Comparaison de groupes de Picard en dimension 1

Henri Lombardi (*), Claude Quitté (†)

Octobre 2006

Résumé

Nous comparons deux groupes de Picard en dimension 1. Le résultat est obtenu de manière constructive et il généralise un résultat de J. Sands [11].

Abstract

We compare two Picard group in dimension one. Our proofs are constructive and the results generalize a theorem of J. Sands [11].

MSC 2000 : 13C15, 13C20, 03F65, 13F45

Mots clés : Dimension de Krull, Groupe de Picard, Mathématiques constructives.

Introduction

Dans l'article [11] Sands, généralisant un théorème de Siegel [13] explique le lien entre le groupe de Picard d'un anneau d'entiers d'un corps de nombre et celui d'un sous-anneau ayant même corps de fractions. Il applique ses résultats au calcul de bornes sur les régulateurs.

Nous donnons dans l'article présent une extension des résultats de Sands relatifs aux groupes de Picard pour le cas de deux anneaux intègres $A \subset B$ de dimension 1 lorsque B est fini sur A avec même corps de fractions. Notre preuve est constructive et donne donc un algorithme qu'on peut implémenter (par exemple pour le calcul du groupe de Picard de courbes algébriques) lorsque les hypothèses sont satisfaites de manière explicite.

On rappelle que le conducteur $\mathrm{c}(A, B)$ de A dans B (lorsque A est un sous-anneau de B) est l'idéal commun de A et de B défini par :

$$\mathrm{c}(A, B) = \{x \in A \mid xB \subset A\}$$

Le fait que dans notre énoncé nous remplacions le conducteur de A dans B par un idéal non nul contenu dans le conducteur, supprime, par rapport au théorème original, une difficulté de calcul non négligeable.

Dans la première section, nous donnons des résultats partiels dans le cas d'une extension arbitraire d'anneaux. Cela englobe une construction de Schanuel en rapport avec la notion de seminormalité. La deuxième section est consacrée à des rappels concernant le traitement constructif de la dimension de Krull. La section 3 donne la démonstration du théorème principal de cet article :

* Laboratoire de Mathématiques, CNRS UMR 6623, UFR des Sciences et Techniques, Université de Franche-Comté, 25 030 BESANÇON cedex, FRANCE, email : henri.lombardi@univ-fcomte.fr, partiellement financé par le réseau européen RAAG CT-2001-00271

† Laboratoire de Mathématiques, CNRS UMR 6086, SP2MI, Boulevard 3, Teleport 2, BP 179, 86960 FUTUROSCOPE Cedex, FRANCE, email : quitte@mathlabo.univ-poitiers.fr

Théorème 7 *Soient $A \subset B$ deux anneaux intègres de dimension 1 ayant même corps des fractions et tels que B soit un A-module de type fini. Si $\mathfrak{f}$ est un idéal non nul de B contenu dans le conducteur de A dans B, alors la suite :*

$$1 \longrightarrow U(B)/U(A) \xrightarrow{i\ :\ [b] \mapsto [b]} U(B/\mathfrak{f})/U(A/\mathfrak{f}) \xrightarrow{j\ :\ [b] \mapsto [bA+\mathfrak{f}]} \mathrm{Pic}(A) \xrightarrow{\pi\ :\ [\mathfrak{a}] \mapsto [\mathfrak{a}B]} \mathrm{Pic}(B) \longrightarrow 1$$

est exacte.

Signalons que ce théorème est dû à Dedekind [5] en théorie des nombres dans le cas où B est l'anneau de tous les entiers d'un corps de nombres.

Nos preuves sont dans le style de l'algèbre constructive (cf. [9]). Nous ne faisons aucune hypothèse nœthérienne. Nous utilisons une caractérisation simple « sans idéaux premiers » de la dimension de Krull ([2]) : celle-ci a déjà permis de donner une forme élémentaire et constructive à de nombreux résultats d'algèbre commutative qui étaient auparavant de nature purement idéale (cf. [3, 4, 6, 8]).

Notre théorème est donc nouveau sous deux points de vue. Premièrement il n'utilise pas d'hypothèse nœthérienne, deuxièmement il fournit un algorithme qui explicite l'exactitude de la suite en chacun de ses termes. Il peut donc intéresser toute la communauté mathématique et en particulier celle du calcul formel. Signalons enfin que les théorèmes dont les hypothèses font intervenir la dimension de Krull ne pouvaient avoir de réalisation algorithmique avant que cette dernière ait été mise sous forme explicite.

Remerciements : Nous remercions le rapporteur pour sa relecture attentive et ses commentaires pertinents.

1 Suites exactes pour un groupe de modules inversibles

On se donne deux anneaux commutatifs $A \subset B$. On note $U(C)$ le groupe des inversibles d'un anneau arbitraire C.

Nous dirons qu'un sous-A-module M de B est *inversible* s'il existe un sous-A-module N de B tel que $M.N = A$. Cette définition coïncide avec celle de Bourbaki [1] dans le cas où B est le localisé de A par une partie multiplicative constituée d'éléments réguliers. On a alors pour tout sous-A-module M' de B : $M.M' \simeq M \otimes_A M'$ via l'homomorphisme canonique. En effet, on dispose de $x_1, \ldots, x_n$ dans M, $y_1, \ldots, y_n$ dans N tels que $1 = \sum_i x_i y_i$ et $x_i y_j$ dans A ; pour tout élément $\sum_k z_k \otimes z'_k$ dans $M \otimes_A M'$ on a, en remarquant que $y_i z_k \in N.M = A$

$$\sum_k z_k \otimes z'_k = \sum_{k,i} x_i y_i z_k \otimes z'_k = \sum_{k,i} x_i\,(y_i z_k) \otimes z'_k = \sum_{k,i} x_i \otimes (y_i z_k)\, z'_k = \sum_i x_i \otimes \sum_k y_i z_k z'_k,$$

donc la surjection canonique $M \otimes_A M' \to M.M'$ est injective. En particulier les modules inversibles sont projectifs de rang 1.

On notera $\mathcal{M}_{\mathrm{inv}}(A, B)$ le groupe formé des sous-A-modules inversibles de B et $\mathcal{I}_{\mathrm{fr}}(B)$ le groupe des idéaux fractionnaires inversibles de B : autrement dit $\mathcal{I}_{\mathrm{fr}}(B) = \mathcal{M}_{\mathrm{inv}}(B, \mathrm{Frac}(B))$, où $\mathrm{Frac}(B)$ est l'anneau total des fractions de B. On note aussi $\mathcal{P}_{\mathrm{fr}}(A, B)$ le sous-groupe de $\mathcal{M}_{\mathrm{inv}}(A, B)$ constitué des sous-A-modules de B monogènes. Enfin $\mathrm{Pic}(A)$ est le groupe des classes d'isomorphismes des modules projectifs de rang 1.

On fixe un idéal $\mathfrak{f}$ de B tel que $\mathfrak{f}B \subset A$ de sorte que $\mathfrak{f}$ est aussi un idéal de A. Autrement dit $\mathfrak{f}$ est un idéal de B contenu dans le conducteur de A dans B.

1.1 Première suite exacte

On définit alors une première suite exacte

$$\boxed{1 \longrightarrow U(A/\mathfrak{f}) \longrightarrow U(B/\mathfrak{f}) \xrightarrow{j} \mathcal{M}_{\mathrm{inv}}(A,B)}$$

• Puisque $\mathfrak{f}$ est un idéal de A et de B, on a $A/\mathfrak{f} \subset B/\mathfrak{f}$ donc $U(A/\mathfrak{f}) \subset U(B/\mathfrak{f})$ ce qui définit la flèche (injective) de gauche.

• Voyons la flèche notée j. Posons d'abord, pour $b \in B$, $j(b) = bA + \mathfrak{f}$; pour l'instant $j(b)$ est seulement un sous A-module de B. Il est clair que $j(1) = A$ et que $b_1 \equiv b_2 \pmod{\mathfrak{f}}$ entraîne $j(b_1) = j(b_2)$. Remarquons que si $b_1 \in B$ est inversible modulo $\mathfrak{f}$, alors $b_1\mathfrak{f}+\mathfrak{f}^2 = \mathfrak{f}$, égalité obtenue en multipliant $b_1B + \mathfrak{f} = B$ par $\mathfrak{f}$. Alors pour tout $b_2 \in B$, on a $j(b_1b_2) = j(b_1)j(b_2)$; en effet :

$$j(b_1)j(b_2) = b_1b_2A + b_1\mathfrak{f} + b_2\mathfrak{f} + \mathfrak{f}^2 = b_1b_2A + (b_1B + \mathfrak{f})\mathfrak{f} + b_2\mathfrak{f} = b_1b_2A + \mathfrak{f} = j(b_1b_2)$$

Cela permet donc de définir la flèche $j : U(B/\mathfrak{f}) \mapsto \mathcal{M}_{\mathrm{inv}}(A,B)$ qui à la classe modulo $\mathfrak{f}$ d'un élément $b \in B$ inversible modulo $\mathfrak{f}$ associe $bA+\mathfrak{f}$ (qui est bien un A-module inversible à cause de la multiplicativité de j).

Notons aussi que $j(b)B = B$ pour tout $b \in U(B/\mathfrak{f})$.

Pour montrer l'exactitude de la suite, on doit calculer $\ker j$. Soit $b \in B$ inversible modulo $\mathfrak{f}$, tel que $j(b) = A$ i.e. $\mathfrak{f} + bA = A$. On a alors $bA \subset A$ donc $b \in A$ et l'égalité $\mathfrak{f} + bA = A$ dit que l'élément b, qui maintenant est dans A, est inversible modulo $\mathfrak{f}$.

Dans toute la suite, lorsque $b \in B$ nous utiliserons sans commentaire précis les notations $\overline{b}$, $\widehat{b}$, $\widetilde{b}$ pour désigner l'image de b dans un ensemble considéré, disons X, pour l'application naturelle de B dans X.

On peut énoncer le résultat précédent sous la forme suivante :

Proposition 1 *L'application $j : U(B/\mathfrak{f}) \to \mathcal{M}_{\mathrm{inv}}(A,B)$ définie par $j(\overline{b}) = bA + \mathfrak{f}$ induit un isomorphisme de $U(B/\mathfrak{f})/U(A/\mathfrak{f})$ sur un sous-groupe de $\mathcal{M}_{\mathrm{inv}}(A,B)$ constitué de A-modules inversibles $\mathfrak{a}$ de B tels que $\mathfrak{a}B = B$.*

1.2 Deuxième suite exacte

On suppose désormais que B est entier sur A.

Le noyau de l'homomorphisme $U(B) \to U(B/\mathfrak{f})/U(A/\mathfrak{f})$ est égal à $U(A)$ (un élément de A inversible dans B est inversible dans A). Ceci donne i dans « la seconde suite exacte » suivante :

$$\boxed{1 \longrightarrow U(B)/U(A) \xrightarrow{i} U(B/\mathfrak{f})/U(A/\mathfrak{f}) \xrightarrow{j} \mathcal{M}_{\mathrm{inv}}(A,B)/\mathcal{P}_{\mathrm{fr}}(A,B)}$$

Concernant l'exactitude il nous reste à calculer $\ker j$ (nous avons conservé le nom j). Soit $b \in B$ inversible modulo $\mathfrak{f}$ tel que $j(b)$ soit monogène, c'est-à-dire $bA + \mathfrak{f} = b'A$ avec $b' \in B$. On multiplie cette égalité par B : $bB + \mathfrak{f} = b'B$, c'est-à-dire $B = b'B$, de sorte que b' est inversible dans B. On multiplie $bA + \mathfrak{f} = b'A$ par b'^{-1} et en posant $a = bb'^{-1}$, on obtient $aA + \mathfrak{f} = A$ de sorte que $a \in A$ et est inversible modulo $\mathfrak{f}$, et on a bien $\overline{b} = i(\widehat{b'})$.

L'exactitude peut encore s'énoncer ainsi :

Proposition 2 *On suppose que B est entier sur A. L'application $j : U(B/\mathfrak{f})/U(A/\mathfrak{f}) \to \mathcal{M}_{\mathrm{inv}}(A,B)$ définie par $j(\tilde{b}) = bA + \mathfrak{f}$ induit un isomorphisme de $U(B/\mathfrak{f})/U(A/\mathfrak{f})U(B)$ sur un sous-groupe du quotient $\mathcal{M}_{\mathrm{inv}}(A,B)/\mathcal{P}_{\mathrm{fr}}(A,B)$: autrement dit, pour $b \in B$ inversible modulo $\mathfrak{f}$, le sous-A-module $bA + \mathfrak{f}$ est monogène si et seulement si il existe $u \in U(B)$ tel que $ub \in A$.*

Précisons le « autrement dit » : soit $b \in B$ un élément inversible modulo $\mathfrak{f}$. Sa classe est dans $U(A/\mathfrak{f})U(B)$ si et seulement si $b = ab' \pmod{\mathfrak{f}}$ avec $a \in A$ inversible modulo $\mathfrak{f}$ et $b' \in U(B)$. On prend alors $u = b'^{-1}$. Réciproquement, si un tel u existe l'élément $a = ub$ est dans A et sa classe modulo $\mathfrak{f}$ est inversible dans $B/\mathfrak{f}$, donc inversible dans $A/\mathfrak{f}$ puisque $B/\mathfrak{f}$ est entier sur $A/\mathfrak{f}$.

1.3 Application : seminormalité

Soit $A \subset A[\alpha]$ avec α^2 et $\alpha^3 \in A$. On pose $B = A[\alpha] = A + \alpha A$ et $\mathfrak{f} = \alpha^2 B = \alpha^2 A + \alpha^3 A$. Pour tout $a \in A$ l'élément $b = 1 + a\alpha$ est inversible modulo $\mathfrak{f}$ (d'inverse $1 - \alpha a$) et le sous-A-module $j(\overline{b})$ est inversible. Par définition $j(\overline{b}) = bA + \alpha^2 A + \alpha^3 A$ est aussi égal à $bA + \alpha^2 A$ ou $bA + \alpha^3 A$ (puisque $\alpha^3 = \alpha^3 b - (a\alpha^2)\alpha^2$ et $\alpha^2 = \alpha^2 b - a\alpha^3$).

En conséquence on obtient un homomorphisme $\varphi : (A, +) \to \mathrm{Pic}(A)$ en composant $A \to U(B/\mathfrak{f})$, $a \mapsto \overline{1 + a\alpha}$ et j.

Supposons maintenant $A[\alpha]$ réduit et remplaçons A par $A[X]$, B par $B[X]$ et α par αX. On obtient un homomorphisme $\varphi : (A[X], +) \to \mathrm{Pic}(A[X])$ qui à $P \in A[X]$ associe la classe du $A[X]$-module projectif $M(X) = (1+\alpha XP)A[X]+(\alpha X)^2 A[X]$. D'après la proposition 2, le module précédent est libre si et seulement si il existe $V \in U(B[X])$ tel que $V(1 + \alpha XP) \in A[X]$. Comme B est réduit $U(B[X]) = U(B)$. On a donc la condition $\exists v \in U(B)$, $v + \alpha vXP \in A[X]$, i.e., $v \in A$ et $\alpha vP \in A[X]$. Mais v est inversible dans B donc dans A : le module est libre si et seulement si $\alpha P \in A[X]$. Pour $P = 1$ on trouve ainsi « l'exemple de Schanuel » : $M(0)$ est libre, et $M(X)$ est étendu (i.e. libre) si et seulement si $\alpha \in A$. Voir à ce sujet [7] pages 29-30 et 39-40.

2 Rappels sur la dimension 1 (en mathématiques constructives)

On peut trouver la définition constructive de la dimension de Krull dans [2]. Des applications de cette notion ont été données notamment dans [3, 4, 6, 8].

L'anneau trivial est caractérisé par la dimension -1. Pour les dimensions 0 et 1, on a les caractérisations élémentaires suivantes.

Lemme 3 (dimensions 0 et 1) *Soit A un anneau commutatif.*

1. *A est de dimension ≤ 0 si et seulement si pour tout $x \in A$ il existe $n \in \mathbb{N}$ et $a \in A$ tels que : $x^n(1 + ax) = 0$*
2. *A est de dimension ≤ 1 si et seulement si pour tout $x, y \in A$ il existe $m, n \in \mathbb{N}$ et $a, b \in A$ tels que : $y^m(x^n(1 + ax) + by) = 0$*

En outre on est capable de montrer que les anneaux les plus couramment étudiés qui sont de dimension ≤ 0 ou 1 au sens de la définition classique usuelle vérifient de manière explicite la caractérisation élémentaire donnée dans le lemme précédent.

Le lemme suivant apparaît avec une preuve constructive sous une forme un tout petit peu plus générale dans [6] (lemme 4.3).

Lemme 4 (lemme d'évitement en dimension 1) *Soit A un anneau intègre de dimension ≤ 1. Soit $\mathfrak{a}$ un idéal inversible de A et $\mathfrak{b}$ un idéal non nul. Alors il existe un élément $u \neq 0$ de $\mathrm{Frac}(A)$ tel que l'idéal $u\,\mathfrak{a}$ est entier (contenu dans A) et comaximal à $\mathfrak{b}$.*

Le célèbre « théorème un et demi » se trouve également avec une preuve constructive dans [6] (théorème 2.32) sous la forme générale suivante.

Théorème 5 (théorème un et demi) *Soit A un anneau commutatif de dimension ≤ 1 et $\mathfrak{a}$ un idéal inversible. Soit $x \in \mathfrak{a}$ un élément régulier. Alors il existe $y \in \mathfrak{a}$ tel que pour tout $n \geq 1$, $\mathfrak{a} = x^n\mathfrak{a} + yA$. En particulier $\mathfrak{a} = \langle x^n, y \rangle$.*

3 Une suite exacte au niveau des groupes de classes

3.1 La situation particulière que nous examinons

On se donne deux anneaux intègres $A \subset B$ *ayant même corps des fractions.*

Rappelons que le conducteur $\mathrm{c}(A,B)$ de A dans B est l'annulateur du A-module B/A, et c'est aussi le plus grand idéal de B contenu dans A.

On suppose de plus que A est un anneau de dimension 1 et que B est un A-module de type fini, donc un anneau de dimension 1.

Les hypothèses « $\mathrm{Frac}(A) = \mathrm{Frac}(B)$ » et « B est un A-module de type fini » entraînent que B est un idéal fractionnaire de A (considérer un système fini de générateurs de B sur A et multiplier par un A-dénominateur commun). En fait, $\mathrm{Frac}(A) = \mathrm{Frac}(B)$ dit que B/A est un A-module de torsion et le fait que B soit un A-module de type fini (ce qui équivaut à dire que B/A est un A-module de type fini) entraîne que son annulateur (i.e. le conducteur de A dans B) n'est pas réduit à 0.

Ce contexte se trouve notamment en théorie des nombres : B est l'anneau des entiers d'un corps de nombres K et A est un anneau de nombres de K (i.e. un sous-anneau de B qui est un $\mathbb{Z}$-module de rang égal à la dimension de K sur $\mathbb{Q}$). Il y d'autres applications, par exemple en géométrie où les anneaux A, B sont des $\mathbf{k}[T]$-algèbres de type fini (algèbres des coordonnées de courbes affines). Voir [10] et le compte rendu qu'en fait J.-P. Serre dans [12].

Dans la suite on fixe un idéal $\mathfrak{f}$ de B non nul et contenu dans le conducteur $\mathrm{c}(A,B)$.

3.2 Retour sur la première suite exacte

On a tout l'abord l'analogue suivant de la première suite exacte (section 1.1) :

$$\boxed{1 \longrightarrow U(A/\mathfrak{f}) \longrightarrow U(B/\mathfrak{f}) \xrightarrow{j} \mathcal{I}_{\mathrm{fr}}(A) \xrightarrow{\pi} \mathcal{I}_{\mathrm{fr}}(B)}$$

où π est l'application canonique $\mathfrak{a} \mapsto \mathfrak{a}B$ et j reste défini par $\overline{b} \mapsto bA + \mathfrak{f}$. Les preuves pour l'exactitude jusqu'à $\mathcal{I}_{\mathrm{fr}}(A)$ sont identiques et il nous reste à calculer $\ker \pi$. Soit $\mathfrak{a}$ un idéal fractionnaire de A vérifiant $\mathfrak{a}B = B$. On multiplie cette égalité par $\mathfrak{f}$: $\mathfrak{a}\mathfrak{f} = \mathfrak{f}$ donc $\mathfrak{f} \subset \mathfrak{a}$. D'après le théorème 5 il existe $b \in \mathfrak{a}$ tel que $bA + \mathfrak{f} = \mathfrak{a}$. On multiplie cette égalité par B, ce qui donne $bB + \mathfrak{f} = \mathfrak{a}B = B$, donc $b \in B$ et b est inversible modulo $\mathfrak{f}$: $\mathfrak{a} = j(\overline{b})$.

Reprenons la proposition 1.

Proposition 6 *L'application $j : U(B/\mathfrak{f}) \to \mathcal{I}_{\mathrm{fr}}(A)$ définie par $j(\overline{b}) = bA + \mathfrak{f}$ induit un isomorphisme de $U(B/\mathfrak{f})/U(A/\mathfrak{f})$ sur le sous-groupe de $\mathcal{I}_{\mathrm{fr}}(A)$ constitué des idéaux fractionnaires inversibles $\mathfrak{a}$ de A tels que $\mathfrak{a}B = B$.*

3.3 La suite exacte canonique

C'est l'analogue suivant de la deuxième suite exacte (section 1.2) :

$$\boxed{1 \longrightarrow U(B)/U(A) \longrightarrow U(B/\mathfrak{f})/U(A/\mathfrak{f}) \xrightarrow{j} \mathrm{Pic}(A) \xrightarrow{\pi} \mathrm{Pic}(B) \longrightarrow 1}$$

Puisque B est intègre, le groupe $\mathrm{Pic}(B)$ est isomorphe à $\mathcal{I}_{\mathrm{fr}}(B)/\mathcal{P}_{\mathrm{fr}}(B)$. Si B est un anneau de Prüfer, $\mathrm{Pic}(B) = \mathcal{I}_{\mathrm{fr}}(B)/\mathcal{P}_{\mathrm{fr}}(B)$ est le groupe habituel des classes d'idéaux de type fini.

Théorème 7 *Soient $A \subset B$ deux anneaux intègres de dimension 1 ayant même corps des fractions et tels que B soit un A-module de type fini. Si $\mathfrak{f}$ est un idéal non nul de B contenu dans le conducteur, alors la suite :*

$$1 \longrightarrow U(B)/U(A) \xrightarrow{i\ :\ [b]\mapsto[b]} U(B/\mathfrak{f})/U(A/\mathfrak{f}) \xrightarrow{j\ :\ [b]\mapsto[bA+\mathfrak{f}]} \mathrm{Pic}(A) \xrightarrow{\pi\ :\ [\mathfrak{a}]\mapsto[\mathfrak{a}B]} \mathrm{Pic}(B) \longrightarrow 1$$

est exacte.

Preuve.
Il nous reste à montrer la surjectivité de π : soit $\mathfrak{b}$ un idéal fractionnaire inversible de B. D'après le lemme d'évitement en dimension 1 (lemme 4), on peut supposer que $\mathfrak{b}$ est un idéal entier de B comaximal à $\mathfrak{f}$; soit $1 = b + f$ avec $b \in \mathfrak{b}$, $f \in \mathfrak{f}$ et posons $\mathfrak{b}' = b\mathfrak{b}^{-1}$. On a $b \in A$ car $\mathfrak{f} \subset A$; $\mathfrak{b}'$ est un idéal entier de B comaximal à $\mathfrak{f}$ (car $1 = b + f \in \mathfrak{b}' + \mathfrak{f}$) vérifiant $\mathfrak{b}\mathfrak{b}' = bB$. En posant $\mathfrak{a} = \mathfrak{b} \cap A$, $\mathfrak{a}' = \mathfrak{b}' \cap A$, d'après le lemme d'évitement du conducteur qui suit on a $\mathfrak{a}B = \mathfrak{b}$ et $\mathfrak{a}\mathfrak{a}' = bA$.
On a donc que $\mathfrak{a}$ est inversible dans A et que $\pi([\mathfrak{a}]) = [\mathfrak{b}]$. □

Lemme 8 (lemme d'évitement du conducteur, Dedekind ; cf. Sands [11] Théorème 3.1) *Soit $A \subset B$ deux anneaux. Soit $\mathfrak{f}$ un idéal de B contenu dans le conducteur. Alors les deux applications $\mathfrak{a} \mapsto \mathfrak{a}B$ et $\mathfrak{b} \mapsto \mathfrak{b} \cap A$ sont des bijections réciproques l'une de l'autre conservant l'intersection, la somme et le produit lorsqu'on les restreint aux idéaux entiers étrangers à $\mathfrak{f}$.*

Preuve.
Montrons seulement que les deux applications sont réciproques l'une de l'autre.
Soit $\mathfrak{a}$ un idéal de A avec $\mathfrak{a} + \mathfrak{f} = A$. Montrons que $\mathfrak{a}B \cap A = \mathfrak{a}$. On a $a + f = 1$ avec $a \in \mathfrak{a}$ et $f \in \mathfrak{f}$. Si $a' \in \mathfrak{a}B \cap A$, $a' = aa' + a'f$ avec $aa' \in \mathfrak{a}$ et $a'f \in \mathfrak{a}Bf \subset \mathfrak{a}A = \mathfrak{a}$.
Soit $\mathfrak{b}$ un idéal de B tel que $fb + \mathfrak{f} = B$. Montrons que $(\mathfrak{b} \cap A)B = \mathfrak{b}$. On a $b + f = 1$ avec $b \in \mathfrak{b}$ et $f \in \mathfrak{f}$, donc $b \in \mathfrak{b} \cap A$. Si $b' \in \mathfrak{b}$, $b' = bb' + b'f$ avec $bb' \in (\mathfrak{b} \cap A)B$ et $b'f \in \mathfrak{b} \cap A$. □

Références

[1] Bourbaki *Algèbre commutative, chapitre 2, Localisation.* Hermann 1961. 2

[2] Coquand T., Lombardi H. *Hidden constructions in abstract algebra (3) Krull dimension of distributive lattices and commutative rings.* dans : Commutative ring theory and applications. Eds : Fontana M., Kabbaj S.-E., Wiegand S. Lecture notes in pure and applied mathematics vol 131. M. Dekker. (2002) 477–499. 2, 4

[3] Coquand T., Lombardi H., Quitté C. *Generating non noetherian modules constructively.* Manuscripta mathematica **115**, (2004), 513–520. 2, 4

[4] Coquand T., Lombardi H., Quitté C. *Dimension de Heitmann des treillis distributifs et des anneaux commutatifs* Publications mathématiques de Besançon. Algèbre et Théorie des Nombres. (2006), 57–100. 2, 4

[5] Dedekind R. *Über die Anzahl der Ideal-Klassen in den verschiedenen Ordnungen eines endlichen Körpers.* 1–55 in Festschrift der Technischen Hochschule in Braunschweig zur Säkularfeier des Geburtstages von C. F. Gauß. 2

[6] Ducos L., Lombardi H., Quitté C., Salou M. *Théorie algorithmique des anneaux arithmétiques, des anneaux de Prüfer et des anneaux de Dedekind.* Journal of Algebra. **281**, (2004), 604–650. 2, 4

[7] Lam T. Y. *Lectures on Modules and Rings.* Springer GTM 189 (1998). 4

[8] Lombardi H., Quitté C., Yengui I. *Hidden constructions in abstract algebra (6) The theorem of Maroscia, Brewer and Costa.* Preprint 2005. 2, 4

[9] Mines R., Richman F., Ruitenburg W. *A Course in Constructive Algebra.* Springer-Verlag (1988). 2

[10] Rosenlicht M. *Generalized Jacobian varieties.* Ann. of Math. (2) **59** (1954), 505–530. 5

[11] Sands J. *Generalization of a theorem of Siegel.* Acta Arithmetica. **58** (1), (1991), 47–56. 1, 6

[12] Serre J.-P. *Groupes algébriques et corps de classes.* Hermann, Paris, 1975. 5

[13] Siegel C. *Abschätzung von Einheiten.* Nachr. Göttingen. **9**, (1969), 71–86. 1

Table des matières