel ... qui me l'a soufflé et de Philippe ... qui ne sait pas l'écrire.

(**) Pour la signification de ces signes, voir le grand chef INCA.

§ IV.3 Extensions algébriques

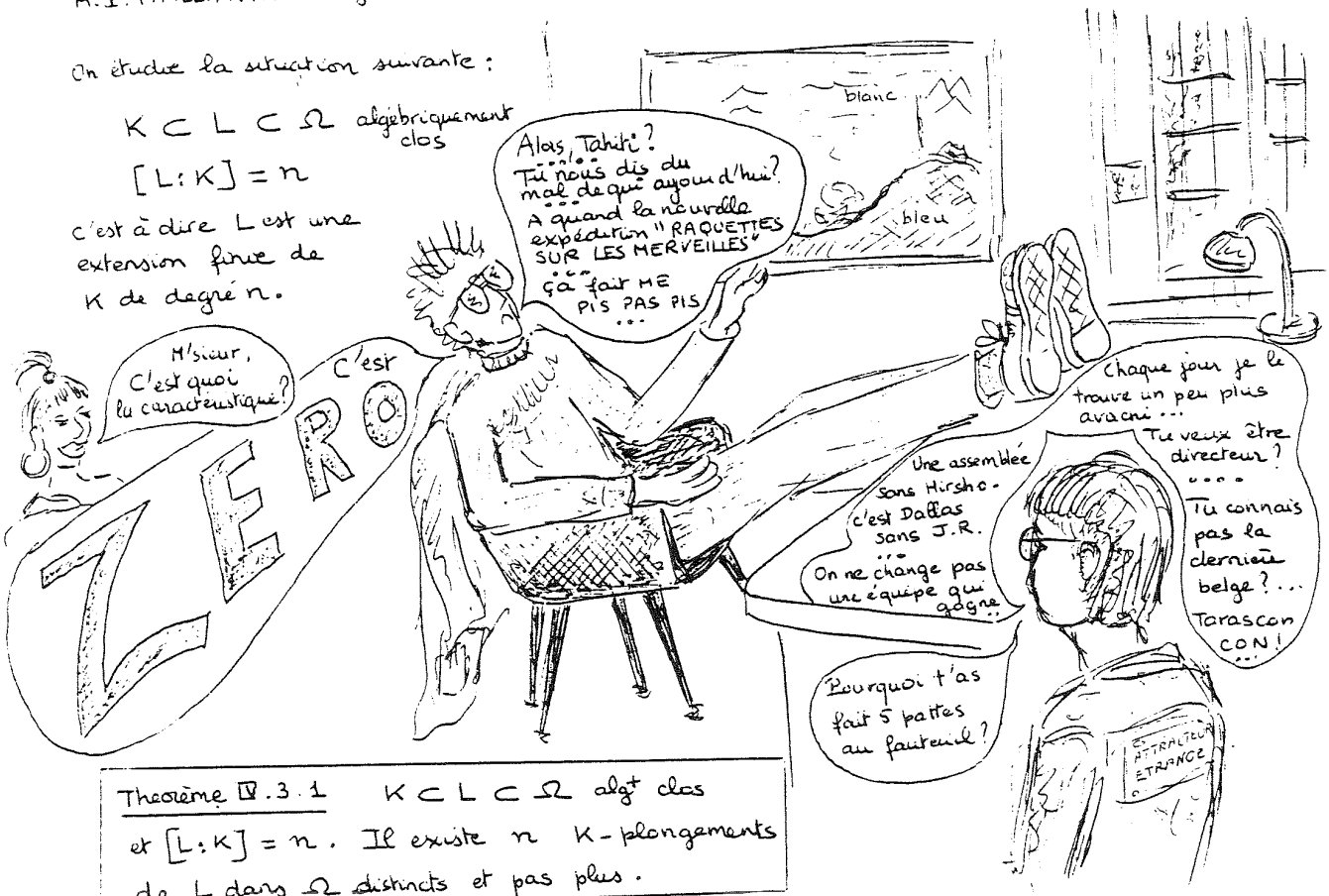
Je me place délibérément dans le cas des corps de <u>caractéristique 0</u> ; en cas de caractéristique non nulle, et de toutes façons, pour en savoir plus, consulter M.P. MALLIAVIN - Algèbre Commutative - chap 6 et 7.

On étudie la situation suivante :

$K \subset L \subset \Omega$ algébriquement clos

$[L:K] = n$

c'est à dire L est une extension finie de K de degré n.



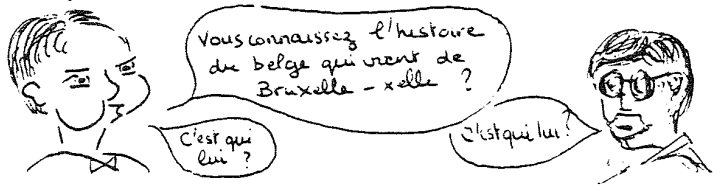
Théorème IV.3.1 $K \subset L \subset \Omega$ alg^t clos et $[L:K] = n$. Il existe n K-plongements de L dans Ω distincts et pas plus.

Preuve : on fait une récurrence sur n ; pour $n \geq 2$, soit $\alpha \in L - K$, f le polynôme minimal de α sur K ; pour toute racine β de f dans Ω, on a un isomorphisme :

$$\frac{K[x]}{(f)} \xrightarrow{\sim} K[\alpha] \xrightarrow{\sim} K[\beta]$$

d'où un K-plongement de $K[\alpha]$ dans Ω d'image $K[\beta]$. Comme f admet d racines distinctes ($d = [K[\alpha]:K]$) dans Ω, on obtient d K-plongements distincts de $K[\alpha]$ dans Ω (nécessairement, puisque f est à coefficients dans K, un K plongement envoie α sur un de ses conjugués). Remarquez que si la caractéristique est non nulle, on doit ici supposer que l'extension L est SEPARABLE, c'est à dire que le polynôme minimal de chaque élément de L n'a que des racines distinctes dans Ω. Or $[L:K[\alpha]] = n/d < n$ et on applique l'hypothèse de récurrence. Pour que la récurrence soit bien correcte j'aurais du énoncer : tout plongement σ d'un corps K dans Ω se prolonge par n plongements de L dans Ω (si L est une extension de K de degré n) ... Je ne vais pas recommencer pour si peu !

Ex : $\mathbb{Q} \subset \mathbb{Q}[\sqrt[3]{2}+\sqrt{3}] \subset \mathbb{C}$.



Corollaire IV.3.2 (Théorème de l'élément primitif) :

Soit L une extension finie de K ; $\exists\, \omega \in L$ tel que $L = K[\omega]$
$car(K) = 0$

Par récurrence sur $n = [L:K]$ on se ramène à $L = K[\alpha, \beta]$ pour α et β dans $L - K$.
Soit $\lambda \in K$; si $K[\alpha + \lambda\beta] \neq L$, il existe strictement moins de n K-plongements de $K[\alpha+\lambda\beta]$ dans Ω ; donc parmi les n K-plongements de L dans Ω, $(\sigma_1, \cdots, \sigma_n)$ il en existe au moins deux, σ_i et σ_j $(i \neq j)$ qui sont égaux sur $K[\alpha+\lambda\beta]$:

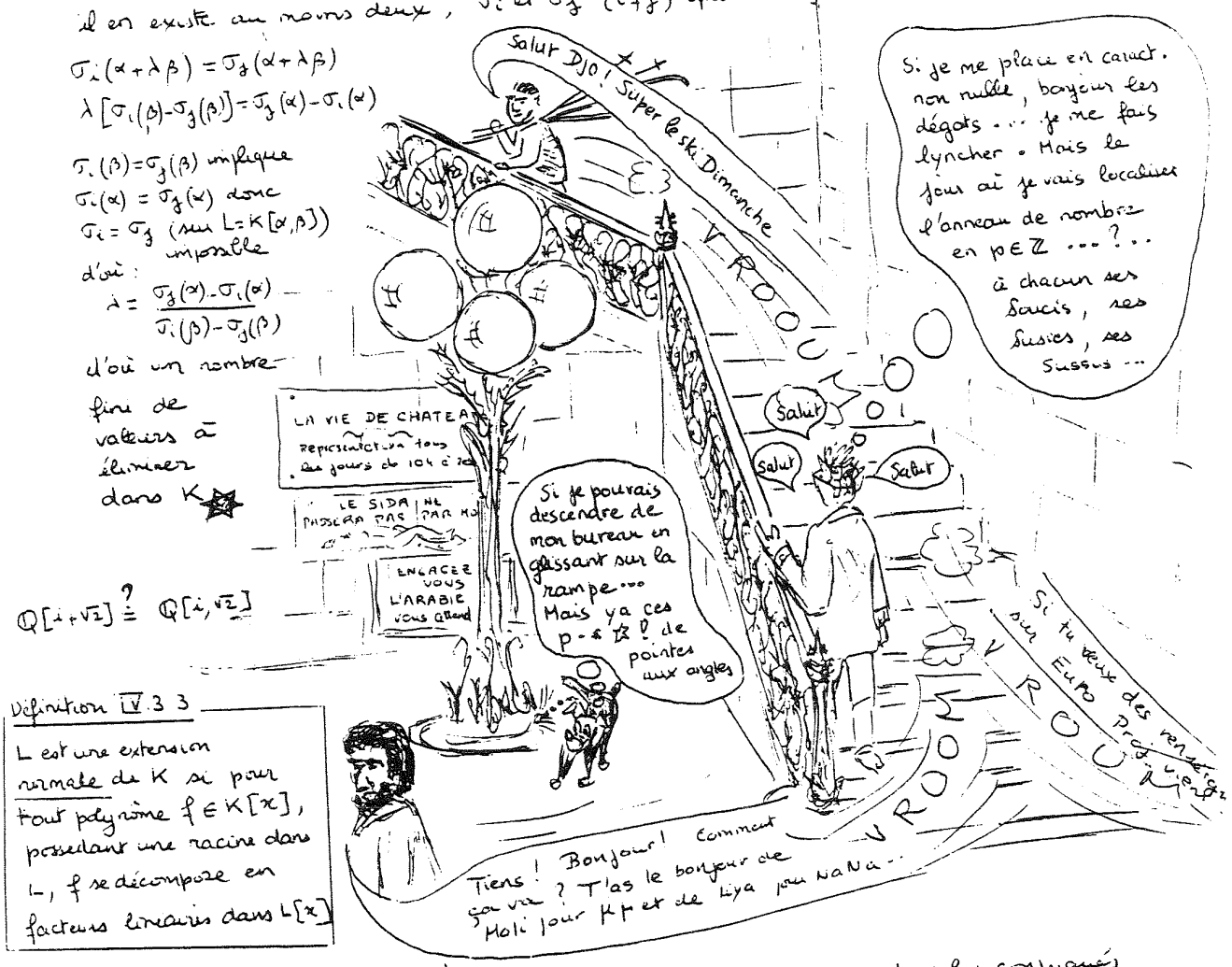
$\sigma_i(\alpha+\lambda\beta) = \sigma_j(\alpha+\lambda\beta)$
$\lambda[\sigma_i(\beta) - \sigma_j(\beta)] = \sigma_j(\alpha) - \sigma_i(\alpha)$

$\sigma_i(\beta) = \sigma_j(\beta)$ implique
$\sigma_i(\alpha) = \sigma_j(\alpha)$ donc
$\sigma_i = \sigma_j$ (sur $L = K[\alpha,\beta]$) impossible
d'où :

$$\lambda = \frac{\sigma_j(\alpha) - \sigma_i(\alpha)}{\sigma_i(\beta) - \sigma_j(\beta)}$$

d'où un nombre fini de valeurs à éliminer dans K ✡

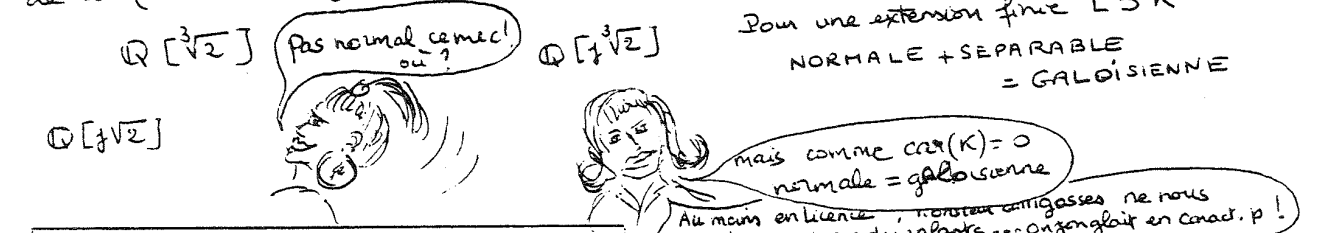
$\mathbb{Q}[i+\sqrt{2}] \overset{?}{=} \mathbb{Q}[i, \sqrt{2}]$



Définition IV.3.3

L est une extension normale de K si pour tout polynôme $f \in K[x]$, possédant une racine dans L, f se décompose en facteurs linéaires dans $L[x]$

Il revient au même de dire, pour $K \subset L \subset \Omega$, que si $\alpha \in L$, tous les conjugués de α (racines du polynôme minimal de α sur K) sont dans L.



Pour une extension finie $L \supset K$
NORMALE + SEPARABLE
= GALOISIENNE

Corollaire IV.3.4 :
$K \subset L \subset \Omega$ $\quad [L:K] = n$
Il y a équivalence entre
(i) L est une extension galoisienne de K
(ii) Tout K-plongement de L dans Ω est un automorphisme de L.
(iii) L possède n K-automorphismes

Remarque : si $L = K[\alpha]$, $\alpha = \alpha_1, \cdots, \alpha_n$ les conjugués de α sur K, alors $M = K[\alpha_1, \cdots \alpha_n]$ est une extension normale de L et de K.
(si σ est un K plongement de M, $\sigma f(\alpha_1, \cdots \alpha_n) = f(\sigma\alpha_1, \cdots \sigma\alpha_n)$ ...)

IV.35 Correspondance de Galois (Rappel)

$K \subset L$ extension galoisienne $\quad n = [L:K] = \#G \quad G = Gal(L/K)$

$\mathcal{H} = \{H / H \text{ sous groupes de } G\} \underset{\beta}{\overset{\alpha}{\rightleftarrows}} \mathcal{L} = \{M / K \subset M \subset L\}$

sous groupes de G — extensions intermédiaires

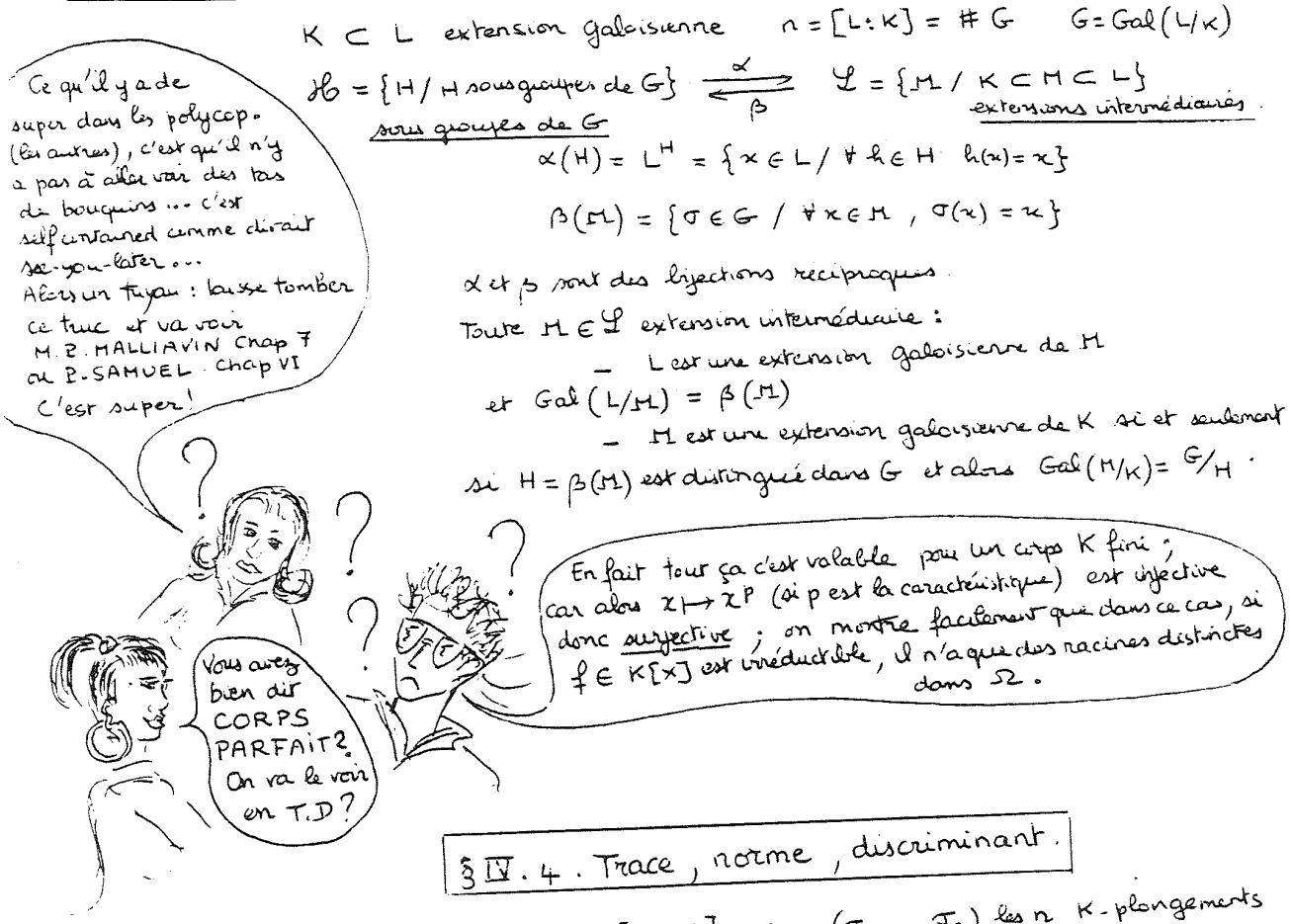
$$\alpha(H) = L^H = \{x \in L / \forall h \in H \quad h(x) = x\}$$

$$\beta(M) = \{\sigma \in G / \forall x \in M, \ \sigma(x) = x\}$$

α et β sont des bijections réciproques.

Toute $M \in \mathcal{L}$ extension intermédiaire :

- L est une extension galoisienne de M et $Gal(L/M) = \beta(M)$
- M est une extension galoisienne de K si et seulement si $H = \beta(M)$ est distingué dans G et alors $Gal(M/K) = G/H$.



§IV.4. Trace, norme, discriminant.

$K \subset L \subset \Omega \qquad [L:K] = n \qquad (\sigma_1, \dots, \sigma_n)$ les n K-plongements de L dans Ω.

Pour $\alpha \in L$ on définit et on propose :

$$\boxed{\begin{aligned} Tr_{L/K}(\alpha) &= \sigma_1(\alpha) + \dots + \sigma_n(\alpha) = \text{trace de } \alpha . 1_L \\ N_{L/K}(\alpha) &= \sigma_1(\alpha) \times \dots \times \sigma_n(\alpha) = \text{déterminant de } \alpha . 1_L \end{aligned}}$$

$\alpha . 1_L$ est l'endomorphisme K-linéaire de L = multiplication par α ; si $P = X^d + a_1 X^{d-1} + \dots + a_d$ est le polynôme minimal de α sur K, on voit que :

$$\boxed{\begin{aligned} Tr_{L/K}(\alpha) &= \frac{n}{d}(-a_1) \\ N_{L/K}(\alpha) &= \left[(-1)^d a_d\right]^{\frac{n}{d}} \end{aligned}}$$

La matrice de $\alpha . 1_{K[\alpha]}$ dans la base canonique $(1, \alpha, \dots \alpha^{d-1})$ est la matrice compagnon(*) du polynôme P. En prenant une base de L sur $K[\alpha]$ on voit alors que le polynôme minimal de $\alpha . 1_L$ est P, le polynôme caractéristique $(P)^{\frac{n}{d}}$.

Chaque K plongement de $K[\alpha]$ dans Ω qui à α associe un de ses conjugués se prolonge en $\frac{n}{d}$ K-plongement de L dans Ω : $\sigma_1(\alpha) + \dots + \sigma_n(\alpha) = \frac{n}{d} \times (-a_1) \dots$

Proposition IV.4.2

$$\begin{array}{c} A \\ \cap \\ K = \mathrm{Frac}(A) \subset L \subset \Omega \end{array}$$

si A est normal, et si $\alpha \in L$ est entier sur A, $\mathrm{Tr}_{L/K}(\alpha)$ et $N_{L/K}(\alpha) \in A$.

C'est clair, puisque les conjugués de α sont aussi entiers sur A, donc les polynômes symétriques ...

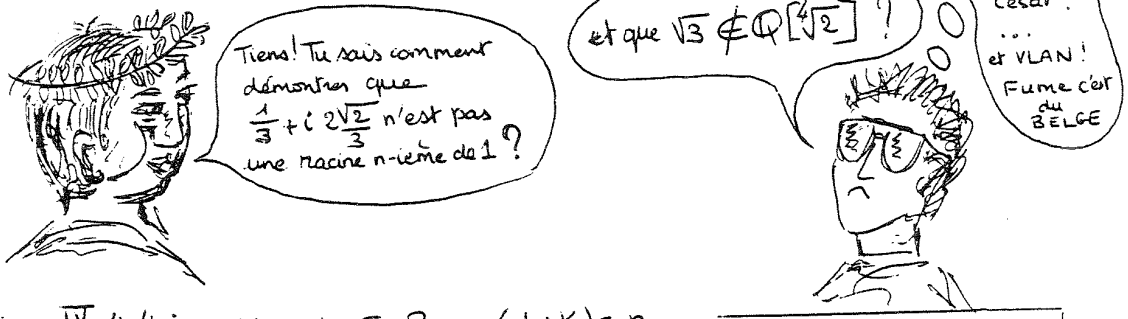
Proposition IV.4.3 (transitivité)

$K \subset L \subset M$ extensions finies ; $\alpha \in M$

$$\mathrm{Tr}_{M/K}(\alpha) = \mathrm{Tr}_{L/K}\left(\mathrm{Tr}_{M/L}(\alpha)\right) \qquad N_{M/K}(\alpha) = N_{L/K}\left(N_{M/L}(\alpha)\right)$$

Soit $(\sigma_1 \cdots \sigma_n)$ les K-plongements de L, $(\tau_1, \cdots \tau_m)$ les L plongements de M, ω un élément primitif : $M = K[\omega]$, $(\omega_1, \cdots \omega_{mn})$ les conjugués de ω, $M' = K[\omega_1, \cdots, \omega_{mn}]$ une extension galoisienne de M et de K.
Les σ_i et les τ_j se prolongent en des automorphismes de M' ce qui permet de définir mn plongements $\sigma_i \circ \tau_j$ de M dans Ω laissant fixe K = ce sont les mn plongements distincts (en effet si $\sigma_i \circ \tau_j = \sigma_{i'} \circ \tau_{j'}$, comme $\tau_j = \tau_{j'} = 1_L$ en restriction à L, $i = i'$ d'où $j = j'$). D'où

$$\mathrm{Tr}_{L/K}\left(\mathrm{Tr}_{M/L}(\alpha)\right) = \sum_{i=1}^{n} \sigma_i\left(\sum_{j=1}^{m} \tau_j(\alpha)\right) = \sum_{i,j} \sigma_i \circ \tau_j(\alpha) = \mathrm{Tr}_{M/K}(\alpha) \quad .$$



Théorème IV.4.4 : $K \subset L \subset \Omega$ $\quad (L:K) = n$

$(\alpha_1, \cdots, \alpha_n) \in L^n$; $(\sigma_1 \cdots \sigma_n)$ les n K-plongements de L dans Ω

1) $\mathrm{Disc}_{L/K}(\alpha_1, \cdots \alpha_n) := \left[\mathrm{Det}(\sigma_i(\alpha_j))\right]^2 = \mathrm{Det}\left(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j)\right) \in K$.

2) $\mathrm{Disc}_{L/K}(\alpha_1, \cdots, \alpha_n) \neq 0 \iff (\alpha_1, \cdots, \alpha_n)$ indépendants sur K.

3) Si $L = K[\omega]$, $\omega_i = \sigma_i(\omega)$ les n conjugués de ω, P le polynôme minimal de ω sur K, $\mathrm{Disc}_{L/K}(1, \omega, \cdots \omega^{n-1}) = \prod_{i<j} (\omega_i - \omega_j)^2 = (-1)^{\frac{n(n-1)}{2}} N_{L/K}(P'(\omega))$

Preuve : 1) Soit la matrice $\Lambda = (\sigma_i(\alpha_j))$; calculer ${}^t\Lambda \cdot \Lambda$.

2) Si $(\alpha_1, \cdots, \alpha_n)$ sont liés sur K, les colonnes de Λ aussi et le déterminant est nul.

Réciproquement, soit $\lambda_1 \cdots \lambda_n$ non tous nuls tels que $\lambda_1 R_1 + \cdots + \lambda_n R_n = 0$ où $R_1 \cdots R_n$ sont les colonnes de la matrice $\left(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j)\right)$ et soit $\alpha = \lambda_1 \alpha_1 \cdots + \lambda_n \alpha_n$.

On a : $\mathrm{Tr}_{L/K}(\alpha\alpha_j) = \lambda_1 \mathrm{Tr}_{L/K}(\alpha_1\alpha_j) + \cdots + \lambda_n \mathrm{Tr}_{L/K}(\alpha_n\alpha_j) = 0 \quad \forall j$.

Or si $(\alpha_1, \cdots, \alpha_n)$ étaient indépendants sur K, $L = K\alpha_1 + \cdots + K\alpha_n$,

$\alpha \neq 0$, $\frac{1}{\alpha} = \sum \rho_j \alpha_j$, $1 = \sum \rho_j \alpha \alpha_j$ $\cdots$ $\mathrm{Tr}_{L/K}(1) = n = \sum \rho_j \mathrm{Tr}_{L/K}(\alpha\alpha_j) = 0$.

3) $\mathrm{Disc}_{L/K}(1, \omega, \cdots \omega^{n-1}) = \left[\mathrm{Det}\left(\sigma_i(\omega^j)\right)\right]^2 = \left[\mathrm{Det}\left((\omega_i)^j\right)\right]^2$

déterminant de Van der Monde $\cdots$

Corollaire IV.4.5 :

$$\begin{array}{c} A \\ \cap \\ K = \mathrm{Fract}(A) \subset L \subset \Omega \end{array}$$

Si A est normal, $(\alpha_1, \cdots, \alpha_n)$ entiers sur A, $\mathrm{Disc}_{L/K}(\alpha_1, \cdots \alpha_n) \in A$.

Théorème IV.4.6 :

$$\begin{array}{ccc} A & \subset & B \\ \cap & & \cap \\ K & \subset & L \end{array}$$

A normal

B = fermeture intégrale de A dans L

$(L:K) = n$

$(\alpha_1, \cdots, \alpha_n) \in B^n$, base de L sur K ; $d = \mathrm{Disc}_{L/K}(\alpha_1 \cdots \alpha_n)$

$$A\alpha_1 \oplus \cdots \oplus A\alpha_n \subset B \subset \left\{ \frac{m_1\alpha_1 + \cdots + m_n\alpha_n}{d} \Big/ m_i^2 \in Ad \right\} \subset A\frac{\alpha_1}{d} \oplus \cdots \oplus A\frac{\alpha_n}{d}$$

Soit $\alpha \in B$; $\alpha = \sum_{i=1}^{n} x_i \alpha_i$ avec $x_i \in K$.

$$\forall j : \sigma_j(\alpha) = \sum x_i \sigma_j(\alpha_i)$$

On peut résoudre ce système par Cramer : $\delta = \mathrm{Det}(\sigma_j(\alpha_i))$ $(d = \delta^2)$

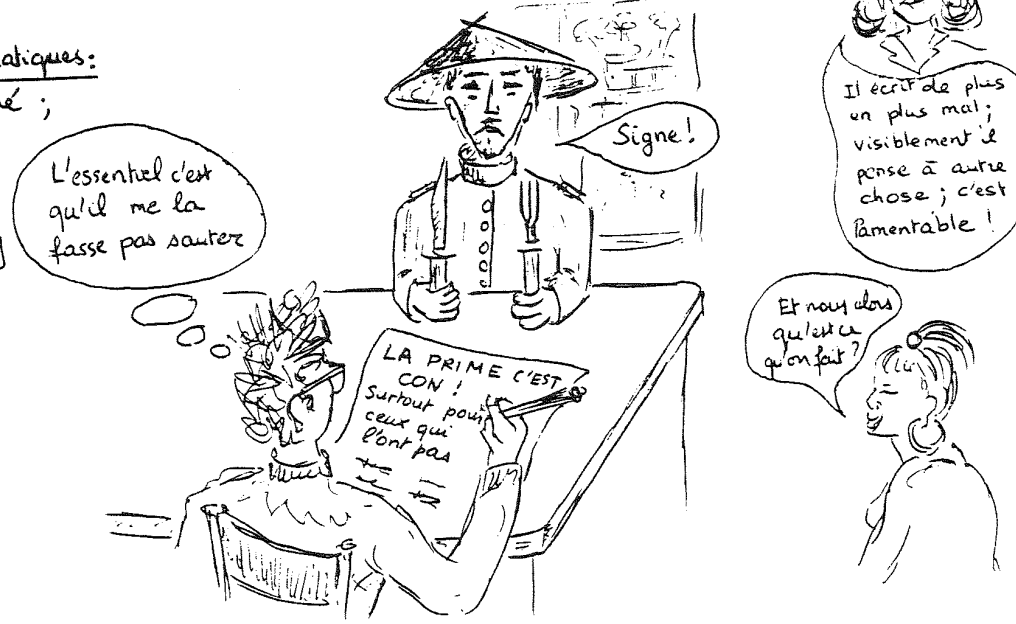
et $x_i = \frac{\gamma_i}{\delta}$ où $\gamma_i \in \overline{A}$ car il est obtenu comme développement d'un déterminant ne faisant intervenir que des $\sigma_j(\alpha)$ et $\sigma_j(\alpha_i)$ entiers sur A (dans Ω). Donc $\delta\gamma_i = x_i\delta^2$ est entier sur A (δ vérifie $\delta^2 = d \in A$), appartient à K donc à A...

D'où, si $m_i = x_i d = \delta\gamma_i \in A$, $\alpha = \frac{\sum_{i=1}^{n} m_i\alpha_i}{d}$.

De plus $\frac{m_i^2}{d} = \gamma_i^2 \in B \cap K = A$.

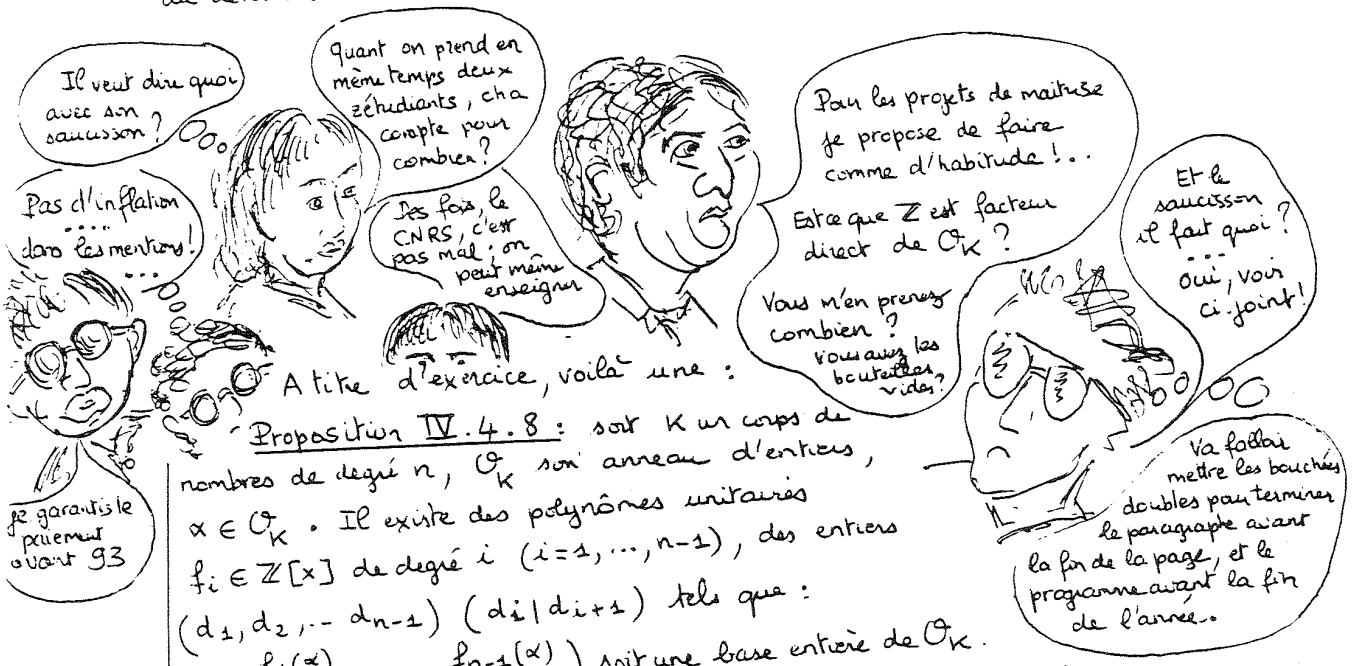
Extensions Quadratiques :

$m \in \mathbb{Z}$, sans carré ; quel est l'anneau d'entiers de $\mathbb{Q}[\sqrt{m}]$? [selon $m \equiv 1\ (4)$]



Corollaire IV.4.7 : $\mathbb{Z} \subset \mathbb{Q} \subset K$ un corps de nombres de degré n, $\mathcal{O}_K$ son anneau d'entiers ; $\mathcal{O}_K$ est un $\mathbb{Z}$ module libre de rang n.

C'est une conséquence immédiate du théorème de la fourchette puisque $A = \mathbb{Z}$ est principal ; on peut alors parler de *base entière* de $\mathcal{O}_K$: $(\beta_1, \dots \beta_n)$ base de $\mathcal{O}_K$ sur $\mathbb{Z}$, et de *discriminant absolu* $\mathrm{Disc}(\mathcal{O}_K) = \mathrm{Disc}(\beta_1 \dots \beta_n) \in \mathbb{Z}$ (un changement de base a pour effet de multiplier le discriminant par le carré du déterminant de la matrice de $GL(n,\mathbb{Z})$, donc 1 ...).



A titre d'exercice, voilà une :

Proposition IV.4.8 : soit K un corps de nombres de degré n, $\mathcal{O}_K$ son anneau d'entiers, $\alpha \in \mathcal{O}_K$. Il existe des polynômes unitaires $f_i \in \mathbb{Z}[x]$ de degré i $(i = 1, \dots, n-1)$, des entiers $(d_1, d_2, \dots d_{n-1})$ $(d_i \mid d_{i+1})$ tels que : $\left(1, \frac{f_1(\alpha)}{d_1}, \dots, \frac{f_{n-1}(\alpha)}{d_{n-1}}\right)$ soit une base entière de $\mathcal{O}_K$.

Remarque : $\mathcal{O}_K \subset \frac{1}{d}\mathbb{Z}[\alpha]$ (d discriminant $(1, \alpha, \dots \alpha^{n-1})$) et $\left(\frac{d}{d_{n-1}}, \frac{d}{d_{n-2}}, \dots, \frac{d}{d_1}, d\right)$ sont les facteurs invariants de $\mathcal{O}_K$ dans $\frac{1}{d}\mathbb{Z}[\alpha]$.

Idée : soit, pour $1 \leq k \leq n$, $R_k = \mathcal{O}_K \cap \frac{1}{d}[\mathbb{Z} \oplus \mathbb{Z}\alpha \dots \oplus \mathbb{Z}\alpha^{k-1}]$, autrement dit les éléments de $\mathcal{O}_K$ qui sont des polynômes en α de degré $< k$; $R_1 = \mathbb{Z}$, $R_n = \mathcal{O}_K$. Supposons, par récurrence, avoir trouvé une base $\left(1, \frac{f_1(\alpha)}{d_1}, \dots, \frac{f_{k-1}(\alpha)}{d_{k-1}}\right)$ de R_k ; soit Π_k la composante sur $\frac{\alpha^k}{d}$, $\beta \in R_{k+1}$ tel que $\Pi_k(\beta)$ soit un générateur de l'idéal $\Pi_k(R_{k+1})$; $p_k = \Pi_k(\beta)$ divise $d = \Pi_k(\alpha^k)$, $d_k = \frac{d}{p_k}$. On montre que $\left(1, \frac{f_1(\alpha)}{d_1}, \dots, \frac{f_{k-1}(\alpha)}{d_{k-1}}, \beta\right)$ est une base de R_{k+1} sur $\mathbb{Z}$ ... facile, et il reste à voir que β est de la forme voulue : $\frac{f_k(\alpha)}{d_k}$. Or $\alpha \cdot \frac{f_{k-1}(\alpha)}{d_{k-1}}$ est égal à $m\beta + v$ $(m \in \mathbb{Z}, v \in R_k)$, d'où $d_k = m\, d_{k-1}$ et $\beta = \frac{\alpha^k}{d_k} + \dots$ en identifiant.

Comprendre avec $\mathbb{Q}[i\sqrt{3}]$, $\mathbb{Q}[\sqrt{5}]$, $\mathbb{Q}[\sqrt[3]{10}]$ ... pour le dernier on propose $\left(1, \alpha, \frac{\alpha^2+\alpha+1}{3}\right)$ comme $\mathbb{Z}$-base de $\mathcal{O}_K$.

§ IV.5 Corps cyclotomiques

$\omega = e^{\frac{2i\pi}{m}}$

$m = 1$ ou 2 $\quad \mathbb{Q}[\omega] = \mathbb{Q}$

$m = 3$ ou 6 $\quad \mathbb{Q}[\omega] = \mathbb{Q}[e^{\frac{2i\pi}{6}}] = \mathbb{Q}[j]$

m impair, $\quad \mathbb{Q}[\omega] = \mathbb{Q}[e^{\frac{2i\pi}{2m}}]$ car $e^{\frac{2i\pi}{2m}} = -(\omega)^{\frac{m+1}{2}}$

$m = p$ premier, $\mathbb{Q}[\omega]$ de degré $p-1$. $(x^{p-1} + \dots + 1) \in \mathbb{Q}[x]$ irréductible.

Proposition IV.5.1 : $\omega = e^{\frac{2i\pi}{m}}$

Les $\{\omega^k \,/\, 1 \le k \le m,\ (k,m)=1\}$ sont les conjugués de ω et $\mathbb{Q}[\omega]$ est de degré $\varphi(m)$.

preuve : si ω' est conjugué de ω (i.e racine du polynôme minimal de ω), ω' est racine m-ième de 1 mais non racine n-ième de 1 pour $n < m$ (sinon $\omega'^n = 1$ donc $\omega^n = 1$ ce qui est faux). Donc $\omega' = \omega^k$ avec $(k,m) = 1$.

Réciproquement soit k, $1 \le k \le m$, $(k,m) = 1$ et $\theta = \omega^k$; soit f le polynôme (unitaire dans $\mathbb{Z}[x]$) minimal de θ entier : $x^m - 1 = f(x)\,g(x)$ dans $\mathbb{Z}[x]$.

Soit p premier ne divisant pas m ; si θ^p n'est pas conjugué de θ, $g(\theta^p) = 0$ et $g(x^p)$ est divisible par $f(x)$. ; on aurait alors, dans $\mathbb{F}_p[x]$, $\bar{g}(x^p) = (\bar{g}(x))^p$ et $(\bar{f}(x), \bar{g}(x))$ admettraient un facteur commun $\bar{h}$; $\bar{h}^2$ diviserait $x^m - 1$, donc $\bar{h}$ diviserait $\bar{m}\, x^{m-1}$; comme $\bar{m} \neq 0$, $\bar{h}$ serait un monôme et diviserait $x^m - 1$: absurde.

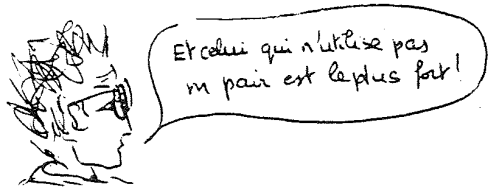
Donc θ et θ^p sont conjugués : $\omega \sim \omega^{p_1} \sim \omega^{p_1 p_2} \dots \sim \omega^k$ en prenant la décomposition de k en produit de nombres premiers.

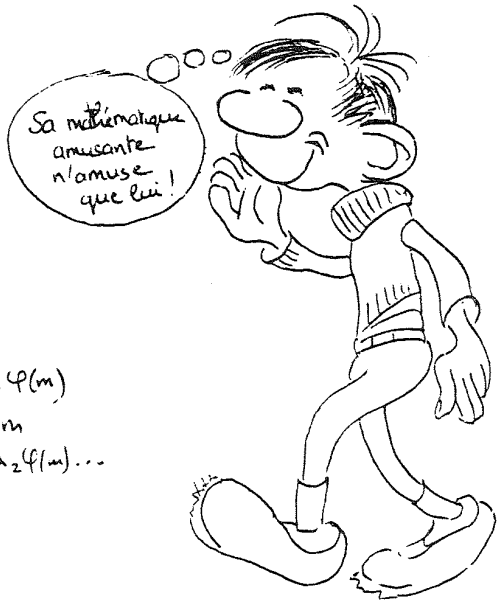
Corollaire IV.5.2 : $\mathbb{Q}[\omega]$ est une extension galoisienne de degré $\varphi(m)$ et son groupe de Galois est isomorphe au groupe multiplicatif $\left(\mathbb{Z}/m\mathbb{Z}\right)^*$

$k \in \left(\mathbb{Z}/m\mathbb{Z}\right)^*$
$\sigma_k(\omega) = \omega^k$ définit le $\mathbb{Q}$-automorphisme σ_k ...

Corollaire IV.5.3 : pour m pair, les racines de 1 dans $\mathbb{Q}[\omega]$ sont les racines m-ièmes ; et les corps cyclotomiques pour m pair sont deux à deux non isomorphes.

Soit $\theta \in \mathbb{Q}[\omega]$, $\theta^k = 1$, k ne divisant pas m ; si r est le ppcm de k et m, $\mathbb{Q}[\omega]$ contient une racine primitive r-ième de 1 (de la forme $\theta^u \omega^v$) et donc contient le r-ième corps cyclotomique ; d'où $\varphi(r) \le \varphi(m)$ ce qui est impossible sauf si $r = m$: $r = \lambda m = \lambda_1 \lambda_2 m$ avec $(\lambda_1, m) = 1$; $\varphi(r) = \varphi(\lambda_1)\,\varphi(\lambda_2 m)$ et $\varphi(\lambda_2 m) = \lambda_2 \varphi(m) \dots$





d'après Franquin
"le bureau des gaffes en gros"
GASTON $\mathbb{R}^2$

Théorème IV.5.4 Soit $\mathbb{Q}[\omega]$, $\omega = e^{\frac{2i\pi}{m}}$, un corps cyclotomique ; l'anneau de nombres correspondant est : $\mathcal{O}_{\mathbb{Q}[\omega]} = \mathbb{Z}[\omega]$.

Supposons d'abord $m = p^r$, p premier

$K = \mathbb{Q}[\omega]$, $\mathcal{O}_K \supset \mathbb{Z}[\omega] = \mathbb{Z}[1-\omega]$; $\varphi(m) = p^r\left(1-\frac{1}{p}\right)$; $\operatorname{disc}(\omega) = \operatorname{dis}(1,\omega,\dots\omega^{(\varphi(m)-1)}) = \operatorname{dis}(1-\omega)$

Lemme IV.5.5 :

$$\prod_{\substack{1\le k\le m\\ (k,m)=1}} (1-\omega^k) = p = N(1-\omega)$$

$$f(x) = \frac{x^{p^r}-1}{x^{p^{r-1}}-1} = 1 + x^{p^{r-1}} + \dots + x^{(p-1)p^{r-1}} = \prod_{\substack{1\le k\le m\\ (k,m)=1}} (x-\omega^k)$$

puisqu'il est du bon degré c'est le polynôme minimal de ω.

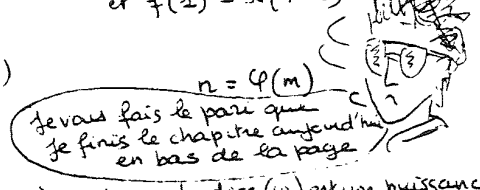
et $f(1) = N(1-\omega) = p$

$x^m - 1 = f(x)\,g(x)$ dans $\mathbb{Z}[x]$

$m\,x^{m-1} = f'(x)\,g(x) + f(x)\,g'(x)$

$m\,\omega^{m-1} = f'(\omega)\,g(\omega)$

$m = f'(\omega) \times \omega\, g(\omega)$



et en prenant la norme : $m^{\varphi(m)} = \pm \operatorname{disc}(\omega) \times N(\omega g(\omega))$; donc $d = \operatorname{disc}(\omega)$ est une puissance de p.

Supposons $\alpha \in \mathcal{O}_K$; on sait (Théorème IV.4.6) : $\alpha = \dfrac{m_1 + m_2(1-\omega) + \dots + m_n(1-\omega)^{n-1}}{d}$; $m_i \in \mathbb{Z}$.

supposons $\beta = \dfrac{m_i(1-\omega)^{i-1} + \dots + m_n(1-\omega)^{n-1}}{p} \in \mathcal{O}_K$ avec m_i non divisible par p ; alors,

d'après le lemme, p est divisible par $(1-\omega)^n$ dans $\mathbb{Z}[\omega]$ et donc $\dfrac{p}{(1-\omega)^i} \in \mathbb{Z}[\omega]$

d'où $\dfrac{p}{(1-\omega)^i}\beta = \dfrac{m_i}{1-\omega} + \dots \in \mathcal{O}_K$, d'où $\dfrac{m_i}{1-\omega} \in \mathcal{O}_K$.

On prend la norme : $N\left(\dfrac{m_i}{1-\omega}\right) = m_i^n \times \dfrac{1}{p} \in \mathbb{Z}$ impossible puisque m_i non divisible par p ...

Supposons maintenant $m = m_1 \cdot m_2 \quad (m_1, m_2) = 1$

donc en fait $K = K_1 \cdot K_2$ et $\mathbb{Z}[\omega] = \mathbb{Z}[\omega_1] \cdot \mathbb{Z}[\omega_2]$

$\omega_1 = e^{\frac{2i\pi}{m_1}} = \omega^{m_2}$ $\quad \omega_2 = e^{\frac{2i\pi}{m_2}} = \omega^{m_1}$ $\quad \omega = e^{\frac{2i\pi}{m}} = \omega_1^u \omega_2^v$

$\varphi(m) = \varphi(m_1)\,\varphi(m_2)$

Lemme IV.5.6 : soit K_1, K_2 deux corps de nombres de degré n_1 et n_2 ; on suppose $(K_1 \cdot K_2 : \mathbb{Q}) = n_1 n_2$, et $d = \operatorname{pgcd}(\operatorname{disc}(\mathcal{O}_{K_2}), \operatorname{disc}(\mathcal{O}_{K_2}))$.

Alors $\mathcal{O}_{K_1K_2} \subset \frac{1}{d}\mathcal{O}_{K_1}\mathcal{O}_{K_2}$ (et si $d=1$, $\mathcal{O}_{K_1K_2} = \mathcal{O}_{K_1} \cdot \mathcal{O}_{K_2}$).

Soit $(\alpha_1 \dots \alpha_{n_1})$ une base entière de $\mathcal{O}_{K_1}$, $(\beta_1 \dots \beta_{n_2})$ de $\mathcal{O}_{K_2}$, donc $(\alpha_i\beta_j)$ base de $\mathcal{O}_{K_1}\cdot\mathcal{O}_{K_2}$ sur $\mathbb{Z}$ et tout élément $x \in \mathcal{O}_{K_1K_2}$ s'écrit $x = \sum \frac{m_{ij}}{r}\alpha_i\beta_j$ avec les m_{ij}, r dans $\mathbb{Z}$ premiers entre eux.

Si $K_2 = \mathbb{Q}[\gamma]$, γ de degré n_2, $K_1K_2 = K_1[\gamma]$ et le polynôme minimal de γ sur $\mathbb{Q}$ est égal à son polynôme minimal sur K_1 : un plongement σ de K_1 dans $\mathbb{C}$ s'étend en un plongement laissant fixe K_2 :

$$\sigma(x) = \sum \frac{m_{ij}}{r}\sigma(\alpha_i)\beta_j = \sum_i \left(\sum_j \frac{m_{ij}}{r}\beta_j\right)\sigma(\alpha_i)$$

en faisant cela pour $\sigma = \sigma_1, \dots, \sigma_{n_1}$ et en résolvant par Cramer on trouve $\sum_j \frac{m_{ij}}{r}\beta_j = \frac{\gamma_i}{\delta}$ où $\delta^2 = \operatorname{disc}\mathcal{O}_{K_1}$ et γ_i entier algébrique.

$\operatorname{disc}(\mathcal{O}_{K_1}) \cdot \left(\sum_j \frac{m_{ij}}{r}\beta_j\right) = \delta\gamma_i \in \mathcal{O}_{K_2}$.

Comme $(\beta_1 \dots \beta_{n_2})$ est une base entière de $\mathcal{O}_{K_2}$, r divise tous les $\operatorname{disc}(\mathcal{O}_{K_1}) \times m_{ij}$ donc $\operatorname{disc}(\mathcal{O}_{K_1})$. On échange les rôles : r divise d.

Chap. V : Anneaux de DEDEKIND

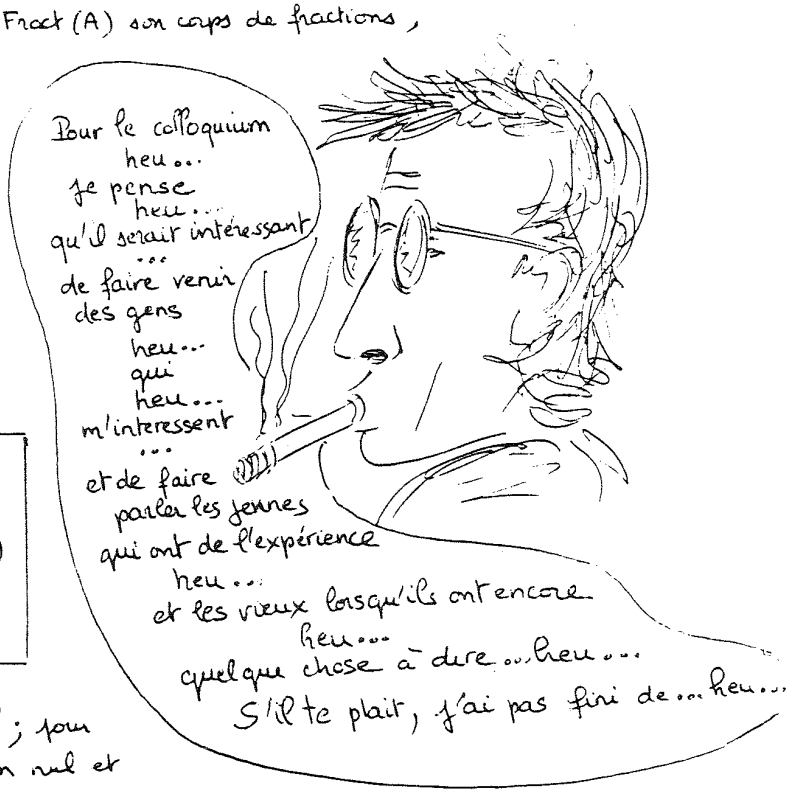
§V.1 Idéaux généralisés

A commutatif, unitaire, intègre ; $K = \mathrm{Frac}(A)$ son corps de fractions,

$\mathcal{Y} = \{ I \,/\, 0 \subsetneq I \subset K \}$
sous A-module

$\mathcal{Y}$ est muni des lois associatives :
$I+J$, $I.J$, $I \cap J$

Pour $I \in \mathcal{Y}$ on définit son transporteur dans A :
$(A:I) = \{ x \in K / xI \in A \}$
(nul ou élément de $\mathcal{Y}$).



Proposition V.1.1 : soit $I \in \mathcal{Y}$; le morphisme de A-modules :
$$\Phi : (A:I) \longrightarrow \mathrm{Hom}_A(I,A), \quad x \longmapsto x.$$
est un isomorphisme.

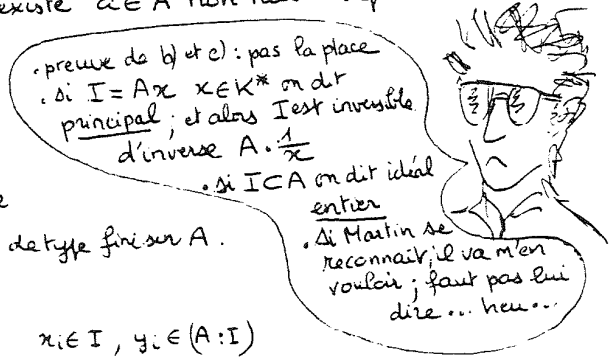
Seul point non évident : la surjectivité ; pour $\varphi \in \mathrm{Hom}_A(I,A)$ on choisit $i \in I$ non nul et on pose $x = \frac{\varphi(i)}{i}$; si $j \in I$, a un dénominateur commun de i et j,
$\varphi(ai\,j) = ai\,\varphi(j) = aj\,\varphi(i)$ d'où $\varphi(j) = \frac{\varphi(i)}{i} \cdot j$.

Définition . Proposition V.1.2 : on dit que $I \in \mathcal{Y}$ est inversible s'il existe $J \in \mathcal{Y}$ tel que $I.J = A$. Pour $I \in \mathcal{Y}$, I inversible $\iff (A:I)\,I = A$.

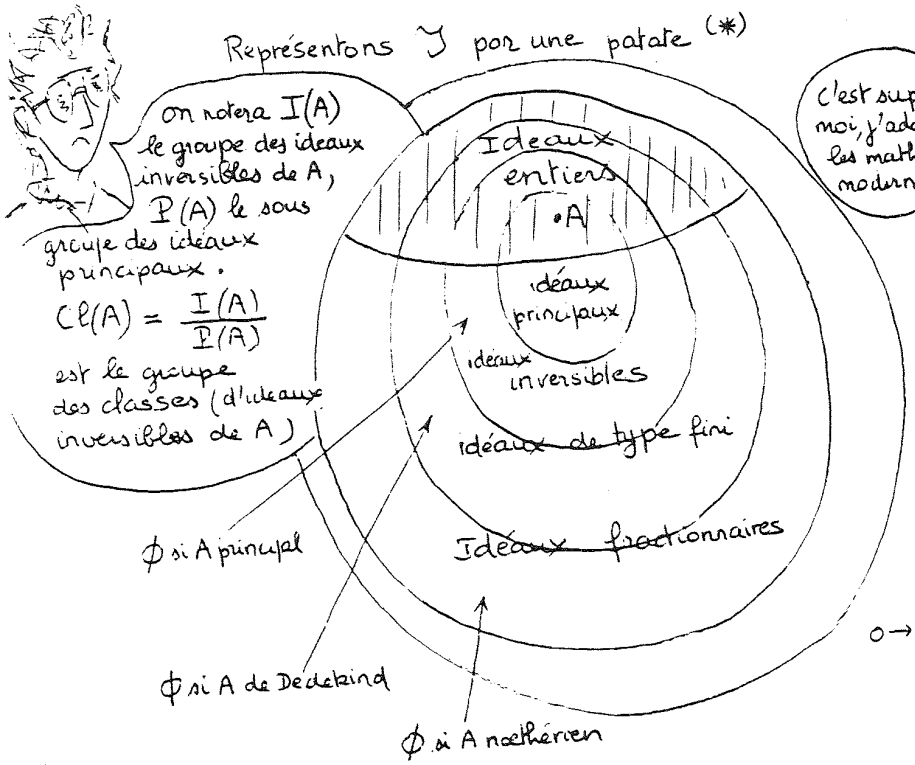
(si $J.I = A$, $J \subset (A:I)$ par définition ; et comme $I.(A:I) \subset A$, $J\,I.(A:I) = (A:I) \subset J$).

Définition V.1.3 : I est fractionnaire s'il existe $a \in A$ non nul tel que $aI \subset A$
autrement dit $(A:I) \neq 0$.

Proposition V.1.4 : Soit $I \in \mathcal{Y}$
a) I inversible $\Rightarrow$ I de type fini sur A
b) I de type fini sur A $\Rightarrow$ I fractionnaire
c) si A est noethérien, I fractionnaire $\Leftrightarrow$ de type fini sur A.



preuve de a) : $I.J = A$ implique $1 = \sum_{i=1}^{n} x_i y_i$ $x_i \in I$, $y_i \in (A:I)$
et $\forall x \in I$ s'écrit $x = \sum_{i=1}^{n} (x.y_i)\,x_i$ et les x_i engendrent I sur A.



$$0 \to P(A) \longrightarrow I(A) \longrightarrow Cl(A) \to 0$$
$$0 \to A^* \longrightarrow K^* \longrightarrow P(A) \to 0$$
$$0 \to A^* \longrightarrow K^* \longrightarrow I(A) \longrightarrow Cl(A) \to 0$$

Définition - proposition V.1.5 : un A-module P est projectif s'il satisfait à l'une des propriétés équivalentes suivantes :

(i) Il existe un A-module N tel que $P \oplus N$ soit libre

(ii) Tout morphisme surjectif $\pi : V \longrightarrow P$ possède une section

(iii) Il existe une famille $(x_\lambda)_{\lambda \in \Lambda}$ d'éléments de P, une famille $(f_\lambda)_{\lambda \in \Lambda}$ d'éléments de P^* (dual de P) telles que : $\forall y \in P$, $f_\lambda(y)$ est nul pour presque tout $\lambda \in \Lambda$ et $y = \sum_{\lambda \in \Lambda} f_\lambda(y)\, x_\lambda$.

Proposition V.1.6 :
Un module projectif est plat.

exercice : trouver un plat non projectif, un projectif non libre ... Penser à $\mathbb{Q}$ sur $\mathbb{Z}$ et à ... ce qu'on va voir à la page suivante.

(*) La plupart des bonnes idées de ce chapitre proviennent du cours de G. Elencwajg (année 87-88) ; pour les références et pour les plaintes, s'adresser à lui : Tel 93 52 98 38

(**) illisible

Lemme V.1.7 : soit M un A-module projectif de type fini et de rang 1 ; il est isomorphe à un idéal fractionnaire inversible I de A.

Preuve : comme M est de rang 1, $M \otimes_A K \xrightarrow{\sim} K$. ($rg(M) = \dim_K(M \otimes_A K)$)
comme M est projectif : $M \simeq M \otimes_A A \hookrightarrow M \otimes_A K$
en composant on obtient $f : M \hookrightarrow K$ et M est isomorphe à $f(M) = I$.
On applique alors :

Sous lemme V.1.8 : $I \in \mathcal{Y}$; I projectif $\Leftrightarrow$ I inversible.

Supposons I projectif ; $((x_\lambda),(\xi_\lambda))_{\lambda \in \Lambda}$ vérifiant la condition (iii) de V.1.5. ;
d'après V.1.1, $\xi_\lambda = y_\lambda \cdot$ pour $y_\lambda \in (A:I)$ et $y \in I$ s'écrit $y = \sum \xi_\lambda(y) x_\lambda = \sum y_\lambda y x_\lambda$
avec $(y_\lambda y)$ presque tous nuls ; en simplifiant par y non nul : $1 = \sum y_\lambda x_\lambda$ et $I.(A:I) = A$.
Réciproquement : $(A:I)I = A$ et $1 = \sum_{\lambda=1}^{k} y_\lambda x_\lambda$ avec $y_\lambda \in (A:I)$, somme finie ; de manière évidente $(\xi_\lambda = y_\lambda \cdot , x_\lambda)_{\lambda = 1 \dots k}$ forme une pseudo-bi-base finie.

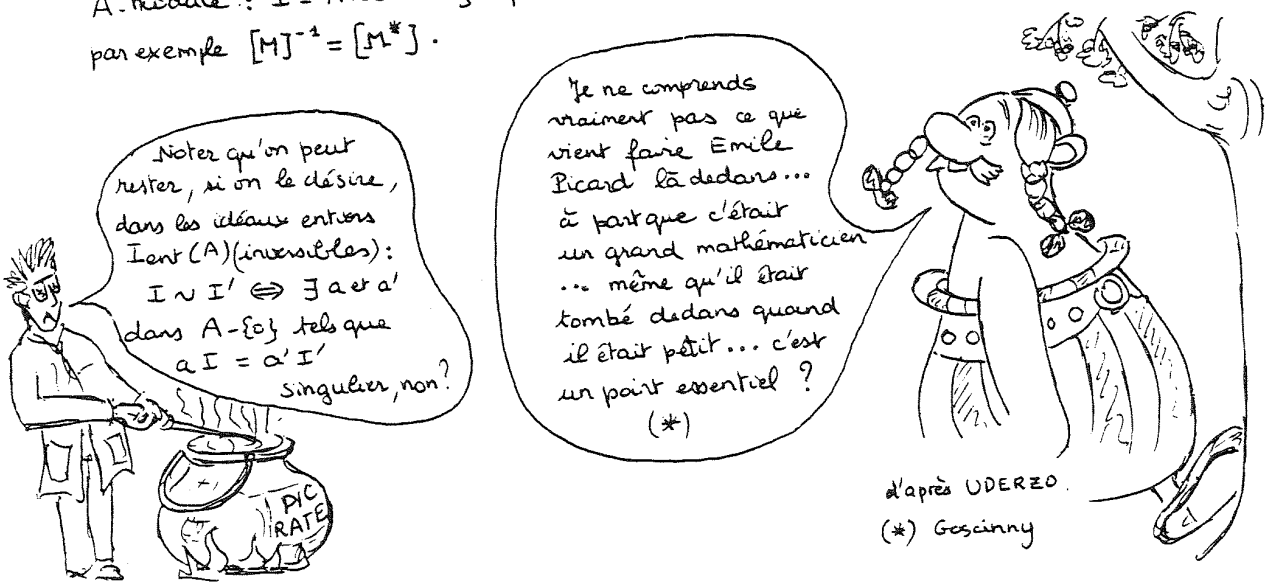
Lemme V.1.9 : $I \in \mathcal{I}(A)$ (inversible), $J \in \mathcal{Y}$; le morphisme canonique
$I \otimes_A J \longrightarrow I.J$ (donné par $x \otimes y \mapsto xy$) est un isomorphisme.

On a : $J \hookrightarrow K$ et on tensorise par $I \otimes_A \cdot$ qui est exact car I inversible donc projectif, donc plat.

Théorème V.1.10 : Soit $Pic(A)$ l'ensemble des classes d'isomorphismes de A-modules de type fini de rang 1 muni de la loi $[M].[N] = [M \otimes N]$;
On a un isomorphisme de groupes :

$$Cl(A) = \frac{\mathcal{I}(A)}{\mathcal{P}(A)} \longrightarrow Pic(A)$$
$$I \bmod \mathcal{P}(A) \mapsto [I]$$

On vient de voir qu'on a bien un morphisme de monoïdes de $\mathcal{Y}$ dans $Pic(A)$ qui à I associe sa classe : $[I \otimes J] = [IJ] = [I].[J]$. ; il est surjectif d'après V.1.7, et son noyau est l'ensemble des I inversibles et isomorphes à A comme A-module : $I = A.a$. Ça prouve donc en plus que $Pic(A)$ est un groupe ; par exemple $[M]^{-1} = [M^*]$.



§ V.2. Anneaux de Dedekind

Définition V.2.1 : A est un anneau de Dedekind si il vérifie
a) intègre
b) noethérien
c) tout idéal premier non nul est maximal
d) normal

Exemple V.2.2 fondamental
K corps de nombres $A = \mathcal{O}_K$ son anneau d'entiers est de Dedekind.

En route pour le théorème fondamental de décomposition des idéaux :

Preuve : A est intègre de corps de fractions K, noethérien car $\mathbb{Z}$-module libre de rang n, normal par définition ; reste à voir c) et il suffit pour cela de montrer que pour I premier non nul $\frac{A}{I}$ est fini (intègre donc corps). Cela découle du lemme suivant :

lemme V.2.3 : $a \in A = \mathcal{O}_K$ non nul ; $\frac{A}{Aa}$ est fini.

en effet $N_{K/\mathbb{Q}}(a) = a\sigma_2(a)\dots\sigma_n(a) = ac = b \in \mathbb{Z}$
or c est entier, $c = \frac{b}{a} \in K$ donc $c \in A$ et $b \in Aa$.
On a donc une surjection canonique : $\frac{A}{bA} \simeq \left(\frac{\mathbb{Z}}{b\mathbb{Z}}\right)^n \longrightarrow \frac{A}{Aa} \to 0$
(où $n = (K:\mathbb{Q})$).
Exemple : $\mathbb{Z}[\sqrt{-5}]$ est de Dedekind, non factoriel.

lemme V.2.4 : A noethérien, intègre ; $I \subset A$ un idéal propre non nul $\Rightarrow$ I contient un produit d'idéaux premiers non nuls.

prendre I maximal dans la famille des idéaux vérifiant les hypothèses et pour les quels la conclusion est fausse ...
... si cette famille est non vide !

lemme V.2.5 : A vérifiant a), b), c), $A \neq K$.
$I \subsetneq A$ idéal propre $\Rightarrow (A:I) \supsetneq A$

Alors I n'est pas premier et $\exists$ a, b dans A, $ab \in I$ $a \notin I$, $b \notin I$. $I + Aa \supsetneq I$, $I + Ab \supsetneq I$, $(I+Aa)(I+Ab) \subset I$. Conclure.

Pour $I \neq 0$, prendre $a \in I - \{0\}$, $Aa \supset \mathcal{P}_1 \dots \mathcal{P}_r$, $\mathcal{P}_1 \dots \mathcal{P}_r$ premiers non nuls (lemme V.2.4) avec r minimal ; et soit $M \supset I$ maximal : $M \supset I \supset aA \supset \mathcal{P}_1 \dots \mathcal{P}_r$. M contient l'un des $\mathcal{P}_i$, par exemple $\mathcal{P}_1$, donc $M = \mathcal{P}_1$. Si $r = 1$, $M = I = Aa$, $(A:I) = A \cdot \frac{1}{a} \supsetneq A$.
Si $r > 1$, Aa ne contient pas $\mathcal{P}_2 \dots \mathcal{P}_r$ (r minimal) ; soit $b \in \mathcal{P}_2 \dots \mathcal{P}_r - Aa$ et soit $c = \frac{b}{a}$.
$c \notin A$ (puisque $b \notin Aa$) et $c \in (A:I)$ puisque $cI \subset cM = c\mathcal{P}_1 \subset \frac{1}{a}\mathcal{P}_1 \dots \mathcal{P}_r \subset \frac{1}{a}Aa = A$.

Lemme V.2.6 : A noethérien, intègre, normal. Pour tout idéal fractionnaire $I \subset K$ non nul on a :

$$(I : I) = A$$

$A \subset (I:I)$ est évident. Réciproquement si $s \in (I:I)$, I est un $A[s]$ module, de type fini sur A. Donc $A[s]$ qui s'injecte dans I non nul est de type fini sur A, donc $s \in \overline{A} = A$.

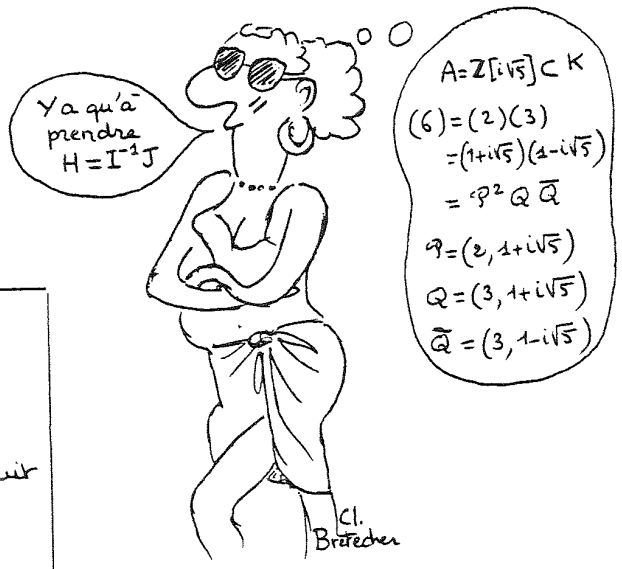
Théorème V.2.7 fondamental des anneaux de Dedekind :
Tout idéal fractionnaire non nul I d'un anneau de Dedekind A est inversible :

$$I \cdot (A:I) = A$$

Soit $J = I \cdot (A:I) \subset A$; on a $(A:J)\,J = (A:J) \cdot I\,(A:I) \subset A$
donc $(A:J)(A:I) \subset (A:I)$ (*)
on en déduit que $(A:J) \subset ((A:I)(A:I)) = A$ d'après le lemme V.2.6.
Or, d'après V.2.5, si J était propre, on aurait $(A:J) \supsetneq A$; donc $J = A$.

Définition V.2.8 : si I et J sont deux idéaux fractionnaires de A, on dit que I divise J s'il existe H entier tel que $J = IH$.

Corollaire V.2.9 : A de Dedekind, I et J idéaux fractionnaires de A ; alors :
I divise $J \iff I \supset J$



Théorème V.2.10 : de décomposition des idéaux dans un anneau de Dedekind.
A de Dedekind, $0 \subsetneq I \subsetneq A$ un idéal entier ; I s'écrit de manière unique (à permutation près) comme produit d'idéaux maximaux : $I = \mathcal{P}_1 \mathcal{P}_2 \cdots \mathcal{P}_r$
$\mathcal{P}_i \in \operatorname{Spec max}(A)$, $r \in \mathbb{N}^*$.

unicité : $\mathcal{P}_1 \cdots \mathcal{P}_r = Q_1 \cdots Q_s$; $\mathcal{P}_1 \supset Q_1 \cdots Q_s$, donc Q_1 par exemple d'où $\mathcal{P}_1 = Q_1$.
On multiplie par $\mathcal{P}_1^{-1}$ et on recommence.

existence : soit I maximal dans la famille des idéaux qui ne peuvent pas s'écrire ... (si cette famille est non vide) ; $I \subset M$ idéal maximal de A et $I \neq M$ puisque I est dans la famille ; donc $I = MJ$ et $J \not\subset I$; donc J n'est pas dans la famille en question, se décompose en produit d'idéaux premiers, donc $I = MJ$ aussi : contradiction.
∴

Corollaire V.2.11 : A anneau de Dedekind, $\mathcal{P} = \operatorname{Spec max}(A)$. Tout idéal fractionnaire I de A s'écrit de façon unique :

$$I = \prod_{\mathcal{P} \in \mathcal{P}} \mathcal{P}^{n_\mathcal{P}} \qquad n_\mathcal{P} \in \mathbb{Z}$$
presque tous nuls.

Prendre $d \neq 0$ dans A tel que $dI \subset A$; décomposer Ad et I dans A ...
Autre façon de dire la même chose : $I(A)$, $\times$ est un groupe libre de base $\mathcal{P}$.

les questions, la semaine prochaine ! vous voyez pas qu'il y a de la neige de printemps ?

§ V.3. Norme d'un idéal dans l'anneau de nombres

$$\begin{array}{ccc} \mathbb{Z} & \subset & A=\mathcal{O}_K \\ \cap & & \cap \\ \mathbb{Q} & \subset & K \end{array}$$

K corps de nombres de degré n.

Définition V.3.1 :
$I \subset A$ idéal non nul ;
norme de $I = N(I) = \#\left(\frac{A}{I}\right)$

Proposition V.3.2 : pour deux idéaux I et J entiers non nuls on a : $N(IJ) = N(I)N(J)$

On se ramène immédiatement au cas où $J = \mathfrak{P}$ maximal (par récurrence sur le nombre de facteurs de la décomposition de J) ; $I/\mathfrak{P}I$ est un A-module tué par $\mathfrak{P}$, donc un $k = \frac{A}{\mathfrak{P}}$ espace vectoriel ; les sous-espaces vectoriels de $I/\mathfrak{P}I$ correspondent aux idéaux L intermédiaires $I \supset L \supset \mathfrak{P}I$; par unicité de la décomposition, $L = I$ ou $L = \mathfrak{P}I$, donc $\frac{I}{\mathfrak{P}I}$ est de dimension 1 sur k et $N(\mathfrak{P}I) = N(I) \times N(\mathfrak{P})$ par la suite exacte : $0 \to \frac{I}{\mathfrak{P}I} \to \frac{A}{\mathfrak{P}I} \to \frac{A}{I} \to 0$

Proposition V.3.3 : Soit I un idéal entier non nul de A ; I est libre de rang n sur $\mathbb{Z}$ et si $(x_1, \dots, x_n)$ est une $\mathbb{Z}$-base de I :

$$N(I) = \sqrt{\left|\frac{\mathrm{Disc}(x_1, \dots, x_n)}{\mathrm{Disc}(A)}\right|}$$

Si $(a_1 \cdots a_n)$ est une $\mathbb{Z}$-base de A, $(x_1, \dots, x_n) = \Lambda(a_1, \dots a_n)$ $N(I) = |\mathrm{Det}(\Lambda)|$ (produit des facteurs invariants) et $\mathrm{Disc}(x_1 \cdots x_n) = [\mathrm{Det}(\Lambda)]^2 \mathrm{Disc}(a_1 \cdots a_n)$.

Cas particulier : $I = Aa$ $a \in A - \{0\}$

$$N(Aa) = |N_{K/\mathbb{Q}}(a)|$$

On applique à : $(x_1 = aa_1, \dots, x_n = aa_n)$
$\mathrm{Disc}(A) = [\mathrm{Det}(\sigma_i(aa_j))]^2 = [\prod \sigma_i(a)]^2 \cdot \mathrm{Disc}(A)$

(*) Suit une explication tellement compliquée qu'il n'est pas question de l'exposer au niveau maîtrise.

(**) On a réussi à perdre un poste et à séparer un nouveau couple !

§ V.4 Extension et localisation d'anneaux de Dedekind

théorème V.4.1 (Akizuki-Krull) : A de Dedekind, $K = \mathrm{Fract}(A)$, $L \supset K$ une extension finie ; alors $B = \mathcal{O}_L$ anneau des entiers de L sur A est de Dedekind.

Le théorème a été démontré pour $A = \mathbb{Z}$ (exemple V.2.2) ; lorsque L est une extension séparable, la preuve est semblable, mais on doit remplacer "$\frac{A}{I}$ intègre fini $\Rightarrow$ $\frac{A}{I}$ corps" par : "k corps, R intègre $\supset k$, R k-esp. vect. de dim. finie $\Rightarrow$ R corps".

Lorsque L n'est pas une extension séparable de K, la preuve du caractère noethérien est plus délicate : Bourbaki, Alg. comm., chap VII, § 2,5 corollaire 2 page 225.

$\mathrm{Spec}A \longleftarrow \mathrm{Spec}B$

$\mathfrak{P} = Q \cap A \longleftarrow Q$

$$\begin{array}{ccc} A & \subset & B \\ \cap & & \cap \\ K & \subset_{n} & L \end{array}$$

Q premier au dessus de $\mathfrak{P}$ = Q divise $\mathfrak{P}B$.

Remarque V.4.2 : $\mathfrak{P}$ et Q idéaux maximaux de A et B respectivement ; il y a équivalence :
$\mathfrak{P} \subset Q$; $\mathfrak{P}B \subset Q$; $\mathfrak{P} = A \cap Q$; Q divise $\mathfrak{P}B$; $Q \cap K = \mathfrak{P}$.

$$\mathfrak{P}B = Q_1^{e_1} Q_2^{e_2} \dots Q_g^{e_g}.$$

$Q_1 \dots Q_g$ idéaux maximaux distincts de B au dessus de $\mathfrak{P}$.

e_i = indice de ramification de $\mathfrak{P}$ en Q_i

Proposition V.4.3 :
a) Q maximal de B $\Rightarrow$ $Q \cap A$ maximal dans A.
b) $\mathfrak{P} \subset A$ maximal $\Rightarrow$ $\exists$ Q maximal de B au dessus de $\mathfrak{P}$.

preuve de a) : $\frac{A}{Q \cap A} \hookrightarrow \frac{B}{Q}$ corps ; si $x \in \frac{A}{Q \cap A}$ non nul, $\frac{1}{x} \in \frac{B}{Q}$ est entier sur $\frac{A}{Q \cap A}$ et vérifie : $\left(\frac{1}{x}\right)^m + a_1 \left(\frac{1}{x}\right)^{m-1} + \dots + a_m$; d'où $\frac{1}{x} = -a_1 - a_2 x \dots - a_m x^{m-1} \in \frac{A}{Q \cap A}$.

preuve de b) : soit $\gamma \in (A : \mathfrak{P})$, $\gamma \in K - A$ (lemme V.2.5) ; si $\mathfrak{P}B = B$ on aurait $1 = \sum p_i b_i$, $p_i \in \mathfrak{P}$, d'où $\gamma = \sum (\gamma p_i) b_i \in B \cap K = A$ (A normal) ...

Théorème V.4.4 :
$$\begin{array}{ccc} A & \subset & B = \mathcal{O}_K \text{ de Dedekind.} \\ \cap & & \cap \\ K & \subset & L \text{ extension séparable de degré } n \end{array}$$

$\mathfrak{P}B = Q_1^{e_1} \dots Q_g^{e_g}$

$f_i = \left(\frac{B}{Q_i} : \frac{A}{\mathfrak{P}}\right)$ degré résiduel en Q_i

$$\sum_{i=1}^{g} e_i f_i = \left(\frac{B}{\mathfrak{P}B} : \frac{A}{\mathfrak{P}}\right)$$

preuve : La filtration de B : $B \supsetneq Q_1 \dots \supsetneq Q_1^{e_1} \supsetneq Q_1^{e_1} Q_2 \dots \supsetneq Q_1^{e_1} Q_2^{e_2} \dots \supsetneq \mathfrak{P}B$ est maximale ; chaque étape est de la forme $\mathfrak{a} \supset \mathfrak{a}Q_i$ (propriété des anneaux de Dedekind donnée par l'unicité de la décomposition).
Or $\frac{\mathfrak{a}}{\mathfrak{a}Q_i}$ est un $\frac{B}{Q_i}$-espace vectoriel de dimension 1, donc de dimension f_i sur $\frac{A}{\mathfrak{P}}$. D'où la dimension de $\frac{B}{\mathfrak{P}B}$ sur $\frac{A}{\mathfrak{P}}$ est $\sum_{\mathfrak{a} \supset \mathfrak{a}Q_i} f_i = \sum_{i=1}^{g} e_i f_i$.

lemme V 4.5 : si B est libre sur A, B est libre de rang n et $\sum e_i f_i = n$; c'est vrai si A est principal.

En effet, B est finie sur A d'où rang de B sur $A = \dim_K (B \otimes K) = (L : K) = n$. Et alors, $B = \bigoplus_{i=1}^{n} A x_i$, $\frac{B}{\mathfrak{P}B} = \bigoplus_{i=1}^{n} \frac{A}{\mathfrak{P}} \overline{x_i}$ de dimension n sur $\frac{A}{\mathfrak{P}}$. De plus on a vu que si A est principal, par le théorème de la fourchette (V.4.6) que B est libre.

Théorème V.4.6 :
$$\sum_{i=1}^{g} e_i f_i = n$$

Soit $S = A - \mathfrak{P}$, $A_{\mathfrak{P}} = S^{-1}A$ le localisé de A en $\mathfrak{P}$
$B_{\mathfrak{P}} = S^{-1}B = B \otimes_A A_{\mathfrak{P}}$.

Les idéaux premiers de $A_{\mathfrak{P}}$ sont en correspondance avec les idéaux premiers de A inclus dans $\mathfrak{P}$: il n'y a que 0 et $\mathfrak{P}A_{\mathfrak{P}}$: $A_{\mathfrak{P}}$ est un anneau de Dedekind avec un unique idéal maximal = c'est un anneau de valuation discrète.
En prenant la fermeture entière dans L : $\overline{A}_{\mathfrak{P}} = (\overline{A})_{\mathfrak{P}} = B_{\mathfrak{P}}$

$$\begin{array}{ccc} A & \subset & B \\ \cap & & \cap \\ A_{\mathfrak{P}} & \subset & B_{\mathfrak{P}} \\ \cap & & \cap \\ K & \subset & L \end{array}$$

Comme $A_{\mathfrak{P}}$ est principal, par le lemme :
$\left(\frac{B_{\mathfrak{P}}}{\mathfrak{P}B_{\mathfrak{P}}} : \frac{A_{\mathfrak{P}}}{\mathfrak{P}A_{\mathfrak{P}}} \right) = n$
or $\mathfrak{P}B = \prod_{i=1}^{g} Q_i^{e_i}$ et par le foncteur S^{-1} :
$\mathfrak{P}B_{\mathfrak{P}} = \prod_{i=1}^{g} (Q_i B_{\mathfrak{P}})^{e_i}$
$(Q_i \cap S = Q_i \cap S \cap A = \mathfrak{P} \cap S = \emptyset)$

d'où $n = \sum_{i=1}^{g} e_i f'_i$ où $f'_i = \left(B_{\mathfrak{P}}/Q_i B_{\mathfrak{P}} : B_{\mathfrak{P}}/\mathfrak{P}B_{\mathfrak{P}} \right)$; reste à voir $f_i = f'_i$:

$$\begin{array}{ccc} B/Q_i & \xrightarrow{\approx} & B_{\mathfrak{P}}/Q_i B_{\mathfrak{P}} \\ (f_i) \uparrow & & \uparrow (f'_i) \\ A/\mathfrak{P} & \xrightarrow{\approx} & B_{\mathfrak{P}}/\mathfrak{P}B_{\mathfrak{P}} \end{array}$$

En résumé :

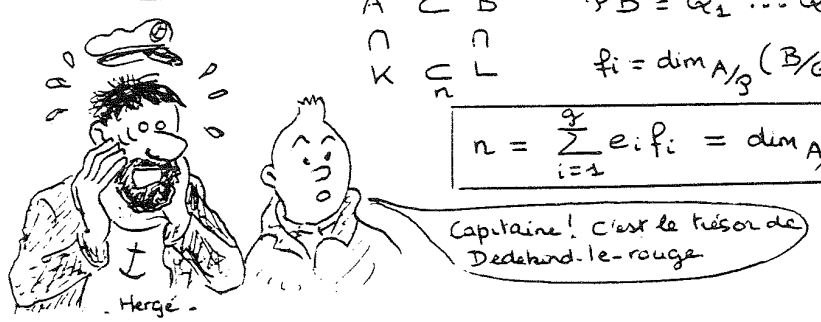
$$\begin{array}{ccc} A & \subset & B \\ \cap & & \cap \\ K & \subset_n & L \end{array}$$

$\mathfrak{P}B = Q_1^{e_1} \dots Q_g^{e_g}$

$f_i = \dim_{A/\mathfrak{P}} (B/Q_i)$

$\frac{B}{\mathfrak{P}B} = \prod_{i=1}^{g} \frac{B}{Q_i^{e_i}}$ par le théorème chinois.

$$n = \sum_{i=1}^{g} e_i f_i = \dim_{A/\mathfrak{P}} \left(\frac{B}{\mathfrak{P}B} \right)$$



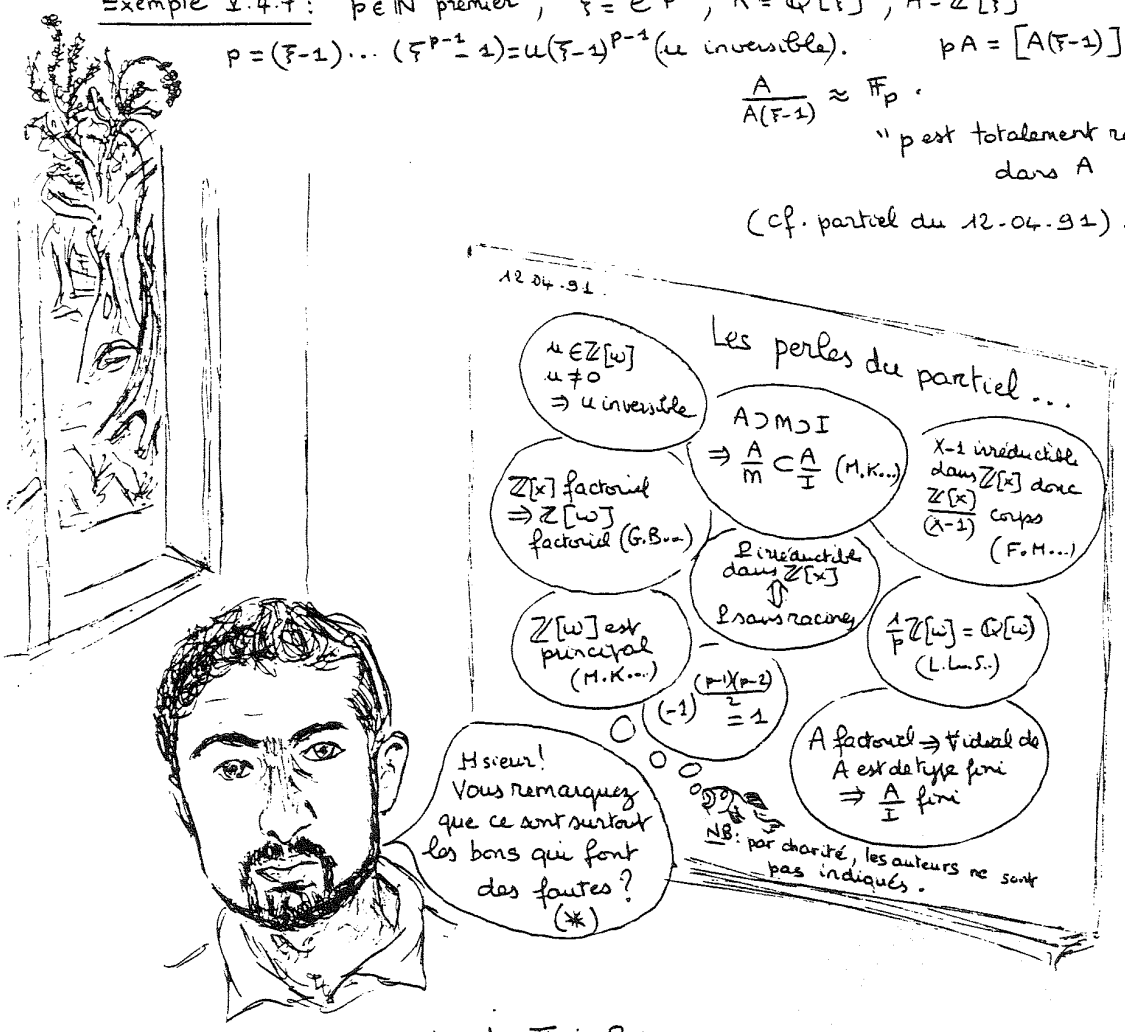
Exemple V.4.7 : $p \in \mathbb{N}$ premier, $\xi = e^{\frac{2i\pi}{p}}$, $K = \mathbb{Q}[\xi]$, $A = \mathbb{Z}[\xi]$

$p = (\xi - 1)\cdots(\xi^{p-1} - 1) = u(\xi - 1)^{p-1}$ (u inversible). $\quad pA = [A(\xi-1)]^{p-1}$

$\frac{A}{A(\xi-1)} \approx \mathbb{F}_p$.

" p est totalement ramifié " dans A

(cf. partiel du 12-04-91).



L'algorithme de Dedekind - V.4.8 :

K corps de nombres de degré n sur $\mathbb{Q}$, $A = \mathcal{O}_K$; on suppose $A = \mathbb{Z}[\theta]$

P polynôme minimal de θ sur $\mathbb{Z}$, $\overline{P}$ sa classe dans $\mathbb{F}_p[T]$,

$\overline{P}(T) = \overline{P}_1^{e_1} \cdots \overline{P}_g^{e_g}$ sa factorisation en produit d'irréductibles distincts et unitaires dans $\mathbb{F}_p[T]$, $f_i = \deg(\overline{P}_i)$, P_i un relevé de $\overline{P}_i$ dans $\mathbb{Z}[T]$.

$Q_i = (p, P_i(\theta)) \subset A = \mathbb{Z}[\theta]$.

Alors : $\quad pA = \prod_{i=1}^{g} Q_i^{e_i}$

$A \approx \frac{\mathbb{Z}[T]}{(P(t))} \longrightarrow \frac{\mathbb{F}_p[T]}{(\overline{P}_i)} \approx \frac{A}{Q_i}$

$\frac{\mathbb{F}_p[T]}{(\overline{P}(t))}$

$Q_1^{e_1} \cdots Q_g^{e_g} \subset (p, P_1^{e_1}\cdots P_g^{e_g}(\theta) = 0) = pA$

pA divise $Q_1 \cdots Q_g$ et on utilise l'égalité fondamentale pour conclure ($\sum_{i=1}^{g} e_i f_i = n$).

On peut aussi vérifier avec la norme.

NB : on vérifiera également dans la scène ci dessus, que l'on a quitté l'aquarium, mais qu'il y a toujours des bulles.

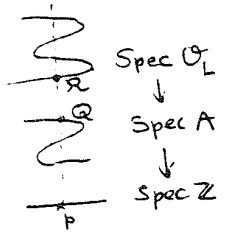
(*) seuls les acteurs comprendront.

Théorème V.4.9 : K un corps de nombres de degré n, $A = \mathcal{O}_K$; si $p \in \mathbb{Z}$ se ramifie dans A, alors p divise $\mathrm{Disc}(A)$.

Supposons $pA = \mathcal{Q}^e \mathcal{Q}_2^{e_2} \cdots \mathcal{Q}_g^{e_g}$ $e \geq 2$, $e_2 \cdots e_g \geq 1$; $\sigma_1 \cdots \sigma_n$ les n plongements de K dans $\mathbb{C}$, L une extension galoisienne de $\mathbb{Q}$ contenant K, $(\tilde{\sigma}_1, \cdots, \tilde{\sigma}_n) \in \mathrm{Gal}(L/\mathbb{Q})$ prolongeant $\sigma_1, \cdots, \sigma_n$. Soit $\alpha \in I - pA$ où $I = \mathcal{Q}\mathcal{Q}_2^{e_2-1} \cdots \mathcal{Q}_g^{e_g}$, soit $(a_1 \cdots a_n)$ une $\mathbb{Z}$-base de A, $\alpha = m_1 a_1 + \cdots + m_n a_n$; un des m_i, disons m_1 n'est pas divisible par p.

$$\mathrm{Disc}(\alpha, a_2 \cdots a_n) = m_1^2 \, \mathrm{Disc}(a_1 \cdots a_n) = m_1^2 \, \mathrm{Disc}(A).$$

Comme p ne divise pas m_1, il suffit de prouver que p divise $\mathrm{Disc}(\alpha, a_2 \cdots a_n)$.



Soit $\mathcal{R} \in \mathrm{Spec}\, \mathcal{O}_L$ au dessus de p : donc $\mathcal{R} \cap A = \mathcal{Q}, \mathcal{Q}_2$ ou $\mathcal{Q}_g$.
Pour $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$, $\sigma^{-1}(\mathcal{R})$ reste premier au dessus de p, donc puisque $\alpha \in I \subset \mathcal{Q}\mathcal{Q}_2 \cdots \mathcal{Q}_g$, $\sigma_i(\alpha) \in \mathcal{Q}$ $\forall i$.

$$\mathrm{Disc}(\alpha, a_2 \cdots a_n) = \left[\det(\sigma_i(\alpha), \sigma_i(a_2) \cdots, \sigma_i(a_n))\right]^2$$
$$\in \mathcal{Q}^2 \cap \mathbb{Z} \subset \mathcal{Q} \cap \mathbb{Z} = p\mathbb{Z}.$$

Corollaire V.4.10 : il n'existe qu'un nombre fini de $p \in \mathbb{Z}$ qui se ramifient dans $A = \mathcal{O}_K$.

§ V.5 : Extensions Galoisiennes

$$\begin{array}{ccccc} \mathbb{Z} & \subset & A & \subset & B \\ \cap & & \cap & & \cap \\ \mathbb{Q} & \subset & K & \underset{n}{\subset} & L \end{array}$$

$A = \mathcal{O}_K$ $\quad B = \mathcal{O}_L$

L extension galoisienne de K.

$G = \mathrm{Gal}(L/K)$

Proposition V.5.1 : $\mathcal{P}$ idéal maximal de A, $\mathcal{Q}_1 \cdots \mathcal{Q}_g$ les idéaux premiers de B au dessus de $\mathcal{P}$; G opère transitivement sur $\{\mathcal{Q}_1, \cdots, \mathcal{Q}_g\}$.

Soit $\mathcal{Q}_2$, par exemple n'appartenant pas à l'orbite de $\mathcal{Q}_1$ sous G. Par le théorème chinois on a une surjection : $\dfrac{B}{\mathcal{P}B} \longrightarrow \left(\prod_{\mathcal{Q} \in \Sigma} \left(\dfrac{B}{\mathcal{Q}}\right)\right) \times \dfrac{B}{\mathcal{Q}_2}$

où Σ est l'orbite de Q_1. Soit $1 = x + \lambda$, $x \in Q_2$, $\lambda \in \prod_{Q \in \Sigma} \mathcal{P}$

$x \equiv 1 \bmod Q$. pour $Q \in \Sigma$

$N(x) = x \prod_{\sigma \in G - id} \sigma(x) \in A \cap Q_2 = \mathcal{P}$.

Or si $\sigma \in G$, $\sigma(x) \notin Q_1$ (sinon $x \in \sigma^{-1} Q_1 = Q$ contraire à $x \equiv 1 \bmod Q$) ;

donc $N(x) \notin Q_1$, ce qui contredit $N(x) \in \mathcal{P} \subset Q_1$.

M'sieur ! C'est pour sa nana qu'il s'est fait descendre, Evariste ?

Corollaire V.5.2 :

$$\mathcal{P}B = (Q_1 \cdots Q_g)^e$$

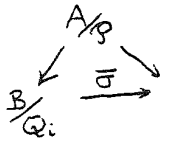
$$\dim_{A/\mathcal{P}} (B/Q_f) = f$$

$$e f g = n$$

En effet : pour i et j entre 1 et g, soit $\sigma \in G$ tel que $\sigma(Q_i) = Q_j$.

$\mathcal{P}B = Q_1^{e_1} \cdots Q_g^{e_g} = \sigma(\mathcal{P}B) = \sigma(Q_1)^{e_1} \cdots \sigma(Q_g)^{e_g}$; par unicité $e_j \geq e_i$ et par symétrie (en appliquant σ^{-1}) $e_i = e_j = e$.

D'autre part :



σ par passage au quotient donne un isomorphisme $\bar{\sigma}$ des extensions de $A/\mathcal{P}$ et donc $f_i = f_j = f$.

Avant d'aborder la suite, on a intérêt à réviser le rappel III.3.5 sur la correspondance de Galois.

Q idéal premier de B au dessus de $\mathcal{P}$

Définition V.5.3

$$G \supset D = D_Q = \{\sigma \in G / \sigma(Q) = Q\} \supset T = T_Q = \{\sigma \in G / \forall x \in B \ \ \sigma(x) - x \in Q\}$$

D : stabilisateur de Q. "sous groupe de décomposition" de Q.

T : "sous groupe d'inertie"

$$K \subset L_D = L^{Dec} = \{x \in L / \forall \sigma \in D \ \ \sigma(x) = x\} \subset L_T = \{x \in L / \forall \sigma \in T \ \ \sigma(x) = x\} \subset L$$

extensions intermédiaires correspondantes.

Lemme V.5.4 : on a la suite exacte de groupes :

$$1 \longrightarrow T \longrightarrow D \longrightarrow Gal(\bar{L}/\bar{K}) \longrightarrow 1$$

$$\bar{K} = \frac{A}{\mathcal{P}} \qquad \bar{L} = \frac{B}{Q}$$

Evariste n'était pas un polytechnicien à roulettes

Fred. Philémon à l'heure du second T

Si $\sigma \in D$, σ induit $\bar{\sigma} \in Gal(\bar{L}/\bar{K})$; $\bar{\sigma} = id$ équivaut à $\sigma(x) - x \in Q$ pour tout $x \in B$, c'est à dire $\sigma \in T$. Le degré de l'extension $(\bar{L} : \bar{Q})$ est f et on va voir dans un moment $\#T = e$ et $\#D = ef$.

Comme G opère transitivement sur $(Q_1 = Q, Q_2, \cdots, Q_g)$, et que D est le stabilisateur de Q, on a $\#D = \frac{n}{g} = ef$. Donc $(L : L_D) = ef$ nombre d'éléments de son groupe de Galois. A priori L_D n'est pas une extension Galoisienne de K (équivaut à D distingué).

On note B^D l'anneau d'entiers de L^D, $\mathfrak{R} = B^D \cap Q$ et on montre :

a) Q est le seul idéal premier de B au dessus de $\mathfrak{R}$.

b) Réciproquement si E est une extension intermédiaire possédant la propriété : Q seul idéal de B au dessus de $Q \cap \mathcal{O}_E$, alors $E \supset L^D$.

En effet : les idéaux premiers de B au dessus de $\mathfrak{R}$ sont permutés transitivement par le groupe de Galois D de L sur L^D ...
Si $\sigma \in Gal(L/E)$, $\sigma(Q) = Q$ donc $Gal(L/E) \subset Gal(L/L_D) = D$ ...

c) Montrons : $\mathfrak{R} = Q \cap B^D$; $e(\mathfrak{R}/\mathfrak{P}) = 1$ et $f(\mathfrak{R}/\mathfrak{P}) = 1$

$ef = (L : L^D) = e(Q/\mathfrak{R})\, f(Q/\mathfrak{R})\, g(Q/\mathfrak{R})$ car L sur L^D galoisienne.

$e = e(Q/\mathfrak{P}) = e(Q/\mathfrak{R}) \times e(\mathfrak{R}/\mathfrak{P})$ formule des tours pour l'indice de ramification

$f = f(Q/\mathfrak{P}) = f(Q/\mathfrak{R}) \cdot f(\mathfrak{R}/\mathfrak{P})$ formule des tours pour le degré résiduel.

On fait le produit des deux dernières égalités et on compare à la première.

d) $\mathfrak{S} = Q \cap B^T$; montrons $f(Q/\mathfrak{S}) = 1$ soit $\frac{B^T}{\mathfrak{S}} \xrightarrow{\sim} \frac{B}{Q}$.

Soit $\bar{\theta} \in \frac{B}{Q}$; $P(x) = \prod_{\sigma \in T} (x - \sigma(\theta)) \in B[x]$; $\bar{P}(x) = \prod_{\sigma \in T} (x - \bar{\theta}) = (x - \bar{\theta})^m \in \frac{B}{Q}[x]$ où $m = \#T$.

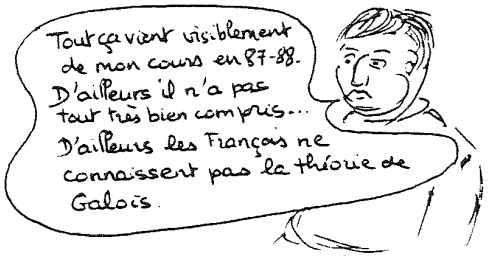
P est invariant par $\tau \in T$: $\tau . P(x) = \prod_{\sigma \in T} (x - \tau\sigma(\theta)) = \prod_{\sigma' \in T} (x - \sigma'(\theta)) = P(x)$
et donc $P(x)$ est à coefficient dans $B^T = B \cap L^T$; donc $\bar{P}(x) \in \frac{B^T}{\mathfrak{s}}[x]$. Le polynôme minimal de $\bar{\theta}$ sur $\frac{B^T}{\mathfrak{s}}$ divise donc $(x-\bar{\theta})^m$, c'est donc $x - \bar{\theta}$ ce qui signifie $\bar{\theta} \in \frac{B^T}{\mathfrak{s}}$.

e) $f = f(Q|S)\, f(S|R)\, f(R|\mathfrak{p}) = f(S|R)$ car on a vu $f(R|\mathfrak{p}) = 1$ et $f(Q|\mathfrak{s}) = 1$.
$(L^T : L^D) = \#(\frac{D}{T})$ est donc au moins égal à f, d'où la surjectivité $\frac{D}{T} \to \mathrm{Gal}(\bar{L}/\bar{K})$ qui est de cardinal f par définition ; d'où $\#(\frac{D}{T}) = f$ et $\#(T) = e$.

Théorème V.5.5

	degré des extensions	indice de ramification	degré résiduel
$L \supset B \supset Q$	e	e	1
$L^T \supset B^T \supset Q^T = \mathfrak{s}$	f	1	f
$L^D \supset B^D \supset Q^D = R$	g	1	1
$K \supset A \supset \mathfrak{p}$			

$\mathfrak{p} B^D = R R'$ R' non divisible par R :
$R B^T = \mathfrak{s}$ premier.
$\mathfrak{s} B = Q^e$



Chap. VI : INEGALITES GEOMETRIQUES

Bon ! D'accord ! C'est entièrement piqué dans P. Samuel : "Théorie algébrique des nombres", chap IV : "Classe d'idéaux - Théorème des unités" - Vous vous en seriez aperçu ... c'est pour ça que je le dis - Et puis lui, il l'a bien pris quelque part ! Dans Minkowski, par exemple ! Alors, puisque c'est comme ça, je vous le raconte sous forme de questions ; et, si vous sèchez, allez voir la correction dans le magnifique petit livre argenté cité.

§ VI.1 : Sous groupes discrets de $\mathbb{R}^n$

Théorème VI.1.1 : Soit $H \subset \mathbb{R}^n$ un sous groupe non nul.
H discret $\iff \exists (e_1, \dots, e_r)$ $\mathbb{R}$-indépendants tels que $H = \bigoplus_{i=1}^{r} \mathbb{Z} \cdot e_i$

Là, je suis heureux de vous annoncer que ce chapitre n'est pas au programme cette année

a) Prouver : H discret $\iff$ $\forall K$ compact de $\mathbb{R}^n$, $K \cap H$ fini.

b) Soit H discret et $(e_1 \dots e_r)$ dans H, $\mathbb{R}$-indépendants avec r maximum ; soit $\mathcal{P} = \sum_{1 \le i \le r} [0,1] e_i$ le parallélotope compact construit sur $(e_1 \dots e_r)$. On suppose $H \cap \mathcal{P} = \{a_1, \dots a_N\}$; montrer que : $H \subset H \cap \mathcal{P} + \sum_{i=1}^{r} \mathbb{Z} e_i$;

Montrer que pour tout $a \in H$, $\exists (j,k), j \neq k$, tels que $(j-k)a \in \sum_{i=1}^{r} \mathbb{Z} e_i$

et en déduire l'existence de $d \in \mathbb{N}^*$ tel que $H \cap \mathcal{P} \subset \sum_{i=1}^{r} \mathbb{Z} \frac{e_i}{d}$, puis $H \subset \sum_{i=1}^{r} \mathbb{Z} \cdot \frac{e_i}{d}$.

Conclure.

On note $\mu(S)$ la mesure de Lebesgue d'une partie intégrable S de $\mathbb{R}^n$.

(*) En tous cas, je ne me sens absolument pas obligé de vous dire que c'est de P.J. Proudhon.

Définition VI.1.2 : on dit que H est un réseau de $\mathbb{R}^n$ si H est un sous groupe discret de rang n ; si $e = (e_1, \dots, e_n)$ est une $\mathbb{Z}$-base de H, on note $\mathcal{P}_e = \sum_{i=1}^{n} [0,1]\, e_i$ le parallélotope élémentaire construit sur e, et $\mathrm{Vol}(H) = \mu(\mathcal{P}_e)$ le volume du réseau.

c) Vérifier que $\mu(\mathcal{P}_e)$ ne dépend pas du choix de la base e du réseau.

Théorème VI.1.3 (H. Minkowski) : soit H un réseau de $\mathbb{R}^n$, $S \subset \mathbb{R}^n$ une partie intégrable de mesure $\mu(S) > \mathrm{Vol}(H)$. Alors $\exists\, (x,y)$ dans S, $x \neq y$ et $x - y \in H$.

d) Vérifier : $S = \bigcup_{h \in H} [S \cap (h + \mathcal{P}_e)]$; $\mu(S) = \sum_{h \in H} \mu(S \cap (h + \mathcal{P}_e)) = \sum_{h \in H} \mu((S-h) \cap \mathcal{P}_e)$.

Si les parties $(S-h) \cap \mathcal{P}_e$ étaient deux à deux disjointes, on aurait $\mu(S) \leq \mu(\mathcal{P}_e)$; terminer la preuve du théorème de Minkowski.

Corollaire VI.1.4 : Soit H un réseau de $\mathbb{R}^n$, S une partie intégrable de $\mathbb{R}^n$, symétrique par rapport à 0 et convexe. Sous l'une des deux hypothèses :

α) $\mu(S) > 2^n \mathrm{Vol}(H)$

β) $\mu(S) \geq 2^n \mathrm{Vol}(H)$ et S compacte,

alors $S \cap H$ contient un élément z non nul.

e) Avec l'hypothèse α), appliquer le théorème à $S' = \frac{1}{2} S$ et prendre $z = x - y$.

Avec l'hypothèse β), appliquer la partie α) du corollaire à $(1+\varepsilon) S$, $\varepsilon > 0$, et contempler $\bigcap_{\varepsilon > 0} [(H - \{0\}) \cap (1+\varepsilon) S]$.

§ VI.2 : Plongement canonique d'un corps de nombres

Soit K un corps de nombres de degré n ; on numérote les n $\mathbb{Q}$-plongements de K dans $\mathbb{C}$: $\{\sigma_1, \cdots, \sigma_{r_1}\}$ les plongements réels ($\sigma_i(K) \subset \mathbb{R}$), et $\{\sigma_{r_1+1}, \cdots, \sigma_{r_1+r_2}\ ;\ \overline{\sigma}_{r_1+1}, \cdots, \overline{\sigma}_{r_1+r_2}\}$ les plongements non réels (si $\sigma_i(K) \not\subset \mathbb{R}$, le

Rob. Valter
(† le 27.04.91)

conjugué $\overline{\sigma_i}$ est encore un plongement, distinct de σ_i).

Définition VI.2.1 : $\sigma = (\sigma_1, \cdots, \sigma_{r_1}, \sigma_{r_1+1}, \cdots \sigma_{r_1+r_2}) : K \hookrightarrow \mathbb{R}^{r_1}\mathbb{C}^{r_2} \simeq \mathbb{R}^n$
$n = r_1 + 2r_2$, s'appelle le plongement canonique de K.

Lemme VI.2.2 : Soit $M \subset K$ un $\mathbb{Z}$-module libre de rang n, $\sigma : K \to \mathbb{R}^n$ le plongement canonique ; alors $\sigma(M)$ est un réseau de volume :

$$\mathrm{Vol}(\sigma(M)) = \frac{1}{2^{r_2}} \left| \underset{1 \le i,j \le n}{\mathrm{Det}} \left(\sigma_i(x_j)\right) \right| \quad \text{où } (x_1, \cdots, x_n) \text{ est une } \mathbb{Z}\text{-base de } M.$$

f) Démontrer le lemme (dans la matrice $(\sigma_i(x_j))$ on introduira les combinaisons de lignes $\frac{\sigma_i(x_j) + \overline{\sigma_i(x_j)}}{2}$ et $\frac{\sigma_i(x_j) - \overline{\sigma_i(x_j)}}{2}$ pour $i = r_1+1, \cdots, r_1+r_2$.

Proposition VI.2.3 : Soit $A = \mathcal{O}_K$ l'anneau d'entiers d'un corps de nombres K de degré n, $d = \mathrm{Disc}(A)$ son discriminant absolu, $I \subset A$ un idéal entier non nul ; alors $\mathrm{Vol}(\sigma(A)) = \frac{1}{2^{r_2}}\sqrt{|d|}$ et $\mathrm{Vol}(\sigma(I)) = \frac{1}{2^{r_2}}\sqrt{|d|}\, N(I)$.

g) Pour démontrer la proposition, appliquer le lemme VI.2.2 à une base de A adaptée à I (sous $\mathbb{Z}$-module libre de rang n - voir V.3.3).

Théorème VI.2.4 : Soit K un corps de nombre de degré n, $A = \mathcal{O}_K$ son anneau d'entiers, $I \subset A$ un idéal entier non nul. Il existe $x \in I - \{0\}$ tel que :

$$|N(x)| \le \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|d|}\; N(I)$$

h) Soit σ le plongement canonique de K dans $\mathbb{R}^{r_1}\mathbb{C}^{r_2} \simeq \mathbb{R}^n$; pour $t > 0$,

$$B_t = \left\{ (x_1, \cdots, x_{r_1}; z_1, \cdots, z_{r_2}) \in \mathbb{R}^{r_1}\mathbb{C}^{r_2} \Big/ \sum_{i=1}^{r_1} |x_i| + 2 \sum_{j=1}^{r_2} |z_j| \le t \right\}$$

est un compact, convexe, symétrique de $\mathbb{R}^n$.

Par récurrence sur r_1 et r_2, montrer que : $\mathrm{Vol}(B_t) = 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2} \frac{t^n}{n!}$.

On fixe t pour avoir $\mathrm{Vol}(B_t) = 2^n \mathrm{Vol}(\sigma(I)) = 2^{n-r_2}\sqrt{|d|}\, N(I)$, et le théorème de Minkowski assure l'existence de x non nul dans I tel que $\sigma(x) \in B_t$. En déduire le théorème VI.2.4 en majorant $N(x)$

au moyen de l'inégalité, dans $\mathbb{R}^{+*}$: $a_1 \times \cdots \times a_n \leq \left(\frac{a_1 + \cdots + a_n}{n}\right)^n$.

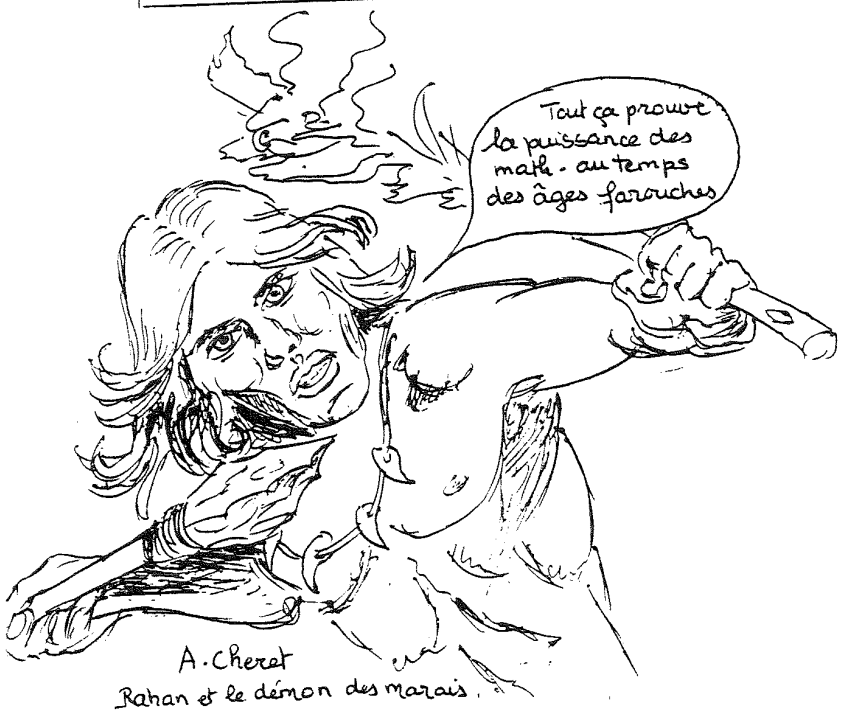
Corollaire VI.2.5 : Dans toute classe $\mathcal{C}$ d'idéaux fractionnaires de K il existe un idéal entier I vérifiant : $N(I) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|d|}$

i) Soit $J \in \mathcal{C}$, $J' = J^{-1}$ qu'on peut supposer entier en remplaçant J par $\frac{1}{\lambda} J$, $\lambda \in \mathbb{N}$ assez grand.
Appliquer le théorème VI.2.4 à J' pour trouver $x \in J' - \{0\}$ et montrer que $I = (Ax).J$ convient.

Théorème VI.2.6 (Hermite-Minkowski) : Soit K un corps de nombres de degré $n \geq 2$; son discriminant absolu d vérifie $|d| > 1$

j) D'après le corollaire VI.2.5, $|d| \geq a_n = \left(\frac{n^n}{n!}\right)^2 \left(\frac{\pi}{4}\right)^n$; en déduire, par récurrence, $|d| \geq \frac{\pi}{3} \left(\frac{3\pi}{4}\right)^{n-1}$.

Théorème VI.2.7 (Dirichlet) : Pour tout corps de nombres, le groupe des classes d'idéaux est fini.



A. Cheret
Rahan et le démon des marais.

k) Pour chaque classe $C \in Cl(K)$ on choisit un représentant I entier de norme $N(I) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|d|}$.
Il suffit donc de montrer que pour tout entier ℓ donné, il n'existe qu'un nombre fini d'idéaux I de $A = \mathcal{O}_K$ de norme ℓ.
Or $\ell \in I$, donc I divise ℓA et ℓA n'a qu'un nombre fini de diviseurs dans A anneau de Dedekind !

Théorème VI.2.8 (Hermite)
Dans $\mathbb{C}$, il n'existe qu'un nombre fini de corps de nombres de discriminant d donné.

ℓ) On suppose d, r_1, r_2 fixés et soit $\sigma : K \hookrightarrow \mathbb{R}^{r_1}\mathbb{C}^{r_2}$ le plongement canonique. On définit dans $\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$ le compact convexe symétrique B

$B = \{(x_1,\dots,x_{r_1}; z_1,\dots,z_{r_2})\}$ en posant :

si $r_1 \neq 0$: $|x_1| \leq 2^{n-1}\left(\frac{\pi}{2}\right)^{-r_2}\sqrt{|d|}$; $|x_i| \leq \frac{1}{2}$ $i=2,\dots r_1$; $|z_j| \leq \frac{1}{2}$ $j=1\dots r_2$

si $r_1 = 0$: $|Re(z_1)| \leq \frac{1}{8}$, $|Im(z_1)| \leq 2^{3r_2-1}\pi^{1-r_2}\sqrt{|d|}$; $|z_j| \leq \frac{1}{2}$ $j=2\dots r_2$.

Vérifier : $Vol(B) = 2^n \times 2^{-r_2}\sqrt{|d|}$ et en déduire, par Minkowski, l'existence de $a \in \mathcal{O}_K = A$ tel que $\sigma(a) \in B$, a non nul.

Si $\mathbb{Q}[a] \subsetneq K$, il existe $i_0 > 1$ tel que $\sigma_{i_0}(a) = \sigma_1(a)$; or, à priori, seul $|\sigma_1(a)|$ peut être $> \frac{1}{2}$, et on trouve $|N(a)| = \prod_{i=1}^{n} |\sigma_i(a)| \leq \frac{1}{2}$ … impossible !

Donc $K = \mathbb{Q}[a]$ avec a racine de $f(x) = \prod_{i=1}^{n}(x-\sigma_i(a)) \in \mathbb{Z}[x]$. Il ne reste plus qu'à voir que les coefficients de f ne peuvent prendre qu'un nombre fini de valeurs (bornées en fonction de d, r_1, r_2).

Enfin n est borné en fonction de $|d|$ (d'après γ)), donc r_1 et r_2.

(*) Remplissez la bulle ; la meilleure bulle gagne un exemplaire entier du polycopié.

§VI.3 : Extensions quadratiques (Exercices d'application)

Soit $K = \mathbb{Q}[\sqrt{d}]$ un corps quadratique, où d est un entier sans facteur carré, et soit $A = \mathcal{O}_K$ son anneau d'entiers.

a) - Montrer que A est principal pour $d = 2, 3, 5, 13, -1, -2, -3, -7$.

b) - Montrer que tout idéal fractionnaire de K est équivalent à un idéal entier de norme 1 ou 2 pour $d = 6, 7, 17, 21, 29, 33, -5, -11, -15, -19$. Déterminer ceux de ces corps dans les quels $2A$ est premier (on trouve $d = 21, 29, -11, -19$) et montrer que leurs anneaux d'entiers sont principaux.

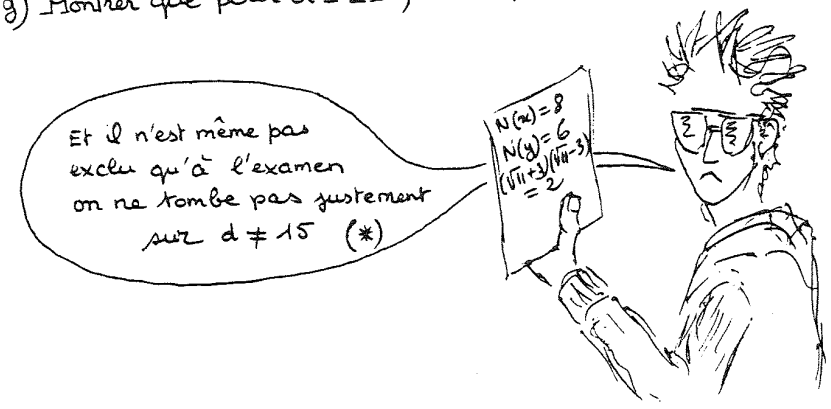
c) On suppose $d \equiv 2$ ou 3 mod. 4. Montrer que A admet un idéal principal de norme 2 si et seulement si il existe $(a,b) \in \mathbb{Z}^2$ vérifiant $a^2 - db^2 = \pm 2$. En déduire que A est principal pour $d = 6, 7$ et que A admet deux classes d'idéaux pour $d = -5$.

d) On suppose $d \equiv 1$ mod. 4. Montrer que A admet un idéal principal de norme 2 si et seulement si $a^2 - db^2 = \pm 8$ a une solution $(a,b) \in \mathbb{Z}^2$. En déduire que A est principal pour $d = 17, 33$, et qu'il admet deux classes d'idéaux pour $d = -15$.

e) Montrer que pour $d = 10$ et $d = -6$, K admet deux classes d'idéaux (Noter que tout idéal fractionnaire de K est équivalent à un idéal entier de norme 1, 2 ou 3 et étudier les décompositions de $2A$ et $3A$ en produit d'idéaux premiers de A).

f) Montrer que pour $d = -23$, K admet trois classes d'idéaux et qu'on a des idéaux premiers non principaux $\mathfrak{P}, \mathfrak{P}', \mathfrak{Q}, \mathfrak{Q}'$ de A tels que $2A = \mathfrak{P}\mathfrak{P}'$, $3A = \mathfrak{Q}\mathfrak{Q}'$. Etudier les décompositions de Ax et Ay en produit d'idéaux premiers pour $x = \frac{3+i\sqrt{23}}{2}$, $y = \frac{1+i\sqrt{23}}{2}$.

g) Montrer que pour $d = 11$, A est principal.



(*) Ne vous affolez pas! Il s'agit de l'examen de Juin 90.

§ VI.4 : Théorème des unités

Soit $A = \mathcal{O}_K$ l'anneau d'entiers d'un corps de nombres K de degré n, A^* le groupe multiplicatif des unités de A. On sait que $x \in A^* \Leftrightarrow N(x) = 1$.

Soit $\sigma = (\sigma_1, \cdots, \sigma_{r_1}, \sigma_{r_1+1}, \cdots, \sigma_{r_1+r_2}) : K \longrightarrow \mathbb{R}^{r_1}\mathbb{C}^{r_2}$ le plongement canonique, $L : K^* \longrightarrow \mathbb{R}^{r_1+r_2}$ le plongement logarithmique défini par $L(x) = (\log|\sigma_1(x)|, \cdots \log|\sigma_{r_1+r_2}(x)|)$, et par restriction, $L : A^* \longrightarrow \mathbb{R}^{r_1+r_2}$; $G = \operatorname{Ker} L = \{x \,/\, |\sigma_i(x)| = 1 \ \forall i\}$ est un groupe fini (les polynômes symétriques des $\sigma_i(x)$ sont bornés si $|\sigma_i(x)| = 1$), et c'est exactement l'ensemble des racines de l'unité contenues dans A^*.

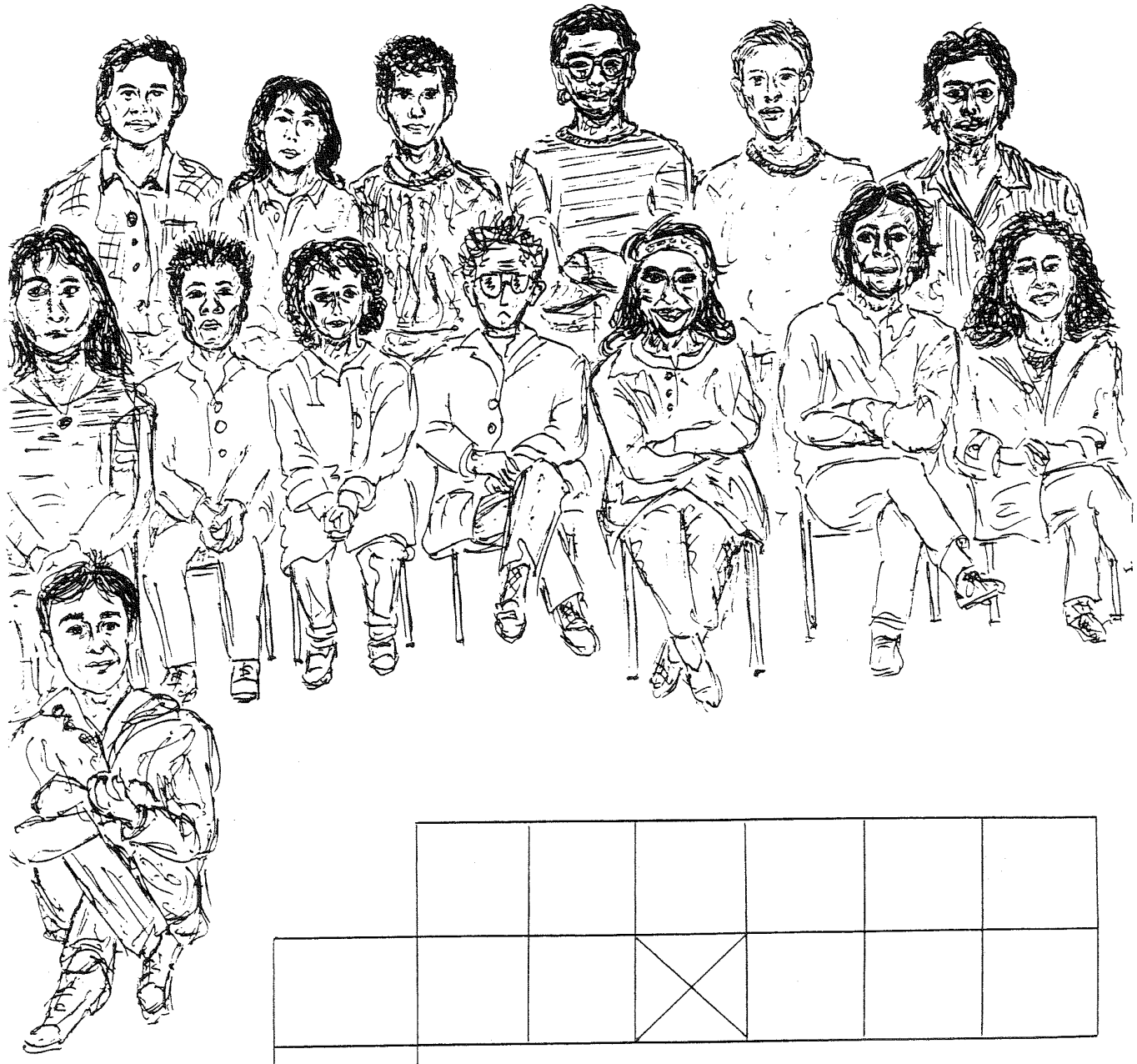
Ce groupe est cyclique : soit $\gamma \in G$ d'ordre le p.p.c.m des ordres des éléments de G (existe par le théorème de classification) ; si m est son ordre, $\gamma^m = 1$, et tout élément de G est racine de $X^m - 1$; donc G est engendré par γ.

Théorème VI.4.1 (Dirichlet) : soit K un corps de nombres de degré $n = r_1 + 2r_2$, A^* le groupe des unités de $A = \mathcal{O}_K$, G le groupe cyclique fini des racines de 1 contenues dans A ; alors : $A^* \approx \mathbb{Z}^{r_1+r_2-1} \times G$

C'est à dire : il existe un système $(u_1, \cdots, u_r)$ d'unités "fondamentales" $(r = r_1 + r_2 - 1)$ tel que toute unité x de A s'écrive de manière unique $x = \gamma u_1^{n_1} u_2^{n_2} \cdots u_r^{n_r}$ avec $\gamma \in G$ et $(n_1, \cdots, n_r) \in \mathbb{Z}^r$.

EXERCICES

En plus, votre cadeau :
la photo de classe (noir et blanc) à
accrocher dans votre salon. Facultatif : mettre des noms.



- Bande décimée -

SUITES EXACTES COURTES

Feuille de T.D. N°I

1) Soit E un A-module, et E_1, E_2, F, F_1, F_2 des sous-modules de E tels que : $E = E_1 \oplus E_2$, $F = F_1 \oplus F_2$, $F_1 \subset E_1$, $F_2 \subset E_2$.

Montrer que : $\frac{E}{F} \approx \frac{E_1}{F_1} \oplus \frac{E_2}{F_2}$ (isomorphisme canonique).

2) Soient F et G deux sous-modules d'un A-module E. Montrer : $\frac{F+G}{G} \approx \frac{F}{F \cap G}$ (isomorphisme canonique).

Soient $E \subset F \subset G$ des A-modules. Montrer : $(G/E)/(F/E) \approx G/F$

3) Soit la suite exacte courte de A-modules : $0 \longrightarrow E \xrightarrow{u} F \xrightarrow{v} G \longrightarrow 0$

Montrer l'équivalence des conditions suivantes :

(i) $\mathrm{Im}(u)$ est facteur direct de F (i.e. $\exists\, H \subset F$ tel que $F = \mathrm{Im}(u) \oplus H$)

(ii) v admet une section (i.e. $s : G \longrightarrow F$ tel que $v \circ s = 1_G$)

(iii) u admet une rétraction (i.e. $r : F \longrightarrow E$ tel que $r \circ u = 1_E$)

On dit alors que <u>la suite exacte est scindée</u>.

4) Soit la suite exacte courte : $0 \longrightarrow E \xrightarrow{u} F \xrightarrow{v} G \longrightarrow 0$

a) Montrer que si la suite exacte est scindée, F est isomorphe à $E \oplus G$.

b) Montrer que si G est libre, la suite est scindée.

c) Etudier les exemples :

- $A = K$ corps.
- $A = \mathbb{Z}$; $0 \longrightarrow \mathbb{Z} \xrightarrow{2\times} \mathbb{Z} \xrightarrow{\text{can}} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$

  $0 \longrightarrow \mathbb{Z} \xrightarrow{u} \mathbb{Z}^2 \xrightarrow{\text{can}} \mathbb{Z}^2/\mathrm{Im}(u) \longrightarrow 0 \qquad u(t) = (at, bt) \quad a \neq 0$

  $0 \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow \mathbb{R}/\mathbb{Z} \longrightarrow \mathbb{R}/\mathbb{Q} \longrightarrow 0$ (Remarquer que $\mathbb{Q}$ est facteur direct de $\mathbb{R}$ comme $\mathbb{Q}$ espace vectoriel, donc comme $\mathbb{Z}$-module).
- $A = k[x,y]$, k corps ; $0 \longrightarrow A \xrightarrow{u} A^2 \xrightarrow{v} M \longrightarrow 0$

  $u(t) = (ty, -tx) \qquad v(p,q) = px + qy \qquad M = Ax + Ay$

5) On dit qu'un A-module P est <u>projectif</u> si : pour tout $v : F \longrightarrow G$ morphisme surjectif, tout $h : P \longrightarrow G$, il existe $\bar{h} : P \longrightarrow F$, $v \circ \bar{h} = h$.

a) Montrer que P est projectif si et seulement si P est facteur direct d'un A-module libre (i.e. il existe L libre , $a : P \longrightarrow L$ injectif , et $M \subset L$ tels que $L = a(P) \oplus M$) .

b) Montrer que si G est projectif , la suite exacte courte de l'exercice 3) est scindée .

c) On prend $A = \mathbb{Z}/6\mathbb{Z}$; établir l'égalité : $\mathbb{Z}/6\mathbb{Z} = (\mathbb{Z}/2\mathbb{Z}) + (\mathbb{Z}/3\mathbb{Z})$; les A-modules $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$ sont ils libres ? Projectifs ?

6) On dit qu'un A-module I est <u>injectif</u> si pour tout morphisme injectif $u : E \longrightarrow F$ et tout $h : E \longrightarrow I$, il existe $\bar{h} : F \longrightarrow I$, $\bar{h} \circ u = h$.

a) Montrer que si E est injectif , la suite exacte courte de l'exercice 3) est scindée .

b) On prend $A = \mathbb{Z}$; A n'est pas un A-module injectif !

Feuille de T.D. N°2

IDEAUX PREMIERS - IDEAUX MAXIMAUX

(A désigne un anneau commutatif unitaire)

1) On dit que $a \in A$ est une unité si il existe $b \in A$ tel que $ab = 1$.
Montrer que les unités de A forment un groupe abélien (pour la multiplication) ; on le note A^*.
Que dire d'un idéal de A qui contient une unité ?
Déterminer les groupes $\mathbb{Z}[i]^*$, $\mathbb{Z}[x]^*$, $\mathbb{Q}[x]^*$.

2) Soit M un idéal de A distinct de A ; On suppose que tout élément de A qui n'est pas dans M est une unité . Montrer que M est un idéal maximal de A , et que A ne possède pas d'autre idéal maximal . (On dit alors que A est un anneau local).
Réciproquement , montrer que si A possède un unique idéal maximal M , A-M est le groupe des unités de A .
Exemples : K étant un corps commutatif , l'anneau $K[[x]]$ des séries formelles et l'anneau $K[x]_{(x)}$ des fractions rationnelles dont le dénominateur ne s'annule pas en 0 sont des anneaux locaux . Préciser leurs idéaux maximaux .

3) Soit M un idéal maximal de A . On suppose que pour tout $x \in M$, $1+x$ est une unité de A . Montrer que M est l'unique idéal maximal de A .

4) Soit A un anneau principal . Montrer que tout idéal premier non nul est maximal .

5) On dit que $x \in A$ est nilpotent si il existe un entier positif n tel que $x^n = 0$.

a) Montrer que l'ensemble N des éléments nilpotents de A est un idéal de A ("nilradical" de A , noté 0) .

Exemple : déterminer le nilradical de l'anneau quotient ; $\mathbb{C}[x.y]/(x^2y^3)$.

b) Montrer que l'anneau A/N est <u>réduit</u> , c'est à dire qu'il n'a pas d'élément nilpotent non nul .

6) Soit $x \in A$; montrer : x nilpotent $\Longrightarrow$ $1 - x$ unité

7) Montrer que le nilradical de A est l'intersection des idéaux premiers de A . (Pour x non nilpotent , appliquer le lemme de Zorn à la famille Σ des idéaux de A ne coupant pas $(x^n)_{n>0}$ et montrer qu'un élément maximal de Σ est un idéal premier .)

8) Soit R l'intersection de tous les idéaux maximaux de A . Montrer :

$$x \in R \iff \forall y \in A \ , \ 1 - xy \in A^*$$

9) Soit I un idéal de A ; la <u>racine</u> de I est : $\sqrt{I} = \left\{ x \in A \ / \exists n>0 \ \ x^n \in I \right\}$

Vérifier que c'est encore un idéal , puis montrer :

(i) $\sqrt{I} \supset I$; $\sqrt{\sqrt{I}} = \sqrt{I}$; $\sqrt{IJ} = \sqrt{I} \cap \sqrt{J} = \sqrt{I \cap J}$

(ii) $\sqrt{I} = A \iff I = A$

(iii) $\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$

(iv) I premier $\Rightarrow \sqrt{P^n} = P \quad \forall n>0$

10) Montrer que $\sqrt{I} = I$ si et seulement si A/I est réduit . Montrer que I est l'intersection des idéaux premiers contenant I (Utiliser 7)) .

11) On prend $A = \mathbb{Z}$, $I = m\mathbb{Z}$ où $m = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ (décomposition en facteurs premiers) . Reconnaître $\sqrt{I}$.

12) On prend $A = \mathbb{C}[x,y]$, I l'idéal (x^2-y^3, xy) ; montrer que $\sqrt{I} = (x,y)$.

13) On prend $A = k[x,y]$ où k est un corps infini .

a) Montrer , pour $f \in A$ non nul , l'existence d'un idéal maximal M de A ne contenant pas f (considérer $(a,b) \in k^2$ tel que $f(a,b) \neq 0$) .

b) En déduire que l'intersection des idéaux maximaux de A est réduite à 0 .

14) Soit A principal , ayant une infinité d'éléments irréductibles ; $\bigcap_{I \text{ max.}} I = 0$.

MODULES ET ANNEAUX QUOTIENTS

LEMME DE NAKAYAMA

Feuille de T.D. N°3

1) A désigne toujours un anneau commutatif et unitaire .

a) Soit I un idéal de A , M un A/I -module ; montrer que M est un A-module .

b) Soit M un A-module . On pose $\mathrm{Ann}(M) = \{ a \in A \ / \ aM = 0 \}$ ("annulateur")

Montrer que $\mathrm{Ann}(M)$ est un idéal de A .

Montrer que M est "naturellement" un A/I -module si et seulement si $I \subset \mathrm{Ann}(M)$.

c) Soient N et N' des A/I -modules . Montrer que $f : N \longrightarrow N'$ est A-linéaire si et seulement si elle est A/I-linéaire .

2) Soient I un idéal de A et M un A-module . On pose :

$$IM = \left\{ \sum_k a_k m_k \ , \text{ sommes finies } / \ a_k \in I \quad m_k \in M \right\}$$

a) Montrer que IM est un sous-module de M . Etudier le cas où M est un idéal de A .

b) Soient M' et M" des sous-modules de M ; comparer $I(M'+M")$ et $IM'+IM"$; $I(M' \cap M")$ et $IM' \cap IM"$. Y-a-t-il des inclusions évidentes ? (on pourra regarder $A = k[x,y]$, $M' = Ax$, $M" = Ay$, $I = (x,y)$).

c) Montrer que M/IM est naturellement un A/I-module .

Qu'est-ce que $I(M/IM)$?

3) Soit I un idéal de A . Montrer que l'on a un isomorphisme de A-modules :

$$\mathrm{Hom}_A(I , A/I) \xrightarrow{\approx} \mathrm{Hom}_{A/I} (I/I^2 , A/I)$$

4) Soient I et J deux idéaux de A ; on note $\bar{I}$ et $\bar{J}$ les images de I et J dans A/I . Monter que :

$$\bar{I} + \bar{J} = \overline{I+J} \quad , \quad \bar{I} \cap \bar{J} = \overline{I \cap J} \quad , \quad \bar{I}\,\bar{J} = \overline{IJ}$$

5) On prend $A = k[x]$, $B = \{ P \in A \ / \ P'(0) = 0 \}$; vérifier que B est

un sous-anneau de A . Montrer que l'ensemble $I = \{P \in A \ / \ P(0) = P'(0) = 0\}$ est un idéal non principal de B .

6) Soient A un anneau local d'idéal maximal M , E un A-module de type fini non réduit à 0 . Soit $(e_1, e_2, \ldots, e_k)$ un système de générateurs de E de cardinal minimum .

a) Montrer que l'application f de M^k dans E qui à $(a_1, a_2, \ldots, a_k)$ associe l'élément $a_1e_1+a_2e_2+\ldots+a_ke_k$ de E est A-linéaire et non surjective (montrer $e_1 \notin \mathrm{Im}(f)$).

b) En déduire $ME \neq E$. (Lemme de Nakayama) .

7) Soit I un idéal de A et : $E \xrightarrow{u} F \xrightarrow{v} G \longrightarrow 0$ une suite exacte de A-modules . Montrer que la suite qui s'en déduit :

$$E/IE \xrightarrow{\bar{u}} F/IF \xrightarrow{\bar{v}} G/IG \longrightarrow 0$$

est aussi exacte .

Application : soit $f : E \longrightarrow F$ un morphisme de A-modules , avec F de type fini et A local d'idéal maximal M . Montrer que si $\bar{f}$ de E/ME vers F/MF est surjective , alors f est surjective (poser $G = \mathrm{Coker}(f)$ et appliquer le lemme de Nakayama) .

8) Soit A un anneau local noethérien d'idéal maximal M , de corps résiduel $k = A/M$;

a) Montrer que le nombre minimum de générateurs d'un idéal I de A est égal à : $\dim_k(I/MI)$.

b) On suppose $\dim_k(M/M^2) = 1$; soit $t \in M$, $t \notin M^2$. Montrer que la multiplication par t définit une application linéaire f de A vers M surjective et en déduire $M=At$.

ANNEAUX DE VALUATION DISCRETE

Feuille de T.D. N°4

Partie I

Soit A un anneau local, intègre, noethérien, et soit M son idéal maximal ; on suppose que M est principal, et on note t un générateur. On note $K = \mathrm{Frac}(A)$.

1) Soit $a \in M^n$ pour tout entier n ; on écrit : $a = tu_1 = t^2u_2 = t^3u_3 = \ldots$ Montrer : $(u_1) \subset (u_2) \subset (u_3) \ldots$ et en déduire $a = 0$. D'où : $\bigcap M^n = 0$.

2) Pour a non nul dans A, montrer l'existence de n entier tel que $a \in M^n$ et $a \notin M^{n+1}$. En déduire l'écriture unique : $a = t^n u$; u inversible. On pose $v(a) = n$ (et $v(0) = +\infty$).

3) Montrer que tous les idéaux de A sont de la forme M^n (pour un $n \in \mathbb{N}$).

4) Pour $x \in K$, x s'écrit a/b avec $a \in A$ et $b \in A - \{0\}$. On pose : $v(x) = v(a) - v(b)$. Montrer que v est bien définie de K dans $\mathbb{Z}$ et vérifie : $v(x + y) \geqslant \mathrm{Min}(v(x), v(y))$; $v(xy) = v(x) + v(y)$.

Partie II

Soit A un anneau noethérien intègre, $K = \mathrm{Frac}(A)$. On suppose que tout $x \in K$ vérifie $x \in A$ ou $1/x \in A$.

1) Montrer que la somme $(a) + (b)$ de deux idéaux principaux de A est un idéal principal. (Distinguer selon que $a/b \in A$ ou $b/a \in A$). Montrer que A est principal.

2) Soient a et b dans A avec $a+b$ inversible dans A. Montrer que soit a soit b est inversible dans A ; utiliser pour cela l'égalité : $1/b = (a+b)^{-1}(1 + a/b)$. En déduire que A est local.

Partie III

Soit A un anneau local noethérien admettant un unique idéal premier $\neq 0$ noté M (qui est bien sûr maximal).

1) Montrer que tout idéal I de A non nul contient une puissance de M (Considérer un élément maximal de la famille des idéaux non nuls

de A ne satisfaisant pas la propriété demandée - si cette famille est non vide - . Voir aussi le lemme V.2.4) .

2) On suppose de plus A intègre ; soit K=Frac(A) ; on pose : $I = \{ x \in K \ / \ xM \subset A \}$ Montrer : $I \supset A \supset IM \supset M$. Soit $a \in M$ non nul , r minimal tel que $M^r \subset Aa$. De $M^{r-1} \not\subset Aa$, déduire qu'il existe $b \in A$, $b/a \in I - A$. Conclure $I \neq A$.

3) On suppose A intégralement clos dans K ; montrer que $IM = M$ implique $I = A$, et conclure $IM = A$.

4) Soit $\mathcal{F}$ la famille des idéaux J de A tels que $J \neq M^s$ pour tout $s \in \mathbb{N}$; On suppose $\mathcal{F}$ non vide , et on prend un élément J_o maximal dedans . Montrer $J_o \subset J_o I \subset A$ puis $J_o \neq J_o I$.

5) Conclure : $J_o I = M^t$ puis $J_o = M^{t+1}$ d'où la contradiction .

Partie IV

Démontrer le théorème suivant : soit A un anneau noethérien intègre et K = Frac(A) ; les conditions suivantes sont équivalentes :

(i) $A \neq K$, est local et principal .

(ii) A est local et $\dim_k(M/M^2) = 1$ (M est l'idéal maximal et $k=A/M$)

(iii) $A \neq K$ est local et M est principal .

(iv) $A \neq K$ est local et tout idéal de A est de la forme M^s , $s \in \mathbb{N}$.

(v) $A \neq K$ et les idéaux de A sont totalement ordonnés par inclusion .

(vi) $A \neq K$ et les idéaux principaux de A sont totalement ordonnés par inclusion .

(vii) Pour $x \in K$, si $x \notin A$ alors $1/x \in A$.

(viii) Il existe un morphisme de grouges non nul $v : K \longrightarrow \mathbb{Z}$ vérifiant $v(x+y) \geqslant \mathrm{Min}(v(x), v(y))$ et $x \in A \Leftrightarrow v(x) \geqslant 0$

(ix) A possède un seul idéal premier non nul et A est intégralement clos dans K .

Indication : montrer les implications

$$(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (iv) \Rightarrow (v) \Rightarrow (vi) \Rightarrow (vii) \Rightarrow (i)$$

puis $(i) \Rightarrow (ix) \Rightarrow (iv)$ et $(iii) \Rightarrow (viii) \Rightarrow (i)$

On appelle anneau de valuation discrète un anneau local principal ; la terminologie vient de (viii) , l'application v étant appelée une valuation discrète .

Partie V

Soit A un anneau de valuation discrète et $K = \mathrm{Frac}(A)$. Soit B un sous anneau noethérien de K avec : $A \subset B \subset K$.

1) Montrer que B est un anneau de valuation discrète (utiliser (vii)) .

2) Si N désigne l'idéal maximal de B (et M celui de A) , discuter de $N \cap A \neq 0$: montrer alors que $A = B$.

COMPLEXIFIE D'UN ESPACE VECTORIEL REEL

Feuille de T.D. N°5

1) Soit V un espace vectoriel réel et J un endomorphisme de V avec $J^2 = -\mathrm{id}_V$
Montrer que si V est de dimension finie, $\dim_{\mathbb{R}} V$ est paire.

2) Montrer que la loi externe suivante : $\mathbb{C} \times V \longrightarrow V$

a et b réels $\qquad (a+ib, x) \longmapsto ax + bJ(x)$

fait de V un espace vectoriel sur $\mathbb{C}$. En déduire qu'il existe une infinité de structures d'espace vectoriel complexe sur un espace vectoriel réel non nul de dimension paire (compatibles avec la structure réelle).

3) Soit E un espace vectoriel réel, $V = E \oplus E$ et $J : V \longrightarrow V$ défini par $J(x,y) = (-y,x)$. Vérifier $J^2 = -\mathrm{id}_V$; on note $E^{\mathbb{C}}$ l'espace vectoriel complexe ainsi obtenu. Calculer $i.(x,0)$. On identifie E à un sous espace réel de $E^{\mathbb{C}}$ par $x \longmapsto (x,0)$. Tout vecteur de $E^{\mathbb{C}}$ s'écrit alors de manière unique $x + iy$ avec $x \in E$, $y \in E$. L'espace $E^{\mathbb{C}}$ s'appelle le complexifié de E. Lorsque $\dim_{\mathbb{R}} E$ est finie, que vaut $\dim_{\mathbb{C}} E^{\mathbb{C}}$?

4) Montrer la propriété universelle de $E^{\mathbb{C}}$: pour toute application $\mathbb{R}$-linéaire $u : E \longrightarrow W$ où W est un espace vectoriel complexe, u admet un prolongement $\mathbb{C}$-linéaire unique $\bar{u} : E^{\mathbb{C}} \longrightarrow W$.
En particulier si $f : E \longrightarrow F$ est une application $\mathbb{R}$-linéaire entre espaces vectoriels réels, on lui associe $f^{\mathbb{C}} : E^{\mathbb{C}} \longrightarrow F^{\mathbb{C}}$ $\mathbb{C}$-linéaire.
Montrer qu'on vient de définir un foncteur de la catégorie des espaces vectoriels réels vers celle des espaces vectoriels complexes.

5) Soit E un espace vectoriel réel ; montrer que $E \otimes_{\mathbb{R}} \mathbb{C}$ est naturellement muni d'une structure de $\mathbb{C}$-espace vectoriel (par opération de $\mathbb{C}$ sur le second facteur), et qu'on a un isomorphisme : $E \otimes_{\mathbb{R}} \mathbb{C} \longrightarrow E^{\mathbb{C}}$
qui à $x \otimes z$ associe $z.x$.

EXTENSIONS QUADRATIQUES IMAGINAIRES ET RESEAUX DANS $\mathbb{C}$.

Feuille de T.D. N°6

Soit $D \geqslant 1$ un entier qui n'est pas divisible par le carré d'un nombre premier . On pose $w_D = i\sqrt{D}$ si $D \equiv 1$ ou $2 \pmod 4$

$w_D = \frac{1 + i\sqrt{D}}{2}$ si $D \equiv 3 \pmod 4$

et on note $A = \mathbb{Z}[w_D]$.

1) Dans le plan complexe , on désigne par A , B , C les images respectives des nombres 0 , 1 , w_D et par T le triangle enveloppe convexe de A,B,C. Le rayon du cercle circonscrit à T est noté R .

a) Montrer que pour tout point de T on a : $\inf(MA,MB,MC) \leqslant R$

b) On pose : $k = \sup_{z \in \mathbb{C}} \left(\inf_{u \in A} |z - u|^2 \right)$

Prouver l'égalité : $k = \sup_{M \in T} \left(\inf (MA^2, MB^2, MC^2) \right)$

c) En déduire :

$k = \frac{D + 1}{4}$ si $D \equiv 1$ ou $2 \pmod 4$ $\qquad$ $k = \frac{(D + 1)^2}{16D}$ si $D \equiv 3 \pmod 4$

2) Soient a et b deux éléments de $A = \mathbb{Z}[w_D]$, $b \neq 0$. Montrer qu'il existe $c \in A$ tel que $|a - bc|^2 \leqslant k\,|b|^2$.

En déduire que A est un anneau Euclidien pour D égal à l'une des valeurs suivantes : 1 , 2 , 3 , 7 , 11 .

3) Trouver les unités de $A = \mathbb{Z}[w_D]$.

4) Entiers de Gauss .

Soit $R = \mathbb{Z}[i]$, $N(a+ib) = a^2+b^2$.

a) Montrer que si $N(v)$ est un nombre premier , v est irréductible dans R . Montrer que la conclusion est la même lorsque $N(v) = r^2$ avec r premier , $r \equiv 3 \pmod 4$.

Donner la décomposition de 2 et de 5 en produit de facteurs irréductibles.

b) Soit p un nombre premier, $p \equiv 1 \pmod 4$.

En utilisant le fait que le groupe multiplicatif $\mathbb{Z}/p\mathbb{Z}^*$ est cyclique, montrer l'existence d'un entier n tel que $n^2 \equiv -1 \pmod p$.

En déduire que p est réductible dans R (sinon p diviserait $n^2+1 = (n+i)(n-i)$ ...).

En déduire que p est la somme de deux carrés.

c) Décrire les éléments irréductibles de $\mathbb{Z}[i]$.

5) Soit $B = \mathbb{Z}[i\sqrt{3}]$

Soit I l'idéal de B engendré par 2 et $1+i\sqrt{3}$. Montrer que $I \neq 2B$ et $I^2 = 2I$. Montrer que $I = \{ a+bi\sqrt{3} \ / \ a \equiv b \mod 2 \}$ est un idéal premier, et que c'est l'unique idéal premier contenant $2B$. En déduire que $2B$ ne peut s'écrire comme produit d'idéaux premiers.

6) Soit $A = \mathbb{Z}[i\sqrt{5}]$

a) montrer que $N(a) = 2$ ou $N(a) = 3$ est impossible pour $a \in A$.

b) Montrer que 2, 3, $1+i\sqrt{5}$, et $1-i\sqrt{5}$ sont irréductibles dans A.

c) Contempler l'égalité $6 = 2\times 3 = (1+i\sqrt{5})(1-i\sqrt{5})$ et conclure que A n'est pas factoriel.

7) Soit $A = \mathbb{Z}\left[\frac{1+i\sqrt{11}}{2}\right]$

On cherche les solutions dans $\mathbb{Z}$ de l'équation : $y^2 = x^3 - 11$.

a) Dresser la table des carrés de $\mathbb{Z}/8\mathbb{Z}$ et montrer que x est impair. Montrer que x ne peut être multiple de 11.

b) Soit $d \in A$ un facteur commun à $y+i\sqrt{11}$ et $y-i\sqrt{11}$ dans A. Montrer que $N(d)$ divise 44 et x^3. En déduire que $N(d) = 1$ puis que $y+i\sqrt{11}$ et $y-i\sqrt{11}$ sont premiers entre eux.

c) Montrer que $y+i\sqrt{11}$ est un cube $\left(a + b\,\frac{1+i\sqrt{11}}{2} \right)^3$ dans A et que : $x = a^2 + ab + 3b^2$; $2 = b\,(3a^2 + 3ab - 2b^2)$ avec $(a,b) \in \mathbb{Z}^2$.

d) En déduire les solutions de l'équation : $(3 , \pm 4)$ et $(15 , \pm 58)$.

ANNEAUX ET CORPS DE NOMBRES

Feuille de T.D. N°7

Soit $P(x) = x^3 + x^2 - 2x + 8$.

1) Vérifier que P est irréductible dans $\mathbb{Q}[x]$. Soit α une racine de P et $K = \mathbb{Q}[\alpha]$. Calculer Disc(M) où $M = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\alpha^2$.

2) On pose $\beta = 4/\alpha$. Montrer $\beta \in \mathcal{O}_K$; vérifier les relations :

$\alpha^2 = -\alpha + 2 - 2\beta$ et $\beta^2 = -2\alpha - 2 + \beta$.

On pose $M' = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\beta \subset \mathcal{O}_K$. Vérifier $M' \supset M$ et $M' \neq M$.

En déduire $M' = \mathcal{O}_K$ et $\mathrm{Disc}(\mathcal{O}_K) = 503$.

3) On cherche à décomposer l'idéal $2.\mathcal{O}_K$. Si $\mathcal{P}$ est un idéal premier de $\mathcal{O}_K$ au dessus de 2 , montrer que dans le diagramme commutatif :

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathcal{O}_K = \mathbb{Z}[\alpha,\beta] \\ \downarrow & & \varphi\downarrow \\ \mathbb{F}_2 & \longrightarrow & \mathcal{O}_K/\mathcal{P} \end{array}$$

on a :

$\bar{\alpha}^2 = \bar{\alpha}$, $\overline{\alpha\beta} = 0$, $\bar{\alpha}^2 = \bar{\beta}$ où $\bar{\alpha} = \varphi(\alpha)$ et $\bar{\beta} = \varphi(\beta)$.

En déduire le degré résiduel : $f_{\mathcal{P}} = (\mathcal{O}_K/\mathcal{P} : \mathbb{F}_2) = 1$.

4) Soient $\varphi, \varphi', \varphi''$ les morphismes d'anneaux de $\mathcal{O}_K$ dans $\mathbb{F}_2$ définis par:

$$\begin{cases} \varphi(\alpha) = 0 \\ \varphi(\beta) = 0 \end{cases} \qquad \begin{cases} \varphi'(\alpha) = 1 \\ \varphi'(\beta) = 0 \end{cases} \qquad \begin{cases} \varphi''(\alpha) = 0 \\ \varphi''(\beta) = 1 \end{cases}$$

Soient $\mathcal{P}_2$, $\mathcal{P}_2'$, $\mathcal{P}_2''$ leurs noyaux respectifs . Grâce à ce qui précède , montrer que $2\mathcal{O}_K = \mathcal{P}_2\,\mathcal{P}_2'\,\mathcal{P}_2''$.

5) On écrit $I|J$ pour I divise J (ou $I \supset J$) ; (x) pour $x\mathcal{O}_K$.

Montrer : $N(\alpha) = N(\beta) = 8$. En déduire que tout idéal premier diviseur de (α) ou (β) est au dessus de 2 . Montrer :

$$\begin{cases} \mathcal{P}_2 \mid (\alpha) \\ \mathcal{P}_2 \mid (\beta) \end{cases} \qquad \begin{cases} \mathcal{P}_2' \nmid (\alpha) \\ \mathcal{P}_2' \mid (\beta) \end{cases} \qquad \begin{cases} \mathcal{P}_2'' \mid (\alpha) \\ \mathcal{P}_2'' \nmid (\beta) \end{cases}$$

De $(\alpha)(\beta) = (4) = (\mathfrak{P}_2\,\mathfrak{P}_2'\,\mathfrak{P}_2'')^2$ déduire : $(\alpha) = \mathfrak{P}_2\,\mathfrak{P}_2''^2$ $(\beta) = \mathfrak{P}_2\,\mathfrak{P}_2'^2$

6) Calculer les termes constants des polynômes :

$P(x+2)$, $P(x-2)$, $P(x+1)$, $P(x-3)$

et les normes des idéaux : $(\alpha-2)$, $(\alpha+2)$, $(\alpha-1)$, $(\alpha+3)$.

En déduire que tout diviseur premier de ces quatre idéaux est au dessus de 2 .

Montrer que $\mathfrak{P}_2'$ divise $(\alpha-1)$ et $(\alpha+3)$, mais ni $\mathfrak{P}_2$ ni $\mathfrak{P}_2''$ ne divisent $(\alpha-1)$ ou $(\alpha+3)$.

En déduire : $(\alpha-1) = \mathfrak{P}_2'^3$ et $(\alpha+3) = \mathfrak{P}_2'^2$; puis que $\mathfrak{P}_2'$ est principal .

7) Montrer que $\mathfrak{P}_2$ et $\mathfrak{P}_2''$ divisent $(\alpha+2)$ et $(\alpha-2)$, mais que $\mathfrak{P}_2'$ ne divise ni l'un ni l'autre .

Soit A l'anneau de valuation discrète $\mathcal{O}_{K,\mathfrak{P}_2''}$ et $v : A \longrightarrow N$ la valuation associée , normalisée :

$$v(x) = n \iff x \in \mathfrak{P}_2''^n \text{ et } x \notin \mathfrak{P}_2''^{n+1}$$

Montrer : $v(\alpha \pm 2) = 1$ (Utiliser $v(x+y) = \inf(v(x), v(y))$ lorsque $v(x) = v(y)$) .

En déduire , vu les normes : $(\alpha-2) = \mathfrak{P}_2^3\mathfrak{P}_2''$ et $(\alpha+2) = \mathfrak{P}_2^2\mathfrak{P}_2''$

8) Montrer que $\mathfrak{P}_2$ est principal , puis que $\mathfrak{P}_2''$ est principal .

UNIVERSITE DE NICE
U.A 168 - LABORATOIRE DE MATHEMATIQUES
ANNEE 1987/1988.

M 2 - ALGEBRE APPROFONDIE
Premier partiel (8 février 1988)

AUCUN DOCUMENT AUTORISE

I. - Soit R l'anneau des entiers de $\mathbb{Q}(\sqrt{-29})$.

a) Décomposer de deux façons non équivalentes l'entier 30 en produits d'irréductibles de R .

b) Décomposer l'idéal $30R$ de R en produit d'idéaux premiers.

c) Donner la liste des idéaux entiers de R qui contiennent 30.

d) L'anneau R est-il principal ?

II.- a) Si $G,+$ est un groupe abélien fini, prouver qu'il existe un entier $n > 0$ avec $nG = \{0\}$ i.e. $\forall g \in G$, $ng = 0$.

b) Prouver que si $I \subset A$ est un idéal non-nul de l'anneau des entiers d'un corps de nombres, alors $N(I) \in I$.

c) Quels sont les idéaux de $\mathbb{Z}[\sqrt{2}]$ dont la norme est 18 ?

III.- Soit $\alpha = \exp\left(\frac{2i\pi}{23}\right)$. L'idéal principal (α) de l'anneau $\mathbb{Z}[\alpha]$ est-il premier ? maximal ? A-t-on $\mathbb{Z}[\alpha]/_{(\alpha)} \simeq \mathbb{Z}$ (isomorphismes d'anneaux) ?

I M S P MATHEMATIQUES, Année 1987/1988

1ère SESSION d'EXAMENS JUIN 1988

MAITRISE DE MATHEMATIQUES FONDAMENTALES

M 2 - A L G E B R E

Jeudi 2 Juin 1988

DOCUMENTS INTERDITS.

I . Soit $P(X)$ le polynôme $X^3 + X^2 - 2X - 1 \in \mathbb{Q}[X]$.

I. 1) Prouver que P est irréductible (sur $\mathbb{Q}$) .

I. 2) Soit $f(Y) = P(Y - \frac{1}{3})$; Prouver que f possède trois racines réelles notées (η_1, η_2, η_3) et Calculer $\prod_{i=1}^{3} f'(\eta_i)$.

En déduire que P a trois racines réelles (ξ_1, ξ_2, ξ_3) et calculer $\prod_{i=1}^{3} P'(\xi_i)$.

I. 3) On fixe ξ une racine de P et on note $K = \mathbb{Q}(\xi)$ le corps de nombres et $A = \mathcal{O}_K$ son anneau d'entiers.

Démontrer $\mathrm{Disc}\ \mathbb{Z}[\xi] \subset A \subset \frac{1}{7}\mathbb{Z}[\xi]$.

Exprimer $\mathrm{Disc}\ \mathbb{Z}[\xi]$ en fonction de $\mathrm{Disc}\ A$ et de l'indice de $\mathbb{Z}[\xi]$ dans A ; prouver que l'inclusion stricte $\mathbb{Z}[\xi] \subsetneq A$ conduirait à une valeur interdite pour $\mathrm{Disc}\ A$.

I. 4) Calculer le nombre de classe (s) de K .

I. 5) Décomposer $2A$, $3A$, $7A$ en produit d'idéaux premiers.

II . Soit $\theta = e^{2i\pi/7}$, $L = \mathbb{Q}(\theta)$ l'extension cyclotonique de niveau 7 de $\mathbb{Q}$, $B = \mathcal{O}_L$ son anneau d'entiers.

II. 1) Déterminer les extensions intermédiaires $\mathbb{Q} \subsetneq M \subsetneq L$ (on précisera leur degré sur $\mathbb{Q}$; sont-elles galoisiennes sur $\mathbb{Q}$?) .

II. 2) On pose $\alpha = \theta + \theta^6$; calculer le polynôme minimal de α sur $\mathbb{Q}$ et prouver que $\mathbb{Q}[\alpha] = L \cap \mathbb{R} = K$.

II. 3) Décomposer $2B$ et $3B$ en produit d'idéaux premiers (utiliser pour cela la question I.5) . Calculer le nombre de classes de L .

IMSP MATHEMATIQUES
2ème SESSION DE SEPTEMBRE 1988

Maîtrise de Mathématiques Fondamentales

M 2 - A L G E B R E
MERCREDI 14 Septembre 1988

A U C U N D O C U M E N T A U T O R I S E

DUREE : 3heures

On désigne par α la racine réelles dun polynôme $X^3 + X + 1$, par β et $\bar{\beta}$ ses deux autres racines dans $\mathbb{C}$; on pose $K = \mathbb{Q}[\alpha]$ et on désigne par $A = \mathcal{O}_K$ l'anneau des entiers de K .

1 . Etablir que $A = \mathbb{Z}[\alpha]$ et que A est principal .

2 . Montrer : $\beta + \bar{\beta} = -\alpha$, $\beta\bar{\beta} = -\frac{1}{\alpha}$, $[(\beta-\alpha)(\bar{\beta}-\alpha)(\beta-\bar{\beta})]^2 = -31$ et en déduire que $K[i\sqrt{31}] = \mathbb{Q}[\alpha, \beta, \bar{\beta}]$. Montrer que ce corps de nombres $L = \mathbb{Q}[\alpha, \beta, \bar{\beta}]$ est une extension galoisienne de degré 6 de $\mathbb{Q}$ et déterminer son groupe de Galois G .

3 . Montrer que l'anneau des entiers $B = \mathcal{O}_L$ est $A\left[\frac{1+i\sqrt{31}}{2}\right]$.

4 . Décomposer 31 dans A ; montrer que la décomposition de 31 dans B est de la forme $\mathfrak{p}_1^2\ \mathfrak{p}_2^2\ \mathfrak{p}_3^2$ où $\mathfrak{p}_1$, $\mathfrak{p}_2$ et $\mathfrak{p}_3$ désignent des idéaux premiers distincts.

5 . Soit $M = \mathbb{Q}[i\sqrt{31}]$ et $C = \mathcal{O}_M$ son anneau d'entiers.

Décomposer 2 et 3 dans C . Montrer que toute classe d'idéaux de C contient un idéal de norme au plus 3 . Déterminer le groupe des classes de C .

N.B - On rappelle la formule de majoration $\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}|d|^{1/2}$

MAITRISE DE MATHEMATIQUES FONDAMENTALES — PARTIEL N°1

M 2 ALGEBRE 88-89 — Mardi 18 Avril 89

(I)- Soit $P(x) = x^5 - x + 1$

1) Décomposer P dans $\mathbb{Z}/2\mathbb{Z}[x]$, $\mathbb{Z}/3\mathbb{Z}[x]$, $\mathbb{Z}[x]$.

2) Soit $(\zeta_i)_{1 \leq i \leq 5}$ les racines de P dans $\mathbb{C}$; comparer $\prod \zeta_i P'(\zeta_i)$ et $P(\frac{5}{4})$; en déduire la valeur de $\prod P'(\zeta_i)$.

3) Soit $K = \mathbb{Q}(\alpha)$ où α est l'unique racine réelle de P ; déterminer l'anneau de nombres $A = \mathcal{O}_K$ correspondant .

4) Décomposer 2A en produit d'idéaux premiers dans A et donner la norme de ces idéaux .

5) Déterminer l'idéal de A au dessus de 19 en lequel 19 se ramifie .

NB : $2869 = 151 \cdot 19$

(II)- Soit $\theta = \sqrt[3]{3}$

1) Montrer que $K = \mathbb{Q}(\theta)$ est une extension de degré 3 ; soit $A = \mathcal{O}_K$ l'anneau d'entiers correspondant ; montrer que $A \subset \frac{1}{9}\mathbb{Z}[\theta]$.

2) Soit $\gamma = \frac{1}{3}(a+b\theta+c\theta^2)$ dans A , avec a , b , c dans $\mathbb{Z}$. Calculer γ^2 , sa trace ; en déduire que a est multiple de 3 et que $\frac{b}{3}\theta^2$ est dans A . En déduire : $A = \mathbb{Z}[\theta]$.

3) Soit $L = K(j)$ où $j = \exp(\frac{2i\pi}{3})$. Montrer que $L = \mathbb{Q}[\theta, j\theta, j^2\theta]$ et est une extension Galoisienne de $\mathbb{Q}$. Soit $\lambda = \frac{\theta^2}{j-1}$; calculer λ^6 . Décomposer 3 dans $\mathcal{O}_L$.

(III)- Soit $M = \mathbb{Q}(\zeta)$, $\zeta = \exp(\frac{2i\pi}{20})$, l'extension cyclotomique de hauteur 20 de $\mathbb{Q}$.

1) Déterminer le degré de l'extension M et le polynôme minimal Q de ζ .

2) Soit (η_k) les racines de $x^{10}+1 = S$; calculer $\prod_k \eta_k S'(\eta_k)$ et en déduire le discriminant absolu de M .

3) Quel est le groupe de Galois $G = \mathrm{Gal}(M/\mathbb{Q})$? Quels sont les éléments de G d'ordre 2 ?

4) Décomposer $2\mathcal{O}_M$ en produit d'idéaux premiers de $\mathcal{O}_M$. Déterminer le groupe de décomposition et le groupe d'inertie d'un idéal premier de $\mathcal{O}_M$ au dessus de 2 .

MAITRISE DE MATHEMATIQUES FONDAMENTALES — PARTIEL N°2

M 2 ALGEBRE — Mardi 23 Mai 89

PROBLEME I

Soit $(p,q)\in \mathbb{Z}^2$, $P(x) = x^3 + px + q \in \mathbb{Z}[x]$. On suppose P irréductible et $d = -(4p^3+27q^2) < 0$.

1) Montrer que P admet une unique racine réelle α ; on note $K = \mathbb{Q}[\alpha]$ et $A = \mathcal{O}_K$ l'anneau d'entiers de K . Quelle est la structure des unités de A ? Montrer que les unités positives de A sont de norme 1 et qu'elles forment un groupe libre admettant pour générateur la plus petite unité strictement supérieure à 1 .

2) Soit u une unité de A , $u>1$; on pose $u = \rho^2$, $(\rho>0)$; montrer que les conjugués de u sont de la forme $\frac{1}{\rho} e^{i\theta}$ et $\frac{1}{\rho} e^{-i\theta}$ où $\theta\in\mathbb{R}$; en déduire que $|d'| \leqslant 4u^3+24$ où $d'=\mathrm{Disc}(1,u,u^2)$. Montrer que le discriminant absolu d de A divise d' . On suppose $|d| > 4u^{3/2}+24$; montrer que u est générateur des unités positives de A .

3) On prend : $P(x) = x^3 + 10x + 1$; vérifier toutes les hypothèses utilisées plus haut ; déterminer A , d , et montrer que $-\frac{1}{\alpha} = \alpha^2 + 10$ est générateur du groupe des unités positives de A .

NB : 4027 est premier .

PROBLEME II

Soit $P(x) = x^5 - x + 1 \in \mathbb{Z}[x]$

1) Etudier la décomposition de P modulo 2 , 3 , 5 . Montrer que P est irréductible sur $\mathbb{Q}$.

2) Déterminer le nombre de racines réelles de P ; soit α une racine de P dans $\mathbb{C}$, $K = \mathbb{Q}[\alpha]$ le corps de nombres associé . Quel est le nombre de plongements réels de K ?

3) Calculer le discriminant de $\mathbb{Z}[\alpha]$ et en déduire : $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

NB : $2869 = 19 \times 151$

4) Donner la décomposition de (2) , (3) , (5) en produit d'idéaux premiers dans $\mathcal{O}_K$ et donner la norme des idéaux qui interviennent .

5) Montrer que $\mathcal{O}_K$ est principal .

UNIVERSITE DE NICE
IMSP MATHEMATIQUES

1ère SESSION D'EXAMENS 88/89.

MAITRISE DE MATHEMATIQUES FONDAMENTALES
M 2 - ALGEBRE

Mardi 6 Juin 89 de 9h à 12h

DOCUMENTSAUTORISES.
LES PARTIES I et II DU PROBLEME SONT INDEPENDANTES.

P A R T I E I .

Soit le polynôme $P(X) = X^3 - 3X + 1$ de $\mathbb{Z}[X]$.

1) Etudier la décomposition de P modulo 2, 3 et 5 . Montrer que P est irréductible et possède trois racines réelles. Soit α l'une de ces racines, $K = \mathbb{Q}[\alpha]$, $A = \mathcal{O}_K$ l'anneau de nombres correspondant et $A' = \mathbb{Z}[\alpha]$. Montrer :

$$A' \subset A \subset \frac{1}{9} A' .$$

2) Montrer que α et $\alpha + 2$ sont des unités de A' et que $(\alpha + 1)^3 = 3\alpha(\alpha + 2)$. Comparer la norme de $(\alpha + 1)$ et le nombre d'éléments de $A'/(\alpha + 1)A'$; en déduire $A = A' + (\alpha + 1)A$, puis $A = A' + 3A$, enfin $A' = A$.

3) Montrer que A est principal.

4) Montrer que $\alpha^2 - 2$ est aussi racine de P ; quels sont les corps conjugués de K sur $\mathbb{Q}$? K est-il une extension galoisienne de $\mathbb{Q}$?

P A R T I E II .

Soit L l'extension cyclotomique de hauteur 9 de $\mathbb{Q}$, $\xi = e^{2i\pi/9}$, $B = \mathcal{O}_L$ L'anneau des entiers de L .

1) Déterminer le polynôme minimal de ξ sur $\mathbb{Z}$, les conjugués de ξ , le groupe de Galois G de L sur $\mathbb{Q}$.

2) Déterminer le sous-groupe H de G d'ordre 3 ; l'extension intermédiaire S, $\mathbb{Q} \subset S \subset L$, formée des points fixes de L sous l'action des éléments de H ; l'anneau d'entiers $C = \mathcal{O}_S$.

3) Calculer le discriminant absolu de L sur $\mathbb{Q}$; quels sont les nombres premiers qui se ramifient dans B ?

PARTIE III

1) En utilisant la relation $\cos 3u = 4\cos^3 u - 3\cos u$, déterminer les valeurs possibles de u tel que $\alpha = 2\cos u$. En déduire $K = L \cap \mathbb{R}$. Quel est le groupe de Galois de L sur K ?

2) Montrer que S engendre un idéal premier dans A et dans C . Quelle peut être la décomposition de SB dans B ?

3) Majorer le nombre de classes d'idéaux fractionnaires de L ; B est-il principal ?

Université de Nice
I.M.S.P. Mathématiques

2ème SESSION DE SEPTEMBRE 1989

MAITRISE DE MATHEMATIQUES FONDAMENTALES

M2 – ALGEBRE

Mercredi 13 Septembre 89 de 9h à 12h.

DOCUMENTSAUTORISES

On note $z = e^{2i\pi/5}$ et $K = \mathbb{Q}(z)$ l'extension cyclotomique de $\mathbb{Q}$ de hauteur 5 .

I. Quel est le polynôme minimal de z sur $\mathbb{Q}$, l'anneau A des entiers de K , le discriminant absolu de A ?

Quels nombres premiers se ramifient dans A ? Donner la décomposition de ces nombres dans A . A est-il principal ?

II. Décrire le groupe de Galois de K sur $\mathbb{Q}$. Soit $K' = K \cap \mathbb{R}$; montrer que K' est une extension quadratique de $\mathbb{Q}$, unique extension intermédiaire entre $\mathbb{Q}$ et K . Montrer que $K' = \mathbb{Q}\left(\frac{-1+\sqrt{5}}{2}\right)$. Soit A' l'anneau des entiers de K' ; A' est-il principal ? Décrire le groupe A'^* des unités de A'.

III. a) Montrer que K ne contient d'autres racines de l'unité que les racines 10ème de l'unité. On note G le groupe des racines 10ème de l'unité.

b) En utilisant le théorème des unités, montrer que si a est une unité de module 1 de l'anneau A , alors a appartient à G .

c) Soit $a = \rho e^{i\theta}$ $(\rho > 0)$ une unité de A ; montrer que $\rho^2 \in A'^*$ et que $e^{2i\theta} \in G$. Montrer également que $\rho \in A'^*$ équivaut à $e^{i\theta} \in G$.

d) Montrer qu'aucun élément de $(1-z^3)K'$ n'est une unité de A et que A n'admet aucune unité d'argument $\frac{\pi}{10}$.

En déduire que le groupe A des unités de A est le produit direct du groupe G et du groupe U des unités positives de A' .

MAITRISE DE MATHEMATIQUES FONDAMENTALES M 2 ALGEBRE

PARTIEL N° 1 - 27 Mars 90

Exercices à la carte

(I)

Soit A un anneau commutatif , unitaire , intègre ; K son corps de fractions ; I et J deux idéaux généralisés non nuls . On considère l'application $\alpha : (J:I) \longrightarrow \mathrm{Hom}_A(I,J)$ qui à un élément du transporteur de I dans J associe la multiplication par cet élément .

1) Etudier α : α est-il un morphisme de A-modules ? Est-il injectif ? Est-il surjectif ? (Indication : pour f appartenant à $\mathrm{Hom}_A(I,J)$, comparer $f(x)/x$ et $f(y)/y$ lorsque x et y sont deux éléments non nuls de I .)

2) Lorsque I est inversible , comparer $(J:I)$ et $J.I^{-1}$.

(II)

Soit K un corps de nombres , $A = \mathcal{O}_K$ l'anneau d'entiers de K , $N = N_{K/\mathbb{Q}}$ la norme de K sur $\mathbb{Q}$.

1) Pour un élément a de A , montrer l'équivalence : (a inversible) équivaut à ($N(a) = 1$ ou $N(a) = -1$) .

2) Déterminer les éléments inversibles de A pour $K = \mathbb{Q}[i\sqrt{d}]$ où $d \in \mathbb{N}^*$ sans carré dans sa décomposition en facteurs premiers .

(III)

Soit K un corps de nombres , $A = \mathcal{O}_K$ l'anneau d'entiers de K , I un idéal non nul de A , N(I) sa norme .

1) Montrer que pour a non nul dans I , N(I) divise N(Aa) , et que $N(I) = N(Aa)$ si et seulement si $I = Aa$. Montrer que N(I) premier implique I premier .

2) Soit $K = \mathbb{Q}[i\sqrt{13}]$, $A = \mathcal{O}_K$. L'idéal $I = 2A + A(1+i\sqrt{13})$ est-il premier ? Principal ? Quelle est sa norme ? Et l'idéal $J = 3A$?

(IV)

Soit $K = \mathbb{Q}[i\sqrt{7}]$, $A = \mathbb{Z}[i\sqrt{7}]$, I l'idéal de A engendré par 2 et $1 + i\sqrt{7}$.

1) A est-il de Dedekind ? Montrer que $I^2 = 2I$ et que I n'est pas inversible .

2) Calculer $(A:I)$ et $(A:I).I$.

(V)

Soit $\zeta = \exp(\frac{2i\pi}{11})$ et $K = \mathbb{Q}[\zeta]$ l'extension cyclotomique de $\mathbb{Q}$ de hauteur 11 .

1) Identifier le groupe de Galois G de K sur $\mathbb{Q}$ et donner deux éléments de G d'ordre 2 et 5 respectivement . Quels sont les sous-groupes de G et les extensions intermédiaires (entre $\mathbb{Q}$ et K) ?

2) Soit $\eta = \zeta + \frac{1}{\zeta} = 2\cos(\frac{2\pi}{11})$; montrer que $\mathbb{Q}[\eta] = K \cap \mathbb{R}$ et calculer le polynôme minimal de η.

(VI)

Soit $K = \mathbb{Q}[\sqrt{10}]$ et $A = \mathbb{Z}[\sqrt{10}]$.

1) Etudier les idéaux $I = (1 + \sqrt{10}, 3)$, $I' = (1 - \sqrt{10}, 3)$, $J = (\sqrt{10}, 2)$, $I.I'$, J^2 : sont ils premiers ? Quelle est leur norme ? Décomposer $6A$ en produit d'idéaux premiers de A .

2) Montrer qu'il n'existe pas d'éléments de A de norme 2 (Etudier modulo 5 l'équation correspondante) et que 2 est irréductible dans A . En utilisant $6 = (\sqrt{10} - 2)(\sqrt{10} + 2)$ en déduire que A n'est pas un anneau factoriel .

(VII)

Soit $\alpha = \sqrt[3]{10}$, $K = \mathbb{Q}[\alpha]$, $A = \mathcal{O}_K$.

1) Etablir : $\mathcal{O}_K \subset \frac{1}{30}\mathbb{Z}[\alpha]$; puis $\mathcal{O}_K \subset \frac{1}{3}\mathbb{Z}[\alpha]$.

2) Soit $\beta = \frac{3}{\alpha - 1} = \frac{\alpha^2 + \alpha + 1}{3}$; montrer que β est entier . Calculer $\mathrm{Disc}(1, \alpha, \beta)$. Montrer que $(1, \alpha, \beta)$ est une base entière de $\mathcal{O}_K$.

(VIII)

Soit $P(x) = x^3 + x - q \in \mathbb{Z}[x]$ avec $q \in \mathbb{N}^*$ impair .

On note α l'unique racine réelle de P , β et $\overline{\beta}$ les deux autres (avec partie imaginaire de β positive) , $\theta = i\sqrt{4 + 27\,q^2}$.

1) Montrer que P est irréductible . Calculer β et $\overline{\beta}$ en fonction de α et θ . Soit $K = \mathbb{Q}[\alpha]$, $L = \mathbb{Q}[\alpha, \beta, \overline{\beta}]$; montrer que $L = K[\theta]$. Identifier le groupe de Galois de L sur $\mathbb{Q}$.

2) Calculer $\mathrm{Disc}(1, \alpha, \alpha^2, \theta, \theta\alpha, \theta\alpha^2)$.

MAITRISE DE MATHEMATIQUES FONDAMENTALES

M 2 ALGEBRE

PARTIEL N°2

Mardi 22 Mai 90

On donne : $p = 1 + 3\alpha$, $q = 1 + 3\beta$ deux nombres premiers au moins égaux à 5 , $\alpha \in \mathbb{N}$, $\beta \in \mathbb{N}$, $\alpha \neq \beta \mod 3$;
u et v les réels positifs vérifiant : $u^3 = p^2 q$, $v^3 = p q^2$.
$K = \mathbb{Q}[u]$ le corps de nombres engendré par u , $A = \mathcal{O}_K$ son anneau d'entiers , $B = \mathbb{Z} + \mathbb{Z}u + \mathbb{Z}v$.

PARTIE I

1) Montrer que K est une extension de degré 3 de $\mathbb{Q}$, que $K = \mathbb{Q}[v]$ et que B est un sous-anneau de A .
Calculer $\mathrm{Disc}_{K/\mathbb{Q}}(1,u,u^2)$ et $\mathrm{Disc}_{K/\mathbb{Q}}(1,u,v)$. En déduire : $A \subset \frac{1}{3pq} B$.

2) Soit $x = a + bu + cv$ avec $(a,b,c) \in \mathbb{Q}^3$. Calculer les traces ($\mathrm{Tr}_{K/\mathbb{Q}}$) des éléments : x , ux , vx , x^2 , ux^2 , vx^2 ; montrer l'inclusion : $A \subset \frac{1}{3} B$.
Soit $x = a + bu + cv$ avec $(a,b,c) \in \mathbb{Z}^3$; on suppose $y = \frac{x}{3}$ dans A ; montrer que $a = b = c$ modulo 3 .

3) Soit $z = \frac{1}{3}(1 + u + v)$. Calculer la norme de z (on peut , si on veut , calculer le polynôme minimal de z sur $\mathbb{Q}$ en développant $(z - \frac{1}{3})^3 = (\frac{u+v}{3})^3$).
Montrer que z n'est pas dans A , et conclure : $A = B$.

4) Donner la matrice des composantes de $(1 , x=a+bu+cv , x^2)$ dans la base $(1 , u , v)$ et calculer $\mathrm{Disc}_{K/\mathbb{Q}}(1,x,x^2)$. Montrer que l'équation $b^3p - c^3q = \pm 1$ n'admet pas de solution $(b,c) \in \mathbb{Z}^2$ pour $p = 7$, $q = 13$ (étudier l'équation modulo 13) . En déduire que dans ce cas , A n'admet pas de $\mathbb{Z}$-base de la forme $(1,x,x^2)$.

PARTIE II

Soit $L = \mathbb{Q}[u , ju , j^2u]$ où $j = \exp(\frac{2i\pi}{3})$.

1) Montrer que $L = K[j]$; que L est une extension Galoisienne de $\mathbb{Q}$, et que son groupe de Galois s'identifie au groupe $\mathfrak{S}_3$ des

permutations de (u , ju , j^2u) .
Décrire les extensions intermédiaires entre $\mathbb{Q}$ et L ; sont elles Galoisiennes ?

2) En considérant $(u - 1)^3$ et $(v - 1)^3$ dans $A = \mathcal{O}_K$, montrer que $3A$ est le cube d'un idéal premier de A .
Quelle est la forme de la décomposition de 3 dans $\mathcal{O}_K$, $\mathcal{O}_{\mathbb{Q}[j]}$, $\mathcal{O}_L$?

3) Montrer que l'injection $\mathbb{Z}[u] \hookrightarrow A$ induit un isomorphisme de $\mathbb{Z}[u]/2\mathbb{Z}[u]$ sur $A/2A$; en déduire la décomposition de $2A$ dans A .
Quelle est la forme de la décomposition de 2 dans $\mathcal{O}_K$, $\mathcal{O}_{\mathbb{Q}[j]}$, $\mathcal{O}_L$?

4) Donner une majoration du nombre de classes d'idéaux de $\mathcal{O}_K$ et $\mathcal{O}_L$.

U.F.R. FACULTÉ DES SCIENCES
SESSION DE JUIN 1990

MAÎTRISE DE MATHÉMATIQUES FONDAMENTALES
U.V. M2 ALGÈBRE

MARDI 12 JUIN 1990 - 9H-12H

(documents autorisés)

Soit $\xi = e^{\frac{2i\pi}{7}}$, $K = \mathbb{Q}[\xi]$ l'extension cyclotomique de $\mathbb{Q}$ engendrée par ξ, $A = \mathcal{O}_K$ son anneau d'entiers.

1) On note $g(x)= x^7-1$ et $f(x)$ le polynôme minimal de ξ sur $\mathbb{Q}$. Calculer les normes $N_{K/\mathbb{Q}}(\xi)$, $N_{K/\mathbb{Q}}(g'(\xi))$; en déduire $N_{K/\mathbb{Q}}(f'(\xi))$ et le discriminant absolu $d = \mathrm{Disc}(A)$.

2) Donner la liste des polynômes unitaires irréductibles de degré 2 et 3 de $\mathbb{F}_2[x]$. Quelle est la décomposition de 2A en produit d'idéaux premiers ? Les idéaux qui interviennent dans cette décomposition sont-ils principaux ?

3) On admet que 3A est un idéal premier de A ; A est-il principal ?

4) a) Décrire le groupe de Galois G de K sur $\mathbb{Q}$; quels sont ses sous-groupes ?

b) Soit $u = 2\cos\frac{2\pi}{7}$. Montrer que $K \cap \mathbb{R} = \mathbb{Q}[u]$ et que c'est la seule extension intermédiaire entre $\mathbb{Q}$ et K de degré 3.

c) Déterminer l'unique extension intermédiaire entre $\mathbb{Q}$ et K de degré 2, et son anneau d'entiers.

5) Soit $\eta = 2^{\frac{1}{7}}$; $L = \mathbb{Q}[\eta]$; $B = \mathcal{O}_L$.

a) Montrer l'inclusion $\mathcal{O}_L \subset \frac{1}{7^3 2^3}\mathbb{Z}[\eta]$, puis l'inclusion $\mathcal{O}_L \subset \frac{1}{7^3}\mathbb{Z}[\eta]$.

b) Montrer que l'inclusion $\mathbb{Z}[\eta] \longrightarrow \mathcal{O}_L$ induit un isomorphisme de $\frac{\mathbb{Z}[\eta]}{\eta\,\mathbb{Z}[\eta]}$ sur $\frac{\mathcal{O}_L}{\eta\,\mathcal{O}_L}$. Quelle est la décomposition de $2\,\mathcal{O}_L$ en produit d'idéaux premiers ?

6) Soit $M = \mathbb{Q}[\xi, \eta]$ et $\mathcal{O}_M$ son anneau d'entiers.
Quel est le degré de M sur $\mathbb{Q}$? M est-elle Galoisienne ?
Quelle est la forme de la décomposition de $2\,\mathcal{O}_M$ en produit d'idéaux premiers ?

U.F.R. FACULTE DES SCIENCES

Session de Septembre 1990

MAITRISE DE MATHEMATIQUES FONDAMENTALES

U.V. M 2 - ALGEBRE

Mardi 11 Septembre 1990 , 14h-17h

Soit $\zeta = \exp(\frac{2i\pi}{5})$, $K = \mathbb{Q}[\zeta]$ l'extension cyclotomique de $\mathbb{Q}$ engendrée par ζ, $A = \mathcal{O}_K$ son anneau d'entiers .

1) On note $g(x) = x^5-1$, et $f(x)$ le polynôme minimal de ζ sur $\mathbb{Q}$. Calculer les normes $N_{K/\mathbb{Q}}(\zeta)$, $N_{K/\mathbb{Q}}(g'(\zeta))$, $N_{K/\mathbb{Q}}(f'(\zeta))$ ainsi que le discriminant absolu $d = \mathrm{Disc}_{K/\mathbb{Q}}(A)$.

2) Décomposer $2A$ et $3A$ en produit d'idéaux premiers .

3) A est-il principal ?

4) Déterminer l'unique extension intermédiaire K' , $\mathbb{Q} \subsetneq K' \subsetneq K$; quel est son anneau d'entiers ?

5) Soit $\eta = \sqrt[5]{2}$, $L = \mathbb{Q}[\eta]$, $B = \mathcal{O}_L$.
Montrer l'inclusion : $B \subset \frac{1}{25}\mathbb{Z}[\eta]$. Quelle est la décomposition de $2B$ en produit d'idéaux premiers ?

6) Soit $M = \mathbb{Q}[\zeta, \eta]$; quel est le degré de cette extension ? M est elle Galoisienne ? Quelle est la forme de la décomposition de $2\mathcal{O}_M$ en produit d'idéaux premiers ?

MAITRISE DE MATHEMATIQUES FONDAMENTALES

M 2 - ALGEBRE

PARTIEL N°1

Vendredi 22 Février 91

PARTIE I

A désigne un anneau factoriel , f_1 et f_2 deux éléments non nuls de A , $I = Af_1 + Af_2$ l'idéal de A engendré par f_1 et f_2 , $\chi : A \longrightarrow A/I$ l'application canonique de passage au quotient .

On considère la suite :

$$(*) \qquad 0 \longrightarrow A \xrightarrow{\Psi} A^2 \xrightarrow{\varphi} A \xrightarrow{\chi} A/I \longrightarrow 0$$

où : $\varphi(u_1,u_2) = u_1 f_1 + u_2 f_2$

$\Psi(v) = (-v f_2 , v f_1)$

On note $B = A/Af_1$, $\overline{\chi} : B \longrightarrow A/I$ l'application canonique de passage au quotient , $\overline{\varphi}$ la multiplication dans B par la classe de f_2 .

On considère aussi la suite :

$$(**) \qquad 0 \longrightarrow B \xrightarrow{\overline{\varphi}} B \xrightarrow{\overline{\chi}} A/I \longrightarrow 0$$

1) Indiquer , sans explication , à quels niveaux les suites (*) et (**) sont toujours exactes .

Comparer les assertions : (i) f_1 et f_2 sont premiers entre eux

(ii) la suite (*) est exacte

(iii) la suite (**) est exacte

2) On note d le p.g.c.d. de f_1 et f_2 . Comment modifier Ψ dans (*) pour retrouver une suite exacte ?

3) On suppose $A = R[x]$ où R est un anneau principal , et on suppose que f_1 est un polynôme unitaire de degré p . Montrer l'équivalence des assertions : (i) f_1 et f_2 sont premiers entre eux

(iv) $A/I \otimes_R \mathrm{Fract}(R) = 0$

4) Avec les hypothèses de la question précédente , on prend :

$$f_1 = x^3 + ax + b \qquad f_2 = ux^2 + v$$

Ecrire la matrice de $\overline{\varphi}$ dans la base canonique $(\dot{1},\dot{x},\dot{x}^2)$ de B sur R .

Dans le cas où f_1 et f_2 sont premiers entre eux , on note $(\alpha_1,\alpha_2,\alpha_3)$ les facteurs invariants de $\mathrm{Im}\,\overline{\varphi}$ dans B ; donner les valeurs de α_1 , $\alpha_1\alpha_2$, $\alpha_1\alpha_2\alpha_3$ sous forme de p.g.c.d. de polynômes en a,b,u,v .

Dans le cas particulier $u = 0$, à quoi est isomorphe A/I comme R-module?

Même question pour $v = 0$.

PARTIE II

A désigne un anneau commutatif unitaire , $(f_1, \ldots, f_n)$ n éléments de A , I l'idéal engendré par ces éléments , $\chi : A \longrightarrow A/I$ la surjection canonique . On note $\mathfrak{A}$ le sous A module de $M_n(A)$ des matrices anti-symétriques $\alpha = (\alpha_{i,j})$: $\alpha_{i,j} = -\alpha_{j,i}$ pour $i \neq j$ et $\alpha_{i,i} = 0$.
On définit la suite :

$$(*) \qquad \mathfrak{A} \xrightarrow{\Psi} A^n \xrightarrow{\varphi} A \xrightarrow{\chi} A/I \longrightarrow 0$$

où : $\varphi(u_1, \ldots u_n) = \sum_{1 \leq i \leq n} u_i f_i$ et $\Psi(\alpha) = \left(\sum_{1 \leq j \leq n} \alpha_{i,j} f_j \right)_{1 \leq i \leq n}$

1) Montrer l'équivalence entre :
(i) $\operatorname{Ker} \varphi \subset \operatorname{Im} \Psi$ et (ii) la suite $(*)$ est exacte .
Lorsque ces conditions sont satisfaites nous dirons que la suite $(f_1, \ldots, f_n)$ est régulière dans A .

2) On suppose A intègre et on note K le corps des fractions de A . Que vaut $K \otimes_A A/I$? Que devient la suite $(*)$ lorsqu'on lui applique le foncteur $K \otimes_A \cdot$, la suite $(f_1, \ldots, f_n)$ étant supposée régulière dans A ? Que vaut alors : $\dim_K(\operatorname{Ker}(1_K \otimes \Psi))$?

3) On note $B = A/Af_1$, $(\dot{f}_2, \ldots, \dot{f}_n)$ la suite des classes dans B des éléments $(f_2, \ldots, f_n)$. Montrer les implications :

(iii) f_1 est non diviseur de 0 dans A et la suite $(\dot{f}_2, \ldots, \dot{f}_n)$ est
$\Downarrow$ régulière dans B .
(i) la suite $(f_1, \ldots, f_n)$ est régulière dans A .
$\Downarrow$
(iv) la suite $(\dot{f}_2, \ldots, \dot{f}_n)$ est régulière dans B .

4) On suppose que pour tout $i = 1, \ldots, n$ la classe de f_i n'est pas diviseur de zéro dans $A_{i-1} = A/(Af_1 + \ldots Af_{i-1})$ (avec la convention $A_0 = A$) . Montrer que la suite $(f_1, \ldots, f_n)$ est régulière dans A .

5) Dans cette question on suppose que A est un anneau local noethérien d'idéal maximal $\mathfrak{M}$. A la suite $(f_1, \ldots, f_{n-1})$ on associe les applications φ_{n-1} et Ψ_{n-1} analogues à φ et Ψ , et les sous modules de A^{n-1} : $T = \operatorname{Im}(\Psi_{n-1})$ et $K = \operatorname{Ker}(\varphi_{n-1})$. Montrer que si la suite $(f_1, \ldots, f_n)$ est régulière dans A , on a l'inclusion : $K \subset T + f_n K$.

En déduire , par le lemme de Nakayama , que si f_n est dans $\mathfrak{M}$, la suite $(f_1, \ldots, f_{n-1})$ est régulière dans A .

Que peut on conclre lorsque $(f_1, \ldots, f_n)$ est une suite d'éléments de $\mathfrak{M}$?

MAITRISE DE MATHEMATIQUES FONDAMENTALES

M 2 - ALGEBRE

PARTIEL N°1 bis

Vendredi 12 Avril 91

PARTIE I

Soient : p premier au moins égal à 3 ; $w = \exp(\frac{2i\pi}{p})$; $K = \mathbb{Q}[w]$; $\mathcal{O}_K$ l'anneau d'entiers de K ; $P(x) = x^{p-1} + x^{p-2} + \ldots + x + 1 \in \mathbb{Z}[x]$.

On se propose, dans cette question, de démontrer : $\mathcal{O}_K = \mathbb{Z}[w]$.

1) On pose : $P_1(z) = P(1+z) = z^{p-1} + a_1 z^{p-2} + \ldots + a_{p-1}$; déterminer $z P_1(z)$ et montrer que $a_1, a_2, \ldots, a_{p-1}$ sont divisibles par p . En déduire que P est irréductible (on a droit au critère d'Eisenstein : si p divise $a_1, \ldots, a_{p-1}$, et si p^2 ne divise pas a_{p-1} , alors le polynôme P_1 est irréductible dans $\mathbb{Z}[z]$) .

Quelles sont les racines de P_1 ?

On désigne par N la norme $N_{K/\mathbb{Q}}$; montrer : $N(w-1) = p = (w-1)^{p-1} u$ où u est un élément inversible de $\mathbb{Z}[w]$.

2) Soit : $x = b_i (w-1)^i + b_{i+1} (w-1)^{i+1} + \ldots + b_{p-2} (w-1)^{p-2} \in \mathbb{Z}[w]$ pour $0 \leqslant i \leqslant p-2$; on suppose que $y = \frac{x}{p}$ est dans $\mathcal{O}_K$; montrer que b_i est divisible par p . (On pourra commencer par multiplier par $(w-1)^{p-2-i}$) . En déduire : $(\frac{1}{p}\mathbb{Z}[w]) \cap \mathcal{O}_K \subset \mathbb{Z}[w]$.

3) Montrer que : $p w^{p-1} = (w-1) P'(w)$ et calculer le discriminant $\mathrm{Disc}_{K/\mathbb{Q}}(1, w, \ldots, w^{p-2})$. Montrer que : $\mathcal{O}_K = \mathbb{Z}[w]$.

PARTIE II

Soient w un entier algébrique de degré n , $P \in \mathbb{Z}[x]$ son polynôme minimal , $K = \mathbb{Q}[w]$, $A = \mathbb{Z}[w]$, $N = N_{K/\mathbb{Q}}$.

4) Etant donné $Q \in \mathbb{Z}[x]$ tel que $Q(w) = 0$, montrer que $N(Q(w))$

est égal , au signe près , au résultant des polynômes P et Q .
En déduire : $N(Q(w)) = \#(A/AQ(w))$. (On pourra introduire la multiplication par la classe de Q dans $\mathbb{Z}[x]/\mathbb{Z}[x]P$) .

5) Soit I un idéal non nul de A . Montrer que I est un $\mathbb{Z}$-module libre de rang n et que A/I est fini . On pose $N(I) = \#(A/I)$.
Montrer que $N(I) \in I$.

6) Prouver qu'un idéal premier non nul de A est maximal .
Montrer que pour deux idéaux I et J de A , I premier non nul et J non inclus dans I , on a : $N(IJ) = N(I).N(J)$. (On pourra commencer par démontrer : $I + J = A$) .

PARTIE III

On prend : $p = 5$; $w = \exp(\frac{2i\pi}{5})$; $K = \mathbb{Q}[w]$; $P(x) = x^4 + x^3+x^2+x+1$

7) Montrer que le quotient de $\mathbb{Z}[x]$ par l'idéal engendré par $P(x)$ et $x-1$ est un corps ; que vaut $N(A(w-1))$ et $N(A.5)$? ($A = \mathbb{Z}[w]$) .

8) Déterminer l'unique extension intermédiaire $\mathbb{Q} \subset L \subset K$ (en identifiant le groupe de Galois $Gal(K/\mathbb{Q})$, en déterminant son sous groupe non trivial , et les points fixes de ce sous groupe) .

9) Soit $h = w + w^4$; quel est le polynôme minimal de h ? Quel est l'anneau d'entiers de $\mathbb{Q}[h]$? L'idéal engendré par 5 est-il premier dans cet anneau ?

MAITRISE DE MATHEMATIQUES FONDAMENTALES

M 2 - ALGEBRE

PARTIEL N°2

Vendredi 17 Mai 91

PARTIE I

Soient : θ un entier algébrique de degré n , $P \in \mathbb{Z}[x]$ son polynôme minimal , $R = \mathbb{Z}[\theta]$; on dit que deux idéaux I et J de R sont dans la même classe s'il existe deux éléments non nuls a et b de R tels que : $aI = bJ$. On note $M(n,\mathbb{Z})$ l'espace des matrices $n \times n$ à coefficients entiers , $M_n(P)$ le sous ensemble de $M(n,\mathbb{Z})$ des matrices A telles que $P(A) = 0$.

1) Soit $A \in M_n(P)$; montrer l'existence de $x = (x_1, \ldots, x_n)$ non nul dans R^n tel que : $A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \theta \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$.

2) Montrer que $\mathbb{Z}x_1 + \mathbb{Z}x_2 + \ldots + \mathbb{Z}x_n$ est un idéal de R , et que sa classe est indépendante du vecteur propre x choisi . On note I_A cette classe .

3) Soit Q un élément de $GL(n,\mathbb{Z})$; montrer que : $I_A = I_{Q^{-1}AQ}$.

4) Soit J un idéal non nul de R , $(y_1, \ldots, y_n)$ une $\mathbb{Z}$-base de J ; montrer qu'il existe $B \in M(n,\mathbb{Z})$ telle que : $B \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \theta \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$ et que $P(B) = 0$.

5) Montrer qu'il existe une bijection entre l'ensemble des classes de similitude des matrices de $M_n(P)$ et l'ensemble des classes d'idéaux non nuls de R .

6) Montrer que les conditions suivantes sont équivalentes :

(i) R est un anneau principal .

(ii) Il existe une seule classe de similitude dans $M_n(P)$.

PARTIE II

Soient : D un entier naturel , $D \equiv 3 \pmod 4$, $K = \frac{D+1}{4}$, $P(x) = x^2 - x + K$, $w_D = \frac{1 + i\sqrt{D}}{2}$, A un élément de $M(2,\mathbb{Z})$ dont le polynôme caractéristique est P .

1) Soit $B = \begin{pmatrix} -a & -b \\ c & a+1 \end{pmatrix}$ une matrice semblable à A telle que a soit minimum .

En calculant $Q^{-1}AQ$ lorsque Q est l'une des matrices suivantes : $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ $\begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix}$ $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ montrer que l'on peut supposer que les coefficients de B vérifient : $a \geqslant 0$, $c \geqslant 2a+1$, $b \geqslant 2a+1$ et $3(a^2 + a) + 1 \leqslant K$.

2) On suppose que $K + a^2 + a$ est un nombre premier quel que soit $a \geqslant 0$ vérifiant $3(a^2+a)+1 \leqslant K$. Prouver que $\mathbb{Z}[w_D]$ est un anneau principal .

3) Montrer que $\mathbb{Z}[w_D]$ est principal pour D = 3 , 7 , 11 , 19 , 43 , 67 , 163 .

PARTIE III

On dit qu'un anneau unitaire intègre est Euclidien s'il existe $\lambda : R-\{0\} \longrightarrow \mathbb{N}$ telle que , pour tout a , b non nuls de R , il existe q et r dans R vérifiant $a = bq + r$ et $r = 0$ ou $\lambda(r) < \lambda(b)$.

1) Quelles sont les unités de $R = \mathbb{Z}[w_D]$?

2) On suppose $R = \mathbb{Z}[w_D]$ Euclidien pour une application λ ; soit b un élément non nul et non inversible de R tel que $\lambda(b)$ soit minimum . Montrer que $\#(R/Rb)$ est égal à 2 ou 3 .

3) En déduire que pour D = 19 , 43 , 67 , 163 , $\mathbb{Z}[w_D]$ est un anneau principal non Euclidien .

PARTIE IV

Etudier le corps de nombres : $L = \mathbb{Q}\left[i , \sqrt{19}\right]$. On pourra , par exemple , déterminer le groupe de Galois $G=Gal(L/\mathbb{Q})$, les extensions intermédiaires , les anneaux de nombres associés , les décompositions de (2) et (3) dans ces anneaux ....


EXAMEN DE JUIN 91
Non! Mais vous ne pensiez quand même pas que j'allais vous donner les sujets à l'avance!
ISSUE DE CE COURS
ℤ[i√15] est principal non euclidien
ERRATUM :
i√163
M'sieur! On a le droit de faire des dessins?
Ici, pour les avions, c'est vraiment super
Finalement, et tout bien réfléchi, je trouve qu'il a fait son cours à un niveau un peu faible pour moi!
Rature + Caricature + Humour = Union Nigoise des SAnisettes
MEDECIN Sans frontière URUGUAY ARG