Pierre Samuel

THÉORIE ALGÉBRIQUE DES NOMBRES

COLLECTION MÉTHODES

HERMANN, ÉDITEURS DES SCIENCES ET DES ARTS

Pierre Samuel, docteur ès sciences, professeur à l'Université de Paris XI, est né en 1921. Ses travaux concernent principalement l'algèbre commutative et la géométrie algébrique.

Deuxième édition revue et corrigée, 1971
Nouveau tirage, 1997

ISBN 2 7056 5589 1

Table

IV. CLASSES D'IDÉAUX. THÉORÈME DES UNITÉS

V. DÉCOMPOSITION DES IDÉAUX PREMIERS DANS UNE EXTENSION

VI. EXTENSIONS GALOISIENNES DES CORPS DE NOMBRES

Introduction

La Théorie des Nombres, ou Arithmétique, est souvent qualifiée de « Reine des Mathématiques ». La simplicité de son objet (les nombres entiers et leurs généralisations), l'élégance et la diversité de ses méthodes, les nombreux problèmes non résolus qu'elle contient, exercent en effet un incontestable attrait sur de nombreux mathématiciens, qu'ils soient des débutants, des arithméticiens professionnels, ou des spécialistes d'autres branches. On ne s'étonnera donc pas trop de voir que l'auteur de ce livre est un géomètre-algébriste, qui n'a aucune publication originale dans le domaine de l'Arithmétique proprement dite.

Ce livre ne se distinguera donc, ni par sa profondeur, ni par son étendue. Bien plus, il ne contient qu'un seul des points de vue par lesquels on peut aborder la Théorie des Nombres, à savoir le point de vue algébrique. A part un résultat élémentaire de Minkowski sur les réseaux de $\mathbf{R}^n$, on n'y verra aucune des belles et fécondes méthodes analytiques.

La primauté donnée au point de vue algébrique me semble toutefois justifiée par plusieurs raisons. Il permet tout d'abord de se placer rapidement dans le cadre où les problèmes se posent le plus naturellement, même s'ils ne concernent que les nombres entiers naturels. On verra, par exemple, que la recherche des solutions en nombres entiers de l'équation de Pell-Fermat $x^2 - dy^2 = \pm 1$ (d : entier donné, sans facteurs carrés) est un problème qui concerne essentiellement le corps quadratique $\mathbf{Q}(\sqrt{d})$. Pour la « grande » équation de Fermat $x^n + y^n = z^n$, c'est le corps des racines n-ièmes de l'unité qui joue le rôle décisif. Pour décomposer un entier en somme de deux (resp. quatre) carrés, on verra qu'il y a grand avantage à se placer dans l'anneau $\mathbf{Z}[i]$ des entiers de Gauss (resp. dans un anneau de quaternions convenablement choisi). La loi de réciprocité quadratique fait intervenir les corps quadratiques et les racines de l'unité. Dans tout ceci apparaissent des corps plus généraux que $\mathbf{Q}$, des anneaux plus généraux que $\mathbf{Z}$, ainsi que les corps et anneaux quotients de ces derniers, c'est-à-dire les corps finis et les algèbres sur ceux-ci.

Ainsi, sans épuiser la Théorie des Nombres, la méthode algébrique amène toutefois rapidement à des résultats substantiels. En poussant dans la même direction, on arriverait à des théorèmes plus profonds, comme ceux de la théorie du corps de classes.

D'autre part, celui qui aime les méthodes analytiques s'aperçoit qu'elles n'acquièrent leur pleine efficacité que si on les applique à des corps de nombres algébriques, et pas seulement à $\mathbf{Q}$. Par exemple il est regrettable d'avoir à étudier la seule fonction $\zeta(s)$ sans pouvoir traiter en même temps de la fonction $\zeta_K(s)$ d'un corps de nombres K, ni des nombreuses « séries L ».

Pour l'étudiant enfin, le développement de la méthode algébrique a l'avantage de fournir de très nombreux exemples illustrant les notions introduites en Propédeutique (maintenant « premier cycle ») et en Licence (maintenant « maîtrise » ou « licence ») : groupes, anneaux, corps, idéaux, anneaux et corps quotients, homomorphismes et isomorphismes, modules et espaces vectoriels. Un autre avantage est qu'il voit introduites en chemin plusieurs notions algébriques nouvelles qui sont fondamentales, non seulement pour l'arithmétique, mais aussi pour d'autres branches des Mathématiques, la Géométrie Algébrique en particulier : par exemple, les éléments entiers sur un anneau, les extensions de corps, la théorie de Galois, les modules sur les anneaux principaux, les anneaux et modules nœthériens, les anneaux de Dedekind et les anneaux de fractions.

Ce qui précède a implicitement décrit ce que le lecteur pourra trouver dans ce livre, et mentionné ce qu'il n'y trouvera pas. J'ai supposé qu'il connaît l'algèbre de Propédeutique et de Licence : notions élémentaires sur les groupes, anneaux, corps, polynômes, espaces vectoriels, — maniement des sous-objets, des objets-quotients et des objets-produits, — mécanisme du passage au quotient par un idéal ou un sous-module, — notions diverses d'homomorphisme et d'isomorphisme. Il trouvera tout ce qui est nécessaire sur ces questions dans un livre élémentaire d'algèbre dite « moderne », par exemple les excellents « Cours d'Algèbre » de R. Godement et « Algebra » de S. Lang [1]. J'utiliserai donc sans aucune hésitation ce langage et ces résultats, et j'espère montrer au lecteur qu'ils sont fort efficaces pour arriver rapidement à des théorèmes substantiels d'arithmétique. Par contre, bien que ce soit assez souvent traité dans l'option « algèbre » de l'ancienne licence Française (ou dans le certificat C. 3 de la nouvelle « maîtrise »), j'ai pensé qu'il serait plus commode pour le lecteur de trouver ici ce qui lui sera nécessaire au sujet des éléments entiers sur un anneau, des extensions algébriques de corps, de la théorie de Galois, des modules et anneaux nœthériens, et des anneaux de fractions. J'ai tenté de le faire sans ambages, mais aussi sans inutile sophistication.

1. Bien entendu la portée de ces deux ouvrages est nettement plus grande.

Ce livre est directement issu d'un cours de « Mathématiques approfondies » fait à l'Université de Paris en 1965, et répété en 1966; des notes polycopiées, rédigées par Alfred Vidal-Madjar, élève à l'École Normale Supérieure, que je tiens à vivement remercier, ont servi de première rédaction. Certains passages proviennent de cours faits à l'École Normale Supérieure de Jeunes Filles et à l'Université de Clermont-sur-Tiretaine. Enfin l'influence et les conseils de nombreux mathématiciens m'ont été fort précieux; parmi eux je tiens à remercier spécialement le maître de ma génération, N. Bourbaki, qui a eu l'obligeance de me montrer ses manuscrits non encore publiés, ainsi que mes amis Emil Grosswald, Georges Poitou, Jean-Pierre Serre et John Tate.

Préface a la deuxième édition.

J'adresse mes sincères remerciements à plusieurs lecteurs de la première édition, en particulier Germaine Revuz, Alain Bouvier et Pierre Cartier, qui ont envoyé de très utiles listes de corrections. Les remarques du traducteur de l'édition anglaise, Alan Silberger, ont aussi été précieuses.

juillet 1971

A NICOLE

qui a su créer autour de moi
une atmosphère favorable à ce livre

Rappel de notations de définitions et de résultats

On utilise les notations classiques de la théorie des ensembles : $\in$, $\subset$, $\cup$, $\cap$. Le complémentaire d'une partie B d'un ensemble A est noté A — B. Le cardinal (ou puissance, ou nombre d'éléments) d'un ensemble A est noté card (A); si A est un groupe on dit aussi l'ordre de ce groupe.

On suppose connues les notions de groupe, anneau, corps et espace vectoriel, ainsi que la théorie élémentaire des espaces vectoriels (appelée aussi « algèbre linéaire »). Dans ce livre, à l'exception du chap. V, § 7, « anneau » (resp. « corps ») veut dire anneau (resp. corps) *commutatif à élément unité.*

Étant donnés un groupe fini et un sous-groupe H de G, on rappelle que card (H) divise card (G); le quotient card (G)/card (H) s'appelle l'indice de H dans G et se note (G : H).

Étant données deux parties A, B d'un groupe G noté additivement, A + B désigne l'ensemble des sommes $a + b$ où $a \in A$ et $b \in B$.

Étant donné un anneau A, on désigne par A[X] ou par A[Y] (lettre majuscule) l'anneau des polynômes (formels) à une variable sur A; notations $A[X_1, \ldots, X_n]$ pour les polynômes à n variables et A[[X]] pour les séries formelles.

Par convention, un sous-anneau A d'un anneau B contient l'élément unité de B. Étant donnés un anneau B, un sous-anneau A de B, et un élément $x \in B$, on désigne par $A[x]$ le sous-anneau de B engendré par A et x, c'est-à-dire l'intersection des sous-anneaux de B qui contiennent A et x; c'est l'ensemble des sommes de la forme $a_0 + a_1x + \cdots + a_nx^n$ $(a_i \in A)$; notation $A[x_1, , \ldots x_n]$ et résultats analogues pour le sous-anneau de B engendré par A et une famille finie $(x_1, \ldots, x_n)$ d'éléments de B.

Un anneau A est dit *intègre* (ou sans diviseurs de zéro) si le produit de deux éléments non nuls quelconques de A est non nul, et si A n'est pas réduit à 0.

Un idéal $\mathfrak{b}$ d'un anneau A est un sous-groupe additif tel que $x \in \mathfrak{b}$ et $a \in A$ impliquent $ax \in \mathfrak{b}$. L'anneau tout entier et l'ensemble réduit à 0 (et noté (0)) sont des idéaux, parfois qualifiés de « triviaux ». Un corps n'en a pas d'autres, et ceci caractérise les corps parmi les anneaux. Étant donnée une famille (b_i) d'éléments d'un anneau A, l'intersection des idéaux de A contenant les b_i est un idéal de A, appelé idéal engendré par les b_i; c'est l'ensemble des sommes finies $\sum_i a_i b_i$ avec $a_i \in A$. Un idéal engendré par un élément b est dit principal; notation Ab ou (b).

Étant donnés un anneau A et un idéal $\mathfrak{b}$ de A, les classes d'équivalence $a + \mathfrak{b} (a \in A)$ forment un anneau, appelé anneau quotient de A par $\mathfrak{b}$ et noté $A/\mathfrak{b}$. Les idéaux de $A/\mathfrak{b}$ sont de la forme $\mathfrak{b}'/\mathfrak{b}$ où $\mathfrak{b}'$ parcourt l'ensemble des idéaux de A contenant $\mathfrak{b}$. Pour que $A/\mathfrak{b}$ soit un corps il faut et il suffit que $\mathfrak{b}$ soit maximal parmi les idéaux de A distincts de A; on dit alors que $\mathfrak{b}$ est maximal. Un idéal $\mathfrak{p}$ est dit premier si $A/\mathfrak{p}$ est intègre.

Étant donnés deux anneaux A, A', d'éléments unités e et e', un homomorphisme $f : A \to A'$ est une application f de A dans A' telle que:

$$f(a+b) = f(a) + f(b), \qquad f(ab) = f(a)f(b), \qquad f(e) = e'.$$

Étant donné un anneau A, une A-*algèbre* est un anneau B muni d'un homomorphisme $\varphi : A \to B$. Si A est un corps, φ est injectif, et on identifie souvent alors A à son image $\varphi(A)$ (qui est un sous-anneau de B).

Étant donnés un corps L et un sous-corps K de L, on dit souvent que L est une extension de K.

L'élément unité d'un anneau A sera le plus souvent noté 1.

La notion de *module* sur un anneau A (ou de A-module), est la généralisation directe de la notion d'espace vectoriel sur un corps. Un A-module M est un groupe abélien (noté additivement) muni d'une application $A \times M \to M$ (notée multiplicativement) telle que $a(x+y) = ax + ay$, $(a+b)x = ax + bx$, $a(bx) = (ab)x$, $1\,x = x (a,\ b \in A,\ x,\ y \in M)$. On a les notions de sous-module et de module quotient. Étant donnés deux A-modules, M, M' un homomorphisme (ou application A-linéaire) de M dans M' est une application $f : M \to M'$ telle que

$$f(x+y) = f(x) + f(y) \qquad f(ax) = af(x) \qquad (a \in A,\quad x, y \in M).$$

Étant donné un homomorphisme $f : X \to X'$ (de groupes, d'anneaux ou de modules), on appelle *noyau* de f et on note ker (f) l'image réciproque de l'élément neutre de X' par f; c'est un sous-groupe invariant (ou un idéal, ou un sous-module) de X; pour que f soit injectif il faut et il suffit que ker (f) soit réduit à l'élément neutre de X. On appelle *image* de f la partie $f(X)$ de X'; c'est un sous-groupe (ou un sous-anneau, ou un sous-module) de X'.

1. A cause de l'anglais « kernel », ou de l'allemand « kern ».

Étant donnés deux ensembles X, X′, une application f de X dans X′, est souvent désignée par la notation $f: \mathrm{X} \to \mathrm{X}'$ (flèche droite). Lorsqu'une application $f: \mathrm{X} \to \mathrm{X}'$ est décrite par la valeur qu'elle prend en un élément arbitraire x de X, on emploie la notation $x \mapsto f(x)$ (flèche barrée). Ainsi la fonction sinus, sin : $\mathbf{R} \to \mathbf{R}$ peut être définie par

$$x \mapsto \sum_{n=0}^{\infty} (-1)^n \frac{x^{2+1}}{(2n+1)!}.$$

Nous emploierons les notations classiques des objets mathématiques courants :

N : ensemble des entiers naturels $(0, 1, 2, \ldots, n, \ldots)$ (N pour « nombres »).

Z : anneau des entiers rationnels ou relatifs (entiers naturels et leurs opposés) (Z pour « Zahlen »).

Q : corps des nombres rationnels (quotients d'éléments de **Z**) (Q pour « quotients »).

R : corps des nombres réels (R pour « réels »).

C : corps des nombres complexes (C pour « complexes »).

$\mathbf{F}_q$: corps fini à q éléments (F pour « fini » ou « field »).

CHAPITRE I

Anneaux principaux

1.1. Relation de divisibilité dans les anneaux principaux

Soient A un anneau intègre, K son corps des fractions, x et y des éléments de K. On dit que x *divise* y s'il existe $a \in A$ tel que $y = ax$. Expressions synonymes : x est diviseur de y, y est multiple de x; notation $x|y$. Cette relation entre éléments de K dépend essentiellement de l'anneau A; s'il faut préciser, on dit qu'il s'agit de la relation de divisibilité dans K *par rapport à* A.

Étant donné $x \in K$, l'ensemble des multiples de x est Ax, avec la notation classique. Ainsi $x|y$ s'écrit aussi $y \in Ax$, ou encore $Ay \subset Ax$. L'ensemble Ax s'appelle un *idéal fractionnaire principal* de K par rapport à A; si $x \in A$, Ax est l'idéal principal (ordinaire) de A engendré par x. Comme la relation de divisibilité $x|y$ équivaut à la relation d'*ordre* $Ay \subset Ax$, elle a les deux propriétés suivantes des relations d'ordre.

1. $x|x$; si $x|y$ et $y|z$, alors $x|z$.

Par contre, si $x|y$ et $y|x$, on ne peut pas en général conclure que $x = y$; on a seulement $Ax = Ay$, ce qui (si $y \neq 0$) veut dire que le quotient xy^{-1} est un élément *inversible* de A; deux tels éléments sont dits *associés*; ils sont indistingables du point de vue de la divisibilité.

Exemple. Les éléments de K associés à 1 sont les éléments inversibles de A; on les appelle souvent les *unités* de A; ils forment un groupe pour la multiplication, que nous noterons A^*. La détermination des unités d'un anneau A est un problème intéressant, que nous traiterons dans le cas où A est l'anneau des entiers d'un corps de nombres (voir chap. IV). Voici quelques exemples simples :

a) Si A est un corps, A^* est l'ensemble des éléments non nuls de A;

b) Si $A = \mathbf{Z}$, A^* se compose de $+1$ et de -1.

c) Les unités de l'anneau de polynômes $B = A[X_1, \ldots, X_n]$ sont, lorsque A est intègre, les constantes inversibles; autrement dit; $B^* = A^*$.

d) Les unités de l'anneau de séries formelles $A[[X_1, \ldots, X_n]]$ sont les séries formelles dont le terme constant est inversible.

DÉFINITION 1. *Un anneau* A *est dit principal s'il est intègre et si tout idéal de* A *est principal.*

On a vu en Math. Élém. [1] que l'anneau $\mathbf{Z}$ est principal (Rappel : étant donné un idéal $\mathfrak{a} \neq (0)$ de $\mathbf{Z}$, il contient un plus petit entier $b > 0$; par division euclidienne de $x \in \mathfrak{a}$ par b, on voit que x est un multiple de b). Si k est un corps, on a vu en MGP [2] ou en Spéciales que l'anneau $k[X]$ des polynômes à *une* variable sur k est principal (même méthode; prendre un polynôme non nul $b(X)$ de plus petit degré de l'idéal donné $\mathfrak{a}$, et utiliser la division enclidienne, c'est-à-dire suivant les puissances décroissantes, par $b(X)$). Cette méthode se généralise aux anneaux qu'on appelle « euclidiens » ([1], chap. VIII, § 1, exercices; ou [9], chap. I). Si k est un corps, on voit facilement que tout idéal non nul de l'anneau de séries formelles $A = k[[X]]$ est de la forme AX^n avec $n \geqslant 0$, de sorte que $A = k[[X]]$ est principal.

La divisibilité dans le corps des fractions K d'un anneau *principal* A a une forme particulièrement simple. Comme c'est la généralisation immédiate du cours d'Arithmétique de Math. Élém., nous serons très brefs :

I. Deux éléments quelconques u, v de K ont un *plus grand commun diviseur* (p.g.c.d.), c'est-à-dire un élément d tel que les relations

1. « $x|u$ et $x|v$ » et « $x|d$ »

soient équivalentes. En effet il revient au même de dire que Au et Av ont une *borne supérieure* dans l'ensemble ordonné des idéaux fractionnaires principaux; or celle-ci est $Au + Av$, qui est un idéal fractionnaire principal car l'anneau A est principal (clair pour $u, v \in A$; on se ramène à ce cas en mulitpliant u et v par un dénominateur commun). Nous obtenons une information supplémentaire (« l'*identité de Bezout* ») : il existe des éléments a, b *de* A tels que le p.g.c.d. d de u et v s'écrive

2. $d = au + bv$.

Le p.g.c.d. de u et v est déterminé à un élément inversible près de A.

II. Deux éléments quelconques u, v et K ont un *plus petit commun multiple* (p.p.c.m.), c'est-à-dire un élément m tel que les relations

3. « $u|x$ et $v|x$ » et « $m|x$ »

soient équivalentes. On peut le voir en remarquant que le passage à l'inverse $t \mapsto t^{-1}$ renverse les relations de divisibilité, ce qui nous ramène au p.g.c.d.; cette méthode nous apporte aussitôt le sous-produit suivant:

4. p.p.c.m. $(u, v) =$ (p.g.c.d. $(u^{-1}, v^{-1}))^{-1}$ (pour $u, v \neq 0$),

d'où on déduit sans peine la formule classique.

5. p.g.c.d. (u, v). p.p.c.m. $(u, v) = uv$.

1. Terminale C dans la nouvelle terminologie.
2. Appelé « MP » à partir de 1966.

On peut aussi procéder comme dans 1) et remarquer que l'existence du p.p.c.m. de u et v équivaut à celle d'une *borne inférieure* de Au et Av dans l'ensemble ordonné des idéaux fractionnaires principaux; or celle-ci est $Au \cap Av$.

III. Deux éléments a, b *de* A sont dits *étrangers* (ou *premiers entre eux*) si 1 est un de leurs p.g.c.d. Rappelons l'important LEMME D'EUCLIDE. *Soient* a, b, c *des éléments d'un anneau principal* A; *si* a *divise* bc *et est étranger à* b, *alors* a *divise* c.

Démonstration succinte : par Bezout (2), on a a' et $b' \in A$ tels que $1 = a'a + b'b$; d'où $c = a'ac + b'bc$; comme a divise chaque terme du second membre, il divise c.

IV. Enfin on a l'importante « décomposition en facteurs premiers » :

THÉORÈME. *Étant donnés un anneau principal* A *et son corps des fractions* K, *il existe une partie* P *de* A *telle que tout* $x \in K$ *s'écrive de façon unique*

$$6. \quad x = u \prod_{p \in P} p^{v_p(x)}$$

où u *est un élément inversible de* A, *et où les exposants* $v_p(x)$ *sont des éléments de* $\mathbf{Z}$, *tous nuls sauf un nombre fini d'entre eux.*

Pour un exposé plus systématique de ces questions, nous renvoyons le lecteur à [1], *Algèbre*, chap. VI, § 1 et chap. VII, § 1. Une partie de la théorie (plus précisément tout ce qui ne tourne pas autour de l'identité de Bezout) s'étend à des anneaux plus généraux que les anneaux principaux, à savoir les anneaux *factoriels*; voir [7], ou [2] Algèbre commutative, chap. VII, § 3.

1.2. Un exemple : les équations $x^2 + y^2 = z^2$ et $x^4 + y^4 = z^4$

Une des parties les plus attirantes de la Théorie des Nombres est l'étude des *équations diophantiennes.* Il s'agit d'équations polynômes $P(x_1, ..., x_n) = 0$ à coefficients dans $\mathbf{Z}$ (resp. dans $\mathbf{Q}$), dont on cherche les solutions (x_i) en nombres entiers (resp. en nombres rationnels). On peut remplacer $\mathbf{Z}$ (resp. $\mathbf{Q}$) par des anneaux A (resp. des corps K) plus généraux; nous en verrons un exemple plus tard (§ 6).

Nous allons étudier ici deux cas particuliers de la fameuse *équation de Fermat:*

$$1. \quad x^n + y^n = z^n.$$

Fermat a affirmé avoir démontré que, pour $n \geqslant 3$, cette équation n'a pas de solution (x, y, z) en nombres entiers tous non-nuls; sa démonstration n'a pas été retrouvée. De très nombreux mathématiciens ont, depuis, intensément travaillé sur ce problème, et montré que l'affirmation de Fermat est vraie pour un grand nombre de valeurs de l'exposant n; cependant aucune démonstration générale (i. e. valable pour tout n) n'a été trouvée.

L'opinion aujourd'hui la plus courante est que, dans sa « démonstration », Fermat avait commis une erreur, mais une erreur digne de ce mathématicien de premier ordre. Par exemple il aurait pu avoir l'idée (géniale pour son époque) d'opérer dans l'anneau des entiers du corps des racines n-ièmes de l'unité, et avoir cru que cet anneau est toujours principal. En effet, on sait démontrer l'assertion de Fermat pour tout exposant n tel que cet anneau soit principal; mais il ne l'est pas pour tout n; bien plus, pour n premier, cet anneau n'est principal que pour un nombre fini de valeurs de n [1].

Pour $n = 2$, l'équation (1) a des solutions entières, par exemple (3,4,5). On peut en donner une description complète :

THÉORÈME 1. *Si x, y, z sont des entiers $\geqslant 1$ tels que $x^2 + y^2 = z^2$, il existe un entier d et des entiers étrangers u, v tels que (à une permutation près de x et y) on ait:*

2. $x = d(u^2 - v^2) \qquad y = 2\,duv \qquad z = d(u^2 + v^2)$

Un calcul facile montre que les formules (2) donnent des solutions de $x^2 + y^2 = z^2$. Réciproquement soient x, y, z des entiers $\geqslant 1$ tels que $x^2 + y^2 = z^2$. Quitte à diviser x, y, z par leur p.g.c.d., on peut les supposer étrangers dans leur ensemble; ils sont alors étrangers deux à deux, car, si, par exemple, x et z ont un facteur premier commun p, alors p divise $y^2 = z^2 - x^2$ et donc y. En particulier deux des nombres x, y, z sont impairs, et le troisième est nécessairement pair. Les nombres x et y ne peuvent être tous deux impairs, car sinon, on aurait $x^2 \equiv 1 \pmod{4}$, $y^2 \equiv 1 \pmod{4}$ d'où $z^2 \equiv 2 \pmod{4}$ contrairement au fait que z^2 est un carré. On a donc, après échange éventuel de x et y.

3. x impair, y pair, z impair.

Écrivons l'équation

4. $y^2 = z^2 - x^2 = (z - x)(z + x)$.

Comme le p.g.c.d. de $2x$ et de $2z$ est 2, et que $2x = (z + x) - (z - x)$ et $2z = (z + x) + (z - x)$, le p.g.c.d. de $z - x$ et $z + x$ ne peut être que 2. Posons $y = 2y'$, $z + x = 2x'$, $z - x = 2z'$, où y', x', z' sont des entiers, car y, $z + x$ et $z - x$ sont pairs par (3). On a alors $y'^2 = x'z'$. Comme x' et z' sont étrangers, la décomposition en facteurs premiers de y'^2 montre que x' et z' sont des *carrés* u^2 et v^2 : en effet tout facteur premier de y'^2 va, avec son exposant pair, soit tout entier dans x', soit tout entier dans z'. On a donc $z + x = 2u^2$, $z - x = 2v^2$, $y^2 = 2u^2 . 2v^2$, d'où $x = u^2 - v^2$, $y = 2uv$, $z = u^2 + v^2$. Ici u et v sont étrangers, sinon x, y, z auraient un facteur premier commun. On en déduit (2) en remultipliant par d le p.g.c.d. CQFD.

1. Voir C. L. Siegel — « Gesammelte Werke », t. III, p. 436-442.

THÉORÈME 2. *L'équation* $x^4 + y^4 = z^2$ *n'a pas de solution en nombres entiers* $x, y, z \geqslant 1$.

Raisonnons par l'absurde. On a alors une solution (x, y, z) où z est *minimal*. Pour celle-ci, x, y et z sont étrangers deux à deux : en effet, si par exemple, x et y avaient un facteur premier commun p, alors p^4 diviserait z^2, donc p^2 diviserait z, et $\left(\frac{x}{p}, \frac{y}{p}, \frac{z}{p^2}\right)$ serait une solution contredisant la minimalité de z; les deux autres cas sont analogues et plus faciles. Comme notre équation s'écrit $(x^2)^2 + (y^2)^2 = z^2$, on peut lui appliquer le th. 1 : après permutation éventuelle de x et y, on voit qu'on a des entiers $u, v \geqslant 1$ et étrangers tels que

5. $x^2 = u^2 - v^2, \qquad y^2 = 2uv, \qquad z = u^2 + v^2.$

Comme $4 | y^2$, la relation $y^2 = 2uv$, montre que l'un des deux nombres u et v est pair; l'autre est nécessairement impair; la répartition « u pair, v impair » donne $u^2 \equiv 0$ (mod. 4), $v^2 \equiv 1$ (mod. 4), d'où $x^2 = u^2 - v^2 \equiv -1$ (mod. 4) ce qui est absurde; donc u est impair et $v = 2v'$. La relation $y^2 = 4uv'$ et le fait que u et v' sont étrangers montrent que u et v' sont des carrés a^2 et b^2. Appliquons encore le th. 1, cette fois à l'équation $x^2 + v^2 = u^2$ (cf. (5)); comme x et u sont impairs, v pair, et x, v, u étrangers deux à deux, on a des entiers étrangers $c, d \geqslant 1$ tels que :

6. $x = c^2 + d^2, \qquad v = 2cd, \qquad u = c^2 + d^2.$

Or, de $v = 2v' = 2b^2$, on déduit $cd = b^2$, de sorte que c et d sont encore des carrés x'^2 et y'^2, car ils sont étrangers. Comme $u = a^2$, la dernière équation (6) s'écrit

7. $a^2 = x'^4 + y'^4$

et a la *même forme* que l'équation donnée. Mais, on a, par (5), $z = u^2 + v^2 = a^4 + 4b^4 > a^4$, d'où $z > a$, ce qui contredit le caractère minimal de z. Notre assertion est donc démontrée

Une légère variante de notre démonstration montre que, étant donnée une solution (x, y, z) en entiers $\geqslant 1$ de $x^4 + y^4 = z^2$, on construit une suite (x_n, y_n, z_n) de telles solutions, où la suite (z_n) est strictement décroissante, ce qui est absurde. Ceci est la méthode de *descente infinie*, due à Fermat.

COROLLAIRE. *L'équation* $x^4 + y^4 = z^4$ *n'a pas de solution en nombres entiers* $x, y, z \geqslant 1$.

En effet cette équation s'écrit $x^4 + y^4 = (z^2)^2$, et on applique le th. 2.

1.3. Quelques lemmes sur les idéaux; l'indicateur d'Euler

Soit $n \geqslant 1$ un entier naturel. On appelle *indicateur d'Euler* de n, et on note $\varphi(n)$ le nombre des entiers q premiers à n et tels que $0 \leqslant q \leqslant n$ (il revient au même d'écrire $1 \leqslant q \leqslant n-1$, car 0 et n ne sont pas premiers à n). Si p est un nombre premier, il est clair que :

1. $\varphi(p) = p - 1$

Pour $n = p^s$, puissance de nombre premier, les entiers premiers à p^s sont les entiers non multiples de p; or il y a p^{s-1} multiples de p entre 1 et p^s; on a donc :

2. $\varphi(p^s) = p^s - p^{s-1} = p^{s-1}(p-1)$

A partir de là nous nous proposons de calculer $\varphi(n)$ en utilisant la décomposition de n en facteurs premiers. Pour cela nous aurons besoin de caractérisations de $\varphi(n)$, et de lemmes sur les idéaux qui seront encore utilisés par la suite.

Proposition 1. *Soit* $n \geqslant 1$ *un entier naturel. L'indicateur d'Euler* $\varphi(n)$ *est égal au nombre des éléments de* $\mathbf{Z}/n\mathbf{Z}$ *qui engendrent ce groupe, et aussi au nombre des éléments inversibles de l'anneau* $\mathbf{Z}/n\mathbf{Z}$.

Rappelons que chaque classe de congruence mod. $n\mathbf{Z}$ contient un entier q et un seul tel que $0 \leqslant q \leqslant n-1$; pour un tel entier q, notons $\bar{q}$ sa classe mod. $n\mathbf{Z}$. Il suffit de démontrer, en cercle, les implications : q premier à $n \Longrightarrow \bar{q}$ inversible $\Longrightarrow \bar{q}$ engendre $\mathbf{Z}/n\mathbf{Z} \Longrightarrow q$ premier à n. Si q est premier à n, l'identité de Bezout (§ 1, (2)) montre qu'on a des entiers x et y tels que $qx + ny = 1$; d'où $\bar{q}.\bar{x} = \bar{1}$, et $\bar{q}$ est inversible. Si $\bar{q}$ est inversible, notons x un entier tel que $\bar{q}.\bar{x} = 1$; si $\bar{a}$ est un élément quelconque de $\mathbf{Z}/n\mathbf{Z}$ et si a est un représentant de $\bar{a}$, on a $\bar{a} = \bar{a}\bar{x}\bar{q}$ (dans l'anneau $\mathbf{Z}/n\mathbf{Z}$), d'où $\bar{a} = (ax).\bar{q}$ (dans le groupe additif $\mathbf{Z}/n\mathbf{Z}$); donc $\bar{q}$ engendre le groupe $\mathbf{Z}/n\mathbf{Z}$. Enfin si $\bar{q}$ engendre $\mathbf{Z}/n\mathbf{Z}$, on a un entier x tel que $x.\bar{q} = \bar{1}$, donc tel que $xq \equiv 1 \pmod{n}$; ainsi il existe un entier y tel que $xq - 1 = yn$, d'où $1 = xq - yn$; ceci est une identité de Bezout qui montre que q est premier à n. CQFD.

Lemme 1. *Soient* A *un anneau,* $\mathfrak{a}$ et $\mathfrak{b}$ *des idéaux de* A *tels que* $\mathfrak{a} + \mathfrak{b} = A$ *Alors* $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$ *et l'homomorphisme canonique* $\varphi : A \to A/\mathfrak{a} \times A/\mathfrak{b}$ *définit un isomorphisme* $\theta : A/\mathfrak{a}\mathfrak{b} \to A/\mathfrak{a} \times A/\mathfrak{b}$.

Rappelons que l'homomorphisme φ associe à tout $x \in A$ le couple formé de la classe de x mod. $\mathfrak{a}$, et de la classe de x mod. $\mathfrak{b}$.

On sait qu'on a, en général, $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a}$, $\mathfrak{a}\mathfrak{b} \subset \mathfrak{b}$, d'où $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$; soit alors $x \in \mathfrak{a} \cap \mathfrak{b}$; comme $\mathfrak{a} + \mathfrak{b} = A$ on dispose d'éléments $a \in \mathfrak{a}$ et $b \in \mathfrak{b}$ tels que $a + b = 1$; alors $x = ax + xb$ est somme de deux éléments de $\mathfrak{a}\mathfrak{b}$, d'où $x \in \mathfrak{a}\mathfrak{b}$ et $\mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{a}\mathfrak{b}$. Donc $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$.

Il est clair que le noyau de φ est $\mathfrak{a} \cap \mathfrak{b}$; comme $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$, φ est constante sur chaque classe mod. $\mathfrak{a}\mathfrak{b}$, d'où l'application $\theta : A/\mathfrak{a}\mathfrak{b} \to A/\mathfrak{a} \times A/\mathfrak{b}$;

c'est évidemment un homomorphisme; comme $\varphi^{-1}(0) = \mathfrak{a}\mathfrak{b}$, on a $\theta^{-1}(0) = (0)$, et θ est injective. Reste à montrer que θ est surjective.

Nous avons un peu développé ce raisonnement de « passage au quotient » à titre d'entraînement. Nous serons désormais bien plus brefs pour des raisonnements analogues.

Pour montrer la surjectivité de θ (ou de φ, ce qui revient au même), il s'agit de construire un élément x de A dont les classes modulo $\mathfrak{a}$ et modulo $\mathfrak{b}$ sont arbitrairement données; soient y et z des représentants de ces classes. Or on dispose d'éléments $a \in \mathfrak{a}$ et $b \in \mathfrak{b}$ tels que $a + b = 1$. On prend $x = az + by$. Modulo $\mathfrak{a}$, on a $x \equiv by \equiv (1-a)y \equiv y - ay \equiv y$; par échange des rôles, on en déduit $x \equiv z$ mod. $\mathfrak{b}$.CQFD.

Lemme 2. *Soient* A *un anneau, et* $(\mathfrak{a}_i)_{1 \leqslant i \leqslant r}$ *une famille finie d'idéaux de* A *tels que* $\mathfrak{a}_i + \mathfrak{a}_j = A$ *pour* $i \neq j$. *On a alors un isomorphisme canonique de* $A/\mathfrak{a}_1 \ldots \mathfrak{a}_r$ *sur* $\prod_{i=1}^{r} A/\mathfrak{a}_i$.

Le lemme 1 est le cas $r = 2$ du lemme 2. Nous procéderons à partir de là par récurrence sur r. Posons $\mathfrak{b} = \mathfrak{a}_2 \ldots \mathfrak{a}_r$. Montrons que $\mathfrak{a}_1 + \mathfrak{b} = A$.

En effet, pour $i \geqslant 2$, on a $\mathfrak{a}_1 + \mathfrak{a}_i = A$ et on dispose donc d'éléments $c_i \in \mathfrak{a}_1$ et $a_i \in \mathfrak{a}_i$ tels que $c_i + a_i = 1$. Multiplions membre à membre : il vient $c + a_2 \ldots a_n = 1$, où c est une somme de termes dont chacun contient au moins un c_i en facteur; on a donc $c \in \mathfrak{a}_1$. Comme $a_2 \ldots a_r \in \mathfrak{b}$, on a bien $\mathfrak{a}_1 + \mathfrak{b} = A$.

Par le lemme 1, on a un isomorphisme $A/\mathfrak{a}_1\mathfrak{b} \sim A/\mathfrak{a}_1 \times A/\mathfrak{b}$. D'après l'hypothèse de récurrence on a un isomorphisme

$$A/\mathfrak{b} = A/\mathfrak{a}_2 \ldots \mathfrak{a}_r \sim (A/\mathfrak{a}_2) \times \cdots \times (A/\mathfrak{a}_r).$$

On compose ces isomorphismes et notre assertion s'ensuit. CQFD.

Appliquons maintenant ces lemmes à l'anneau $\mathbf{Z}$:

Proposition 2. *Soient* n *et* n' *des entiers premiers entre eux; alors l'anneau* $\mathbf{Z}/nn'\mathbf{Z}$ *est isomorphe à l'anneau produit* $\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/n'\mathbf{Z}$.

Ceci est un cas particulier de lemme 1, l'hypothèse $n\mathbf{Z} + n'\mathbf{Z} = \mathbf{Z}$ étant l'identité de Bezout.

Corollaire 1. *Si* n *et* n' *sont des entiers* $\geqslant 1$ *premiers entre eux, on a* $\varphi(nn') = \varphi(n)\varphi(n')$.

En effet $\varphi(nn')$ est le nombre des éléments inversibles de $\mathbf{Z}/nn'\mathbf{Z}$ (prop. 1), qui est isomorphe à $\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/n'\mathbf{Z}$. Or un élément (α, β) d'un anneau produit est inversible si et seulement si chacune de ses composantes α, β est inversible. D'où notre assertion, en appliquant encore la prop. 1.

COROLLAIRE 2. *Soient n un entier $\geqslant 1$, et $n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ sa décomposition en facteurs premiers. Alors* $\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \ldots \left(1 - \frac{1}{p_r}\right)$

Par le cor. 1, on a $\varphi(n) = \varphi(p_1^{\alpha_1}) \ldots \varphi(p_r^{\alpha_r})$. Or, par (2), on a $\varphi(p_i^{\alpha_i}) = p_i^{\alpha_i - 1}(p_i - 1) = p_i^{\alpha_i}\left(1 - \frac{1}{p_i}\right)$. Notre formule s'ensuit par multiplication.

1.4. Quelques préliminaires sur les modules

En vue d'étudier les modules sur un anneau principal, quelques préliminaires nous seront nécessaires.

Étant donnés un anneau A et un ensemble I on note $A^{(I)}$ l'ensemble des familles $(a_i)_{i \in I}$, indexées par I, d'éléments de A *telles que* $a_i = 0$ sauf pour un nombre *fini* d'indices $i \in I$; ainsi $A^{(I)}$ est une partie de l'ensemble produit A^I, et aussi un sous-module de A^I si on munit A^I de la structure de A-module définie par composantes.

Si I est fini, on a $A^{(I)} = A^I$.

Pour $j \in I$, la famille $(\delta_{ji})_{i \in I}$ telle que $\delta_{jj} = 1$ et $\delta_{ji} = 0$ pour $i \neq j$ est un élément e_j de $A^{(I)}$. Tout élément $(a_j)_{j \in I}$ de $A^{(I)}$ s'écrit, d'une façon et d'une seule, comme combinaison linéaire (finie) des e_j; plus présisément :

1. $(a_j)_{j \in I} = \sum_{j \in I} a_j e_j$

(noter que, dans la sommation du second membre, tous les termes sont nuls sauf un nombre fini, de sorte que la sommation a un sens). On dit que $(e_j)_{j \in I}$ est la *base canonique* de $A^{(I)}$.

Soient A un anneau, M un A-module, et $(x_i)_{i \in I}$ une famille d'éléments de M. A tout élément $(a_i)_{i \in I}$ de $A^{(I)}$ associons l'élément $\sum_i a_i x_i$ de M (comme ci-dessus la sommation a un sens). On a ainsi défini une application $\varphi : A^{(I)} \to M$, qui est évidemment *linéaire*; si $(e_i)_{i \in I}$ est la base canonique de $A^{(I)}$, on a $\varphi(e_i) = x_i$ pour tout $i \in I$. Les équivalences suivantes sont immédiates :

2. les x_i sont linéairement indépendants $\Longleftrightarrow$ φ est injective.

3. $(x_i)_{i \in I}$ est un système générateur $\Longleftrightarrow$ φ est surjective.

Si φ est *bijective* on dit que $(x_i)_{i \in I}$ est une *base* de M; ceci veut dire que tout élément x de M s'écrit, *d'une façon et d'une seule*, comme combinaison linéaire des x_i. Un module M qui admet une base est appelé un *module libre*.

Contrairement aux espaces vectoriels sur les corps, un module sur un anneau n'admet pas nécessairement de base. Exemple, le $\mathbf{Z}$-module $\mathbf{Z}/n\mathbf{Z}$ où $n \neq 0,1$. Dans la suite nous démontrerons que certains modules sont libres; ce sera rarement trivial.

Un module sera dit *de type fini* s'il admet un système générateur fini. Le théorème suivant est à la base de l'étude des anneaux et modules nœthériens, que nous développerons un peu plus au chapitre III.

THÉORÈME 1. *Soient* A *un anneau,* M *un* A-*module. Les conditions suivantes sont équivalentes:*

a) *Toute famille non vide de sous-modules de* M *possède un élément maximal* (*pour la relation d'inclusion*)*;*

b) *Toute suite croissante* $(\mathrm{M}_n)_{n\geqslant 0}$ (*pour la relation d'inclusion*) *de sous-modules de* M *est stationnaire* (c-à-d. *il existe* n_0 *tel que* $\mathrm{M}_n = \mathrm{M}_{n_0}$ *pour tout* $n \geqslant n_0$)*;*

c) *Tout sous-module de* M *est de type fini.*

Montrons que *a*) implique *c*). Soient E un sous-module de M et Φ la famille des sous-modules de type fini de E; elle n'est pas vide car $\{0\} \in \Phi$. Par *a*), Φ admet un élément maximal F. Pour $x \in \mathrm{E}$, $\mathrm{F} + \mathrm{A}x$ est un sous-module de type fini de E (il est engendré par la réunion de $\{x\}$ et d'un système générateur fini de F). On a donc $\mathrm{F} + \mathrm{A}x = \mathrm{F}$ car $\mathrm{F} + \mathrm{A}x \supset \mathrm{F}$ et car F est maximal. D'où $x \in \mathrm{F}$, $\mathrm{E} \subset \mathrm{F}$, $\mathrm{E} = \mathrm{F}$, et E est de type fini.

Prouvons maintenant que *c*) implique *b*). Soit $(\mathrm{M}_n)_{n\geqslant 0}$ une suite croissante de sous-modules de M. Alors $\mathrm{E} = \bigcup_{n\geqslant 0} \mathrm{M}_n$ est un sous-module de M. Par *c*), il admet un système générateur fini $(x_1, \ldots, x_q)$. Pour tout i, il y a un indice $n(i)$ tel que $x_i \in \mathrm{M}_{n(i)}$. Soit n_0 le plus grand des $n(i)$. On a $x_i \in \mathrm{M}_{n_0}$ pour tout i, d'où $\mathrm{E} \subset \mathrm{M}_{n_0}$ et $\mathrm{E} = \mathrm{M}_{n_0}$. Pour $n \geqslant n_0$, les inclusions $\mathrm{M}_{n_0} \subset \mathrm{M}_n \subset \mathrm{E}$ et l'égalité $\mathrm{M}_{n_0} = \mathrm{E}$ montrent que $\mathrm{M}_{n_0} = \mathrm{M}_n$. Donc la suite (M_n) est stationnaire à partir de n_0.

Reste à montrer que *b*) implique *a*). Or l'équivalence de *a*) et de *b*) est un cas particulier d'un lemme sur les ensembles ordonnés :

LEMME 1. *Soit* T *un ensemble ordonné. Les conditions suivantes sont équivalentes:*

a) *Toute famille non vide d'éléments de* T *admet un élément maximal;*

b) *Toute suite croissante* $(t_n)_{n\geqslant 0}$ *d'éléments de* T *est stationnaire.*

a) $\Longrightarrow$ *b*) : soit t_q un élément maximal de la suite croissante (t_n). Pour $n \geqslant q$ on a $t_n \geqslant t_q$ (croissance), donc $t_n = t_q$ (maximalité).

b) $\Longrightarrow$ *a*). Supposons qu'on ait une partie non vide S de T sans élément maximal. Alors, pour $x \in \mathrm{S}$, l'ensemble des éléments de S strictement supérieurs à S est non vide. Par l'axiome de choix, il existe une application $f\colon \mathrm{S} \to \mathrm{S}$ telle que $f(x) > x$ pour tout $x \in \mathrm{S}$. Comme

S est non vide, on choisit $t_0 \in S$, et on définit par récurrence la suite $(t_n)_{n \geqslant 0}$ au moyen de $t_{n+1} = f(t_n)$. Cette suite est strictement croissante, donc n'est pas stationnaire. Ainsi l'implication $b) \Longrightarrow a)$ est démontrée par l'absurde. CQFD.

Corollaire du théorème 1. *Dans un anneau principal* A, *toute famille non vide d'idéaux de* A *admet un élément maximal.*

En effet, si l'on considère A comme un module sur lui-même, ses sous-modules ne sont autres que ses idéaux. Comme ceux-ci sont principaux, ce sont des A-modules à un générateur, donc de type fini. On applique alors l'implication $c) \Longrightarrow a)$ du th. 1.

1.5. Modules sur les anneaux principaux

Soient A un anneau intègre et K son corps des fractions. Un A-module libre, donc isomorphe à un $A^{(I)}$, peut se plonger dans un espace vectoriel sur $K(K^{(I)}$ dans le cas de $A^{(I)})$. Il en est donc de même de tout sous-module M d'un A-module libre. La dimension du sous-espace engendré par M est appelée le *rang* de M; c'est le nombre maximum d'éléments linéairement indépendants de M. Si M est lui-même libre et admet une base ayant n éléments, alors le rang de M est égal à n.

Théorème 1. *Soient* A *un anneau principal,* M *un* A-*module libre de rang fini* n, *et* M′ *un sous-module de* M. *Alors:*

a) M′ *est libre, de rang* $\leqslant n$;

b) Il existe une base $(e_1, \ldots, e_n)$ *de* M, *un entier* $q \leqslant n$, *et des éléments non nuls* $a_1, \ldots, a_q$ *de* A *tels que* $(a_1e_1, \ldots, a_qe_q)$ *soit une base de* M′, *et que* a_i *divise* a_{i+1} *pour* $1 \leqslant i \leqslant q-1$.

Le théorème étant trivial pour $M' = \{0\}$, on peut supposer $M' \neq \{0\}$. Soit $L(M, A)$ l'ensemble des formes linéaires sur M. Pour $u \in L(M, A)$, $u(M')$ est un sous-A-module de A, donc un idéal de A; nous écrirons $u(M') = Aa_u$ avec $a_u \in A$, car cet idéal est principal. Soit $u \in L(M, A)$ tel que Aa_u soit *maximal* parmi les $Aa_v (v \in L(M, A))$ (§ 4, cor. du th. 1). Prenons une base $(x_1, \ldots, x_n)$ de M, qui identifie M à A^n; soit $pr_i : M \to A$ la forme coordonnée d'indice i, définie par $pr_i(x_j) = \delta_{ij}$. Comme $M' \neq \{0\}$, l'un des $pr_i(M')$ est $\neq \{0\}$; on a donc $a_u \neq 0$. Par construction il existe $e' \in M'$ tel que $u(e') = a_u$. Montrons que, *pour tout* $v \in L(M, A)$, a_u *divisé* $v(e')$. En effet, si d est le p.g.c.d. de a_u et de $v(e')$, on a $d = ba_u + cv(e')$ avec $b, c \in A$, d'où $d = (bu + cv)(e')$; or $bu + cv$ est une forme linéaire w sur M; on a ainsi $Aa_u \subset Ad \subset w(M')$. Le caractère maximal de Aa_u montre qu'on a $Ad = Aa_u$, de sorte que a_u divise bien $v(e')$.

En particulier a_u divise les $pr_i(e')$, soit $pr_i(e') = a_u b_i$ avec $b_i \in A$.

Posons $c = \sum_{i=1}^{n} b_i x_i$; on a $e' = a_u e$. Comme $u(e') = a_u = a_u . u(e)$, on en déduit $u(e) = 1$ (noter que $a_u \neq 0$). *Montrons qu'on a*

1. $M = Ae + \mathrm{Ker}\,(u)$
2. $M' = Ae' + (M' \cap \mathrm{Ker}\,(u))$ (où $e' = a_u e$)

les sommes étant directes. En effet tout $x \in M$ s'écrit $x = u(x)e + (x - u(x)e)$, et on a $u(x - u(x)e) = u(x) - u(x)u(e) = 0$, ce qui démontre (1). Pour $y \in M'$ on a $u(y) = ba_u$ avec $b \in A$, et donc

$$y = ba_u e + (y - u(y)e) = be' + (y - u(y)e);$$

on a encore $y - u(y)e \in \mathrm{Ker}\,(u)$ et aussi $y - u(y)e = y - be' \in M'$; ceci démontre (2). Enfin, pour montrer que les sommes sont directes, il suffit de voir que $Ae \cap \mathrm{Ker}\,(u) = \{0\}$; or, si $x = ce$ est un élément de $Ae (c \in A)$ et si $u(x) = 0$, on a $c = cu(e) = u(ce) = u(x) = 0$, d'où $x = 0$.

Ces préliminaires étant établis, nous allons démontrer *a*) par récurrence sur le rang q de M'. Si $q = 0$, on a $M' = \{0\}$ et c'est trivial. Si $q > 0$ $M' \cap \mathrm{Ker}\,(u)$ est de rang $q - 1$ d'après (2), et est donc libre d'après l'hypothèse de récurrence. Comme, dans (2), la somme est directe, on obtient une base de M' en adjoignant e' à une base de $M' \cap \mathrm{Ker}\,(u)$. Ainsi M' est libre, et *a*) est vraie.

Ceci étant, on va démontrer *b*) par récurrence sur le rang n de M. C'est trivial pour $n = 0$. Par *a*), $\mathrm{Ker}\,(u)$ est libre, et est de rang $n - 1$ car, dans (1), la somme est directe. Appliquons l'hypothèse de récurrence au module libre $\mathrm{Ker}\,(u)$ et à son sous-module $M' \cap \mathrm{Ker}\,(u)$: il existe $q \leqslant n$, une base $(e_2, \ldots, e_n)$ de $\mathrm{Ker}\,(u)$ et des éléments non nuls $a_2, \ldots, a_q$ de A tels que $(a_2 e_2, \ldots, a_q e_q)$ soit une base de $M' \cap \mathrm{Ker}\,(u)$, et que a_i divise a_{i+1} pour $2 \leqslant i \leqslant q - 1$. Avec les notations ci-dessus, on pose $a_1 = a_u$ et $e_1 = e$; alors $(e_1, e_2, \ldots, e_n)$ est une base de M d'après (1), et $(a_1 e_1, \ldots, a_q e_q)$ est une base de M' (d'après (2) et le fait que $e' = a_1 e_1$). Reste à montrer l'assertion de divisibilité $a_1 | a_2$. Or soit v la forme linéaire sur M définie par $v(e_1) = v(e_2) = 1$, $v(e_i) = 0$ pour $i \geqslant 3$; on a $a_1 = a_u = v(a_u e_1) = v(e') \in v(M')$, d'où $Aa_u \subset v(M')$; d'après le caractère maximal de Aa_u on en déduit $v(M') = Aa_u = Aa_1$; comme $a_2 = v(a_2 e_2) \in v(M')$, on a $a_2 \in Aa_1$, c'est-à-dire $a_1 | a_2$. CQFD.

Les idéaux Aa_i du th. 1 s'appellent les *facteurs invariants* de M' dans M. On peut démontrer qu'ils sont uniquement déterminés par la donnée de M et M' ([1], chap. VII, § 3).

COROLLAIRE 1. *Soient* A *un anneau principal, et* E *un* A-*module de type fini. Alors* E *est isomorphe à un produit* $(A/\mathfrak{a}_1) \times (A/\mathfrak{a}_2) \times \cdots \times (A/\mathfrak{a}_n)$, *où les* $\mathfrak{a}_i$ *sont des idéaux de* A *tels que* $\mathfrak{a}_1 \supset \mathfrak{a}_2 \supset \cdots \supset \mathfrak{a}_n$.

Soit, en effet, $(x_1, \ldots, x_n)$ un système générateur de E. D'après le début du § 4, on a un homomorphisme surjectif $\varphi : A^n \to E$, de sorte que E est isomorphe à $A^n/\mathrm{Ker}(\varphi)$. Par le th. 1, on a une base $(e_1, \ldots, e_n)$ de A^n un entier $q \leqslant n$, et des éléments non nuls $a_1, \ldots, a_q$ de A tels que $(a_1e_1, \ldots, a_qe_q)$ soit une base de $\mathrm{Ker}(\varphi)$ et que a_i divise a_{i+1} pour $1 \leqslant i \leqslant q-1$. On pose $a_p = 0$ pour $q+1 \leqslant p \leqslant n$. Alors $A^n/\mathrm{Ker}(\varphi)$ est isomorphe au produit des Ae_i/Aa_ie_i $(1 \leqslant i \leqslant n)$, et Ae_i/Aa_ie_i est isomorphe à A/Aa_i. En posant $\mathfrak{a}_i = Aa_i$, notre assertion s'ensuit. CQFD.

Nous dirons qu'un module E sur un anneau intègre A est *sans torsion* si la relation $ax = 0$ $(a \in A,\ x \in E)$ implique $a = 0$ ou $x = 0$.

Corollaire 2. *Sur un anneau principal* A, *tout module* E *sans torsion de type fini est libre.*

On applique le cor. 1 : $E \sim (A/\mathfrak{a}_1) \times \cdots \times (A/\mathfrak{a}_n)$. En supprimant les facteurs nuls, on peut supposer que $\mathfrak{a}_i \neq A$ pout tout i. Si $\mathfrak{a}_1 \neq (0)$, si a est un élément non nul de $\mathfrak{a}_1$, si x_1 est un élément non nul de $A/\mathfrak{a}_1$, et si $x = (x_1, 0, \ldots, 0)$, on a $ax = 0$ contrairement au fait que E est sans torsion. Donc $\mathfrak{a}_1 = (0)$, $\mathfrak{a}_i = (0)$ pour tout i (car $\mathfrak{a}_i \subset \mathfrak{a}_1$), et E est isomorphe à A^n.

L'hypothèse que E est de type fini est essentielle : par exemple **Q** est un **Z**-module sans torsion non libre.

Corollaire 3. *Sur un anneau principal* A, *tout module* E *de type fini est isomorphe à un produit fini de modules* M_i, *où chaque* M_i *est égal à* A *ou à un quotient* A/Ap^s *avec* p *premier.*

On utilise le cor. 1, et on décompose chaque facteur A/Aa où $a \neq 0$ au moyen du § 3, lemme 2 : si $a = up_1^{s_1} \ldots p_r^{s_r}$ est la décomposition en facteurs premiers de A, A/Aa est isomorphe au produit des $A/Ap_i^{s_i}$.

Corollaire 4. *Soit* G *un groupe commutatif fini. Il existe* $x \in G$ *dont l'ordre est le p.p.c.m. des ordres des éléments de* G.

Un groupe commutatif est un **Z**-module (si on le note additivement). D'après le cor. 1, on a $G \simeq \mathbf{Z}/a_1\mathbf{Z} \times \cdots \times \mathbf{Z}/a_n\mathbf{Z}$ où $a_1|a_2|\ldots|a_n|$. Aucun des a_i n'est nul, sinon G serait infini. Notons y la classe de 1 dans $\mathbf{Z}/a_n\mathbf{Z}$, et posons $x = (0, \ldots, 0, y)$. L'ordre de x est évidemment a_n. Pour $z = (z_1, \ldots, z_n) \in G$, on a $a_nz = 0$ car a_i divise a_n pour tout i; donc a_n est multiple de l'ordre de z. L'élément cherché est donc x.

1.6. Racines de l'unité dans un corps

Théorème 1. *Soient* K *un corps. Tout sous-groupe fini* G *du groupe multiplicatif* K^* *est formé de racines de l'unité, et est cyclique.*

En effet, d'après le § 5, cor. 4 du th. 1, il existe $z \in G$ dont l'ordre n est tel que $y^n = 1$ pour tout $y \in G$. Comme un polynôme de degré n sur un corps (par exemple $X^n - 1$) a au plus n racines dans ce corps, le nombre d'éléments de G est au plus n. Or, comme z est d'ordre n, G contient les n éléments $z, z^2, \ldots, z^n = 1$, qui sont distincts. Donc G est formé par ces éléments, et est cyclique. CQFD.

Si un corps K contient n racines n-ièmes de l'unité, celles-ci forment donc un groupe cyclique d'ordre n (isomorphe à $\mathbf{Z}/n\mathbf{Z}$). Un générateur de ce groupe s'appelle une *racine primitive n-ième de l'unité*; toute racine n-ième de l'unité est alors une puissance d'une telle racine primitive. D'après le § 3, prop. 1, le nombre de ces racines primitives est $\varphi(n)$.

1.7. Corps finis

Soit K un corps. On a un unique homomorphisme d'anneaux $\varphi : \mathbf{Z} \to K$ (défini par $\varphi(n) = 1 + 1 + \cdots + 1$, n fois, pour $n \geqslant 0$ et par $\varphi(-n) = -\varphi(n)$).

— Si φ est injectif, il identifie $\mathbf{Z}$ à un sous-anneau de K; alors K contient aussi le corps des fractions $\mathbf{Q}$ de $\mathbf{Z}$; on dit que K est *de caractéristique* 0.

— Si φ n'est pas injectif, son noyau est un idéal $p\mathbf{Z}$ où $p > 0$; alors $\mathbf{Z}/p\mathbf{Z}$ s'identifie à un sous-anneau de K; il est donc intègre, de sorte que p est un *nombre premier*; on dit que K est *de caractéristique p*. Dans ce cas $\mathbf{Z}/p\mathbf{Z}$ est un corps, qu'on note $\mathbf{F}_p$.

Le sous-corps, $\mathbf{Q}$ ou $\mathbf{F}_p$, de K est le plus petit sous-corps de K; on l'appelle le *sous-corps premier* de K.

Pour tout nombre premier p il existe des corps de caractéristique p, par exemple $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$.

Proposition 1. *Si K est un corps de caractéristique $p \neq 0$, on a $px = 0$ pour tout $x \in K$, et $(x+y)^p = x^p + y^p$ quels que soient $x, y \in K$.*

Pour $x \in K$, on a $p.x = (p.1).x = 0.x = 0$. D'autre part, d'après la formule du binôme, on a $(x+y)^p = x^p + y^p + \sum_{j=1}^{p-1} \binom{p}{j} x^j y^{p-j}$; or le coefficient binomial $\binom{p}{j}$ est un entier qui vaut $\dfrac{p!}{j!\,(p-j)!}$; comme le nombre premier p figure dans son numérateur et ne figure pas dans son dénominateur, $\binom{p}{j}$ est multiple de p pour $1 \leqslant j \leqslant p-1$; le terme correspondant est donc nul.

Par récurrence sur n, on a $(x+y)^{p^n} = x^{p^n} + y^{p^n}$ pour tout $n \geqslant 0$.

Théorème 1. *Soit K un corps fini. Posons $q =$* card (K). *Alors :*

a) *La caractéristique de K est un nombre premier p, K est un espace vectoriel de dimension finie s sur $\mathbf{F}_p$, et on a $q = p^s$.*

b) *Le groupe multiplicatif* K^* *est cyclique d'ordre* $q-1$.

c) *On a* $x^{q-1}=1$ *pour tout* $x\in K^*$, *et* $x^q=x$ *pour tout* $x\in K$.

En effet, comme $\mathbf{Z}$ est infini, K ne peut être de caractéristique 0. Donc il contient $\mathbf{F}_p$, avec p premier. Ainsi K est un espace vectoriel sur $\mathbf{F}_p$; sa dimension s est finie, sinon K serait infini. En tant qu'espace vectoriel, K est isomorphe à $(\mathbf{F}_p)^s$, donc a p^s éléments. L'assertion *b*) résulte du § 6, th. 1. On en déduit aussitôt *c*).

Exemple. Appliquons *b*) à $\mathbf{F}_p$, où p est premier : il existe un entier $x\in\mathbf{Z}$ tel que $0\leqslant x\leqslant p-1$ et que tout entier y non multiple de p soit congru modulo p à une puissance de x. On dit alors que x est *une racine primitive modulo* p. La recherche des racines primitives modulo p n'est nullement triviale. Par exemple il y a $\varphi(6)=2$ racines primitives modulo 7; ce sont 3 et 5 (en effet on a $1^2\equiv 6^2\equiv 1$ (mod. 7) et $2^3\equiv 4^3\equiv 1$ (mod. 7); seuls restent 3 et 5).

Remarque. Il résulte de *c*) qu'un corps fini K à q éléments est l'ensemble des racines du polynôme X^q-X (qui n'a que q racines). On peut en déduire que deux corps finis à q éléments sont isomorphes. On note souvent $\mathbf{F}_q$ un corps fini à q éléments.

A titre d'exercice et d'intermède, nous allons démontrer un élégant théorème relatif aux équations diophantiennes sur un corps fini :

THÉORÈME 2 (Chevalley). *Soient* K *un corps fini, et* $F(X_1,\dots,X_n)$ *un polynôme homogène de degré* d *sur* K. *On suppose* $d<n$. *Il existe alors un point* $(x_1,\dots,x_n)\in K^n$ *distinct de l'origine* $(0,\dots,0)$ *tel que* $F(x_1,\dots,x_n)=0$.

Étant donnés un corps K et un entier j, on dit que K est un *corps* C_j si tout polynôme homogène sur K de degré d et à n variables, *tel que* $n>d^j$, admet un zéro non trivial (i.e. distinct de l'origine) dans K^n. Les corps C_0 sont les corps algébriquement clos. Le théorème de Chevalley exprime que les corps finis sont C_1 (on dit aussi « quasi-algébriquement clos »). On montre que, si K est un corps C_j, le corps K(T) des fractions rationnelles à une variable sur K et le corps K((T)) des séries formelles à une variable sur K sont des corps C_{j+1} ([5]). On s'est longtemps demandé si les corps p-adiques sont C_2, et on a récemment montré qu'il n'en est rien ([8]).

Démontrons le th. 2. Notons q le cardinal de K et p sa caractéristique (de sorte que $q=p^s$). Soit $V\subset K^n$ l'ensemble des zéros de F, i.e. des points $(x_1,\dots,x_n)\in K^n$ tels que $F(x)=0$ (nous employons, ici et dans la suite, l'écriture vectorielle où x désigne un point $(x_1,\dots,x_n)$ de K^n). D'après le th. 1, *c*), on a $F(x)^{q-1}=0$ pour $x\in V$, et $F(x)^{q-1}=1$ pour $x\in K^n-V$; ainsi le polynôme $G(x)=F(x)^{q-1}$ est une *fonction caractéristique de* K^n-V, à valeurs dans $\mathbf{F}_p$. Le nombre modulo p de points de K^n-V sera donc donné par la somme $\sum_{x\in K^n} G(x)$; nous allons calculer cette somme et montrer qu'elle est *nulle*. Alors card (K^n-V) sera multiple de p; comme card $(K^n)=q^n=p^{ns}$ est aussi multiple de p, card (V) sera multiple de p; comme V contient déjà l'origine, il contiendra nécessairement d'autres points, car $p \geqslant 2$; le th. 2 sera ainsi démontré.

Calculons donc $\sum_{x \in K^n} G(x)$. Le polynôme G est combinaison linéaire de monômes $M_\alpha(X) = X_1^{\alpha_1} \ldots X_n^{\alpha_n}$; et on est ramenés à calculer $\sum_{x \in K^n} M_\alpha(x) = \sum_{x \in K^n} x_1^{\alpha_1} \ldots x_n^{\alpha_n} = \left(\sum_{x_1 \in K} x_1^{\alpha_1} \right) \ldots \left(\sum_{x_n \in K} x_n^{\alpha_n} \right)$. Il s'agit donc de calculer des sommes de la forme $\sum_{z \in K} z^\beta (\beta \in \mathbf{N})$.

(a) Pour $\beta = 0$, on a $z^\beta = 1$ pour tout $z \in K$, et la somme vaut $q = 0$;

(b) Pour $\beta > 0$, le terme 0^β est nul, et la somme se réduit à $\sum_{z \in K^*} z^\beta$. Or K^* est un groupe cyclique d'ordre $q - 1$ (th. 1, b); soit ω un générateur de celui-ci. Alors $\sum_{z \in K^*} z^\beta = \sum_{j=0}^{q-2} \omega^{\beta j}$, qui est la somme d'une progression géométrique. Donc:

(b') Si la raison ω^β est $\neq 1$, c'est-à-dire si β n'est pas multiple de $q - 1$, on a $\sum_{j=0}^{q-2} \omega^{\beta j} = \dfrac{\omega^{\beta(q-1)} - 1}{\omega^\beta - 1} = 0$ (car $\omega^{q-1} = 1$).

(b'') Si $\omega^\beta = 1$, c'est-à-dire si β est multiple de $q - 1$, on a

$$\sum_{j=0}^{q-2} \omega^{\beta j} = q - 1.$$

Il résulte de (a), (b') et (b'') que $\sum_{x \in K^n} x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ est nul *sauf si* tous les α_i sont > 0 et multiples de $q - 1$. Le degré $\alpha_1 + \cdots + \alpha_n$ du monôme est, dans ce cas, $\geqslant (q-1)n$. Mais, comme $G = F^{q-1}$, G est de degré $(q-1)d$, et on a $(q-1)d < (q-1)n$ d'après l'hypothèse. On a donc $\sum_{x \in K^n} M_\alpha(x) = 0$ pour tout monôme $M_\alpha(X)$ qui figure dans G avec coefficient non nul. D'où, par addition, $\sum_{x \in K^n} G(x) = 0$. Nous avons vu que cette relation entraîne notre conclusion.

On remarquera qu'il aurait, au lieu de supposer F homogène, suffi de supposer F sans terme constant. Naturellement l'inégalité *stricte* $d < n$ entre degré et nombre de variables est essentielle. Par exemple la *norme* de $\mathbf{F}_{q^n}$ à $\mathbf{F}_q$ (cf. chap. II, § 6) fournit un polynôme homogène de degré n et à n variables sur $\mathbf{F}_q$ qui n'a d'autre zéro que l'origine.

Un exemple. Une forme quadratique à 3 variables sur un corps *fini* K « représente 0 » (i.e. a un zéro non trivial). En passant de K^3 au plan projectif $P_2(K)$, ceci veut dire qu'une *conique* sur K admet un point rationnel sur K (i.e. dont les coordonnées homogènes peuvent être choisies dans K). L'exemple de la conique $x^2 + y^2 + z^2 = 0$ sur $\mathbf{R}$ (resp. $x^2 + y^2 - 3z^2 = 0$ sur $\mathbf{Q}$; pour s'assurer que $x^2 + y^2 - 3z^2 = 0$ n'a pas de solution non triviale dans $\mathbf{Q}$, on se ramène au cas où x, y, z sont des entiers premiers entre eux, et on réduit modulo 4) montre qu'il ne s'agit pas d'une propriété vraie sur tout corps.

CHAPITRE II

Éléments entiers sur un anneau
Éléments algébriques sur un corps

Parmi les nombres complexes, on va s'occuper dans ce livre des nombres *algébriques*, c'est-à-dire ceux qui satisfont à une équation de la forme

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$$

où les a_i sont des nombres rationnels. Lorsque les a_i sont des nombres entiers ($a_i \in \mathbf{Z}$) le nombre algébrique x est appelé un *entier algébrique*; ainsi $\sqrt{2}$, $\sqrt{3}$, i, $e^{2i\pi/5}$ sont des entiers algébriques. Il n'est pas évident à priori que des sommes ou des produits de nombres algébriques (resp. d'entiers algébriques) sont encore des nombres algébriques (resp. des entiers algébriques). Regardons l'exemple de $x = \sqrt{2} + \sqrt{3}$; on calcule $x^2 = 2 + 3 + 2\sqrt{6}$; on isole la racine carrée et il vient $x^2 - 5 = 2\sqrt{6}$; encore une élévation au carré, $(x^2 - 5)^2 = 24$, ce qui montre que x est un entier algébrique. Le lecteur pourra s'exercer sur $\sqrt[3]{5} + \sqrt[5]{7}$, et sera convaincu que la série d'astuces qui mène au résultat n'est pas facilement généralisable.

Pour surmonter cette difficulté, les algébristes du siècle dernier, Dedekind en particulier, ont eu l'idée de « linéariser » le problème, c'est-à-dire d'y introduire des modules. C'est ce que nous allons faire. Le remplacement de $\mathbf{Z}$ (ou $\mathbf{Q}$) par un anneau commutatif quelconque ne coûte aucun effort supplémentaire, et sera fort utile pour la suite. Nous commencerons par le cas général des éléments entiers sur un anneau, et particulariserons ensuite aux éléments algébriques sur un corps.

2.1. Éléments entiers sur un anneau

THÉORÈME 1. *Soient* R *un anneau,* A *un sous-anneau de* R, *et* x *un élément de* R. *Les propriétés suivantes sont équivalentes:*

a) *Il existe* $a_0, \ldots, a_{n-1} \in \mathrm{A}$ *tels que*

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0 \tag{1}$$

(*autrement dit* x *est racine d'un polynôme unitaire sur* A)

b) *L'anneau* $A[x]$ *est un* A-*module de type fini.*

c) *Il existe un sous-anneau* B *de* R, *contenant* A *et* x, *et qui est un* A-*module de type fini.*

Montrons que *a*) implique *b*). Notons M le sous-A-module de R engendré par $1, x, \ldots, x^{n-1}$. Par *a*) on a $x^n \in M$. Par récurrence sur j montrons que $x^{n+j} \in M$; en effet, par multiplication par x^j, (1) donne $x^{n+j} = - a_{n-1}x^{n+j-1} - \cdots - a_0x^j$. Comme $A[x]$ est le A-module engendré par les $x^k (k \geqslant 0)$, on a $A[x] = M$, ce qui démontre *b*).

L'implication *b*) $\Longrightarrow$ *c*) est triviale. Montrons que *c*) implique *a*). Soit $(y_1, \ldots, y_n)$ un système générateur fini du A-module B; on a ainsi $B = Ay_1 + \cdots + Ay_n$. Comme $x \in B$, $y_i \in B$ et que B est un sous-anneau de R, on a $xy_i \in B$, de sorte qu'il existe des éléments a_{ij} de A tels que $xy_i = \sum_{j=1}^{n} a_{ij}y_j$. Ceci s'écrit aussi

$$\sum_{j=1}^{n} (\delta_{ij}x - a_{ij})y_j = 0 \quad (i = 1_1, \ldots, n)$$

On obtient ainsi un système de n équations linéaires homogènes en $(y_1, \ldots, y_n)$ Si on note d le déterminant $\det(\delta_{ij}x - a_{ij})$, le calcul menant aux formules de Cramer montre qu'on a $dy_i = 0$ pour tout i. Comme $B = \sum_i Ay_i$, on en déduit $dB = 0$, d'où $d = d.1 = 0$ car B a un élément unité. Or, si on développe le déterminant

$$d = \det(\delta_{ij}x - a_{ij}),$$

on obtient une équation de la forme $P(x) = 0$ où P est un polynôme de degré n sur A; ce polynôme est unitaire car le terme en x^n provient uniquement du produit $\prod_{i=1}^{n}(x - a_{ii})$ des éléments de la diagonale principale; ainsi *a*) est vraie.

Définition 1. *Soient* R *un anneau et* A *un sous-anneau de* R. *Un élément* x *de* R *est dit entier sur* A *s'il satisfait aux conditions équivalentes* a), b), c) *du th.* 1. *Soit* $P \in A[X]$ *un polynôme unitaire tel que* $P(x) = 0$ (polynôme dont l'existence est affirmée par *a*)); *la relation* $P(x) = 0$ *est appelée une équation de dépendance intégrale de* x *sur* A.

Exemple. L'élément $x = \sqrt{2}$ de $\mathbf{R}$ est entier sur $\mathbf{Z}$; une équation de dépendance intégrale est donnée par $x^2 - 2 = 0$.

Proposition 1. *Soient* R *un anneau,* A *un sous-anneau de* R, *et* $(x_i)_{1 \leqslant i \leqslant n}$ *une famille finie d'éléments de* R. *Si, pour tout* i, x_i *est entier sur* $A[x_1, \ldots, x_{i-1}]$ (*en particulier si tous les* x_i *sont entiers sur* A), *alors* $A[x_1, \ldots, x_n]$ *est un* A-*module de type fini.*

Raisonnons par récurrence sur n. Pour $n = 1$ c'est l'assertion b) du th. 1. Supposons la proposition vraie jusqu'à $n - 1$. Alors $B = A[x_1, \ldots, x_{n-1}]$ est un A-module de type fini, soit $B = \sum_{j=1}^{p} Ab_j$. Par application du cas $n = 1$, $A[x_1, \ldots, x_n] = B[x_n]$ est un B-module de type fini, soit $\sum_{k=1}^{q} Bc_k$. On a alors

$$A[x_1, \ldots, x_n] = \sum_{k=1}^{q} Bc_k = \sum_{k=1}^{q} \left(\sum_{j=1}^{p} Ab_j \right) c_j = \sum_{j,k} Ab_j c_k.$$

Ainsi $(b_j c_k)$ est un système générateur fini du A-module $A[x_1, \ldots, x_n]$.

Corollaire 1. *Soient* R *un anneau,* A *un sous-anneau de* R, x *et* y *des éléments de* R *entiers sur* A. *Alors* $x + y$, $x - y$ *et* xy *sont entiers sur* A.

En effet on a $x + y, x - y, xy \in A[x, y]$. D'après la prop. 1, $A[x, y]$ est, un A-module de type fini. Donc, d'après le c) du th. 1, $x + y$, $x - y$ et xy sont entiers sur A.

Corollaire 2. *Soient* R *un anneau et* A *un sous-anneau de* R. *L'ensemble* A′ *des éléments de* R *qui sont entiers sur* A *est un sous-anneau de* R, *qui contient* A.

En effet, A′ est un sous-anneau de R d'après le cor. 1; il contient A car tout $a \in A$ est racine du polynôme unitaire $X - a$, donc est entier sur A.

Définition 2. *Soient* R *un anneau,* A *un sous-anneau de* R; *l'anneau* A′ *des éléments de* R *entiers sur* A *s'appelle la fermeture intégrale de* A *dans* R. *Soient* A *un anneau intègre et* K *son corps des fractions; la fermeture intégrale de* A *dans* K *s'appelle la clôture intégrale de* A. *Soient* B *un anneau et* A *un sous-anneau de* B; *on dit que* B *est entier sur* A *si tout élément de* B *est entier sur* A (*autrement dit, si la fermeture intégrale de* A *dans* B *est* B *lui-même*).

Proposition 2 (de transitivité). *Soient* C *un anneau,* B *un sous-anneau de* C *et* A *un sous-anneau de* B. *Si* B *est entier sur* A *et si* C *est entier sur* B, *alors* C *est entier sur* A.

En effet, soit $x \in C$. Il est entier sur B, et on a donc une équation de dépendance intégrale $x^n + b_{n-1}x^{n-1} + \cdots + b_0 = 0$ avec $b_i \in B$. Posons $B' = A[b_0, \ldots, b_{n-1}]$; alors x est aussi entier sur B′. Comme B est entier sur A, les b_i sont entiers sur A; donc, d'après la prop. 1 $B'[x] = A[b_0, \ldots, b_{n-1}, x]$ est un A-module de type fini. Par le c) du th. 1, on en conclut que x est entier sur A. Donc C est entier sur A.

Proposition 3. *Soient* B *un anneau intègre et* A *un sous-anneau de* B, *tel que* B *soit entier sur* A. *Pour que* B *soit un corps, il faut et il suffit que* A *soit un corps.*

Supposons que A soit un corps, et soit $b \in B$, $b \neq 0$. Alors $A[b]$ est un espace vectoriel de dimension *finie* sur A (th. 1, *b*)). D'autre part $y \mapsto by$ est une application A-linéaire de $A[b]$ dans lui-même, qui est injective car $A[b]$ est intègre et car $b \neq 0$. Elle est donc surjective, et il existe $b' \in A[b]$ tel que $bb' = 1$. Donc b est inversible dans B et B est un corps [1].

Inversement, supposons que B soit un corps, et soit $a \in A$, $a \neq 0$. Alors a admet un inverse $a^{-1} \in B$, qui satisfait à une équation de dépendance intégrale

$$a^{-n} + a_{n-1}a^{-n+1} + \cdots + a_1a^{-1} + a_0 = 0 \qquad (a_i \in A)$$

En multipliant par a^{n-1}, on obtient $a^{-1} = -(a_{n-1} + \cdots + a_1a^{n-2} + a_0a^{n-1})$, d'où $a^{-1} \in A$, de sorte que A est un corps.

2.2. Anneaux intégralement clos

DÉFINITION. *On dit qu'un anneau* A *est intégralement clos s'il est intègre et si sa clôture intégrale est* A *lui-même.*

Autrement dit, tout élément x du corps des fractions K de A, qui est entier sur A, est élément de A.

Exemple 1. Soient A un anneau intègre et K son corps des fractions. Alors la *clôture intégrale* A′ de A (c.-à.-d. la fermeture intégrale de A dans K) est un anneau intégralemnent clos. En effet la clôture intégrale de A′ est entière sur A′, donc sur A (§ 1, prop. 2); elle est donc égale à A′.

Exemple 2. *Tout anneau principal est intégralement clos.*

En effet un anneau principal A est intègre par définition. Soit x un élément entier sur A de son corps des fractions; on a une équation de dépendance intégrale.

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0 \qquad (a_i \in A) \tag{1}$$

Or on peut écrire $x = a/b$, avec $a, b \in A$ *premiers entre eux*. D'où, en reportant dans (1) et en multipliant par b^n

$$a^n + b(a_{n-1}a^{n-1} + \cdots + a_1ab^{n-2} + a_0b^{n-1}) = 0$$

Ainsi b divise a^n; comme il est premier avec a, l'application répétée du lemme d'Euclide montre qu'il divise a; donc $x = a/b \in A$, et A est intégralement clos.

On notera qu'on a seulement utilisé les propriétés multiplicatives des anneaux principaux (éléments premiers entre eux, lemme d'Euclide). Le raisonnement montre ainsi que tout anneau *factoriel* est intégralement clos.

1. Le même type de raisonnement, utilisant l'homothétie $y \mapsto by$, montre que tout anneau intègre *fini* est un corps.

2.3. Éléments algébriques sur un corps. Extensions algébriques

DÉFINITION. *Soient* R *un anneau, et* K *un sous-corps de* R. *On dit qu'un élément* x *de* R *est algébrique sur* K *s'il existe des éléments non tous nuls* $a_0, \ldots, a_n$ *de* K *tels que* $a_n x^n + \cdots + a_1 x + a_0 = 0$.

Il revient au même de dire que les *monômes* $(x^j)_{j \in \mathbf{N}}$ sont linéairement dépendants sur K. Un élément non algébrique sur K est dit *transcendant* sur K; ceci veut dire que les monômes $(x^j)_{j\in\mathbf{N}}$ sont linéairement indépendants sur K.

Dans la relation de la déf. 1, on peut supposer a_n non nul; il admet alors un inverse a_n^{-1} car K est un corps; en multipliant par a_n^{-1} on obtient une équation de dépendance intégrale. Donc :

1. *Sur un corps, algébrique = entier.*

On peut donc appliquer la théorie des éléments entiers; par exemple, pour $K \subset R$ et $x \in R$, le th. 1, *b*) du § 1 donne :

2. *x algébrique sur* $K \Longleftrightarrow [K[x] : K]$ *finie.*

On dit qu'un anneau R contenant un corps K est *algébrique* sur K si tout élément de R est algébrique sur K; si R lui-même est un corps, on dit alors que R est une *extension algébrique* de K.

Étant donnés un corps L et un sous-corps K de L, la dimension $[L : K]$ s'appelle aussi le *degré* de L sur K. Le th. 1, *c*) du § 1 donne alors :

3. *Si le degré de* L *sur* K *est fini,* L *est extension algébrique de* K.

On appelle *corps de nombres algébriques* (ou *corps de nombres*) toute extension de degré fini de $\mathbf{Q}$.

PROPOSITION 1. *Soient* K *un corps,* L *une extension algébrique de* K *et* M *une extension algébrique de* L. *Alors* M *est extension algébrique de* L. *De plus* $[M : K] = [M : L]\,[L : K]$ (« multiplicativité des degrés »).

La première assertion est un cas particulier de la prop. 2 du § 1. De plus, si $(x_i)_{i\in\mathbf{N}}$ est une base de L sur K et $(y_j)_{j\in J}$ une base de M sur L, alors $(x_i y_j)_{(i,j)\in I\times J}$ est une *base* de M sur K: en effet, c'est un système générateur, comme dans la prop. 1 du § 1; d'autre part une relation $\sum_{i,j} a_{ij} x_i y_j = 0$ avec $a_{ij} \in K$, donne $\sum_j \left(\sum_i a_{ij} x_i \right) y_j = 0$, d'où $\sum_i a_{ij} x_i = 0$ pour tout j (car $\Sigma a_{ij} x_i \in L$), et par conséquent $a_{ij} = 0$ pour tous i, j. Ceci démontre la formule de multiplicativité des degrés.

PROPOSITION 2. *Soient* R *un anneau, et* K *un sous-corps de* R. *Alors*

a) *L'ensemble* K′ *des éléments de* R *algébriques sur* K *est un sous-anneau de* R *contenant* K;

b) *Si* R *est intègre,* K′ *est un sous-corps de* R.

En effet *a*) est un cas particulier du cor. 2 de la prop. 1, § 1, et *b*) résulte de la prop. 3 du § 1.

Nous allons maintenant étudier de plus près les éléments algébriques sur un corps. Soient R un anneau, K un sous-corps de R et x un élément de R. Il existe un homomorphisme φ et un seul de l'anneau de polynômes K[X] dans R tel que $\varphi(X) = x$, et que $\varphi(a) = a$ pour tout $a \in K$; l'image de φ est $K[x]$. La définition des éléments algébriques se traduit par :

4. x *algébrique sur* K $\Longleftrightarrow$ Ker (φ) $\neq$ (0).

Si x est algébrique sur K, l'idéal Ker (φ) est un idéal *principal* (F(X)) (car K[X] est un anneau principal), engendré par un polynôme non nul F(X), qu'on peut supposer *unitaire* car K est un corps; ce polynôme unitaire est déterminé de façon unique par K et x, et on l'appelle le *polynôme minimal* de x sur K. Traduisons sa définition :

5. *Soient* F(X) *le polynôme minimal de* x *sur* K, *et* $G(X) \in K[X]$; *pour qu'on ait* $G(x) = 0$, *il faut et il suffit que* F(X) *divise* G(X) *dans* K[X]. De plus, par passage au quotient, on obtient un *isomorphisme canonique.*

6. $K[X]/(F(X)) \xrightarrow{\sim} K[x]$

Avec les mêmes notations, supposons toujours x algébrique sur K, et soit F(X) son polynôme minimal; en appliquant (5) et la prop. 3 du § 1, on obtient les équivalences.

7. $K[x]$ *corps* $\Longleftrightarrow$ $K[x]$ *intègre* $\Longleftrightarrow$ F(X) *irréductible.*

Inversement, soient K un corps et $F(X) \in K[X]$ un polynôme irréductible; alors K[X]/(F(X)) est un corps contenant K, et, en notant x la classe de X dans ce corps, on a $F(x) = 0$. Ainsi F(X) est divisible par $X - x$ sur ce corps $K[x]$. Plus généralement :

Proposition 3. *Soient* K *un corps, et* $P(X) \in K[X]$ *un polynôme non constant. Il existe une extension algébrique* K′ *de degré fini de* K *telle que* P(X) *se décompose en facteurs du premier degré dans* K′[X].

On raisonne par récurrence sur le degré d de P(X). C'est évident pour $d = 1$. Supposons l'assertion démontrée jusqu'au degré $d - 1$. Soit F(X) un facteur irréductible de P(X). On vient de voir qu'il existe une extension K″ de degré fini de K (à savoir K[X]/(F(X)) et un élément $x \in K''$ tels que F(X) soit multiple de $X - x$ dans K″[X]. On a alors $P(X) = (X - x)P_1(X)$ avec $P_1(X) \in K''[X]$. D'après l'hypothèse de récurrence, $P_1(X)$ se décompose en facteurs du premier degré sur une extension K′ de degré fini de K″. Alors K′ est une extension de degré fini de K (prop. 1), et P(X) se décompose en facteurs du premier degré dans K′[X].

Remarque: corps algébriquement clos. On dit qu'un corps K est *algébriquement clos* si *tout* polynôme non constant $P(X) \in K[X]$ se décompose en facteurs du premier degré dans $K[X]$; il suffit pour cela, par récurrence sur le degré, que tout polynôme non constant $P(X) \in K[X]$ admette une racine $x \in K$. Par application « transfinie » de la prop. 3 (c'est-à-dire en combinant la prop. 3 et le théorème de Zorn; cf. [1], chap. V et [9], chap. II), on démontre que tout corps est un sous-corps d'un corps algébriquement clos.

On démontre en Analyse, par des méthodes variées [1], que le corps $\mathbf{C}$ des *nombres complexes* est algébriquement clos. Cela suffira à nos besoins.

2.4. Éléments conjugués, corps conjugués

Étant donnés deux corps, L, L′ contenant un corps K on appelle K-*isomorphisme* de L sur L′ tout isomorphisme $\varphi : L \to L'$ tel que $\varphi(a) = a$ pour tout $a \in K$; dans ces conditions on dit que L et L′ sont K-*isomorphes*, ou (s'ils sont algébriques sur K) sont des *corps conjugués sur* K. Étant données deux extensions L, L′ de K, on dit que deux éléments $x \in L$ et $x' \in L'$ sont *conjugués* sur K s'il existe un K-isomorphisme $\varphi: K(x) \to K(x')$ tel que $\varphi(x) = x'$; alors φ est unique. Ceci signifie que, ou bien x et x' sont tous deux transcendants sur K, ou bien x et x' sont tous deux algébriques sur K et admettent le même polynôme minimal (cf. (5), § 3).

Exemple. Soit $F(X)$ un polynôme *irréductible* de degré n sur K, et $x_1, \ldots, x_n$ ses racines dans une extension K′ de K (§ 3, prop. 3). Alors les x_i sont deux à deux conjugués sur K (§ 3, (6)), et les corps $K[x_i]$ sont aussi deux à deux conjugués sur K.

LEMME. *Soient* K *un corps de caractéristique* 0 *ou un corps fini,* $F(X) \in K[X]$ *un polynôme unitaire irréductible, et* $F(X) = \prod_{i=1}^{n} (X - x_i)$ *sa décomposition en facteurs du premier degré dans une extension* K′ *de* K (§ 3, prop. 3). *Alors les* n *racines* $x_1, \ldots, x_n$ *de* $F(X)$ *sont distinctes.*

Raisonnons par l'absurde. Dans le cas contraire, $F(X)$ admettrait une racine *multiple* x, qui serait donc aussi racine du polynôme dérivé $F'(X)$; alors $F(X)$ diviserait $F'(X)$ ((4), § 3). Comme $d^oF' < d^oF$, ceci implique que $F'(X)$ est le polynôme nul. Or si

$$F(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \qquad (a_i \in K)$$

1. Pour une démonstration utilisant les propriétés des fonctions continues sur un espace compact, voir [4]. Pour une démonstration utilisant les propriétés des fonctions homolorphes d'une variable complexe, voir [3]. Nous donnerons en appendice à ce chapitre une démonstration plus algébrique, mais n'utilisant d'autre Analyse que les propriétés les plus simples des nombres réels.

on a

$$F'(X) = nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \cdots + a_1.$$

On a donc $n.1 = 0$ et $j.a_j = 0$ pour $j = 1, \ldots, n-1$. Ceci est impossible en caractéristique 0.

En caractéristique $p \neq 0$, ceci implique que p divise n, et qu'on a $a_j = 0$ pour j non multiple de p (on rappelle que p est un nombre premier). Ainsi $F(X)$ est de la forme

$$F(X) = X^{qp} + b_{q-1}X^{(q-1)p} + \cdots + b_1X^p + b_0 \qquad (b_i \in K)$$

Si chacun des b_i est une *puissance p-ème*, soit $b_i = c_i^p$ avec $c_i \in K$, on a $F(X) = (X^q + c_{q-1}X^{q-1} + \cdots + c_0)^p$ (chap. I, § 7, prop. 1), et $F(X)$ n'est pas irréductible. Or, si K est un corps fini et si on note $p(\neq 0)$ sa caractéristique, l'application $x \mapsto x^p$ de K dans K est injective (car $x^p = y^p$ implique $x^p - y^p = 0$, $(x-y)^p = 0$ et $x - y = 0$); elle est donc surjective car K est fini. On a donc une contradiction.

Les corps K de caractéristique $p \neq 0$ tels que $x \mapsto x^p$ soit surjective (i.e. que tout élément de K soit une puissance p-ème) sont appelés les corps *parfaits*; on vient de montrer que tout corps fini est parfait; on convient qu'un corps de caractéristique 0 est parfait. Nous avons démontré que la conclusion du lemme reste vraie sous la seule hypothèse que K est un corps parfait. Le corps $\mathbf{F}_p(T)$ des fractions rationnelles à une variable sur $\mathbf{F}_p$ n'est pas parfait, car la variable T n'est pas une puissance p-ème dans $\mathbf{F}_p(T)$.

THÉORÈME 1. *Soient* K *un corps de caractéristique* 0 *ou fini,* K' *une extension de degré fini* n *de* K, *et* C *un corps algébriquement clos contenant* K. *Alors il existe* n K-*isomorphismes distincts de* K' *dans* C.

Notre assertion est vraie pour une extension *monogène* K', c'est-à-dire de la forme $K' = K[x]$ $(x \in K')$. En effet le polynôme minimal $F(X)$ de x sur K est alors de degré n. Il admet n racines $x_1, \ldots, x_n$ dans C, qui sont distinctes d'après le lemme. Pour $i = 1, \ldots, n$, on a donc un K-isomorphisme $\sigma_i : K' \to C$ tel que $\sigma_i(x) = x_i$.

Nous procéderons alors par récurrence sur le degré n de K'. Soit $x \in K'$; considérons les corps $K \subset K[x] \subset K'$ et posons $q = [K[x] : K]$; on peut supposer $q > 1$. D'après le cas monogène, on a q K-isomorphismes distincts $\sigma_1, \ldots, \sigma_q$ de $K[x]$ dans C. Comme $K[\sigma_i(x)]$ et $K[x]$ sont isomorphes, on peut construire une extension K_i' de $K[\sigma_i(x)]$ et un isomorphisme $\tau_i : K' \to K_i'$ qui prolonge σ_i. Or $K[\sigma_i(x)]$ est un corps de caractéristique 0 ou fini. Comme

$$[K_i' : K[\sigma_i(x)]] = [K' : K[x]] = \frac{n}{q} < n,$$

l'hypothèse de récurrence montre qu'on a $\frac{n}{q}$ $K[\sigma_i(x)]$-isomorphismes distincts θ_{ij} de K'_i dans C. Alors les n composés $\theta_{ij} \circ \tau_i$ fournissent $q \cdot \frac{n}{q} = n$ K-isomorphismes de K′ dans C. Ils sont distincts car $\theta_{ij} \circ \tau_i$ et $\theta_{i'j'} \circ \tau_{i'}$ diffèrent sur $K[x]$ si $i \neq i'$, et, si $i = i'$, θ_{ij} et $\theta_{ij'}$ diffèrent sur K'_i. CQFD.

Le th. 1 s'étend à un corps parfait K : on montre en effet que toute extension algébrique d'un corps parfait (en particulier $K[\sigma_i(x)]$) est un corps parfait; le reste de la démonstration est inchangé.

Corollaire (« théorème de l'élément primitif »). *Soient* K *un corps fini ou de caractétristique* 0, *et* K′ *une extension de* K *de degré fini* n. Il *existe alors un élément* x *de* K′ (*dit « primitif »*) *tels que* $K' = K[x]$.

Si K est fini, K′ est fini, et son groupe multiplicatif K'^* est formé des puissances d'un même élément x (chap. I, § 7, th. 1, b)). On a alors $K' = K[x]$.

Supposons maintenant K de caractéristique 0, donc infini. D'après le th. 1, on a n K-isomorphismes σ_i de K′ dans un corps algébriquement clos C contenant K. Pour $i \neq j$ l'équation $\sigma_i(y) = \sigma_j(y)$ ($y \in K'$) définit une partie V_{ij} de K′, qui est évidemment un sous K-espace vectoriel de K′, et qui est distincte de K′ car $\sigma_i \neq \sigma_j$. Comme K est infini, l'algèbre linéaire montre que la réunion des V_{ij} est distincte de K′. Prenons x en dehors de cette réunion. Les $\sigma_i(x)$ sont alors deux à deux distincts, de sorte que le polynôme minimal F(X) de x sur K a au moins n racines distinctes (les $\sigma_i(x)$) dans C; on a donc $d^\circ F \geqslant n$, c'est-à-dire $[K[x] : K] \geqslant n$. Comme $K[x] \subset K'$ et que $[K' : K] = n$, on en déduit $K' = K[x]$. CQFD.

2.5. Entiers des corps quadratiques

Nous allons interrompre un moment la théorie générale pour donner un exemple.

Définition. *On appelle corps quadratique toute extension de degré* 2 *du corps* Q *des nombres rationnels.*

Si K est un corps quadratique, tout élément x de $K - Q$ est de degré 2 sur Q, donc est élément primitif de K (i.e. $K = Q[x]$, et $(1, x)$ est une base de K sur Q). Soit $F(X) = X^2 + bX + c$ ($b, c \in Q$) le polynôme minimal d'un tel élément $x \in K$. La résolution de l'équation du second degré $x^2 + bx + c = 0$ donne $2x = -b \pm \sqrt{b^2 - 4c}$. Ainsi $K = Q(\sqrt{b^2 - 4c})$[1]. Or $b^2 - 4c$ est un nombre rationnel

1. Par $\sqrt{b^2 - 4c}$ nous entendons l'un des deux éléments de K dont le carré est $b^2 - 4c$.

$\frac{u}{v} = \frac{uv}{v^2}$ avec $u, v \in \mathbf{Z}$; on a donc aussi $K = \mathbf{Q}(\sqrt{uv})$ avec $uv \in \mathbf{Z}$. Par le même procédé on voit qu'on peut enfin écrire $K = \mathbf{Q}(\sqrt{d})$ où d est un entier *sans facteurs carrés* dans sa décomposition en facteurs premiers. On a ainsi prouvé :

PROPOSITION 1. *Tout corps quadratique est de la forme* $\mathbf{Q}(\sqrt{d})$, *où* d *est un entier sans facteurs carrés.*

L'élément $\sqrt{d}$ est une racine du polynôme irréductible $X^2 - d$. Il admet un *conjugué* dans K, à savoir $-\sqrt{d}$. Il existe donc un automophisme σ de K qui applique $\sqrt{d}$ en $-\sqrt{d}$ (§ 4). L'élément général de K est de la forme $a + b\sqrt{d}$ avec $a, b \in \mathbf{Q}$, et on a

1. $\sigma(a + b\sqrt{d}) = a - b\sqrt{d}$

Nous nous proposons d'étudier l'anneau A des *entiers* de K, c'est-à-dire l'ensemble des $x \in K$ qui sont entiers sur $\mathbf{Z}$ (§ 1, cor. 2. de la prop. 2). Si $x \in A$, $\sigma(x)$ est racine de la même équation de dépendance intégrale que x, donc $\sigma(x) \in A$. On a donc $x + \sigma(x) \in A$ et $x.\sigma(x) \in A$. Or, si $x = a + b\sqrt{d}$ avec $a, b \in \mathbf{Q}$, on a, d'après (1),

2. $x + \sigma(x) = 2a \in \mathbf{Q} \qquad x\sigma(x) = a^2 - db^2 \in \mathbf{Q}$

Comme $\mathbf{Z}$ est principal, et donc intégralement clos (§ 2, ex. 2), on a donc

3. $2a \in \mathbf{Z} \qquad a^2 - db^2 \in \mathbf{Z}$

Ces conditions (3) sont nécessaires pour que $x = a + b\sqrt{d}$ soit entier sur $\mathbf{Z}$; elles sont aussi suffisantes car alors x est racine de

$$x^2 - 2ax + a^2 - db^2 = 0$$

D'après (3) on a $(2a)^2 - d(2b)^2 \in \mathbf{Z}$; comme $2a \in \mathbf{Z}$, on a donc $d(2b)^2 \in \mathbf{Z}$. Or d est sans facteurs carrés; si $2b$ n'était pas entier, son dénominateur comporterait un facteur premier p; ce facteur apparaîtrait sous la forme p^2 dans $(2b)^2$, et la multiplication par d ne pourrait pas le ramener dans $\mathbf{Z}$; on a donc $2b \in \mathbf{Z}$.

Bref on peut poser $a = \frac{u}{2}$, $b = \frac{v}{2}$ avec $u, v \in \mathbf{Z}$; la conditions (3) devient alors :

4. $u^2 - dv^2 \in 4\mathbf{Z}$.

Si v est pair, (4) montre que u est pair aussi; on a alors $a, b \in \mathbf{Z}$. Si v est impair, on a $v^2 \equiv 1$ mod. 4; or la classe de u^2 mod. 4 est 0 ou 1 (écrire la table des carrés mod. 4); comme d est sans facteurs carrés, il n'est pas multiple de 4; ainsi on a nécessairement $u^2 \equiv 1$ mod. 4 et $d \equiv 1$ mod. 4. On a donc prouvé ce qui suit :

THÉORÈME 1. *Soit* $K = \mathbf{Q}(\sqrt{d})$ *un corps quadratique, avec* $d \in \mathbf{Z}$ *sans facteurs carrés (et donc* $\not\equiv 0$ mod. 4).

a) *Si* $d \equiv 2$ *ou* $d \equiv 3$ mod. 4, *l'anneau* A *des entiers de* K *est l'ensemble des* $a + b\sqrt{d}$, avec $a, b \in \mathbf{Z}$.

b) Si $d \equiv 1$ mod. 4, A *est l'ensemble des* $\frac{1}{2}(u + v\sqrt{d})$ *avec* $u, v \in \mathbf{Z}$ *de même parité.*

Dans le cas $d \equiv 2$ ou 3 mod. 4, une base du **Z**-module A est évidemment $(1, \sqrt{d})$. Dans le cas $d \equiv 1$ mod. 4, une base du **Z**-module A est $\left(1, \frac{1}{2}(1 + \sqrt{d})\right)$. En effet, par *b*), les éléments 1 et $\frac{1}{2}(1 + \sqrt{d})$ sont dans A. Inversement, pour montrer que $\frac{1}{2}(u + v\sqrt{d})$ (avec u, $v \in \mathbf{Z}$ de même parité) est combinaison **Z**-linéaire de 1 et $\frac{1}{2}(1 + \sqrt{d})$, on se ramène au cas où u et v sont pairs par soustraction éventuelle de $\frac{1}{2}(1 + \sqrt{d})$; dans ce cas on a $\frac{1}{2}(u+v\sqrt{d}) = \left(\frac{u}{2} - \frac{v}{2}\right).1 + v.\frac{1}{2}(1 + \sqrt{d})$.

Pour finir, un peu de *terminologie*. Si $d > 0$, on dit que $\mathbf{Q}(\sqrt{d})$ est un *corps quadratique réel* (car il existe un sous-corps de **R** conjugué de $\mathbf{Q}(\sqrt{d})$ sur $\mathbf{Q}$). Si $d < 0$, on dit que $\mathbf{Q}(\sqrt{d})$ est un *corps quadratique imaginaire.*

2.6. Normes et traces

a) *Rappels d'algèbre linéaire.*

Soient A un anneau, E un A-module *libre* de rang fini, et u un endomorphisme de E. On définit en algèbre linéaire la *trace*, le *déterminant*, et le *polynôme caractéristique* de u. Si une base (e_i) de E a été choisie et si (a_{ij}) est la matrice de u dans cette base, ces quantités valent respectivement

1. $\operatorname{Tr} u = \sum_{i=1}^{n} a_{ii}$, $\det(u) = \det(a_{ij})$, et $\det(X.I_E - u)$

NB. Ces quantités sont indépendantes de la base choisie.

Les formules (1) montrent qu'on a :

2. $\operatorname{Tr}(u + u') = \operatorname{Tr}(u) + \operatorname{Tr}(u')$
   $\det(uu') = \det(u)\det(u')$
   $\det(X.I_E - u) = X^n - (\operatorname{Tr} u).X^{n-1} + \cdots + (-1)^n \det u.$

b) *Normes et traces dans une extension.*

Soient B un anneau, et A un sous-anneau de B tel que B soit un A-module libre de rang fini n (par exemple A peut être un corps, et B une extension de degré n de A). Pour $x \in B$, la multiplication m_x par x (soit $y \mapsto xy$) est un endomorphisme du A-module B.

DÉFINITION 1. *On appelle trace* (resp. *norme*, *polynôme caractéristique*) *de* $x \in B$, *relativement à* B *et* A, *la trace* (resp. *déterminant*, *polynôme caractéristique*) *de l'endomorphisme* m_x *de multiplication par* x.

La trace (resp. norme) de x est notée $\mathrm{Tr}_{A/B}(x)$ (resp. $N_{A/B}(x)$), ou $\mathrm{Tr}(x)$ (resp. $N(x)$) lorsqu'aucune confusion n'est à craindre; ce sont des éléments de A. Le polynôme caractéristique de x est un polynôme unitaire à coefficients dans A.

Pour $x, x' \in B$ et $a \in A$ on a évidemment $m_x + m_{x'} = m_{x+x'}$, $m_x \circ m_{x'} = m_{xx'}$ et $m_{ax'} = am_x$; de plus la matrice de m_a, dans n'importe quelle base de B sur A, est la matrice diagonale dont tous les éléments diagonaux sont égaux à a. Il résulte alors des formules (1) et (2) qu'on a :

3. $\mathrm{Tr}\,(x+x') = \mathrm{Tr}\,(x) + \mathrm{Tr}\,(x')$, $\mathrm{Tr}\,(ax) = a\,\mathrm{Tr}\,(x)$, $\mathrm{Tr}\,(a) = n.a$
$N(xx') = N(x)\,N(x')$, $N(a) = a^n$, $N(ax) = a^n N(x)$

PROPOSITION 1. *Soient* K *un corps de caractéristique* 0 *ou fini*, L *une extension algébrique de degré* n *de* K, x *un élément de* L, *et* $x_1, \ldots, x_n$ *les racines du polynôme minimal de* x *sur* K (*dans une extension convenable de* K; cf. § 3, prop. 3), *chacune répétée* $[L : K[x]]$ *fois. Alors* $\mathrm{Tr}_{L/K}(x) = x_1 + \cdots + x_n$, $N_{L/K}(x) = x_1 \ldots x_n$; *de plus le polynôme caractéristique de* x, *relativement à* L *et* K, *est* $(X - x_1)\ldots(X - x_n)$.

Ainsi ce polynôme caractéristique est la puissance $[L : K[x]]$-ème du polynôme minimal de x sur K.

Traitons d'abord le cas où x est un *élément primitif* de L sur K (cf. § 4, cor. du th. 1). Soit $F(X)$ le polynôme minimal de x sur K; alors L est K-isomorphe à $K[X]/(F(X))$ (§ 3, formule (5)), et $(1, x, \ldots, x^{n-1})$ est une base de L sur K. Posons $F(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$. La matrice de l'endomorphisme m_x dans cette base est :

$$\begin{vmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & \ldots & 0 & \vdots \\ \vdots & 0 & & \vdots & \vdots \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -a_{n-1} \end{vmatrix}$$

Le déterminant de $X.1_L - m_x$ est donc :

$$\begin{vmatrix} X & 0 & \ldots & 0 & a_0 \\ -1 & X & & 0 & a_1 \\ 0 & -1 & & 0 & \vdots \\ \vdots & \vdots & & \vdots & \vdots \\ \vdots & \vdots & & X & a_{n-2} \\ 0 & 0 & & -1 & X + a_{n-1} \end{vmatrix}$$

En développant on obtient le polynôme caractéristique de x, qui est donc égal au polynôme minimal $X^n + a_{n-1}X^{n-1} + \cdots + a_0$. D'après (2) on en déduit $\mathrm{Tr}(x) = -a_{n-1}$ et $N(x) = (-1)^n a_0$. Or, comme x est primitif, on a $F(X) = (X - x_1) \ldots (X - x_n)$; d'où, en comparant,

$$\mathrm{Tr}(x) = x_1 + \cdots + x_n \quad \text{et} \quad N(x) = x_1 \ldots x_n.$$

Passons maintenant au *cas général*, et posons $r = [L : K[x]]$. Il nous suffit de montrer que le polynôme caractéristique $P(X)$ de x relativement à L et K est égal à la puissance r-ème du polynôme minimal de x sur K. Or soient $(y_i)_{i=1,\ldots,q}$ une base de $K[x]$ sur K, et $(z_j)_{j=1,\ldots,r}$ une base de L sur $K[x]$; alors $(y_i z_j)$ est une base de L sur K et on a $n = qr$ (§ 3, prop. 1). Soit $M = (a_{ih})$ la matrice de la multiplication par x dans $K[x]$ par rapport à la base (y_i) : ainsi $xy_i = \sum_h a_{ih} y_h$. On a alors $x(y_i z_j) = \left(\sum_h a_{ih} y_h\right) z_j = \sum_h a_{ih}(y_h z_j)$. Si on ordonne lexicographiquement la base $(y_i z_j)$ de L sur K, on voit donc que la matrice M' de la multiplication par x dans L par rapport à cette base se présente sous la forme d'un tableau diagonal de matrices

$$M_1 = \begin{vmatrix} M & 0 & \ldots & 0 \\ 0 & M & \ldots & 0 \\ - & - & \ldots & \vdots \\ 0 & 0 & \ldots & M \end{vmatrix}$$

La matrice $X.I - M_1$ se présente donc comme tableau diagonal des matrices $X.I_q - M$; d'où $\det(X.I_n - M_1) = (\det(X.I_q - M))^r$. Or le premier membre est $P(X)$, et $\det(X.I_q - M)$ est le polynôme minimal de x sur K d'après la première partie. CQFD.

Donnons enfin un résultat sur les traces et normes d'éléments entiers.

PROPOSITION 2. *Soient* A *un anneau intègre,* K *son corps des fractions,* L *une extension de degré fini de* K, *et* x *un élément de* L *entier sur* A; *on suppose* K *de caractéristique* 0. *Alors les coefficients du polynôme caractéristique* $P(X)$ *de* x *relativement à* L *et* K, *en particulier* $\mathrm{Tr}_{L/K}(x)$ *et* $N_{L/K}(x)$, *sont entiers sur* A.

Utilisons la prop. 1 : on a $P(X) = (X - x_1) \ldots (X - x_n)$; les coefficients de $P(x)$ sont donc, au signe près, des sommes de produits des x_i; il suffit de montrer que les x_i sont entiers sur A (§ 1, cor. 1 de la prop. 1). Or chaque x_i est un conjugué de x sur K (§ 4), et on a un K-isomorphisme $\sigma_i : K[x] \to K[x_i]$ tel que $\sigma_i(x) = x_i$. En appliquant σ_i à une équation de dépendance intégrale de x sur A, on obtient une équation de dépendance intégrale de x_i sur A.

COROLLAIRE. *Supposons de plus* A *intégralement clos. Alors les coefficients du polynôme caractéristique de* x, *en particulier* $\mathrm{Tr}_{L/K}(x)$ *et* $N_{L/K}(x)$, *sont éléments de* A.

En effet ces coefficients sont éléments de K par définition, et sont entiers sur A par la prop. 2.

On remarquera que les quantités $x + \sigma(x)$ et $x.\sigma(x)$ utilisées dans l'étude des corps quadratiques (§ 5) sont la trace et la norme de x. On y a prouvé (§ 5, (3)) un cas particulier du corollaire ci-dessus.

2.7. Discriminant

DÉFINITION 1. *Soient* B *un anneau et* A *un sous-anneau de* B *tel que* B *soit un* A-*module libre de rang fini* n. *Pour* $(x_1, \ldots, x_n) \in B^n$, *on appelle discriminant du système* $(x_1, \ldots, x_n)$ *l'élément de* A *défini par*

1. $\mathrm{D}(x_1, \ldots, x_n) = \det(\mathrm{Tr}_{B/A}(x_i x_j))$

PROPOSITION 1. *Si* $(y_1, \ldots, y_n) \in B^n$ *est un autre système d'éléments de* B *tel que* $y_i = \sum_{j=1}^{n} a_{ij} x_j$ *avec* $a_{ij} \in A$, *on a*

2. $\mathrm{D}(y_1, \ldots, y_n) = \det(a_{ij})^2\, \mathrm{D}(x_1, \ldots, x_n)$

En effet on a $\mathrm{Tr}(y_p y_q) = \mathrm{Tr}\Big(\sum_{ij} a_{pi} a_{qj} x_i x_j\Big) = \sum_{ij} a_{pi} a_{qj} \mathrm{Tr}(x_i y_j)$. D'où l'égalité entre matrices $(\mathrm{Tr}(y_p y_q)) = (a_{pi})\ (\mathrm{Tr}(x_i x_j)) \,.\, {}^t(a_{qj})$ (où ${}^tM$ désigne la transportée de la matrice M). Il suffit de prendre les déterminants. CQFD.

Il résulte de la prop. 1 que les discriminants des bases de B sur A sont deux à deux *associés* dans A : en effet la matrice de passage (a_{ij}) d'une base à une autre est inversible, donc a son déterminant inversible. On peut donc poser la

DÉFINITION 2. *Sous les hypothèses de la déf.* 1, *on appelle discriminant de* B *sur* A, *et on note* $\mathfrak{D}_{B/A}$, *l'idéal principal de* A *engendré par le discriminant de n'importe quelle base de* B *sur* A.

PROPOSITION 2. *Supposons que* $\mathfrak{D}_{B/A}$ *contienne un élément qui n'est pas diviseur de* 0. *Alors, pour qu'un système* $(x_1, \ldots, x_n) \in B^n$ *soit une base de* B *sur* A, *il faut et il suffit que* $\mathfrak{D}_{B/A}$ *soit engendré par* $\mathrm{D}(x_1, \ldots, x_n)$.

La nécessité a été démontrée plus haut. Supposons donc que $d = \mathrm{D}(x_1, \ldots, x_n)$ engendre $\mathfrak{D}_{B/A}$. Soit $(e_1, \ldots, e_n)$ une base de B sur A; posons $d' = \mathrm{D}(e_1, \ldots, e_n)$ et $x_i = \sum_{j=1}^{n} a_{ij} e_j$ avec $a_{ij} \in A$. On a $d = \det(a_{ij})^2 d'$. Par hypothèse on a $Ad = \mathfrak{D}_{B/A} = Ad'$. Il existe donc $b \in A$ tel que $d' = bd$; d'où $d(1 - b\det(a_{ij})^2) = 0$. Or d n'est pas diviseur de 0, car sinon tout élément de $Ad = \mathfrak{D}_{B/A}$ serait diviseur de 0.

On a donc $1 - b \det (a_{ij})^2 = 0$. Ceci montre que $\det (a_{ij})$ est inversible, donc aussi la matrice (a_{ij}) ; par conséquent $(x_1, \ldots, x_n)$ est une base de B sur A.

PROPOSITION 3. *Soient* K *un corps fini ou de caractéristique* 0, L *une extension de degré fini* n *de* K, *et* $\sigma_1, \ldots, \sigma_n$ *les* n K-*isomorphismes distincts de* L *dans un corps algébriquement clos* C *contenant* K (§ 4, th. 1). *Alors, si* $(x_1, \ldots, x_n)$ *est une base de* L *sur* K, *on a*

3. $\mathrm{D}(x_1, \ldots, x_n) = \det (\sigma_i(x_j))^2 \neq 0.$

La première égalité résulte d'un calcul simplet :

$$\mathrm{D}(x_1, \ldots, x_n) = \det (\mathrm{Tr}\,(x_i x_j)) = \det \Big(\sum_k \sigma_k(x_i y_j) \Big) = \det \Big(\sum_k \sigma_k(x_i)\sigma_k(x_j) \Big)$$
$$= \det (\sigma_k(x_i)) . \det (\sigma_k(x_j)) = \det (\sigma_i(x_j))^2.$$

Reste à montrer qu'on a $\det (\sigma_i(x_j)) \neq 0$. Raisonnons par l'absurde. Si $\det (\sigma_i(x_j)) = 0$, il existe $u_1, \ldots, u_n \in \mathrm{C}$, non tous nuls, tels que $\sum_{i=1}^{n} u_i\sigma_i(x_j) = 0$ pour tout j. Par linéarité on en déduit $\sum_{i=1}^{n} u_i\sigma_i(x) = 0$ pour tout $x \in \mathrm{L}$. Or ceci contredit le résultat suivant :

LEMME DE DEDEKIND. *Soient* G *un groupe,* C *un corps, et* $\sigma_1, \ldots, \sigma_n$ *des homomorphismes distincts de* G *dans le groupe multiplicatif* C*. *Alors les* σ_i *sont linéairement indépendants sur* C $\Big($i.e. $\sum_i u_i\sigma_i(g) = 0$ *pour tout* $g \in \mathrm{G}$ *implique que tous les* u_i *sont nuls*$\Big)$.

Si les σ_i sont linéairement dépendants, considérons une relation non triviale $\sum_i u_i\sigma_i = 0 (u_i \in \mathrm{C})$ telle que le nombre q des u_i non nuls soit *minimum*. Après renumérotation, on peut supposer que c'est

4. $u_1\sigma_1(g) + \cdots + u_q\sigma_q(g) = 0$ pour tout $g \in \mathrm{G}$

On a $q \geqslant 2$ car les σ_i sont non nuls. Pour g et h quelconques dans G, on a

$$u_1\sigma_1(hg) + \cdots + u_q\sigma_q(hg) = u_1\sigma_1(h)\sigma_1(g) + \cdots + u_q\sigma_q(h)\sigma_q(g) = 0.$$

Multiplions (4) par $\sigma_1(h)$ et soustrayons; il vient

$$u_2(\sigma_1(h) - \sigma_2(h))\sigma_1(g) + \cdots + u_q(\sigma_1(h) - \sigma_q(h))\sigma_q(g) = 0.$$

Comme ceci a lieu pour tout $g \in \mathrm{G}$ et que q a été choisi minimum, ceci implique $u_2(\sigma_1(h) - \sigma_2(h)) = 0$; d'où $\sigma_1(h) = \sigma_2(h)$ car $u_2 \neq 0$; ceci contredit l'hypothèse que les σ_i sont distincts. CQFD.

Remarque. Sous les conditions de la prop. 3, la relation $\mathrm{D}(x_1, \ldots, x_n) \neq 0$ exprime que la forme bilinéaire $(x, y) \mapsto \mathrm{Tr}_{\mathrm{L/K}}(xy)$ est *non-dégénérée*, c'est-à-dire que $\mathrm{Tr}_{L/K}(xy) = 0$ pour tout $y \in L$ implique $x = 0$. Ainsi l'application K-linéaire qui, à $x \in L$, fait correspondre la forme K-linéaire, $s_x : y \mapsto \mathrm{Tr}_{L/K}(xy)$, est une injection de L dans son dual $\mathrm{Hom}_K(L, K)$ (pour la structure d'espace vectoriel sur K). Comme L et $\mathrm{Hom}_K(L, K)$ sont de même dimension finie n sur K, il en résulte que $x \mapsto s_x$ est une bijection. L'existence de « *bases duales* » sur un espace vectoriel et son dual montre alors que, pour toute base $(x_1, \ldots, x_n)$ de L sur K, il existe une autre base $(y_1, \ldots, y_n)$ telle que

5. $\mathrm{Tr}_{L/K}(x_i y_j) = \delta_{ij} \qquad (1 \leqslant i, j \leqslant n).$

Cette remarque va nous être utile.

THÉORÈME 1. *Soient* A *un anneau intégralement clos,* K *son corps des fractions,* L *une extension de degré fini* n *de* K *et* A′ *la fermeture intégrale de* A *dans* L. *On suppose* K *de caractéristique* 0. *Alors* A′ *est un sous* A-*module d'un* A-*module libre de rang* n.

Soit, en effet, $(x_1, \ldots, x_n)$ une base de L sur K. Chaque x_i est algébrique sur K, d'où $a_n x_i^n + a_{n-1}x_i^{n-1} + \cdots + a_0 = 0$ avec $a_j \in A$ pour $j = 0, \ldots, n$; par multiplication par une puissance de x_i, on peut supposer $a_n \neq 0$; par multiplication par a_n^{n-1}, on voit que $a_n x_i$ est entier sur A. Posons $x'_i = a_n x_i$. Alors $(x'_1, \ldots, x'_n)$ est une base de L sur K contenue dans A′.

D'après la remarque ci-dessus, on a une autre base $(y_1, \ldots, y_n)$ de L sur K telle que $\mathrm{Tr}\,(x'_i y_j) = \delta_{ij}$((5)). Soit alors $z \in A'$. Comme $(y_1, \ldots, y_n)$ est une base de L sur K, on peut écrire $z = \sum_{j=1}^{n} b_j y_j$ avec $b_j \in K$. Pour tout i on a $x'_i z \in A'$ (car $x'_i \in A'$), d'où $\mathrm{Tr}\,(x'_i z) \in A$ (§ 6, cor. de la prop. 2). Or

$$\mathrm{Tr}\,(x'_i z) = \mathrm{Tr}\left(\sum_j b_j x'_i y_j\right) = \sum_j b_j \,\mathrm{Tr}\,(x'_i y_j) = \Sigma b_j \delta_{ij} = b_i$$

On a donc $b_i \in A$ pour tout i. Ainsi A′ est contenu dans le A-module libre $\sum_{j=1}^{n} Ay_j$. CQFD.

COROLLAIRE. *Avec les hypothèses du th.* 1, *supposons de plus* A *principal. Alors* A′ *est un* A-*module libre de rang* n.

En effet un sous-module d'un A-module libre est alors libre (chap. I, § 5, th. 1, *b*)), et de rang $\leqslant n$. D'autre part on a vu au cours de la démonstration du th. 1 que A′ contient une base de L sur K, donc est de rang n.

A titre d'exercice, le lecteur peu familier avec le contenu de la remarque précédent le th. 1 pourra chercher une démonstration plus calculatoire de ce théorème : avec les notations ci-dessus, il posera $d = D(x'_1, \ldots, x'_n)$, et montrera que, si $z = \sum_i c_i x'_i$ $(c_i \in K)$ est entier sur A, alors $dc_i \in A$ (calculer $Tr(zx'_j)$ et utiliser les formules de Cramer).

Un exemple de calcul de discriminant.

Soient K un corps fini ou de caractéristique 0, $L = K[x]$ une extension de degré fini n de K, et $F(X)$ le polynôme minimal de x sur K. Alors

6. $D(1, x, \ldots, x^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{L/K}(F'(x))$

(où $F'(X)$ désigne le polynôme dérivé de $F(X)$). En effet notons $x_1, \ldots, x_n$ les racines de $F(X)$ dans une extension de K; ce sont les conjugués de x (§ 3, prop. 3, et § 4). On a

$$D(1, x, \ldots, x^{n-1}) = \det(\sigma_i(x^j))^2 \text{ (prop. 3)} = \det(x_i^j)^2$$

$$(-1)^{\frac{n(n-1)}{2}} \det(x_i^j)^2 = \prod_{i \neq j} (x_i - x_j) \text{ (Vandermonde)} = \prod_i \Big(\prod_{j \neq i} (x_i - x_j)\Big)$$
$$= \prod_i F'(x_i) = N_{L/K}(F'(x))$$

(car les $F'(x_i)$ sont les conjugués de $F'(x)$).

En particulier, appliquons (6) au cas où $F(X)$ est un *trinôme* $X^n + aX + b (a, b \in K)$. Posons $y = F'(x)$; on a

$$y = nx^{n-1} + a = -(n-1)a - nbx^{-1}$$

(car $x^n + ax + b = 0$, d'où $nx^{n-1} = -na - nbx^{-1}$). On en tire $x = -nb(y + (n-1)a)^{-1}$. Le polynôme minimal de y sur K est le numérateur de $F(-nb(Y + (n-1)a)^{-1})$; tous calculs faits, c'est $(Y + (n-1)a)^n - na(Y + (n-1)a)^{n-1} + (-1)^n b^{n-1}$. La norme de y est $(-1)^n$ fois le terme constant de ce polynôme, donc

$$n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n.$$

D'où

7. $D(1, x, \ldots, x^{n-1}) = [n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n](-1)^{\frac{n(n-1)}{2}}$

Pour $n = 2$ (resp. 3) on retrouve le $4b - a^2$ (resp. $-4a^3 - 27b^2$) bien connu.

2.8. Terminologie des corps de nombres

On appelle *corps de nombres algébriques* (ou *corps de nombres*) toute extension de degré fini (et donc algébrique) de $\mathbf{Q}$. Étant donné un corps de nombres K, le degré $[K : \mathbf{Q}]$ s'appelle le *degré* de K; un corps de nombres de degré 2 (resp. 3) s'appelle un *corps quadratique* (cf. § 5) (resp. un *corps cubique*). Un corps de nombres est de caractéristique 0.

Étant donné un corps de nombres K, les éléments de K qui sont entiers sur **Z**, s'appellent les *entiers de* K. Ils forment un *sous-anneau* A de K (§ 1, cor. 2 de la prop. 1), qui est un **Z**-module *libre* de rang $[K : \mathbf{Q}]$ (§ 7, cor. du th. 1). Les discriminants des bases du **Z**-module A diffèrent par un élément inversible de **Z** (§ 7, déf. 2), qui est même un carré (§ 7, prop. 1); cet élément ne peut donc être que $+1$, de sorte que les discriminants des bases du **Z**-module A sont tous *égaux*; leur valeur commune s'appelle le *discriminant absolu*, ou *discriminant*, de K.

Comme un corps de nombres K détermine de façon unique l'anneau A des entiers de K, on fait souvent l'abus de langage consistant à attribuer à K des notions relatives à A; ainsi lorsqu'on parle d'idéaux (ou d'unités) de K, il s'agit d'idéaux (ou d'unités) de A.

2.9. Corps cyclotomiques

On appelle *corps cyclotomique* tout corps de nombres engendré sur **Q** par des racines de l'unité. Étant donné un nombre premier p, nous désignerons par z une racine primitive p-ème de l'unité (dans **C** par exemple), et nous allons étudier le corps cyclotomique $\mathbf{Q}[z]$. Le nombre z est racine du polynôme $X^p - 1$; comme z est $\neq 1$, il est aussi racine du polynôme $\dfrac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1$, appelé *polynôme cyclotomique*. Il n'est nullement évident que ce polynôme est irréductible sur **Q** (ce qui revient à dire que le corps $\mathbf{Q}[z]$ est de degré $p-1$). Pour le démontrer nous aurons besoin du

CRITÈRE D'EISENSTEIN. *Soient* A *un anneau principal,* $p \in A$ *un élément premier de* A *et* $F(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ *un élément de* $A[X]$ *tel que* p *divise tous les* $a_i (0 \leqslant i \leqslant n-1)$, *mais que* p^2 *ne divise pas* a_0. *Alors* $F(X)$ *est irréductible sur le corps des fractions* K *de* A.

Supposons en effet que l'on ait $F = G.H$ avec $G, H \in K[X]$, G et H *unitaires*. Les racines de F sont *entières* sur A. Or toute racine de G (resp. H) est racine de F, donc est entière sur A. Or les coefficients de G (resp. H) sont des sommes de produits des racines de G (resp. H); ils sont donc entiers sur A (§ 1, cor. 1 de la prop. 1). Comme A est principal, donc intégralement clos (§ 2, ex. 2), on a $G \in A[X]$ et $H \in A[X]$.

Soient alors $\overline{F}, \overline{G}, \overline{H}$ les images de F, G, H dans $(A/Ap)[X]$; on a $\overline{F} = \overline{G}.\overline{H}$. D'après l'hypothèse sur les a_i, on a $\overline{F} = X^n$. Comme A/Ap est un anneau *intègre*, la décomposition $X^n = \overline{G}.\overline{H}$ est nécessairement de la forme $X^n = X^q.X^{n-q}$ (car $\overline{G}$ et $\overline{H}$ sont unitaires); d'où $\overline{G} = X^q$ et $\overline{H} = X^{n-q}$. Si G et H sont tous deux non constants, on en déduit que p divise les termes constants de G et H; donc p^2 divise le terme constant a_0 de F, contrairement à l'hypothèse. Donc G ou H est constant, et F est irréductible. CQFD.

Exemple. Le polynôme $X^3 - 2X + 6$ est irréductible sur $\mathbf{Q}$ (prendre $p = 2$, $A = \mathbf{Z}$).

THÉORÈME 1. *Pout tout nombre premier p, le polynôme cyclotomique* $X^{p-1} + X^{p-2} + \cdots + X + 1$ *est irréductible dans* $\mathbf{Q}[X]$.

Posons en effet $X = Y + 1$. On a

$$X^{p-1} + \cdots + 1 = \frac{X^p - 1}{X - 1} = \frac{(Y+1)^p - 1}{Y}$$

$$= Y^{p-1} + \sum_{j=p-1}^{1} \binom{p}{j} Y^{j-1} = F_1(Y).$$

Or p divise tous les coefficients binômiaux $\binom{p}{j}$, mais p^2 ne divise pas le terme constant $\binom{p}{1} = p$. Donc $F_1(Y)$ est irréductible par le critère d'Eisenstein, donc aussi le polynôme cyclotomique. CQFD.

Soit toujours z une racine primitive p-ème de l'unité. Il résulte du th. 1 que le corps $\mathbf{Q}[z]$ est de degré $p - 1$; donc $(1, z, \ldots, z^{p-2})$ est une base de $\mathbf{Q}[z]$ sur $\mathbf{Q}$. Nous allons étudier l'anneau des entiers de $\mathbf{Q}[z]$ et montrer que c'est $\mathbf{Z}[z]$.

Pour cela nous aurons besoin de calculer quelques *traces et normes* (on écrira $\mathrm{Tr}(x)$ et $N(x)$ au lieu de $\mathrm{Tr}_{\mathbf{Q}[z]/\mathbf{Q}}(x)$ et $N_{\mathbf{Q}[z]/\mathbf{Q}}(x)$). Notons que les conjugués de z sur $\mathbf{Q}$ sont les z^j $(j = 1, \ldots, p-1)$ (th. 1). L'irréductibilité du polynôme cyclotomique donne aussitôt :

1. $\mathrm{Tr}(z) = -1 \quad \mathrm{Tr}(1) = p - 1$

D'où $\mathrm{Tr}(z^j) = -1$ pour $j = 1, \ldots, p-1$, et donc

2. $\mathrm{Tr}(1 - z) = \mathrm{Tr}(1 - z^2) = \cdots = \mathrm{Tr}(1 - z^{p-1}) = p$.

D'autre part le calcul fait dans le th. 1 montre que $N(z - 1) = (-1)^{p-1}p$, d'où $N(1 - z) = p$; comme la norme de $1 - z$ est le produit des conjugués de $1 - z$, on a donc

3. $p = (1 - z)(1 - z^2) \ldots (1 - z^{p-1})$

Notons A l'anneau des entiers de $\mathbf{Q}[z]$ Il contient évidemment z et ses puissances. On va montrer qu'on a

4. $A(1 - z) \cap \mathbf{Z} = p\mathbf{Z}$

En effet on a $p \in A(1 - z)$ d'après (3), d'où $A(1 - z) \cap \mathbf{Z} \supset p\mathbf{Z}$; comme $p\mathbf{Z}$ est idéal maximal de $\mathbf{Z}$, la relation $A(1 - z) \cap \mathbf{Z} \neq p\mathbf{Z}$ entraînerait

$A(1-z) \cap \mathbf{Z} = \mathbf{Z}$, et $1-z$ serait inversible dans A; ses conjugués $1-z^j$ le seraient alors aussi, et donc p également d'après (4); ainsi $\frac{1}{p}$ serait entier sur $\mathbf{Z}$, ce qui est absurde (§ 2, ex. 2).

Montrons enfin que, pour tout $y \in A$, on a

5. $\mathrm{Tr}\,(y(1-z)) \in p\mathbf{Z}$

En effet chaque conjugué $y_j(1-z^j)$ de $y(1-z)$ est multiple (dans A) de $1-z^j$, lequel est multiple de $1-z$ car

$$1-z^j = (1-z)\,(1+z+\cdots+z^{j-1});$$

comme la trace est la somme des conjugués, on a donc

$$\mathrm{Tr}\,(y(1-z)) \in A(1-z);$$

d'où, (5), d'après (4), car la trace d'un entier est dans $\mathbf{Z}$(§ 6, cor. de la prop. 2).

Ceci étant, nous sommes en mesure de déterminer l'anneau des entiers de $\mathbf{Q}[z]$

THÉORÈME 2. *Soient p un nombre premier et z une racine primitive p-ème de l'unité (dans $\mathbf{C}$). Alors l'anneau A des entiers du corps cyclotomique $\mathbf{Q}[z]$ est $\mathbf{Z}[z]$, et $(1, z, \ldots, z^{p-2})$ est une base du $\mathbf{Z}$-module A.*

En effet soit $x = a_0 + a_1 z + \cdots + a_{p-2}z^{p-2} (a_i \in \mathbf{Q})$ un élément de A. On a alors

$$x(1-z) = a_0(1-z) + a_1(z-z^2) + \cdots + a_{p-2}(z^{p-2}-z^{p-1})$$

En prenant les traces, il résulte de 1 et de 2 que

$$\mathrm{Tr}\,(x(1-z)) = a_0\mathrm{Tr}\,(1-z) = a_0 p.$$

D'où, en utilisant (5), $pa_0 \in p\mathbf{Z}$ et $a_0 \in \mathbf{Z}$. Comme $z^{-1} = z^{p-1}$, on a $z^{-1} \in A$, d'où $(x-a_0)z^{-1} = a_1 + a_2 z + \cdots + a_{p-2}z^{p-3} \in A$; en appliquant la première partie du raisonnement à cet élément, on voit que $a_1 \in \mathbf{Z}$. Par applications successives de ce procédé, on voit que chaque $a_i \in \mathbf{Z}$. CQFD.

Remarque. Ce qui a été fait dans ce § s'étend sans peine aux corps cyclotomiques $\mathbf{Q}[t]$ où t est une racine primitive p^r-ème de l'unité (p premier). Un tel corps est de degré $p^{r-1}(p-1)$, et son anneau des entiers est $\mathbf{Z}[t]$. Le polynôme minimal de t sur $\mathbf{Q}$ est

$$X^{p^{r-1}(p-1)} + X^{p^{r-1}(p-2)} + \cdots + X^{p^{r-1}} + 1 = \frac{X^{p^r}-1}{X^{p^{r-1}}-1}.$$

APPENDICE

Le corps C des nombres complexes est algébriquement clos

Étant donné un corps K, considérons les propriétés suivantes :

(*a*) Tout polynôme de degré > 0 sur K est un produit de polynômes du premier degré.

(*b*) Tout polynôme de degré > 0 sur K admet une racine dans K.

Il est clair que *a*) implique *b*). Réciproquement, si *b*) est vraie, si P(X) est un polynôme de degré $d \geqslant 1$ sur K et si $a \in K$ est une racine de P(X), alors P(X) est multiple de $X - a$, et une récurrence sur le degré d montre que *a*) est vraie. Un corps K jouissant des propriétés équivalentes *a*) et *b*) est dit *algébriquement clos.*

Nous allons montrer que $\mathbf{C}(= \mathbf{R}[i],\ i^2 = -1)$ est algébriquement clos par une méthode essentiellement due à Lagrange. Nous utiliserons uniquement les faits suivants :

1. Tout polynôme de degré impair sur **R** admet une racine dans **R**; ceci est un cas particulier facile du théorème des valeurs intermédiaires.

2. Tout polynôme du second degré sur C a ses racines dans C; le calcul élémentaire sur « $ax^2 + bx + c = 0$ » nous ramène à montrer que tout $z = a + ib \in \mathbf{C}$ $(a,\ b \in \mathbf{R})$ admet une racine carrée dans C; or $(x + iy)^2 = a + ib$ $(x,\ y \in \mathbf{R})$ équivaut à $x^2 - y^2 = a,\ 2xy = b$, d'où $a^2 + b^2 = (x^2 + y^2)^2$ et $x^2 + y^2 = \sqrt{a^2 + b^2}$; on en déduit les valeurs de x^2 et y^2, d'où x et y.

3. Étant donné un polynôme non constant $P(X) \in K[X]$, il existe une extension K′ de K telle que P(X) se décompose en facteurs du premier degré dans K′[X]; ceci a été très facilement démontré dans la prop. 3 du § 3 (démonstration quasi indépendante de ce qui la précède; il suffit de savoir que, si F(X) est irréductible, K[X]/(F(X)) est un corps, et ensuite de faire une récurrence).

4. Les relations entre coefficients et racines d'un polynôme.

5. Le fait qu'un polynôme symétrique $G(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$ est un polynôme par rapport aux fonctions symétriques élémentaires $\Sigma X_i,\ \Sigma X_iX_j,\ \ldots,\ X_1 \ldots X_n$ des X_i.

Ceci étant on a :

THÉORÈME. *Le corps* C *des nombres complexes est algébriquement clos.*

Nous utiliserons la propriété (*b*), que tout polynôme non constant $P(X) \in \mathbf{C}[X]$ admet une racine dans C. En considérant $F(X) = P(X)\overline{P}(X)$ ($\overline{P}$: polynôme dont les coefficients sont les complexes conjugués des coefficients

correspondants de P) on se ramène au cas d'un polynôme à coefficients réels : en effet, si $a \in \mathbf{C}$ est une racine de $F(X)$, alors ou bien a est racine de $P(X)$, ou bien a est racine de $\overline{P}(X)$ et alors $\bar{a}$ est racine de $P(X)$. Ceci étant nous mettrons le degré de $F(X) (\in \mathbf{R}[X])$ sous la forme $d = 2^n q$ où q est impair. Nous procéderons par récurrence sur l'*exposant* n de 2. Pour $n = 0$, d est impair et $F(X)$ a une racine dans $\mathbf{R}$ (cf. 1)). Supposons $n \geqslant 1$. Par 3) il existe une extension K' de $\mathbf{C}$ et $x_1, \ldots, x_d \in K'$ tels que $F(X) = \prod_{i=1}^{d} (X - x_i)$ (en supposant $F(X)$ unitaire, ce qui est loisible). Soit c un élément arbitraire de $\mathbf{R}$; considérons les éléments $y_{ij} = x_i + x_j + c x_i x_j$ de $K' (i \leqslant j)$; leur nombre est $\frac{1}{2} d(d+1) = 2^{n-1} q(d+1)$ et $q(d+1)$ est *impair*. Le polynôme $G(X) = \prod_{i \leqslant j} (X - y_{ij})$ a pour coefficients des polynômes symétriques à coefficients réels en les x_i; ce sont donc par 5) des polynômes à coefficients réels en les fonctions symétriques élémentaires des x_i; ainsi les coefficients de $G(X)$ sont réels par 4). Comme son degré est de la forme $2^{n-1} \times$ (impair), l'hypothèse de récurrence montre qu'il admet une racine $z_c \in \mathbf{C}$; l'un des y_{ij}, soit $y_{i(c),\, j(c)} = x_{i(c)} + y_{j(c)} + c x_{i(c)} x_{j(c)}$ est donc égal à z_c.
Or, comme $\mathbf{R}$ est *infini* et l'ensemble des couples (i, j) $(i \leqslant j)$ fini, il existe deux nombres réels distincts, c, c' tels que $i(c) = i(c')$ et $j(c) = j(c')$; notons r, s ces indices. Alors $x_r + x_s + c x_r x_s = z_c \in \mathbf{C}$ et

$$x_r + x_s + c' x_r x_s = z_{c'} \in \mathbf{C}.$$

Par combinaisons linéaires on en déduit $x_r + x_s \in \mathbf{C}$ et $x_r x_s \in \mathbf{C}$. Alors, par 4), x_r et x_s sont racines et une équation du second degré à coefficients dans $\mathbf{C}$. Comme $\mathbf{C} \subset K'$, on a donc $x_r, x_s \in \mathbf{C}$ par 2). Ainsi $F(X)$ a une racine dans $\mathbf{C}$, et le théorème est démontré.

La démonstration donnée paraît utilisable dans un cours de spéciales ou de premıer cycle, et dans une leçon d'Agrégation.

CHAPITRE III

Anneaux nœthériens Anneaux de Dedekind

Le lecteur qui veut savoir pourquoi on a introduit les anneaux de Dedekind pourra se reporter au § 4, et y lire l'exemple et la discussion qui suivent le th. 1. Les anneaux nœthériens, dont nous étudions d'abord un minimum de propriétés, sont plus généraux que les anneaux de Dedekind; Nous les introduisons pour placer ces propriétés dans leur cadre naturel de validité, et aussi parce qu'ils jouent un rôle fondamental dans d'autres applications de l'algèbre, en Géométrie Algébrique par exemple. Enfin la généralisation des anneaux nœthériens aux modules de même nom est un nouveau cas de « linéarisation », méthode dont le lecteur a déjà constaté l'efficacité.

3.1. Modules et anneaux nœthériens

On a démontré au chap. I, § 4, th. 1 le résultat suivant :

Théorème 1. *Soient* A *un anneau, et* M *un* A*-module. Les conditions suivantes sont équivalentes.*

a) *Toute famille non vide de sous-modules de* M *possède un élément maximal.*

b) *Toute suite croissante de sous-modules de* M *est stationnaire.*

c) *Tout sous-module de* M *est de type fini.*

Définition 1. *Un* A*-module* M *est dit nœthérien s'il satisfait aux conditions équivalentes du th.* 1. *Un anneau* A *est dit nœthérien si, considéré comme* A*-module, c'est un module nœthérien.*

On a vu (chap. I, § 4, cor. du th. 1) qu'un anneau principal est nœthérien.

Proposition 1. *Soient* A *un anneau,* E *un* A*-module, et* E′ *un sous-module de* E. *Pour que* E *soit nœthérien, il faut et il suffit que* E′ *et* E/E′ *soient nœthériens.*

Démontrons la nécessité. Supposons E nœthérien. L'ensemble ordonné des sous-modules de E' (resp. de E/E') est isomorphe à l'ensemble ordonné des sous-modules de E contenus dans E' (resp. contenant E'). Ainsi E' et E/E' sont nœthériens par *a*) ou *b*).

Réciproquement, supposons E' et E/E' nœthériens. Soit $(F_n)_{n \geqslant 0}$ une suite croissante de sous-modules de E. Comme E' est nœthérien, il existe un entier n_0 tel que $F_n \cap E' = F_{n+1} \cap E'$ pour tout $n \geqslant n_0$. Comme E/E' est nœthérien, il existe un entier n_1 tel que

$$(F_n + E')/E' = (F_{n+1} + E')/E' \text{ pour tout } n \geqslant n_1;$$

alors on a $F_n + E' = F_{n+1} + E'$. Prenons $n \geqslant \sup(n_0, n_1)$, et montrons qu'on a $F_n = F_{n+1}$; il suffit de voir que $F_{n+1} \subset F_n$. Soit donc $x \in F_{n+1}$; comme $F_{n+1} + E' = F_n + E'$, il existe $y \in F_n$ et $z', z'' \in E'$ tels que $x + z' = y + z''$; alors $x - y = z'' - z' \in F_{n+1} \cap E'$; or $F_{n+1} \cap E' = F_n \cap E'$; on a donc $x - y \in F_n$, d'où $x \in F_n$ car $y \in F_n$. Ainsi $F_{n+1} = F_n$ pour tout $n \geqslant \sup(n_0, n_1)$, et E est nœthérien d'après *b*).

Corollaire 1. *Soient* A *un anneau,* $E_1, \ldots, E_n$ *des* A-*modules nœthériens. Alors le* A-*module produit* $\prod_{i=1}^{n} E_i$ *est nœthérien.*

Pour $n = 2$, E_1 s'identifie au sous-module $E_1 \times (0)$ de $E_1 \times E_2$, et le quotient correspondant est isomorphe à E_2; d'où notre assertion par la prop. 1. Le cas général s'ensuit par récurrence sur n.

Corollaire 2. *Soient* A *un anneau nœthérien et* E *un* A-*module de type fini. Alors* E *est un* A-*module nœthérien* (*et donc tous ses sous-modules sont de type fini*).

En effet (chap. I, § 4), E est isomorphe à un module quotient A^n/R (n étant le cardinal d'un système générateur fini de E). Or A^n est nœthérien par le cor. 1, et A^n/R aussi par la prop. 1.

3.2. Application aux éléments entiers

Proposition 1. *Soient* A *un anneau nœthérien intégralement clos,* K *son corps des fractions,* L *une extension de degré fini* n *de* K, *et* A' *la fermeture intégrale de* A *dans* L. *On suppose* K *de caractéristique* 0. *Alors* A' *est un* A-*module de type fini et un anneau nœthérien.*

En effet on sait que A' est un sous-module d'un A-module libre de rang n (chap. II, § 7, th. 1). Donc A' est une A-module de type fini (§ 1, cor. 2 de la prop. 1), et donc nœthérien (ibid). D'autre part les idéaux de A' sont des cas particuliers de sous-A-modules de A'; ils satisfont donc à la condition maximale (§ 1, th. 1, *a*), de sorte que A' est un anneau nœthérien.

Exemple. L'anneau des entiers d'un corps de nombres L est *nœthérien* (prendre $A = \mathbf{Z}$, $K = \mathbf{Q}$).

3.3. Quelques préliminaires sur les idéaux

Un idéal $\mathfrak{p}$ d'un anneau A est dit *premier* si l'anneau quotient $A/\mathfrak{p}$ est *intègre*. Il revient au même de dire que les relations $x \in A - \mathfrak{p}$, $y \in A - \mathfrak{p}$ impliquent $xy \in A - \mathfrak{p}$, ou encore que le complémentaire $A - \mathfrak{p}$ de $\mathfrak{p}$ est stable pour la multiplication.

Pour qu'un idéal $\mathfrak{m}$ de A soit *maximal* (c'est-à-dire maximal parmi les idéaux de A distincts de A), il faut et il suffit que $A/\mathfrak{m}$ n'ait d'autres idéaux que lui-même et (0), c'est-à-dire que $A/\mathfrak{m}$ soit un *corps*. Ainsi *tout idéal maximal est premier*. La réciproque est fausse, car l'idéal (0) de $\mathbf{Z}$ est premier et non maximal.

LEMME 1. *Soient* A *un anneau,* $\mathfrak{p}$ *un idéal premier de* A *et* A' *un sous-anneau de* A. *Alors* $\mathfrak{p} \cap A'$ *est un idéal premier de* A'

En effet $\mathfrak{p} \cap A'$ est le noyau de l'homomorphisme composé $A' \to A \to A/\mathfrak{p}$, de sorte qu'on a un homomorphisme injectif $A'/\mathfrak{p} \cap A' \to A/\mathfrak{p}$. Or un sous-anneau d'un anneau intègre est intègre.

Étant donnés deux idéaux $\mathfrak{a}$ et $\mathfrak{b}$ d'un anneau A, on appelle *produit* de $\mathfrak{a}$ et de $\mathfrak{b}$, et on note $\mathfrak{a}\mathfrak{b}$, non pas l'ensemble des produits ab où $a \in \mathfrak{a}$ et $b \in \mathfrak{b}$ (ensemble qui n'est pas en général un idéal), mais l'ensemble des *sommes finies* $\Sigma a_i b_i$ de tels produits. On voit aussitôt que $\mathfrak{a}\mathfrak{b}$ est un *idéal* de A, et qu'on a

1. $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$

Il n'y a pas toujours égalité : dans un anneau principal le membre de gauche correspond au produit, et celui de droite au ppcm.

Le produit des idéaux est associatif et commutatif, et A est élément neutre.

Étant donnés un A module E, un sous-module F, et un idéal $\mathfrak{a}$ de A, on définit de même le produit $\mathfrak{a}F$; c'est un sous-module de E.

LEMME 2. *Si un idéal premier* $\mathfrak{p}$ *d'un anneau* A *contient un produit* $\mathfrak{a}_1 \mathfrak{a}_2 \ldots \mathfrak{a}_n$ *d'idéaux, alors* $\mathfrak{p}$ *contient l'un d'eux.*

En effet si $\mathfrak{a}_i \not\subset \mathfrak{p}$ pour tout i, il existe $a_i \in \mathfrak{a}_i$ tel que $a_i \notin \mathfrak{p}$. On a alors $a_1 \ldots a_n \notin \mathfrak{p}$ vu que $\mathfrak{p}$ est premier. Or $a_1 \ldots a_n \in \mathfrak{a}_1 \ldots \mathfrak{a}_n$. Contradiction.

LEMME 3. *Dans un anneau nœthérien, tout idéal contient un produit d'idéaux premiers. Dans un anneau nœthérien intègre* A, *tout idéal non nul contient un produit d'idéaux premiers non nuls.*

Nous allons employer un raisonnement assez typique dans la théorie des anneaux nœthériens. Démontrons la seconde assertion (la démonstration de la première est analogue : il suffit de barrer trois fois « non nuls »). Raisonnons par l'absurde. La famille Φ des idéaux non nuls de A qui ne contiennent aucun produit d'idéaux premiers non nuls, est alors *non vide*. Comme A est nœthérien, Φ admet un élément *maximal* $\mathfrak{b}$ (§ 1, th. 1, *a*). L'idéal $\mathfrak{b}$ n'est pas premier, sinon il contiendrait le produit de la famille réduite à $\mathfrak{b}$. Il existe donc $x, y \in A - \mathfrak{b}$ tels que $xy \in \mathfrak{b}$. Alors les idéaux $\mathfrak{b} + Ax$ et $\mathfrak{b} + Ay$ contiennent strictement $\mathfrak{b}$, donc n'appartiennent pas à Φ vu le caractère maximal de $\mathfrak{b}$ dans Φ. Ils contiennent donc des produits d'idéaux premiers non nuls :

$$\mathfrak{b} + Ax \supset \mathfrak{p}_1 \ldots \mathfrak{p}_n, \qquad \mathfrak{b} + Ay \supset \mathfrak{q}_1, \ldots \mathfrak{q}_r$$

Or, comme $xy \in \mathfrak{b}$, on a

$$(\mathfrak{b} + Ax)(\mathfrak{b} + Ay) \subset \mathfrak{b}; \qquad \text{d'où} \qquad \mathfrak{p}_1 \ldots \mathfrak{p}_n \mathfrak{q}_1 \ldots \mathfrak{q}_r \subset \mathfrak{b},$$

contradiction.

Enfin soient A un anneau *intègre* et K son corps des fractions. On appelle *idéal fractionnaire* de A (ou de K par rapport à A) tout sous A-module I de K tel qu'il existe de $d \in A$, $d \neq 0$ satisfaisant à $I \subset d^{-1}A$; ceci revient à dire que les éléments de I ont un « dénominateur commun » $d \in A$. Les idéaux ordinaires de A sont des idéaux fractionnaires (avec $d = 1$); on les qualifie parfois d'*idéaux entiers* s'il y a risque de confusion. Tout sous A-module *de type fini* I de K est un idéal fractionnaire; en effet, si $(x_1, \ldots, x_n)$ est un système générateur fini de I, les x_i ont un dénominateur commun d (par exemple le produit des dénominateurs d_i, où $x_i = a_i d_i^{-1}$ avec a_i, $d_i \in A$), et d sert de dénominateur commun à I. Réciproquement, si A est *nœthérien*, tout idéal fractionnaire I est un A-module de *type fini* : en effet on a $I \subset d^{-1}A$, et $d^{-1}A$ est un A-module isomorphe à A, donc nœthérien.

On définit le *produit* II' de deux idéaux fractionnaires I, I' comme l'ensemble des sommes finies $\Sigma x_i y_i$ où $x_i \in I$ et $y_i \in I'$. Si I et I' sont deux idéaux fractionnaires, de dénominateurs communs d et d', alors les ensembles

$$I \cap I', \qquad I + I', \qquad II'$$

sont des *idéaux fractionnaires*; en effet ce sont évidemment des sous A-modules de K, et ils admettent respectivement pour dénominateurs communs d(ou d'), dd' et dd'. Les idéaux fractionnaires non nuls de A forment un *monoïde* commutatif pour la multiplication.

3.4. Anneaux de Dedekind

DÉFINITION 1. *Un anneau* A *est appelé un anneau de Dedekind s'il est nœthérien et intégralement clos* (*donc intègre*), *et si tout idéal premier non nul de* A *est maximal.*

L'anneau $\mathbf{Z}$, et plus généralement tout anneau principal, est un anneau de Dedekind. L'anneau des entiers d'un corps de nombres est un anneau de Dedekind, d'après le théorème suivant :

THÉORÈME 1. *Soient* A *un anneau de Dedekind,* K *son corps des fractions,* L *une extension de degré fini de* K *et* A′ *la fermeture intégrale de* A *dans* L. *On suppose* K *de caractéristique* 0. *Alors* A′ *est un anneau de Dedekind et un* A-*module de type fini.*

En effet A′ est intégralement clos par construction, nœthérien et A-module de type fini d'après la prop. du § 2. Reste à montrer que tout idéal premier $\mathfrak{p}' \neq (0)$ de A′ est maximal. Or prenons un élément $x \neq 0$ de $\mathfrak{p}'$ et une équation de dépendance intégrale de x sur A, de degré minimum :

1. $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0 \qquad (a_i \in \mathrm{A})$

On a $a_0 \neq 0$, car sinon on simplifierait par x, et on obtiendrait une équation de dépendance intégrale de degré $n - 1$. Par (1) on a, $a_0 \in \mathrm{A}'x \cap \mathrm{A} \subset \mathfrak{p}' \cap \mathrm{A}$; on a donc $\mathfrak{p}' \cap \mathrm{A} \neq (0)$. Or $\mathfrak{p}' \cap \mathrm{A}$ est un idéal premier de A (§ 3, lemme 1); donc $\mathfrak{p}' \cap \mathrm{A}$ est un idéal maximal de A, et $\mathrm{A}/\mathfrak{p}' \cap \mathrm{A}$ est un corps. Mais $\mathrm{A}/\mathfrak{p}' \cap \mathrm{A}$ s'identifie à un sous-anneau de $\mathrm{A}'/\mathfrak{p}'$, et $\mathrm{A}'/\mathfrak{p}'$ est *entier* sur $\mathrm{A}/\mathfrak{p}' \cap \mathrm{A}$ car A′ est entier sur A. Donc $\mathrm{A}'/\mathfrak{p}'$ est un corps (chap. II, § 1, prop. 3), de sorte que $\mathfrak{p}'$ est maximal. CQFD.

L'intérêt des anneaux de Dedekind vient de ce que l'anneau des entiers d'un corps de nombres est un anneau de Dedekind, mais n'est pas toujours principal.

Exemple. Considérons l'anneau des entiers $\mathrm{A} = \mathbf{Z}[\sqrt{-5}]$ de $\mathbf{Q}[\sqrt{-5}]$ (chap. II, § 5, th. 1). On a

2. $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 2.3.$

Les normes des quatre facteurs sont respectivement 6, 6, 4 et 9; or $1 + \sqrt{-5}$ ne peut avoir de diviseur non-trivial dans A, car la norme d'un tel diviseur devrait être un diviseur non-trivial de 6, et que les équations

$$a^2 + 5b^2 = 2 \qquad \text{et} \qquad a^2 + 5b^2 = 3$$

n'ont pas de solution dans $\mathbf{Z}$. Si A était principal, l'élément $1 + \sqrt{-5}$, qui divise le produit 2.3 par (1), devrait diviser l'un de ses facteurs; mézalor, en prenant les normes, 6 diviserait 4 ou 9, ce qui n'est pas.

Historiquement, l'arithméticien Kummer (1810-1893) s'aperçut de la non principalité de certains anneaux d'entiers de corps de nombres (en fait, de corps cyclotomiques, ceci en liaison avec ses travaux sur l'équation de Fermat; cf. I, § 2). Pour obvier partiellement à cet inconvénient, lui et Dedekind (1831-1916) introduisirent la notion d'*idéal*, et Dedekind étudia les anneaux qui portent maintenant son nom. L'intérêt majeur des anneaux principaux est l'unique décomposition en facteurs premiers. Dans les anneaux de Dedekind celle-ci est heureusement généralisée en une unique décomposition en *idéaux premiers*, qui rend presque autant de services, et que nous allons maintenant décrire :

THÉORÈME 2. *Soit* A *un anneau de Dedekind qui n'est pas un corps. Tout idéal maximal de* A *est inversible dans le monoïde des idéaux fractionnaires de* A.

Soit $\mathfrak{m}$ un idéal maximal de A; on a $\mathfrak{m} \neq (0)$ car A n'est pas un corps. Posons

3. $\mathfrak{m}' = \{x \in \mathrm{K} | x\mathfrak{m} \subset \mathrm{A}\}$

Il est clair que $\mathfrak{m}'$ est un sous A-module de K, et qu'il admet pour dénominateur commun n'importe quel élément non nul de $\mathfrak{m}$; donc $\mathfrak{m}'$ est un idéal fractionnaire de A. Il va nous suffire de montrer que $\mathfrak{m}'\mathfrak{m} = \mathrm{A}$. Or on a $\mathfrak{m}'\mathfrak{m} \subset \mathrm{A}$ d'après (3); d'autre part il est clair que $\mathrm{A} \subset \mathfrak{m}'$ (car $\mathfrak{m}$ est un idéal), d'où $\mathfrak{m} = \mathrm{A}\mathfrak{m} \subset \mathfrak{m}'\mathfrak{m}$. Comme $\mathfrak{m}$ est maximal et que $\mathfrak{m} \subset \mathfrak{m}'\mathfrak{m} \subset \mathrm{A}$; on a soit $\mathfrak{m}'\mathfrak{m} = \mathrm{A}$, soit $\mathfrak{m}'\mathfrak{m} = \mathfrak{m}$. Reste à montrer que $\mathfrak{m}'\mathfrak{m} = \mathfrak{m}$ est impossible.

Or, si $\mathfrak{m}'\mathfrak{m} = \mathfrak{m}$ et si $x \in \mathfrak{m}'$, on a $x\mathfrak{m} \subset \mathfrak{m}$, d'où $x^2\mathfrak{m} \subset x\mathfrak{m} \subset \mathfrak{m}$, et $x^n\mathfrak{m} \subset \mathfrak{m}$ pourtant $n \in \mathbf{N}$ par récurrence. Ainsi n'importe quel élément non nul d de $\mathfrak{m}$ sert de dénominateur commun à tous les x^n, de sorte que $\mathrm{A}[x]$ est un idéal fractionnaire de A. Comme A est nœthérien, $\mathrm{A}[x]$ est un A-module de type fini (§ 3, fin), donc x est *entier* sur A (chap. II, § 1, th. 1). Or A est intégralement clos; on a donc $x \in \mathrm{A}$. Ainsi $\mathfrak{m}'\mathfrak{m} = \mathfrak{m}$ implique $\mathfrak{m}' = \mathrm{A}$. Reste à montrer que $\mathfrak{m}' = \mathrm{A}$ est impossible.

En effet prenons un élément non nul $a \in \mathfrak{m}$. L'idéal $\mathrm{A}a$ contient un produit $\mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_n$ d'idéaux premiers non nuls (§ 3, lemme 3); on peut supposer n minimum. On a $\mathfrak{m} \supset \mathrm{A}a \supset \mathfrak{p}_1 \ldots \mathfrak{p}_n$, donc $\mathfrak{m}$ contient l'un des $\mathfrak{p}_i$ (§ 3, lemme 2), $\mathfrak{p}_1$ par exemple. Comme $\mathfrak{p}_1$ est maximal par hypothèse, on a $\mathfrak{m} = \mathfrak{p}_1$. Posons $\mathfrak{b} = \mathfrak{p}_2 \ldots \mathfrak{p}_n$; on a $\mathrm{A}a \supset \mathfrak{m}\mathfrak{b}$, et $\mathrm{A}a \not\supset \mathfrak{b}$ d'après le caractère minimal de n. Il existe donc un élément $b \in \mathfrak{b}$ tel que $b \notin \mathrm{A}a$. Comme $\mathfrak{m}\mathfrak{b} \subset \mathrm{A}a$, on a $\mathfrak{m}b \subset \mathrm{A}a$, d'où $\mathfrak{m}ba^{-1} \subset \mathrm{A}$; d'après la définition (3) de $\mathfrak{m}'$, ceci prouve que $ba^{-1} \in \mathfrak{m}'$. Or, comme $b \notin \mathrm{A}a$, on a $ba^{-1} \notin \mathrm{A}$; d'où $\mathfrak{m}' \neq \mathrm{A}$. CQFD.

THÉORÈME 3. *Soient* A *un anneau de Dedekind,* P *l'ensemble des idéaux premiers non nuls de* A.

a) *Tout idéal fractionnaire non nul* $\mathfrak{b}$ *de* A *s'écrit, d'une façon et d'une seule, sous la forme*

4. $\mathfrak{b} = \prod_{\mathfrak{p} \in P} \mathfrak{p}^{n_\mathfrak{p}(\mathfrak{b})}$

où les $n_\mathfrak{p}(\mathfrak{b})$ *sont des entiers relatifs, presque tous nuls.*

b) *Le monoïde des idéaux fractionnaires non-nuls de* A *est un groupe.*

Démontrons d'abord l'assertion d'*existence* de *a*), c'est-à-dire que tout idéal fractionnaire $\mathfrak{b}$ est produit de puissances ($\geqslant 0$ ou $\leqslant 0$) d'idéaux premiers. Or il existe un élément non nul de A tel que $d\mathfrak{b} \subset A$; i.e. que $d\mathfrak{b}$ soit un idéal entier de A; ainsi $\mathfrak{b} = (d\mathfrak{b}).(Ad)^{-1}$, et nous sommes ramenés au cas d'un idéal entier $\mathfrak{b}$. Procédons comme dans le lemme 3 du § 3, et considérons la famille Φ des idéaux $\neq (0)$ de A qui ne sont pas produits d'idéaux premiers. Supposons, par l'absurde, que Φ soit non vide; elle admet alors un élément maximal $\mathfrak{a}$, car A est nœthérien. On a $\mathfrak{a} \neq A$, car A est produit de la famille vide d'idéaux premiers. Alors $\mathfrak{a}$ est contenu dans un idéal maximal $\mathfrak{p}$, à savoir un élément maximal de la famille des idéaux non triviaux de A qui contiennent $\mathfrak{a}$. Soit $\mathfrak{p}'$ l'idéal (fractionnaire) inverse de $\mathfrak{p}$. De $\mathfrak{a} \subset \mathfrak{p}$ on déduit $\mathfrak{a}\mathfrak{p}' \subset \mathfrak{p}\mathfrak{p}' = A$. Comme $\mathfrak{p}' \supset A$, on a $\mathfrak{a}\mathfrak{p}' \supset \mathfrak{a}$, et même $\mathfrak{a}\mathfrak{p}' \neq \mathfrak{a}$: en effet, si $\mathfrak{a}\mathfrak{p}' = \mathfrak{a}$ et si $x \in \mathfrak{p}'$, on aurait $x\mathfrak{a} \subset \mathfrak{a}$, $x^n\mathfrak{a} \subset \mathfrak{a}$ pour tout n, x entier sur A et $x \in A$ (comme dans le th. 2); or ceci est impossible car $\mathfrak{p}' \neq A$ (sinon $\mathfrak{p}' = A$ et $\mathfrak{p}\mathfrak{p}' = \mathfrak{p}$). D'après le caractère maximal de $\mathfrak{a}$ dans Φ, on a donc $\mathfrak{a}\mathfrak{p}' \notin \Phi$, et $\mathfrak{a}\mathfrak{p}'$ est un produit $\mathfrak{p}_1 \ldots \mathfrak{p}_n$ d'idéaux premiers. En multipliant par $\mathfrak{p}$, on voit que $\mathfrak{a} = \mathfrak{p}\mathfrak{p}_1 \ldots \mathfrak{p}_n$. Ainsi tout idéal entier de A est produit d'idéaux premiers.

Passons à l'assertion d'*unicité* de *a*). Supposons qu'on ait $\prod_{\mathfrak{p} \in P} \mathfrak{p}^{n(\mathfrak{p})} = \prod_{\mathfrak{p} \in P} \mathfrak{p}^{m(\mathfrak{p})}$ c-à-d. $\prod_{\mathfrak{p} \in P} \mathfrak{p}^{n(\mathfrak{p}) - m(\mathfrak{p})} = A$. Si les $n(\mathfrak{p}) - m(\mathfrak{p})$ ne sont pas tous nuls, on sépare les exposants positifs et les exposants négatifs et on obtient :

5. $\mathfrak{p}_1^{\alpha_1} \ldots \mathfrak{p}_r^{\alpha_r} = \mathfrak{q}_1^{\beta_1} \ldots \mathfrak{q}_l^{\beta_l}$

avec $\mathfrak{p}_i, \mathfrak{q}_j \in P$, $\alpha_i > 0$, $\beta_j > 0$, $\mathfrak{p}_i \neq \mathfrak{q}_j$ pour tous i, j. Alors $\mathfrak{p}_1$ contient $\mathfrak{q}_1^{\beta_1} \ldots \mathfrak{q}_l^{\beta_l}$; il contient donc l'un des $\mathfrak{q}_j$ (§ 3, lemme 2), soit $\mathfrak{p}_1 \supset \mathfrak{q}_1$. Comme $\mathfrak{p}_1$ et $\mathfrak{q}_1$ sont tous deux maximaux, ceci implique $\mathfrak{p}_1 = \mathfrak{q}_1$, ce qui est contradictoire.

Enfin (4) montre que $\prod_{\mathfrak{p} \in P} \mathfrak{p}^{-n_\mathfrak{p}(\mathfrak{b})}$ est l'inverse de $\mathfrak{b}$, ce qui prouve *b*).

Remarque. On vient de voir que le monoïde $I(A)$ des idéaux fractionnaires non nuls d'un anneau de Dedekind A est un groupe. Or les idéaux fractionnaires *principaux* (c.-à.-d. de la forme Ax, $x \in K^*$) forment un sous-groupe $F(A)$ de $I(A)$ (car $(Ax).(Ay)^{-1} = Axy^{-1}$). Le groupe quotient $C(A) = I(A)/F(A)$ s'appelle le *groupe des classes d'idéaux* de A. Pour que A soit principal, il faut et il suffit que $C(A)$ soit réduit à son élément neutre.

Terminons par un *formulaire*, dans lequel $n_\mathfrak{p}(\mathfrak{b})$ désigne d'exposant de $\mathfrak{p}$ dans la décomposition de $\mathfrak{b}$ en produit d'idéaux premiers (cf. (4)).

6. $n_{\mathfrak{p}}(\mathfrak{a}\mathfrak{b}) = n_{\mathfrak{p}}(\mathfrak{a}) + n_{\mathfrak{p}}(\mathfrak{b})$ (trivial)

7. $\mathfrak{b} \subset A \Longleftrightarrow n_{\mathfrak{p}}(\mathfrak{b}) \geqslant 0$ pour tout $\mathfrak{p} \in P$
($\Longrightarrow$ vu en cours de démonstration du th. 4; $\Longleftarrow$ trivial)

8. $\mathfrak{a} \subset \mathfrak{b} \Longleftrightarrow n_{\mathfrak{p}}(\mathfrak{a}) \geqslant n_{\mathfrak{p}}(\mathfrak{b})$ pour tout $\mathfrak{p} \in P$.
(en effet $\mathfrak{a} \subset \mathfrak{b}$ équivaut à $\mathfrak{a}\mathfrak{b}^{-1} \subset A$; on applique alors (6) et (7))

9. $n_{\mathfrak{p}}(\mathfrak{a} + \mathfrak{b}) = \inf\,(n_{\mathfrak{p}}(\mathfrak{a}),\ n_{\mathfrak{p}}(\mathfrak{b}))$
(car $\mathfrak{a} + \mathfrak{b}$ est la borne supérieure de $\mathfrak{a}$ et $\mathfrak{b}$ pour l'inclusion des idéaux; on applique alors (8))

10. $n_{\mathfrak{p}}(\mathfrak{a} \cap \mathfrak{b}) = \sup\,(n_{\mathfrak{p}}(\mathfrak{a}),\ n_{\mathfrak{p}}(\mathfrak{b}))$
(raison analogue; attention au renversement des inégalités dans (8))

3.5. Norme d'un idéal

Dans tout ce §, K *désigne un corps de nombres,* n *son degré, et* A *l'anneau des entiers de* K. On écrit $N(x)$ au lieu de $N_{K/Q}(x)$.

PROPOSITION 1. *Si* x *est un élément non nul de* A, *on a* $|N(x)| = \text{card}\,(A/Ax)$

Notons que, comme $x \in A$, on a $N(x) \in \mathbf{Z}$ (chap. II, § 6, cor. de la prop. 2), de sorte que la formule écrite a un sens.

On sait que A est un $\mathbf{Z}$-module libre de rang n (chap. II, § 8), et Ax un sous $\mathbf{Z}$-module de A. Il est aussi de rang n car la multiplication par x est une bijection $A \to Ax$. D'après le chap. I, § 5, th. 1, il existe une base $(e_1, \ldots, e_n)$ du $\mathbf{Z}$-module A, et des éléments c_i de $\mathbf{N}$ tels que $(c_1e_1, \ldots, c_ne_n)$ soit une base de Ax. Alors A/Ax est isomorphe à $\prod_{i=1}^{n} \mathbf{Z}/c_i\mathbf{Z}$, et son cardinal est $c_1c_2 \ldots c_n$. Notons u l'application $\mathbf{Z}$-linéaire de A sur Ax définie par $u(e_i) = c_ie_i$ pour $i = 1, \ldots, n$; on a $\det(u) = c_1c_2 \ldots c_n$.
D'autre part $(xe_1, \ldots, xe_n)$ est aussi une base de Ax; on a donc un automorphisme v du $\mathbf{Z}$-module Ax tel que $v(c_ie_i) = xe_i$; alors $\det(v)$ est inversible dans $\mathbf{Z}$, d'où $\det(v) = \pm 1$. Mézalor $v \circ u$ est la multiplication par x, et son déterminant est, par définition, $N(x)$ (chap. II, § 6, déf. 1). Comme $\det(v \circ u) = \det(v).\det(u)$; on en déduit

$N(x) = \pm\, c_1c_2 \ldots c_n = \pm\, \text{card}\,(A/Ax)$. CQFD.

DÉFINITION 1. *Étant donné un idéal entier non nul* $\mathfrak{a}$ *de* A, *on appelle norme de* $\mathfrak{a}$ *et on note* $N(\mathfrak{a})$ *le nombre* $\text{card}\,(A/\mathfrak{a})$.

Notons que $N(\mathfrak{a})$ est *fini*; en effet, si a est un élément non nul de a, on a $Aa \subset \mathfrak{a}$, et $A/\mathfrak{a}$ s'identifie à un quotient de A/Aa; d'où $\text{card}\,(A/\mathfrak{a}) \leqslant \text{card}\,(A/Aa)$, qui est fini par la prop. 1. D'autre part celle-ci montre que, pour un idéal principal Ab, on a $N(Ab) = |N(b)|$.

PROPOSITION 2. *Si* $\mathfrak{a}$ *et* $\mathfrak{b}$ *sont deux idéaux entiers non nuls de* A, *on a* $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$.

Par décomposition de $\mathfrak{b}$ en produit d'idéaux maximaux (§ 4, th. 3), il suffit de montrer qu'on a $N(\mathfrak{a}\mathfrak{m}) = N(\mathfrak{a})N(\mathfrak{m})$ pour $\mathfrak{m}$ maximal. Comme $\mathfrak{a}\mathfrak{m} \subset \mathfrak{a}$, on a card $(A/\mathfrak{a}\mathfrak{m})$ = card $(A/\mathfrak{a})$ card $(\mathfrak{a}/\mathfrak{a}\mathfrak{m})$. Il suffit donc de prouver card $(\mathfrak{a}/\mathfrak{a}\mathfrak{m})$ = card $(A/\mathfrak{m})$. Or $\mathfrak{a}/\mathfrak{a}\mathfrak{m}$ est un A-module annulé par $\mathfrak{m}$, donc un espace vectoriel sur $A/\mathfrak{m}$. Ses sous-espaces vectoriels sont ses sous-A-modules, et sont donc de la forme $\mathfrak{q}/\mathfrak{a}\mathfrak{m}$ où $\mathfrak{q}$ est un idéal tel que $\mathfrak{a}\mathfrak{m} \subset \mathfrak{q} \subset \mathfrak{a}$. Or la formule (8) du § 4 montre qu'il n'a aucun idéal strictement compris entre $\mathfrak{a}\mathfrak{m}$ et $\mathfrak{a}$. Donc l'espace vectoriel $\mathfrak{a}/\mathfrak{a}\mathfrak{m}$ est de dimension un sur $A/\mathfrak{m}$. On a donc bien card $(\mathfrak{a}/\mathfrak{a}\mathfrak{m})$ = card $(A/\mathfrak{m})$. CQFD.

Classes d'idéaux Théorème des unités

Le présent chapitre est consacré à deux importants théorèmes de finitude. Quelques outils d'Analyse (empruntés à la Topologie et à l'intégration dans $\mathbf{R}^n$) nous seront utiles.

4.1. Préliminaires sur les sous-groupes discrets de $\mathbf{R}^n$

Un sous-groupe additif H de $\mathbf{R}^n$ est discret si et seulement si, pour tout compact K de $\mathbf{R}^n$, l'intersection $H \cap K$ est finie. Un exemple typique de sous-groupe discret de $\mathbf{R}^n$ est $\mathbf{Z}^n$. Nous allons montrer que c'est à peu près le seul :

THÉORÈME 1. *Soit* H *un sous-groupe discret de* $\mathbf{R}^n$. *Alors* H *est engendré* (*comme* $\mathbf{Z}$-*module*) *par* r *vecteurs linéairement indépendants sur* $\mathbf{R}$ (*d'où* $r \leqslant n$).

Choisissons, en effet, un système $(e_1, \ldots, e_r)$ d'éléments de H qui sont linéairement indépendants sur $\mathbf{R}$ et tels que r soit maximum. Soit

$$1. \quad P = \left\{ \sum_{i=1}^{r} \alpha_i e_i \mid 0 \leqslant \alpha_i \leqslant 1 \right\} \subset \mathbf{R}^n$$

le parallélotope construit sur ces vecteurs; il est clair que P est compact, donc que $P \cap H$ est fini. Soit alors $x \in H$. Vu le caractère maximal de (e_i), x s'écrit $x = \sum_{i=1}^{r} \lambda_i e_i$ avec $\lambda_i \in \mathbf{R}$. Considérons alors, pour $j \in \mathbf{Z}$, l'élément

$$2. \quad x_j = jx - \sum_{i=1}^{r} [j\lambda_i] e_i$$

(où $[\mu]$ désigne la partie entière de $\mu \in \mathbf{R}$). On a alors

$$x_j = \sum_{i=1}^{r} (j\lambda_i - [j\lambda_i]) e_i,$$

d'où $x_j \in P$, et $x_j \in P \cap H$ par 2. Si l'on remarque que $x = x_1 + \sum_{i=1}^{r} [\lambda_i] e_i$, on voit que le $\mathbf{Z}$-module H est engendré par $P \cap H$, et est donc *de type fini*.

D'autre part, comme $P \cap H$ est fini et $\mathbf{Z}$ infini, il existe deux entiers distincts j et k tels que $x_j = x_k$. Il résulte alors de (2) que, pour ces entiers, on a $(j-k)\lambda_i = [j\lambda_i] - [k\lambda_i]$, ce qui montre que les λ_i sont *rationnels*. Ainsi le $\mathbf{Z}$-module H est engendré par un nombre *fini* d'éléments, qui sont combinaisons linéaires à coefficients rationnels des (e_i). Soit d un dénominateur commun ($d \in \mathbf{Z}$, $d \neq 0$) de ces coefficients ; on a alors $d\mathrm{H} \subset \sum_{i=1}^{r} \mathbf{Z} e_i$. Ainsi il existe une base (f_i) du $\mathbf{Z}$-module $\sum_{i=1}^{r} \mathbf{Z}\, e_i$ et des $\alpha_i \in \mathbf{Z}$ tels que $(\alpha_1 f_1, \ldots, \alpha_r f_r)$ engendrent $d\mathrm{H}$ (chap. I, § 5, th. 1). Comme le $\mathbf{Z}$-module $d\mathrm{H}$ a même rang que H et que $\mathrm{H} \supset \sum_{i=1}^{r} \mathbf{Z} e_i$, le rang de $d\mathrm{H}$ est $\geqslant r$; il est donc égal à r et les α_i sont non-nuls. Or les (f_i) sont, comme les (e_i), linéairement indépendants sur $\mathbf{R}$. Donc $d\mathrm{H}$, et par conséquent H, est engendré (sur $\mathbf{Z}$) par r éléments linéairement indépendants sur $\mathbf{R}$.

Exemple d'application. Soit $t = (\theta_1, \ldots, \theta_n) \in \mathbf{R}^n$ tel que l'un au moins des θ_i soit *irrationnel*. Notons $(e_1, \ldots, e_n)$ la base canonique de $\mathbf{R}^n$, et H le sous-groupe de $\mathbf{R}^n$ engendré sur $\mathbf{Z}$ par $(e_1, \ldots, e_n, t)$. Il n'est pas discret sinon, d'après la démonstration du th. 1, t serait combinaison linéaire rationnelle des e_i. Donc, $\varepsilon > 0$ étant donné, il existe un élément non nul de H qui approche 0 à ε près ; donc il existe des entiers $p_i \in \mathbf{Z}$, $q \in \mathbf{N}$, $q \neq 0$ tels que $|q\theta_i - p_i| \leqslant \varepsilon$, donc que $\left|\theta_i - \frac{p_i}{q}\right| \leqslant \frac{\varepsilon}{q}$. Notons que l'intercalation simplette de θ_i entre deux multiples consécutifs de $\frac{1}{q}$ donnerait seulement l'approximation $\left|\theta_i - \frac{n_i}{q}\right| \leqslant \frac{1}{2q}$ ($n_i \in \mathbf{Z}$). Ce que nous venons d'exposer est un des premiers résultats de la très riche théorie de l'approximation des nombres irrationnels par des nombres rationnels ; pour plus de détails sur cette théorie, voir Koksma, « Diophantische Approximationen », Berlin (Springer), 1936.

DÉFINITION 1. *Un sous-groupe discret de rang n de $\mathbf{R}^n$ est appelé un réseau de $\mathbf{R}^n$.*

D'après le th. 1, un réseau est engendré sur $\mathbf{Z}$ par une base de $\mathbf{R}^n$, qui est alors une $\mathbf{Z}$-base dudit réseau. Pour chaque $\mathbf{Z}$-base $e = (e_1, \ldots, e_n)$ d'un réseau H, on désignera par P_e le parallélotope semi-ouvert $\mathrm{P}_e = \left\{ \sum_{i=1}^{n} \alpha_i e_i \mid 0 \leqslant \alpha_i < 1 \right\}$; ainsi tout point de $\mathbf{R}^n$ est congru modulo

H à un point et un seul de P_e (on dit alors que P_e est un *domaine fondamental* pour H). Nous noterons μ la *mesure de Lebesgue* dans $\mathbf{R}^n$; ainsi, pour toute partie intégrable S de $\mathbf{R}^n$, $\mu(S)$ désignera sa mesure (que nous appellerons aussi son volume).

LEMME 1. *Le volume* $\mu(P_e)$ *est indépendant de la base* e *choisie pour* H.

En effet, soit $f = (f_1, \ldots, f_n)$ une autre base de H. On a $f_i = \sum_{j=1}^{n} \alpha_{ij} e_j$ avec $\alpha_{ij} \in \mathbf{Z}$. L'effet bien connu d'une transformation linéaire sur les volumes montre qu'on a $\mu(P_f) = |\det(\alpha_{ij})|\mu(P_e)$. Or, comme c'est un déterminant de changement de base, $\det(\alpha_{ij})$ est inversible dans $\mathbf{Z}$, donc vaut ± 1. Ainsi $\mu(P_f) = \mu(P_e)$. CQFD.

Le volume de l'un quelconque des P_e est appelé *le volume du réseau* H et est noté $v(H)$ (le mot « volume » est ici un abus de langage, car $\mu(H) = 0$; peut-être vaudrait-il mieux dire « maille » du réseau H ?).

THÉORÈME 2 (Minkowski). *Soient* H *un réseau de* $\mathbf{R}^n$ *et* S *un sous-ensemble intégrable de* $\mathbf{R}^n$ *tels que* $\mu(S) > v(H)$. *Il existe alors deux éléments* x, y *de* S *distincts tels que* $x - y \in H$.

En effet, soient $e = (e_1, \ldots, e_n)$ une $\mathbf{Z}$-base de H, et P_e le parallélotope semi-ouvert construit sur e. Comme P_e est un domaine fondamental pour H, S est la réunion disjointe des $S \cap (h + P_e)$ $(h \in H)$; d'où

3. $\mu(S) = \sum_{h \in H} \mu(S \cap (h + P_e))$

Comme μ est invariante par translation, on a

$$\mu(S \cap (h + P_e)) = \mu((-h + S) \cap P_e)$$

Or les ensembles $(-h + S) \cap P_e$ $(h \in H)$ ne peuvent être deux à deux disjoints car, sinon, $\mu(P_e) \geqslant \sum_{h \in H} \mu((-h + S) \cap P_e)$, contrairement à (3) et à l'hypothèse $\mu(P_e) = v(H) < \mu(S)$. Il existe donc deux éléments distincts h, h' de H tels que $P_e \cap (-h + S) \cap (-h' + S) \neq \emptyset$. On a donc des éléments x, y de S tels que $-h + x = -h' + y$, d'où $x - y = h - h' \in H$, et $x \neq y$ car $h \neq h'$. CQFD.

COROLLAIRE. *Soient* H *un réseau de* $\mathbf{R}^n$, *et* S *une partie intégrable, symétrique par rapport à* 0 *et convexe de* $\mathbf{R}^n$. *On suppose qu'une des relations suivantes est vraie :*

a) on a $\mu(S) > 2^n v(H)$

b) on a $\mu(S) \geqslant 2^n v(H)$ *et* S *est compacte.*

Alors $S \cap H$ *contient un point autre que* 0.

Dans le cas a), on applique le th. 1 à

$$S' = \frac{1}{2} S \left(\text{car } \mu(S') = \frac{1}{2^n} \mu(S) > v(H) \right);$$

il existe deux points distincts z, y de S' tels que $y - z \in H$; alors $x = y - z = \frac{1}{2}(2y + (-2z))$ est un point de S (car S est symétrique et convexe), qui répond à la question. Dans le cas b), on applique le cas a) à $(1 + \varepsilon)S$ $(\varepsilon > 0)$; en posant $H' = H - \{0\}$, on voit $H' \cap (1 + \varepsilon)S$ est non vide, et est fini car compact et discret. Alors $\bigcap_{\varepsilon > 0} H' \cap (1 + \varepsilon)S$ est non vide; un élément de cette intersection appartient à $\bigcap_{\varepsilon > 0} (1 + \varepsilon)S$, ensemble qui est égal à S vu que S est compact. CQFD.

L'hypothèse de compacité est nécessaire dans b), comme le montrent le parallélotope ouvert $\left\{ \sum_{i=1}^{n} \lambda_i e_i \,\middle|\, -1 < \lambda_i < +1 \right\}$ et le réseau de base (e_i).

4.2. Le plongement canonique d'un corps de nombres

Soient K un corps de nombres et n son degré. On a vu (chap. II, § 4, th. 1) qu'on a n isomorphismes distincts $\sigma_i : K \to \mathbf{C}$. On en a exactement n, car le polynôme minimal d'un élément primitif de K sur $\mathbf{Q}$ (*ibid.*, cor. du th. 1) n'a que n racines dans $\mathbf{C}$. Soit $\alpha : \mathbf{C} \to \mathbf{C}$ le passage au nombre complexe conjugué; alors, pour tout i, $\alpha \circ \sigma_i$ est l'un des σ_j, et est égal à σ_i si et seulement si $\sigma_i(K) \subset \mathbf{R}$. Notons r_1, le nombre des indices i tels que $\sigma_i(K) \subset \mathbf{R}$; alors les autres indices sont en nombre *pair* $2r_2$, et on a

1. $r_1 + 2r_2 = n$.

Nous numéroterons les σ_i de sorte que $\sigma_i(K) \subset \mathbf{R}$ pour $1 \leqslant i \leqslant r_1$ et que $\sigma_{j+r_2}(x) = \overline{\sigma_j(x)}$ pour $r_1 + 1 \leqslant j \leqslant r_1 + r_2$; ainsi les $r_1 + r_2$ premiers σ_i déterminent les r_2 autres. Pour $x \in K$, nous poserons ;

2. $\sigma(x) = (\sigma_1(x), \ldots, \sigma_{r_1+r_2}(x)) \in \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$

Nous appellerons σ le *plongement canonique* de K dans $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$; c'est un homomorphisme injectif pour les structures d'anneaux. Nous identifierons souvent $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ à $\mathbf{R}^n$ (cf. (1)). Les notations σ, K, n, r_1, r_2 seront utilisées dans toute la suite de ce §.

PROPOSITION 1. *Si* M *est un sous-*$\mathbf{Z}$*-module libre de rang* n *de* K, *et si* $(x_i)_{1 \leqslant i \leqslant n}$ *est une* $\mathbf{Z}$*-base de* M, *alors* $\sigma(M)$ *est un réseau de* $\mathbf{R}^n$, *dont le volume est donné par*

3. $v(\sigma(M)) = 2^{-r_2} \left| \det_{1 \leqslant i,j \leqslant n} (\sigma_i(x_j)) \right|$

En effet, pour i fixé, les composantes de $\sigma(x_i)$ par rapport à la base canonique de $\mathbf{R}^n$ sont données par

$$4. \quad \sigma_1(x_i), \ \ldots, \ \sigma_{r_1}(x_i), \ R(\sigma_{r_1+1}(x_i)), \ I(\sigma_{r_1+1}(x_i)), \ \ldots, \ R(\sigma_{r_1+r_2}(x_i)), \ I(\sigma_{r_1+r_2}(x_i))$$

où R et I désignent la partie réelle de la partie imaginaire. Calculons le déterminant D dont la i-ème colonne est (4); en utilisant les formules $R(z) = \frac{1}{2}(z + \bar{z})$ et $I(z) = \frac{1}{2i}(z - \bar{z})$ $(z \in \mathbf{C})$ et la linéarité par rapport aux lignes, on obtient $\mathrm{D} = \pm (2i)^{-r_2} \det(\sigma_j(x_i))$. Comme les x_i forment une base de K sur $\mathbf{Q}$ on a $\det(\sigma_j(x_i)) \neq 0$ (chap. II, § 7, prop. 3), et donc $\mathrm{D} \neq 0$. Ainsi les vecteurs $\sigma(x_i)$ sont linéairement indépendants dans $\mathbf{R}^n$, de sorte que le $\mathbf{Z}$-module qu'ils engendrent (à savoir $\sigma(\mathrm{M})$) est un réseau de $\mathbf{R}^n$. Le calcul de D fait ci-dessus montre que son volume est bien donné par (3). CQFD.

Proposition 2. *Soient d le discriminant absolu de* K, A *son anneau des entiers, et* $\mathfrak{a}$ *un idéal entier non nul de* A. *Alors* $\sigma(\mathrm{A})$ *et* $\sigma(\mathfrak{a})$ *sont des réseaux, et on a :*

$$5. \quad v(\sigma(\mathrm{A})) = 2^{-r_2}|d|^{1/2} \quad v(\sigma(\mathfrak{a})) = 2^{-r_2}|d|^{1/2}\mathrm{N}(\mathfrak{a}).$$

En effet on sait que A et $\mathfrak{a}$ sont des $\mathbf{Z}$-modules libres de rang n, de sorte qu'on peut appliquer la prop. 1. D'autre part, si (x_i) est une $\mathbf{Z}$-base de A, on a $d = \det(\sigma_i(x_j))^2$ (chap. II, § 7, prop. 3); d'où la première formule (5). La seconde s'en déduit en remarquant que $\sigma(\mathfrak{a})$ est un sous-groupe d'indice $\mathrm{N}(\mathfrak{a})$ de $\sigma(\mathrm{A})$ (chap. III, § 5, déf. 1), et qu'on obtient donc un domaine fondamental pour $\sigma(\mathfrak{a})$ par réunion disjointe de $\mathrm{N}(\mathfrak{a})$ domaines fondamentaux pour $\sigma(\mathrm{A})$.

4.3. Finitude du groupe des classes d'idéaux

Proposition 1. *Soient* K *un corps de nombres, n son degré, r_1 et r_2 les entiers définis au début du § 2, d son discriminant absolu, et $\mathfrak{a}$ un idéal entier non nul de* K. *Alors $\mathfrak{a}$ contient un élément non nul x tel que*

$$1. \quad |\mathrm{N}_{\mathrm{K}/\mathbf{Q}}(x)| \leqslant \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |d|^{1/2}\mathrm{N}(\mathfrak{a}).$$

En effet soit σ le plongement canonique de K dans $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$(§ 2). Soient t un nombre réel > 0 et B_t l'ensemble des

$$(y_1, \ \ldots, \ y_{r_1}, \ z_1, \ \ldots, \ z_{r_2}) \in \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$$

tels que

$$2. \quad \sum_{i=1}^{r_1} |y_i| + 2 \sum_{j=1}^{r_2} |z_j| \leqslant t.$$

Alors B_t est un ensemble compact, convexe et symétrique par rapport à

0, dont on verra en appendice que le volume est

3. $\mu(B_t) = 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{t^n}{n!}$.

Choisissons t tel que $\mu(B_t) = 2^n v(\sigma(\mathfrak{a}))$, c'est-à-dire tel que

$$2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{t^n}{n!} = 2^{n-r_2}|d|^{1/2}\mathrm{N}(\mathfrak{a})$$

(§ 2, prop. 2), ou encore $t^n = 2^{n-r_1}\pi^{-r_2}n!|d|^{1/2}\mathrm{N}(\mathfrak{a})$. D'après le cor. au th. 2, § 1, il existe un élément non nul x de $\mathfrak{a}$ tel que $\sigma(x) \in B_t$. Évaluons sa norme $|\mathrm{N}(x)| = \prod_{i=1}^{r_1} |\sigma_i(x)| \prod_{j=r_1+1}^{r_1+r_2} |\sigma_j(x)|^2$. L'inégalité de la moyenne géométrique montre qu'on a

$$|\mathrm{N}(x)| \leqslant \left[\frac{1}{n}\sum_{i=1}^{r_1}|\sigma_i(x)| + \frac{2}{n}\sum_{j=r_1+1}^{r_1+r_2}|\sigma_j(x)|\right]^n \leqslant \frac{t^n}{n^n} \qquad \text{(par (2))}$$

D'où $|\mathrm{N}(x)| \leqslant \frac{1}{n^n}2^{n-r_1}\pi^{-r_2}n!|d|^{1/2}\mathrm{N}(\mathfrak{a})$, ce qui équivaut à (1) vu que $r_1 + 2r_2 = n$. CQFD.

Corollaire 1. *Avec les mêmes notations, toute classe d'idéaux de* K (chap. III, § 4) *contient un idéal entier* $\mathfrak{b}$ *tel que*

4. $\mathrm{N}(\mathfrak{b}) \leqslant \left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}|d|^{1/2}$.

En effet soit $\mathfrak{a}'$ un idéal de la classe donnée. Par homothétie on peut supposer que $\mathfrak{a} = \mathfrak{a}'^{-1}$ est un idéal entier. Prenons un élément non nul x de $\mathfrak{a}$ tel que (1) soit vraie. Alors $\mathfrak{b} = x\mathfrak{a}^{-1}$ est un idéal entier de la classe donnée, dont la norme satisfait à (4) en vertu de la multiplicativité des normes (chap. III, § 5, prop. 2).

Corollaire 2. *Soient* K *un corps de nombres,* n *son degré, et* d *son discriminant absolu. Alors pour* $n \geqslant 2$ *on a* $|d| \geqslant \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}$, *et* $\frac{n}{\mathrm{Log}\,|d|}$ *est majoré par une constante indépendante de* K.

En effet, comme $\mathrm{N}(\mathfrak{b}) \geqslant 1$, on a $|d|^{1/2} \geqslant \left(\frac{\pi}{4}\right)^{r_2}\frac{n^n}{n!}$. Or $\frac{\pi}{4} < 1$ et $2r_2 \leqslant n$; on a donc $|d| \geqslant a_n$ où $a_n = \left(\frac{\pi}{4}\right)^n\frac{n^{2n}}{(n!)^2}$. Or on a $a_2 = \frac{\pi^2}{4}$ et $\frac{a_{n+1}}{a_n} = \frac{\pi}{4}\left(1 + \frac{1}{n}\right)^{2n} = \frac{\pi}{4}$ (1 + 2 + termes positifs) (par la formule du binôme) $\geqslant \frac{3\pi}{4}$. D'où, pour $n \geqslant 2, |d| \geqslant \frac{\pi^2}{4}\left(\frac{3\pi}{4}\right)^{n-2}$, ce qui donne l'inégalité annoncée. La majoration uniforme de $\frac{n}{\mathrm{Log}\,|d|}$ s'ensuit en prenant les logarithmes.

THÉORÈME 1 (Hermite-Minkowski). *Pour tout corps de nombres* $K \neq \mathbf{Q}$, *le discriminant absolu* d *de* K *est* $\neq \pm 1$.

En effet, d'après le cor. 2, on a $|d| \geqslant \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}$ et $\frac{\pi}{3} > 1$, $\frac{3\pi}{4} > 1$; d'où $|d| > 1$.

THÉORÈME 2 (Dirichlet). *Pour tout corps de nombres* K, *le groupe des classes d'idéaux de* K *est fini* (chap. III, § 4).

En effet, en vertu du cor. 1 à la prop. 1, il suffit de montrer que l'ensemble des idéaux entiers $\mathfrak{b}$ de K, dont la norme est un entier donné q, est fini. Or, pour un tel idéal $\mathfrak{b}$, on a $\operatorname{card}(A/\mathfrak{b}) = q$ (chap. III, § 5), d'où $q \in \mathfrak{b}$, car, dans un groupe, l'ordre d'un élément divise l'ordre du groupe. Ainsi nos idéaux $\mathfrak{b}$ sont parmi ceux qui contiennent Aq, et ces derniers sont en nombre fini (chap. III, § 4, formule (8); ou finitude de A/Aq). CQFD.

THÉORÈME 3 (Hermite). *Dans* $\mathbf{C}$ *il n'y a qu'un nombre fini de corps de nombres de discriminant* d *donné.*

En effet, d'après le cor. 2 à la prop. 1, le degré d'un tel corps est alors majoré. Nous pouvons donc supposer n donné, ainsi que les entiers r_1 et r_2. Soit K un tel corps.

Dans $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ considérons l'ensemble B suivant :

a) Si $r_1 > 0$, B est l'ensemble des $(y_1, \ldots, y_{r_1}, z_1, \ldots, z_{r_2}) \in \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ tels que

$$5. \quad |y_1| \leqslant 2^n \left(\frac{\pi}{2}\right)^{-r_2} |d|^{1/2}, \ |y_i| \leqslant \frac{1}{2} \text{ pour } i = 2, \ldots, r_1,$$
$$|z_j| \leqslant \frac{1}{2} \quad \text{pour} \quad j = 1, \ldots, r_2.$$

b) Si $r_1 = 0$, B est l'ensemble des $(z_1, \ldots, z_{r_2}) \in \mathbf{C}^{r_2}$ tels que

$$6. \quad |z_1 - \bar{z}_1| \leqslant 2^n \frac{8}{\pi}\left(\frac{\pi}{2}\right)^{-r_2} |d|^{1/2}, \quad |z_1 + \bar{z}_1| \leqslant \frac{1}{2},$$
$$|z_j| \leqslant \frac{1}{2} \quad \text{pour} \quad j = 2, \ldots, r_2.$$

Alors B est un ensemble compact, convexe, symétrique par rapport à 0, dont le volume est tout juste $2^n\, 2^{-r_2}|d|^{1/2}$ [1]. En notant σ le plongement canonique de K (§ 2), la prop. 2 du § 2 et le cor. au th. 2 du § 1 montrent qu'il existe un entier $x \neq 0$ de K tel que $\sigma(x) \in B$.

Montrons que x est un élément *primitif* de K sur $\mathbf{Q}$. En effet, dans

1. Le calcul, très simple, de ce volume se fait en remarquant que B est un produit d'intervalles, de disques, et d'un rectangle dans le cas *b*).

le cas *a*), (5) montre qu'on a $|\sigma_i(x)| \leqslant \frac{1}{2}$ pour $i \neq 1$; comme

$$|\mathrm{N}(x)| = \prod_{i=1}^{n} |\sigma_i(x)|$$

est un entier $\neq 0$ (chap. II § 6, cor. de la prop. 2), on en déduit $|\sigma_1(x)| \geqslant 1$, d'où $\sigma_1(x) \neq \sigma_i(x)$ pour tout $i \neq 1$; or, si x n'était pas primitif, $\sigma_1(x)$ coïnciderait avec l'un des $\sigma_i(x)$ pour $i \neq 1$ (chap. II, § 6, prop. 1). Dans le cas *b*), on voit de même qu'on a $|\sigma_1(x)| = |\overline{\sigma_1(x)}| \geqslant 1$, d'où $\sigma_1(x) \neq \sigma_j(x)$ lorsque σ_j est distinct de σ_1 et $\bar{\sigma}_1$; de plus, (6) montre que la partie réelle $|R(\sigma_1(x))|$ est $\leqslant \frac{1}{4}$, de sorte que $\sigma_1(x)$ n' est pas réel et que $\sigma_1(x) \neq \overline{\sigma_1(x)}$; comme dans le cas *a*) on en conclut que x est primitif.

Maintenant les formules (5) et (6) montrent que les conjugués $\sigma_i(x)$ de x sont *bornés*, donc aussi les fonctions symétriques élémentaires des $\sigma_i(x)$, c'est-à-dire les coefficients du polynôme minimal de x. Comme ce sont des éléments de $\mathbf{Z}$ (chap. II, § 6, cor. de la prop. 2), ils ne sont donc susceptibles que d'un nombre fini de valeurs. D'où un nombre fini de polynômes minimaux possibles pour x, et par conséquent seulement un nombre fini de valeurs possibles de x dans $\mathbf{C}$. Comme x engendre K, le th. 3 est démontré CQFD.

4.4. Le théorème des unités

Par abus de langage, on appelle *unités* d'un corps de nombres K les éléments inversibles de l'anneau A des entiers de K. Ces unités forment un groupe multiplicatif, noté A^*. Le résultat suivant nous sera utile.

PROPOSITION 1. *Soient* K *un corps de nombres, et* $x \in \mathrm{K}$. *Pour que* x *soit une unité de* K, *il faut et il suffit que* x *soit un entier de* K, *de norme* ± 1.

En effet, si x est une unité de K, $\mathrm{N}(x)$ et $\mathrm{N}(x^{-1})$ sont des éléments de $\mathbf{Z}$, dont le produit est $\mathrm{N}(1) = 1$; on a donc $\mathrm{N}(x) = \pm 1$. Réciproquement, soit x un entier de K de norme ± 1; son équation caractéristique s'écrit $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x \pm 1 = 0$ avec $a_i \in \mathbf{Z}$ (chap. II, § 6); alors $\pm (x^{n-1} + \cdots + a_1)$ est l'inverse de x, et est un entier de K; donc x est une unité de K.

THÉORÈME 1 (Dirichlet). *Soient* K *un corps de nombres,* n *son degré,* r_1 *et* r_2 *les entiers définis au* § 2, *et* $r = r_1 + r_2 - 1$. *Le groupe* A^* *des unités de* K *est isomorphe à* $\mathbf{Z}^r \times \mathrm{G}$, *où* G *est un groupe cyclique fini, formé par les racines de l'unité contenues dans* K.

Nous montrerons d'abord que A^* est un groupe commutatif de type fini, et nous calculerons ensuite son rang. Considérons le plongement canonique (§ 2) $x \mapsto (\sigma_1(x), \ldots, \sigma_{r_1+r_2}(x))$ de K dans $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$, et l'application

1. $x \mapsto L(x) = (\mathrm{Log}|\sigma_1(x)|, \quad \ldots, \quad \mathrm{Log}|\sigma_{r_1+r_2}(x)|)$

de K^* dans $\mathbf{R}^{r_1+r_2}$; c'est un homomorphisme (i.e. $L(xy) = L(x) + L(y)$), que nous appellerons le *plongement logarithmique* de K^*. Soit B une partie compacte de $\mathbf{R}^{r_1+r_2}$; montrons que l'ensemble B' des unités $x \in A^*$ telles que $L(x) \in B$ est *fini*. En effet, comme B est borné, il existe un nombre réel $\alpha > 1$ tel que, pour tout $x \in B'$, on ait

$$\frac{1}{\alpha} \leqslant |\sigma_i(x)| \leqslant \alpha \quad (i = 1, \ldots, n);$$

les fonctions symétriques élémentaires des $\sigma_i(x)$ sont alors bornées en module; comme ce sont des éléments de $\mathbf{Z}$ (car $x \in A$), elles ne peuvent prendre qu'un nombre fini de valeurs; il n'y a donc qu'un nombre fini de polynômes caractéristiques possibles pour x, d'où un nombre fini de valeurs pour x. La finitude de B' entraîne aussitôt les conséquences suivantes :

a) Le noyau G de la restriction de L à A^* est un groupe fini. Il est donc formé de racines de l'unité, et est *cyclique* (chap. I, § 6, th. 1). Toute *racine de l'unité* contenue dans K appartient d'ailleurs à ce noyau, car c'est un entier de K, et que $|\sigma_i(x)|^q = |\sigma_i(x^q)| = |1| = 1$ implique $|\sigma_i(x)| = 1$.

b) L'image $L(A^*)$ est un sous-groupe discret de $\mathbf{R}^{r_1+r_2}$(§ 1), et est donc un $\mathbf{Z}$-module libre de rang $s \leqslant r_1 + r_2$ (§ 1, th. 1). Comme $L(A^*)$ est libre, A^* est isomorphe à $G \times L(A^*) = G \times \mathbf{Z}^s$. Il nous reste à montrer que le rang s de $L(A^*)$ est égal à $r_1 + r_2 - 1$.

L'inégalité $s \leqslant r_1 + r_2 - 1$ est facile. En effet, pour $x \in A^*$, la relation $\pm 1 = N(x) = \prod_{i=1}^{n} \sigma_i(x) = \prod_{i=1}^{r_1} \sigma_i(x) \prod_{j=r_1+1}^{r_1+r_2} \sigma_j(x)\overline{\sigma_j(x)}$ (prop. 1) implique que le vecteur $L(x) = (y_1, \ldots, y_{r_1+r_2})$ appartient à l'hyperplan W d'équation

2. $\sum_{i=1}^{r_1} y_i + 2 \sum_{j=r_1+1}^{r_1+r_2} y_j = 0$;

ainsi $L(A^*)$ est un sous-groupe discret de W, d'où $s \leqslant r_1 + r_2 - 1$.

Reste à montrer que $L(A^*)$ contient $r = r_1 + r_2 - 1$ vecteurs linéairement indépendants, ce qui va être plus délicat. Il s'agit de montrer que, pour toute forme linéaire $f \neq 0$ sur W, il existe une unité u telle que $f(L(u)) \neq 0$. Comme la projection de W sur $\mathbf{R}^r$ est un isomorphisme (par (2)), on peut écrire, pour tout $y = (y_1, \ldots, y_{r+1}) \in W \subset \mathbf{R}^{r+1}$

3. $f(y) = c_1 y_1 + \cdots + c_r y_r$ avec $c_i \in \mathbf{R}$

Fixons un nombre réel α suffisamment grand, plus précisément

$$\alpha \geqslant 2^n \left(\frac{1}{2\pi}\right)^{r_2} |d|^{1/2}.$$

Pour tout système $\lambda = (\lambda_1, \ldots, \lambda_r)$ de r nombres réels > 0, soit λ_{r+1} le nombre réel >0 tel que $\prod_{i=1}^{r_1} \lambda_i \prod_{j=r_1+1}^{r_1+r_2} \lambda_j^2 = \alpha$. Dans $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ l'ensemble B des $(y_1, \ldots, y_{r_1}, z_1, \ldots, z_{r_2})$ $(y_i \in \mathbf{R},\ z_j \in \mathbf{C})$ tels que $|y_i| \leqslant \lambda_i$ et $|z_j| \leqslant \lambda_j$ est compact, convexe, symétrique, par rapport à 0, et son volume est $\prod_{i=1}^{r_2} 2\lambda_i \prod_{r=r_1+1}^{r_2} \pi\lambda_j^2 = 2^{r_1}\pi^{r_2}\alpha \geqslant 2^n\, 2^{-r_2}|d|^{1/2}$. Donc, d'après la prop. 2 du § 2 et le cor. au th. 2 du § 1, il existe un *entier* x_λ *de* K tel que $\sigma(x_\lambda) \in \mathrm{B}$; autrement dit on a $|\sigma_i(x_\lambda)| \leqslant \lambda_i$ pour $i = 1, \ldots, n$ (en posant $\lambda_{j+r_2} = \lambda_j$ pour $j = r_1 + 1, \ldots, r_1 + r_2$). Comme x_λ est un entier, on a

$$1 \leqslant |\mathrm{N}(x_\lambda)| = \prod_{i=1}^{n} |\sigma_i(x_\lambda)| \leqslant \prod_{i=1}^{r_1} \lambda_i \prod_{j=r_1+1}^{r_1+r_2} \lambda_j^2 = \alpha$$

D'autre part, pour tout i, on a

$$|\sigma_i(x_\lambda)| = |\mathrm{N}(x_\lambda)| \prod_{j \neq i} |\sigma_j(x_\lambda)|^{-1} \geqslant \prod_{j \neq i} \lambda_j^{-1} = \lambda_i\alpha^{-1}$$

D'où $\lambda_i\alpha^{-1} \leqslant |\sigma_i(x_\lambda)| \leqslant \lambda_i$ pour tout i, de sorte qu'on a

4. $0 \leqslant \operatorname{Log}\lambda_i - \operatorname{Log}|\sigma_i(x_\lambda)| \leqslant \operatorname{Log}\alpha.$

D'après (3), on a donc

5. $\left| f(\mathrm{L}(x_\lambda)) - \sum_{i=1}^{r} c_i \operatorname{Log}\lambda_i \right| \leqslant \left(\sum_{i=1}^{r} |c_i| \right) \operatorname{Log}\alpha$

Notons β une constante majorant strictement le second membre de (5), et, pour tout entier $h > 0$, choisissons r nombres réels $\lambda_{i,h} > 0$ $(i = 1, \ldots, r)$ tels que $\sum_{i=1}^{r} c_i \operatorname{Log}\lambda_{i,h} = 2\beta h$; posons

$$\lambda(h) = (\lambda_{1,h}, \ldots, \lambda_{r,h}),$$

et soit x_h l'entier $x_{\lambda(h)}$ correspondant. D'après 5 on a

$$|f(\mathrm{L}(x_h)) - 2\beta h| < \beta,$$

d'où

6. $(2h - 1)\beta < f(\mathrm{L}(x_h)) < (2h + 1)\beta.$

Il résulte de (6) que les nombres $f(\mathrm{L}(x_h))$ $(h \geqslant 0)$ sont tous *distincts*. D'autre part, comme $|\mathrm{N}(x_h)| \leqslant \alpha$, les idéaux $\mathrm{A}x_h$ sont en nombre *fini* (cf. § 3, démonstration du th. 2). Il existe donc deux indices distincts h et k tels que $Ax_h = Ax_k$, d'où une *unité* u de A telle que $x_k = ux_h$. On a alors (comme f est linéaire) $f(L(u)) = f(L(x_k)) - f(L(x_h)) \neq 0$, et u est l'unité cherchée. CQFD.

Remarque. Le th. 1 (appelé « théorème des unités ») montre qu'il existe $r(= r_1 + r_2 - 1)$ unités (u_i) de K telles que toute unité u de K s'écrive, d'une façon et d'une seule, sous la forme

7. $u = zu_1^{n_1} \dots u_r^{n_r}$

avec $n_i \in \mathbf{Z}$ et z racine de l'unité. Alors (u_i) s'appelle un *système d'unités fondamentales* de K

Exemple des corps cyclotomiques. Soient p un nombre premier $\neq 2$, z une racine primitive p-ème de l'unité dans $\mathbf{C}$, et K le corps cyclotomique $\mathbf{Q}[z]$ (cf. chap. II, § 9); on a $[K : \mathbf{Q}] = p - 1$ (*ibid.*, th. 1). Comme aucun conjugué de z dans $\mathbf{C}$ n'est réel, on a $r_1 = 0$, $2r_2 = p - 1$, d'où $r = \frac{p-3}{2}$

4.5. Unités des corps quadratiques imaginaires

Soit K un corps quadratique imaginaire (chap. II, § 5). On a alors $r_1 = 0$, $2r_2 = 2$, $r_2 = 1$ et $r_1 + r_2 - 1 = 0$. Ainsi les seules unités de K sont les racines de l'unité contenues dans K (§ 4, th. 1); celles forment un groupe *fini cyclique*. Un petit calcul va nous redonner ce résultat, et le préciser.

Soit $K = \mathbf{Q}[\sqrt{-m}]$, où m est un entier > 0 sans facteurs carrés. Rappelons que les unités K sont les entiers de norme ± 1 de K (§ 4, prop. 1).

1) Si $m \equiv 1$ ou 2 (mod. 4), l'anneau des entiers de K est $\mathbf{Z} + \mathbf{Z}\sqrt{-m}$ (chap. II, § 5, th. 1). Pour $x = a + b\sqrt{-m}$ $(a, b \in \mathbf{Z})$, on a

$$N(x) = a^2 + mb^2 \geqslant 0.$$

Donc, pour que x soit une unité, il faut et il suffit que $a^2 + mb^2 = 1$. Si $m \geqslant 2$, ceci implique $b = 0$ et $a = \pm 1$, d'où $x = \pm 1$. Si $m = 1$, outre les solutions $x = \pm 1$, il y a les solutions $a = 0, b = \pm 1$, $x = \pm i (i^2 = -1)$.

2) Si $m \equiv 3$ (mod. 4), l'anneau des entiers de K est $\mathbf{Z} + \mathbf{Z}\frac{1 + \sqrt{-m}}{2}$ (chap. II, § 5, th. 1). Pour $x = a + \frac{b}{2}(1 + \sqrt{-m})$ $(a, b \in \mathbf{Z})$, on a $N(x) = \left(a + \frac{b}{2}\right)^2 + \frac{mb^2}{4}$. Donc, pour que x soit une unité, il faut et il suffit que $(2a + b)^2 + mb^2 = 4$. Si $m \geqslant 7$, ceci implique $b = 0$,

d'où $(2a)^2 = 4$, $a = \pm 1$, et $x = \pm 1$. Si $m = 3$, on obtient en outre les solutions $b = \pm 1$, d'où $(2a \pm 1)^2 = \pm 1$, c'est-à-dire

$$x = \frac{1}{2}(\pm 1 \pm \sqrt{-3})$$

(les signes $\pm$ étant indépendants).

En résumé nous avons obtenu le résultat suivant :

PROPOSITION 1. *Si* K *est un corps quadràtique imaginaire, le groupe* G *des unités de* K *est formé de* $+1$ *et de* -1, *sauf dans les deux cas suivants:*

1) *si* $K = \mathbf{Q}[i]$ $(i^2 = -1)$, G *est formé des racines quatrièmes de l'unité* $i, -1, -i, 1$.

2) *si* $K = \mathbf{Q}[\sqrt{-3}]$, G *est formé des racines sixièmes de l'unité* $\left(\frac{1+\sqrt{-3}}{2}\right)^j$ $j = 0, 1, \ldots, 5$.

4.6. Unités des corps quadratiques réels

Ce § va être nettement plus amusant que le précédent. Soit K un corps quadratique réel. Avec les notations habituelles, on a $r_1 = 2$, $r_2 = 0$, d'où $r = r_1 + r_2 - 1 = 1$. Le théorème des unités (§ 4, th. 1) montre que le groupe des unités de K est isomorphe au produit de $\mathbf{Z}$ par le groupe des racines de l'unité contenues dans K. Comme K admet un plongement dans $\mathbf{R}$, celles-ci sont 1 et -1. Donc, en supposant K plongé dans $\mathbf{R}$, on a :

PROPOSITION 1. *Les unités positives d'un corps quadratique réel* $K \subset \mathbf{R}$ *forment un groupe (multiplicatif) isomorphe à* $\mathbf{Z}$.

Ce groupe admet donc un seul générateur > 1; on l'appelle *l'unité fondamentale de* K.

Soit $K = \mathbf{Q}[\sqrt{d}]$ où d est un entier $\geqslant 2$ sans facteurs carrés, et soit $x = a + b\sqrt{d}$ $(a, b \in \mathbf{Q})$ une unité de K; les nombres $x, x^{-1}, -x, -x^{-1}$ sont des unités de K, et, comme $N(x) = (a + b\sqrt{d})(a - b\sqrt{d}) = \pm 1$ (§ 4, prop. 1), ces quatre nombres sont $\pm a \pm b\sqrt{d}$, Pour $x \neq \pm 1$, un seul des quatre nombres $x, x^{-1}, -x, -x^{-1}$ est > 1, et c'est le plus grand des quatre. Donc *les unités* > 1 *de* K *sont les unités de la forme* $a + b\sqrt{d}$ *avec* $a, b > 0$.

a) Supposons d'abord $d \equiv 2$ ou 3 (mod. 4). Alors l'anneau des entiers de K est $\mathbf{Z} + \mathbf{Z}\sqrt{d}$ (chap. II, § 5, th. 1). Comme les unités de K sont les entiers de norme ± 1 (§ 4, prop. 1), les unités > 1 de K sont les nombres $a + b\sqrt{d}$, avec $a, b \in \mathbf{Z}$, $a, b > 0$ tels que

1. $a^2 - db^2 = \pm 1$

On voit donc que les solutions « en nombres entiers naturels » (a, b) de l'équation (1) (dite « *équation de Pell-Fermat* ») s'obtiennent comme suit : on prend l'unité fondamentale $a_1 + b_1\sqrt{d}$ de K, et on pose

2. $a_n + b_n\sqrt{d} = (a_1 + b_1\sqrt{d})^n \qquad (n \geqslant 1)$;

la suite (a_n, b_n) fournit alors *toutes les solutions* de (1).

Remarques. 1) Il résulte de (2) que $b_{n+1} = a_1b_n + b_1a_n$; comme $a_1, b_1, a_n, b_n > 0$, la suite (b_n) est strictement croissante. Ainsi, afin de *calculer* explicitement l'unité fondamentale $a_1 + b_1\sqrt{d}$, on peut écrire la suite des db^2 $(b \in \mathrm{N}, b \geqslant 1)$ et s'arrêter au premier nombre db_1^2 de cette suite qui diffère d'un carré a_1^2 par ± 1; alors $a_1 + b_1\sqrt{d}$ est l'unité fondamentale de K. Par exemple, pour $d = 7$, la suite des db^2 est $7, 28, 63 = 64 - 1 = 8^2 - 1$; on a donc $b_1 = 3$, $a_1 = 8$ et l'unité fondamentale de $\mathbf{Q}[\sqrt{7}]$ est $8 + 3\sqrt{7}$. On voit de même que les unités fondamentales de $\mathbf{Q}[\sqrt{2}]$, $\mathbf{Q}[\sqrt{3}]$ et $\mathbf{Q}[\sqrt{6}]$ sont $1 + \sqrt{2}$, $2 + \sqrt{3}$, $5 + 2\sqrt{6}$. Il y a d'autres procédés de calcul, plus rapides, de l'unité fondamentale, liés à la théorie des fractions continues.

2) Si l'unité fondamentale est de norme 1, les (a_n, b_n) sont tous solutions de (1') $a^2 - db^2 = 1$; alors (1'') $a^2 - db^2 = -1$ n'a pas de solution. Si l'unité fondamentale est de norme -1, les solutions de (1') sont les (a_{2n}, b_{2n}), et celles de (1'') sont les (a_{2n+1}, b_{2n+1}). Le premier cas se produit pour $d = 3$, $d = 6$ et $d = 7$, le second pour $d = 2$ et $d = 10$.

b) Supposons maintenant $d \equiv 1 \pmod{4}$. Les entiers de $\mathrm{K} = \mathbf{Q}[\sqrt{d}]$ sont alors les nombres $\frac{1}{2}(a + b\sqrt{d})$ avec $a, b \in \mathbf{Z}$ de même parité (chap. II, § 5, th. 1). Donc, si $\frac{1}{2}(a + b\sqrt{d})$ est une unité de K, on a (§ 4, prop. 1)

3. $a^2 - db^2 = \pm 4$

Réciproquement pour toute solution (a, b) en nombres entiers de (3), $\frac{1}{2}(a + b\sqrt{d})$ est un entier de K (car sa trace est a, et sa norme est ± 1 par (3)), et donc une unité de K. Comme dans *a*) on voit donc que, si $\frac{1}{2}(a_1 + b_1\sqrt{d})$ désigne l'unité fondamentale de K, les solutions (a, b) de (3) en nombres entiers > 0 forment la suite (a_n, b_n) $(n \geqslant 1)$ définie par

4. $a_n + b_n\sqrt{d} = 2^{1-n}(a_1 + b_1\sqrt{d})^n$

Le calcul de $a_1 + b_1\sqrt{d}$ peut s'effectuer comme dans *a*); les unités fondamentales de $\mathbf{Q}[\sqrt{5}]$, $\mathbf{Q}[\sqrt{13}]$ et $\mathbf{Q}[\sqrt{17}]$ sont $\frac{1}{2}(1 + \sqrt{5})$, $\frac{1}{2}(3 + \sqrt{13})$, $4 + \sqrt{17}$; ces trois unités sont de norme -1. Pour le choix du signe $\pm$ dans (3), on a les mêmes résultats que dans le cas *a*).

Remarque. Dans le cas $d \equiv 1 \pmod{4}$, les solutions de l'équation de Pell-Fermat proprement dite

5. $a^2 - db^2 = \pm 1.$

correspondant aux unités $a + b\sqrt{d}\,(a,\ b > 0)$ de l'anneau $\mathrm{B} = \mathbf{Z}[\sqrt{d}]$, qui est un sous-anneau de l'anneau A des entiers de K. Or les unités > 0 de B forment un sous-groupe G du groupe des unités positives de A. Soit $u = \frac{1}{2}(a + b\sqrt{d})$ l'unité fondamentale de K. Si a et b sont tous deux *pairs,* on a $u \in \mathrm{B}$, de sorte que G *est formé des puissances de* u (c'est le cas si $d = 17$). Si a et b sont tous deux *impairs, on a* $u^3 \in \mathrm{B}$: en effet on a $8u^3 = a(a^2 + 3b^2d) + b(3a^2 + b^2d)\sqrt{d}$; comme $a^2 - db^2 = \pm 4$, on a $a^2 + 3b^2d = 4(b^2d \pm 1)$, qui est multiple de 8 car b et d sont impairs; de même $4a^2 + b^2d = 4(a^2 \pm 1)$, encore multiple de 8 car a est impair. Dans ce cas G *est formé des puissances de* u^3 (en effet on a $u^2 \notin \mathrm{B}$, sinon $u = u^3/u^2 \in \mathrm{B}$); c'est le cas pour $d = 5$ (resp. $d = 13$), et alors $u^3 = 2 + \sqrt{5}$ (resp. $u^3 = 18 + 5\sqrt{13}$).

4.7. Une généralisation du théorème des unités

PROPOSITION 1. *Soit* A *un anneau qui est un* **Z**-*module de type fini. Alors le groupe multiplicatif* A* *des éléments inversibles de* A *est un groupe commutatif de type fini.*

Pour un groupe commutatif G, « de type fini » veut dire « de type fini pour la structure de **Z**-*module* de G ». Un sous-groupe d'un groupe commutatif de type fini est de type fini (chap. III, § 1, cor. 2 du th. 1). Notons d'abord que A est un anneau *nœthérien,* car les idéaux de A sont des sous **Z**-modules de A.

Nous traiterons d'abord le cas où A est *intègre.* Si son corps des fractions K est de caractéristique 0, c'est un **Q**-espace vectoriel de type fini, donc un corps de nombres. D'autre part A est entier sur **Z** (car **Z**-module de type fini, cf. chap. II, § 1, th. 1), donc est un sous-anneau de l'anneau B des entiers de K; alors $\mathrm{A}^* \subset \mathrm{B}^*$ et B* est de type fini par le théorème des unités (§ 4, th. 1). Si K est de caractéristique $p \neq 0$, K est une extension finie de $\mathbf{F}_p$, donc un corps fini; alors A* est fini.

Passons maintenant au cas où A est *réduit* (ce qui veut dire, par définition, que 0 est le seul élément nilpotent de A). Nous aurons besoin du lemme suivant.

LEMME. *Dans un anneau nœthérien réduit* A, *l'idéal* (0) *est intersection finie d'idéaux premiers.*

En effet on sait que, dans un anneau nœthérien, tout idéal contient un produit d'idéaux premiers (chap. III, § 3, lemme 3). Or (0) est le plus petit des idéaux, et donc *est* produit d'idéaux premiers : $(0) = \mathfrak{p}_1^{n_1} \ldots \mathfrak{p}_q^{n_q}$

Soit alors $x \in \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_q$. On a $x^{n_1 + \cdots + n_q} \in \mathfrak{p}_1^{n_1} \ldots \mathfrak{p}_q^{n_q} = (0)$, donc $x^{n_1+\cdots+n_q} = 0$; d'où $x = 0$ car A est réduit. On a donc $(0) = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_q$.

Ceci étant, on $(0) = \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_q$, les $\mathfrak{p}_i$ étant des idéaux premiers. Donc l'homomorphisme canonique $\varphi : A \to \prod_{i=1}^{q} A/\mathfrak{p}_i$ est injectif. Or un élément d'un anneau produit est inversible si et seulement si ses composantes sont toutes inversibles, de sorte que $\left(\prod_i A/\mathfrak{p}_i\right)^* = \prod_i (A/\mathfrak{p}_i)^*$. D'après le cas intègre, chaque $(A/\mathfrak{p}_i)^*$ est de type fini, donc aussi $\Pi\ (A/\mathfrak{p}_i)^*$ et par conséquent $\varphi(A^*)$ (on rappelle que $\mathbf{Z}$ est nœthérien). Ainsi A^* est de type fini, vu que φ est injectif.

Passons enfin au *cas général*. Notons que l'ensemble $\mathfrak{n}$ des éléments nilpotents de A est un *idéal*, car $x^p = 0$, $y^q = 0$ et $a \in A$ entraînent $(x+y)^{p+q-1} = 0$ et $(ax)^p = 0$. D'autre part il existe un entier s tel que $\mathfrak{n}^s = (0)$: en effet, A étant nœthérien, $\mathfrak{n}$ admet un système générateur fini $(x_1, \ldots, x_r)$ avec $x_i^{q_i} = 0$ pour tout i; alors, pour $s = q_1 + \cdots + q_r$, tout monôme de degré s en les x_i est nul, de sorte que $\mathfrak{n}^s = (0)$. Nous procéderons par récurrence sur s. Le cas $s = 1$ est le cas réduit, déjà traité. Supposons donc $s > 1$, et notons φ l'homomorphisme canonique $\varphi : A \to A/\mathfrak{n}^{s-1}$. On a $\varphi(A^*) \subset (A/\mathfrak{n}^{s-1})^*$, de sorte que $\varphi(A^*)$ est un groupe de type fini. D'autre part le noyau de la restriction de φ à A^* est contenu dans $1 + \mathfrak{n}^{s-1}$, et lui est même *égal* car, comme $s > 1$, on a $(\mathfrak{n}^{s-1})^2 \subset \mathfrak{n}^s = (0)$, et tout élément $1 + x$ de $1 + \mathfrak{n}^{s-1}$ est inversible vu que $(1+x)(1-x) = 1 - x^2 = 1$. Reste à montrer que le groupe multiplicatif $1 + \mathfrak{n}^{s-1}$ est de type fini. Or, comme $(\mathfrak{n}^{s-1})^2 = (0)$, on a $(1+x)(1+y) = 1 + x + y$ pour $x, y \in \mathfrak{n}^{s-1}$, de sorte que $x \mapsto 1 + x$ est un isomorphisme du groupe additif $\mathfrak{n}^{s-1}$ sur le groupe multiplicatif $1 + \mathfrak{n}^{s-1}$. Mais, comme A est un $\mathbf{Z}$-module de type fini, il en est de même de $\mathfrak{n}^{s-1}$. CQFD.

En utilisant des méthodes empruntées à la Géométrie Algébrique, on montre que pour tout anneau *réduit* B de la forme $B = \mathbf{Z}[x_1, \ldots, x_n]$ (c'est-à-dire engendré sur $\mathbf{Z}$, en tant qu'anneau, par un nombre fini d'éléments), le groupe B^* des éléments inversibles de B est de type fini ([6]).

APPENDICE

Un calcul de volume

PROPOSITION. *Soient* $r_1, r_2 \in \mathbf{N}$, $n = r_1 + 2r_2$, $t \in \mathbf{R}$ *et* B_t *l'ensemble des* $(y_1, \ldots, y_{r_1}, z_1, \ldots, z_{r_2}) \in \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ *tels que*

1. $\sum_{i=1}^{r_1} |y_i| + 2 \sum_{j=1}^{r_2} |z_j| \leqslant t$

Alors, pour la mesure de Lebesgue, μ, *on a* $\mu(B_t) = 0$ *pour* $t < 0$, *et*

2. $\mu(B_t) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{t^n}{n!}$ *pour* $t \geqslant 0$.

On peut se borner au cas $t \geqslant 0$, car, pour $t < 0$, on a $B_t = \emptyset$ et

$\mu(B_t) = 0$. Posons $\mu(B_t) = V(r_1, r_2, t)$ et procédons par double récurrence sur r_1 et r_2. On a $V(1, 0, t) = 2t$ (segment $[-t, +t]$) et

$$V(0, 1, t) = \frac{\pi t^2}{4}$$

$\left(\text{disque de rayon } \frac{t}{2}\right)$, ce qui est conforme à (2).

Passons de r_1, à $r_1 + 1$. L'ensemble $B_t \subset \mathbf{R} \times \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ correspondant à $r_1 + 1$ et r_2 est défini par

$$|y| + \sum_{i=1}^{r_1} |y_i| + 2 \sum_{j=1}^{r_2} |z_j| \leqslant t \qquad (y \in \mathbf{R})$$

La formule d'intégration « par tranches » nous donne

$$V(r_1 + 1, r_2, t) = \int_{\mathbf{R}} V(r_1, r_2, t - |y|)\, dy = \int_{-t}^{+t} V(r_1, r_2, t - |y|)\, dy.$$

D'après l'hypothèse de récurrence, il vient

$$V(r_1 + 1, r_2, t) = 2 \int_0^t 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{(t - y)^n}{n!}\, dy = 2^{r_1+1} \left(\frac{\pi}{2}\right)^{r_2} \frac{t^{n+1}}{(n + 1)!},$$

ce qui est encore conforme à (2).

Passons enfin de r_2 à $r_2 + 1$. L'ensemble $B_t \subset \mathbf{R}^{r_1} \times \mathbf{C}^{r_2} \times \mathbf{C}$ correspondant à r_1 et $r_2 + 1$ est défini par

$$\sum_{i=1}^{r_1} |y_i| + 2 \sum_{j=1}^{r_2} |z_j| + 2|z| \leqslant t \qquad (z \in \mathbf{C})$$

La formule d'intégration « par tranches » nous donne ici

$$V(r_1, r_2 + 1, t) = \int_{\mathbf{C}} V(r_1, r_2, t - 2|z|)\, d\mu(z) = \int_{|z| \leqslant \frac{t}{2}} V(r_1, r_2, t - 2|z|) d\mu(z)$$

où $d\mu(z)$ désigne la mesure de Lebesgue sur $\mathbf{C}$. En posant

$$z = \rho e^{i\theta} (\rho \in \mathbf{R}_+,\ 0 \leqslant \theta \leqslant 2\pi) \quad \text{on a } d\mu(z) = \rho\, d\rho\, d\theta$$

En utilisant l'hypothèse de récurrence, il vient alors

$$\begin{aligned} V(r_1, r_2 + 1, t) &= \int_0^{t/2} \int_0^{2\pi} 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{(t - 2\rho)^n}{n!} \rho\, d\rho\, d\theta \\ &= 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{2\pi}{n!} \int_0^{t/2} (t - 2\rho)^n \rho\, d\rho \end{aligned}$$

On calcule $\int_0^{t/2} (t - 2\rho)^n \rho\, d\rho$ en posant $2\rho = x$ et en intégrant par parties; on trouve que cette intégrale vaut $\frac{t^{n+2}}{4(n + 1)(n + 2)}$. D'où $V(r_1, r_2 + 1, t) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2+1} \frac{t^{n+2}}{(n + 2)!}$, ce qui est conforme à (2) car $r_1 + 2(r_2 + 1) = n + 2$.

Décomposition
des idéaux premiers dans une extension

Soient K un corps de nombres, A l'anneau des entiers de K, L une extension de degré fini de K, et B la fermeture intégrale de A dans L (qui n'est autre que l'anneau des entiers de L). Étant donné un idéal premier $\mathfrak{p} \neq (0)$ de A, l'idéal $B\mathfrak{p}$ qu'il engendre dans B n'est pas en général premier; il se décompose donc en produit d'idéaux premiers (chap. III, § 4, th. 3), soit $B\mathfrak{p} = \prod_i \mathfrak{P}_i^{e_i}$. Dans ce chapitre nous nous proposons d'étudier cette décomposition. Le cas où B est un A-module *libre* (p. ex. celui où A est un anneau principal; cf. chap. II; § 7, cor. du th. 1) est particulièrement simple. Nous exposerons au § 1 une technique permettant de se ramener à ce cas.

5.1. Préliminaires sur les anneaux de fractions

Définition 1. *Soient* A *un anneau intègre,* K *son corps des fractions, et* S *une partie de* A, *stable pour la multiplication, ne contenant pas* 0 *et contenant* 1. *On appelle anneau de fractions de* A *par rapport à* S, *et on note* $S^{-1}A$, *l'ensemble des éléments* $\frac{a}{s} \in K$ *avec* $a \in A$ *et* $s \in S$.

C'est un anneau commutatif $\left(\text{car } \frac{a}{s} + \frac{a'}{s'} = \frac{s'a + sa'}{ss'} \text{ et } \frac{a}{s} \cdot \frac{a'}{s'} = \frac{aa'}{ss'}\right)$; il contient A (car $1 \in S$). Si S est l'ensemble des éléments non nuls de A, on a $S^{-1}A = K$. Si S est réduit à 1, ou s'il est formé d'éléments inversibles de A, on a $S^{-1}A = A$.

Proposition 1. *Soient* A *un anneau intègre,* S *une partie multiplicativement stable de* A *contenant* 1 *et ne contenant pas* 0, *et* $A' = S^{-1}A$.

1. *Pour tout idéal* $\mathfrak{b}'$ *de* A', *on a* $(\mathfrak{b}' \cap A)A' = \mathfrak{b}'$ *de sorte que* $\mathfrak{b}' \mapsto \mathfrak{b}' \cap A$ *est une injection croissante (pour l'inclusion) de l'ensemble des idéaux de* A' *dans celui des idéaux de* A.

2. *L'application* $\mathfrak{p}' \mapsto \mathfrak{p}' \cap A$ *est un isomorphisme de l'ensemble ordonné (par inclusion) des idéaux premiers de* A' *sur celui des idéaux premiers* $\mathfrak{p}$ *de* A *tels que* $\mathfrak{p} \cap S = \emptyset$. *L'application réciproque est* $\mathfrak{p} \mapsto \mathfrak{p}A'$.

Démontrons 1) Si $\mathfrak{b}'$ est un idéal de A', on a $\mathfrak{b}' \cap A \subset \mathfrak{b}'$, d'où $(\mathfrak{b}' \cap A)A' \subset \mathfrak{b}'$ car $\mathfrak{b}'$ est un idéal. Pour démontrer l'inclusion opposée, soit $x \in \mathfrak{b}'$; on a $x = \frac{a}{s}$ avec $a \in A$ et $s \in S$; or $sx \in \mathfrak{b}'$ car $A \subset A'$ et que $\mathfrak{b}'$ est un idéal; d'où $a \in \mathfrak{b}'$ et $a \in \mathfrak{b}' \cap A$. Alors $x = \frac{1}{s} \cdot a \in A'(\mathfrak{b}' \cap A)$. D'où $\mathfrak{b}' \subset A'(\mathfrak{b}' \cap A)$ et $\mathfrak{b}' = A'(\mathfrak{b}' \cap A)$. Cette formule assure l'injectivité de l'application $\varphi : \mathfrak{b}' \mapsto \mathfrak{b}' \cap A$, car on a une application $\theta : \mathfrak{b} \mapsto A'\mathfrak{b}$ telle que $\theta \circ \varphi =$ identité. La croissance de φ est évidente. Ceci démontre 1).

Passons à 2). Si $\mathfrak{p}'$ est un idéal premier de A', alors $\mathfrak{p} = \mathfrak{p}' \cap A$ est un idéal premier de A (chap. III, § 3, lemme 1); de plus on a $\mathfrak{p} \cap S = \emptyset$ car, si $s \in \mathfrak{p} \cap S$, on a $s \in \mathfrak{p}'$ et $1 = \frac{1}{s} \cdot s \in A'\mathfrak{p}' = \mathfrak{p}'$, ce qui est absurde.

Inversement, soit $\mathfrak{p}$ un idéal premier de A tel que $\mathfrak{p} \cap S = \emptyset$; nous allons montrer que $\mathfrak{p}A'$ est un idéal premier de A' et qu'on a $\mathfrak{p}A' \cap A = \mathfrak{p}$. Notons d'abord que $\mathfrak{p}A'$ *est l'ensemble des* $\frac{p}{s}$ *avec* $p \in \mathfrak{p}$ *et* $s \in S$: en effet tout élément x de $\mathfrak{p}A'$ s'écrit $x = \sum_{i=1}^{n} \frac{a_i}{s_i} p_i (a_i \in A,\ s_i \in S,\ p_i \in \mathfrak{p})$, donc $x = \sum_i \frac{b_i}{s} p_i$ par réduction à un même dénominateur $(b_i \in S,\ s \in S)$ et donc $x = \frac{p}{s}$ avec $p = \Sigma b_i p_i \in \mathfrak{p}$. On en déduit que $1 \notin \mathfrak{p}A'$, car $\mathfrak{p} \cap S = \emptyset$ et qu'on ne peut donc avoir $1 = \frac{p}{s}$ avec $p \in \mathfrak{p}$ et $s \in S$. Montrons que l'idéal $\mathfrak{p}A'$ est premier : soient $\frac{a}{s} \in A'$ et $\frac{b}{t} \in A'$ tels que $\frac{a}{s} \cdot \frac{b}{t} \in \mathfrak{p}A'$; on a alors $\frac{a}{s} \cdot \frac{b}{t} = \frac{p}{u}$ avec $p \in \mathfrak{p}$ et $u \in S$; d'où $abu = pst \in \mathfrak{p}$; comme $\mathfrak{p} \cap S = \emptyset$, on a $u \notin \mathfrak{p}$, d'où $ab \in \mathfrak{p}$ (car $\mathfrak{p}$ est premier); ainsi a ou b appartient à $\mathfrak{p}$, de sorte que $\frac{a}{s}$ ou $\frac{b}{t}$ appartient à $\mathfrak{p}A'$. Montrons enfin que $\mathfrak{p} = \mathfrak{p}A' \cap A$; l'inclusion $\mathfrak{p} \subset \mathfrak{p}A' \cap A$ est évidente; inversement, si $x \in \mathfrak{p}A' \cap A$, on a $x = \frac{p}{s}\ (p \in \mathfrak{p},\ s \in S)$ car $x \in \mathfrak{p}A'$; d'où $sx = p \in \mathfrak{p}$; comme $s \notin \mathfrak{p}$ (on a $\mathfrak{p} \cap S = \emptyset$) et que $\mathfrak{p}$ est premier, on en déduit $x \in \mathfrak{p}$.

Ceci étant, les formules $\mathfrak{p} = \mathfrak{p}A' \cap A$ et $\mathfrak{p}' = A'(\mathfrak{p}' \cap A)$ montrent que les applications $\varphi : \mathfrak{p}' \mapsto \mathfrak{p}' \cap A$ et $\theta : \mathfrak{p}' \mapsto \mathfrak{p}A'$ (restreintes aux idéaux premiers décrits dans l'énoncé) sont des bijections réciproques l'une de l'autre, car leurs composées dans les deux sens sont des applications identiques. Leur croissance est évidente. CQFD.

COROLLAIRE. *Si* A *est un anneau nœthérien intègre, tout anneau de fractions* $S^{-1}A$ *est nœthérien.*

En effet, l'ensemble des idéaux de $S^{-1}A$ s'applique, de façon injective et croissante, dans celui des idéaux de A (prop. 1, 1); il satisfait donc aussi à la condition maximale.

PROPOSITION 2. *Soient* R *un anneau intègre,* A *un sous-anneau de* R, S *une partie multiplicativement stable de* A *avec* $1 \in S$ et $0 \notin S$, *et* B *la fermeture intégrale de* A *dans* R. *Alors la fermeture intégrale de* $S^{-1}A$ *dans* $S^{-1}R$ *est* $S^{-1}B$.

En effet tout élément de $S^{-1}B$ s'écrit $\frac{b}{s}$ avec $b \in B$ et $s \in S$; on a une équation de dépendance intégrale $b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$ avec $a_i \in A$; en divisant par s^n on obtient $\left(\frac{b}{s}\right)^n + \frac{a_{n-1}}{s}\left(\frac{b}{s}\right)^{n-1} + \cdots + \frac{a_0}{s^n} = 0$ ce qui montre que $\frac{b}{s}$ est entier sur $S^{-1}A$. Inversement soit $\frac{x}{s}$ ($x \in R$, $s \in S$) un élément de $S^{-1}R$ entier sur $S^{-1}A$; on a une équation de dépendance intégrale $\left(\frac{x}{s}\right)^n + \frac{a_{n-1}}{t_{n-1}}\left(\frac{x}{s}\right)^{n-1} + \cdots + \frac{a_0}{t_0} = 0$ ($a_i \in A$, $t_i \in S$); en multipliant par $(t_0t_1 \ldots t_{n-1})^n$ on voit que $xt_0 \ldots t_{n-1}/s$ est entier sur A, donc est élément de B; ainsi $\frac{x}{s} = \frac{1}{t_0 \ldots t_{n-1}} \cdot \frac{xt_0 \ldots t_{n-1}}{s}$ est élément de $S^{-1}B$.

COROLLAIRE. *Si* A *est un anneau intégralement clos, tout anneau de fractions* $S^{-1}A$ *est intégralement clos.*

En effet on prend pour R le corps des fractions de A.

PROPOSITION 3. *Si* A *est un anneau de Dedekind, tout anneau de fractions* $S^{-1}A$ *est un anneau de Dedekind.*

En effet $S^{-1}A$ est nœthérien (cor. de la prop. 1) et intégralement clos (cor. de la prop. 2). De plus, comme on « perd » des idéaux premiers en passant de A à $S^{-1}A$ (prop. 1, 2), tout idéal premier non nul de $S^{-1}A$ est maximal.

PROPOSITION 4. *Soient* A *un anneau de Dedekind,* $\mathfrak{p}$ *un idéal premier non nul de* A *et* $S = A - \mathfrak{p}$. *Alors* $S^{-1}A$ *est un anneau principal, et il existe un élément premier* p *de* $S^{-1}A$ *tel que les seuls idéaux non nuls de* $S^{-1}A$ *soient les* $(p^n)_{n \geqslant 0}$.

En effet, comme $\mathfrak{p}$ est le seul idéal premier $\neq (0)$ de A contenu dans $\mathfrak{p}$, c'est-à-dire disjoint de S, le seul idéal premier non nul de $S^{-1}A$ est $\mathfrak{P} = \mathfrak{p}S^{-1}A$ (prop. 1, 2). Comme $S^{-1}A$ est un anneau de Dekedind (prop. 3), ses seuls idéaux non nuls sont les $\mathfrak{P}^n (n \geqslant 0)$. Prenons alors $p \in \mathfrak{P} - \mathfrak{P}^2$; l'idéal (p) qu'il engendre est contenu dans $\mathfrak{P}$ et ne contient pas $\mathfrak{P}^2$;

donc nécessairement $(p) = \mathfrak{P}$; les seuls idéaux non nuls de $S^{-1}A$ sont ainsi les (p^n), et $S^{-1}A$ est principal.

PROPOSITION 5. *Soient* A *un anneau intègre,* S *une partie multiplicativement stable de* A $(1 \in S, 0 \notin S)$ *et* $\mathfrak{m}$ *un idéal maximal de* A *tel que* $\mathfrak{m} \cap S = \emptyset$. *Alors*

$$S^{-1}A/\mathfrak{m}S^{-1}A \simeq A/\mathfrak{m}.$$

Plus précisément l'homomorphisme composé $A \to S^{-1}A \to S^{-1}A/\mathfrak{m}S^{-1}A$ a pour noyau $\mathfrak{m}S^{-1}A \cap A = \mathfrak{m}$ (prop. 1, 2)), d'où une injection φ : $A/\mathfrak{m} \to S^{-1}A/\mathfrak{m}S^{-1}A$. Reste à montrer que φ est surjective. Or soit $x = \frac{a}{s} \in S^{-1}A$ $(a \in A, s \in S)$; comme $s \notin \mathfrak{m}$ (on a $\mathfrak{m} \cap S = \emptyset$) et comme $\mathfrak{m}$ est maximal, s est inversible mod. $\mathfrak{m}$ et il existe b tel que $bs \equiv 1$ (mod. $\mathfrak{m}$); alors $\frac{a}{s} - ab = \frac{a}{s}(1 - bs) \in \mathfrak{m}S^{-1}A$, de sorte que l'image par φ de la classe de ab est égale à la classe de $\frac{a}{s} = x$. CQFD.

5.2. Décomposition d'un idéal premier dans une extension

Dans ce §, *on désigne par* A *un anneau de Dedekind de caractéristique* 0, *par* K *son corps des fractions, par* L *une extension de degré fini* n *de* K, *et par* B *la fermeture intégrale de* A *dans* L. *On rappelle que* B *est un anneau de Dedekind* (chap. III, § 4, th. 1).

Soit $\mathfrak{p}$ un idéal premier non nul de A. Alors $B\mathfrak{p}$ est un idéal de B dont on a une décomposition

1. $$B\mathfrak{p} = \prod_{i=1}^{q} \mathfrak{P}_i^{e_i}$$

où les $\mathfrak{P}_i$ sont des idéaux premiers de B, deux à deux distincts, et où les e_i sont des entiers $\geqslant 1$.

PROPOSITION 1. *Les* $\mathfrak{P}_i$ *sont exactement les idéaux premiers* $\mathfrak{Q}$ *de* B *tels que* $\mathfrak{Q} \cap A = \mathfrak{p}$.

En effet, pour un idéal premier $\mathfrak{Q}$ de B, la relation $\mathfrak{Q} \cap A = \mathfrak{p}$ équivaut à $\mathfrak{Q} \supset \mathfrak{p}B$ ($\Longrightarrow$ évident; $\Longleftarrow$ car $\mathfrak{Q} \cap A$ est un idéal premier de A et que $\mathfrak{p}$ est maximal). La prop. 1 résulte alors du formulaire des anneaux de Dedekind (chap. III, § 4).

Ainsi $A/\mathfrak{p}$ s'identifie à un sous-anneau de $B/\mathfrak{P}_i$. Ces deux anneaux sont des corps. Comme B est un A-module de type fini (chap. III, § 4, th. 1), $B/\mathfrak{P}_i$ est un espace vectoriel de dimension finie sur $A/\mathfrak{p}$; nous noterons f_i cette dimension, et l'appellerons le *degré résiduel* de $\mathfrak{P}_i$ sur A. L'exposant e_i dans (1) s'appelle l'*indice de ramification de* $\mathfrak{P}_i$ sur A. Notons enfin qu'on a $B\mathfrak{p} \cap A = \mathfrak{p}$ ($\supset$ évidente; $\subset$ résulte de $\mathfrak{P}_i \cap A = \mathfrak{p}$), de sorte que $B/B\mathfrak{p}$ est un espace vectoriel sur $A/\mathfrak{p}$, de dimension finie comme ci-dessus.

THÉORÈME 1. *Avec les notations précédentes on a*

2. $\sum_{i=1}^{q} e_i f_i = [B/B\mathfrak{p} : A/\mathfrak{p}] = n$

La première égalité est facile. Considérons la suite d'idéaux

$$B \supset \mathfrak{P}_1 \supset \mathfrak{P}_1^2 \supset \cdots \supset \mathfrak{P}_1^{e_1} \supset \mathfrak{P}_1^{e_1}\mathfrak{P}_2 \supset \cdots \supset \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2} \supset \cdots \supset \mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_q^{e_q} = B\mathfrak{p}.$$

Deux termes consécutifs sont de la forme $\mathfrak{B}$ et $\mathfrak{B}\mathfrak{P}_i$; or, comme il n'y a pas d'idéaux strictement compris entre $\mathfrak{B}$ et $\mathfrak{B}\mathfrak{P}_i$, $\mathfrak{B}/\mathfrak{B}\mathfrak{P}_i$ est un espace vectoriel de dimension 1 sur $B/\mathfrak{P}_i$ (cf. démonstration de la prop. 2, § 5, chap. III); c'est donc un espace vectoriel de dimension f_i sur $A/\mathfrak{p}$. Or, dans la suite ci-dessus, il y a e_i quotients de termes consécutifs de la forme $\mathfrak{B}/\mathfrak{B}\mathfrak{P}_i$ avec i donné. Au total la dimension $[B/B\mathfrak{p} : A/\mathfrak{p}]$ est égale à la somme des dimensions de ces quotients, donc à $\sum_{i=1}^{q} e_i f_i$.

La seconde égalité est facile aussi dans le cas où B est un A-module libre, en particulier lorsque A est *principal* (chap. II, § 7, cor. du th. 1): en effet une base $(x_1, \ldots, x_n)$ du A-module B donne, par réduction mod. $B\mathfrak{p}$, une base de $B/B\mathfrak{p}$ sur $A/\mathfrak{p}$. Nous allons nous ramener à ce cas en considérant la partie multiplicativement stable $S = A - \mathfrak{p}$ de A et les anneaux de fractions $A' = S^{-1}A$ et $B' = S^{-1}B$. On sait que A' est un anneau principal dont $\mathfrak{p}A'$ est le seul idéal maximal (§ 1, prop. 4), et que B' est la fermeture intégrale de A' dans L (§ 1, prop. 2). Par le cas principal, on a donc $[B'/\mathfrak{p}B' : A'/\mathfrak{p}A'] = n$. Considérons alors la décomposition de l'idéal $\mathfrak{p}B'$ dans l'anneau de Dedekind B': de $\mathfrak{p}B = \prod_{i=1}^{q} \mathfrak{P}_i^{e_i}$ on déduit $\mathfrak{p}B' = \prod_{i=1}^{q} (B'\mathfrak{P}_i)^{e_i}$. Comme $\mathfrak{P}_i \cap A = \mathfrak{p}$, (prop. 1), on a $\mathfrak{P}_i \cap S = \emptyset$ et $B'\mathfrak{P}_i$ est un idéal premier non nul de B' (§ 1, prop. 1, 2). La première partie de la démonstration nous donne donc

$$[B'/\mathfrak{p}B' : A'/\mathfrak{p}A'] = \sum_{i=1}^{q} e_i [B'/B'\mathfrak{P}_i : A'/\mathfrak{p}A'].$$

Or on a $A'/\mathfrak{p}A' \simeq A/\mathfrak{p}$ et $B'/B'\mathfrak{P}_i \simeq B/\mathfrak{P}_i$ (§ 1, prop. 5). D'où, en combinant nos égalités, $n = [B'/\mathfrak{p}B' : A'/\mathfrak{p}A'] = \sum_{i=1}^{q} e_i f_i$, ce qui achève de démontrer (2).

PROPOSITION 2. *Avec les mêmes notations, l'anneau* $B/B\mathfrak{p}$ *est isomorphe à* $\prod_{i=1}^{q} B/\mathfrak{P}_i^{e_i}$

En effet, comme $\mathfrak{P}_i$ est le seul idéal maximal de B qui contienne $\mathfrak{P}_i^{e_i}$, on a $\mathfrak{P}_i^{e_i} + \mathfrak{P}_j^{e_j} = \mathrm{B}$ pour $i \neq j$. On applique alors (1) et le lemme 1 du § 3, chap. I.

Exemple des corps cyclotomiques.

Soient p un nombre premier, et $z \in \mathbf{C}$ une racine primitive p^r-ème de l'unité. Les racines p^r-èmes de l'unité, dans $\mathbf{C}$, sont alors les $z^j (j = 1, \ldots, p^r)$; parmi elles les racines primitives sont les z^j telles que j ne soit pas multiple de p, et sont donc au nombre de

$$\varphi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1)$$

(cf. chap. I, § 6). Ces racines primitives p^r-èmes de l'unité sont les racines du polynôme cyclotomique

$$3. \quad \mathrm{F}(\mathrm{X}) = \frac{\mathrm{X}^{p^r} - 1}{\mathrm{X}^{p^{r-1}} - 1} = \mathrm{X}^{p^{r-1}(p-1)} + \mathrm{X}^{p^{r-1}(p-2)} + \cdots + \mathrm{X}^{p^{r-1}} + 1$$

Nous nous proposons de redémontrer ici qu'on a $[\mathbf{Q}[z] : \mathbf{Q}] = p^{r-1}(p-1)$, c'est-à-dire que $\mathrm{F}(\mathrm{X})$ est irréductible (cf. chap. II, § 9). Posons $e = p^{r-1}(p-1)$, et soient $z_1, \ldots, z_e$ les racines primitives p^r-èmes de l'unité. Comme le terme constant de $\mathrm{F}(\mathrm{X}+1)$ est p, on a

$$\prod_{j=1}^{e} (z_j - 1) = \pm p.$$

Soit B l'anneau des entiers de $\mathbf{Q}[z]$; on a évidemment $z_j \in \mathrm{B}$, et aussi $z_j - 1 \in \mathrm{B}(z_k - 1)$ pour tous j, k car z_j est une puissance z_k^q de z_k et qu'on a $z_k^q - 1 = (z_k - 1)(z_k^{q-1} + \cdots + z_k + 1)$; ainsi tous les idéaux $\mathrm{B}(z_k - 1)$ sont égaux. On a donc $\mathrm{B}p = \mathrm{B}(z_1 - 1)^e$.

Or écrivons $\mathrm{B}p = \prod_{i=1}^{q} \mathfrak{P}_i^{e_i}$ où les $\mathfrak{P}_i$ sont des idéaux premiers de B. Les e_i sont donc tous des multiples de e. Mais on a $e \geqslant [\mathbf{Q}[z] : \mathbf{Q}]$ (par (3)), d'où $e \geqslant \sum_{i=1}^{q} e_i f_i$ (th. 1). De ces inégalités en sens contraire on déduit que $q = 1$, $e = e_1$, $f_1 = 1$, $[\mathbf{Q}[z] : \mathbf{Q}] = e$. En résumé :

a) $[\mathbf{Q}[z] : \mathbf{Q}] = e = p^{r-1}(p-1)$

b) $\mathrm{B}(z_1 - 1)$ est un idéal premier de B, de degré résiduel 1.

c) $\mathrm{B}p = \mathrm{B}(z_1 - 1)^e$.

5.3. Discriminant et ramification

Avec les notations du § 2 $\left(\text{soit } \mathrm{B}\mathfrak{p} = \prod_{i=1}^{q} \mathfrak{P}_i^{e_i}\right)$ on dit qu'un idéal premier $\mathfrak{p}$ de A *se ramifie* dans B (ou dans L) si l'un des indices de ramification

e_i est $\geqslant 2$. Au moyen de la théorie du discriminant (chap. II, § 7) nous allons déterminer les idéaux premiers de A qui se ramifient dans B, et voir en particulier qu'ils sont en *nombre fini*. Quelques lemmes sur les discriminants nous seront utiles.

LEMME 1. *Soient* A *un anneau,* $B_1, \ldots, B_q$ *des anneaux contenant* A *et qui sont des* A*-modules libres de rang fini, et* $B = \prod_{i=1}^{q} B_i$ *leur anneau produit. Alors* $\mathfrak{D}_{B/A} = \prod_{i=1}^{q} \mathfrak{D}_{B_i/A}$ (cf. chap. II, § 7, déf. 2).

En effet une récurrence sur q nous ramène au cas $q = 2$. Soient alors $(x_1, \ldots, x_m)$, $(y_1, \ldots, y_n)$ des bases de B_1 et B_2 sur A. Avec l'identification classique de B_1 et B_2 avec $B_1 \times (0)$ et $(0) \times B_2$, $(x_1, \ldots, x_m, y_1, \ldots, y_n)$ est une base de $B = B_1 \times B_2$ sur A. On a $x_i y_j = 0$ par définition de la structure d'anneau produit, d'où $\mathrm{Tr}(x_i y_j) = 0$. Ainsi le déterminant $D(x_1, \ldots, x_m, y_1, \ldots, y_n)$ s'écrit :

$$\left| \begin{array}{c:c} \mathrm{Tr}(x_i x_{i'}) & 0 \\ \hdashline 0 & \mathrm{Tr}(y_j y_{j'}) \end{array} \right|$$

Il vaut donc

$$\det(\mathrm{Tr}(x_i x_{i'})) . \det(\mathrm{Tr}(y_j y_{j'})),$$

d'où

$$D(x_1, \ldots, x_m, y_1, \ldots, y_n) = D(x_1, \ldots, x_m)\, D(y_1, \ldots, y_m). \quad \text{CQFD.}$$

LEMME 2. *Soient* A *un anneau,* B *un anneau contenant* A *et admettant une base finie* $(x_1, \ldots, x_n)$, *et* $\mathfrak{a}$ *un idéal de* A. *Pour* $x \in B$ *notons* $\bar{x}$ *la classe de* x *dans* $B/\mathfrak{a}B$. *Alors* $(\bar{x}_1, \ldots, \bar{x}_n)$ *est une base de* $B/\mathfrak{a}B$ *sur* $A/\mathfrak{a}$ *et on a*

1. $D(\bar{x}_1, \ldots, \bar{x}_n) = \overline{D(x_1, \ldots, x_n)}$

En effet, soit $x \in B$; si la matrice de la multiplication par x, par rapport à la base (x_i) est (a_{ij}) $(a_{ij} \in A)$, la matrice de la multiplication par $\bar{x}$ dans la base $(\bar{x}_i)$ est $(\bar{a}_{ij})$. On a donc $\mathrm{Tr}(\bar{x}) = \overline{\mathrm{Tr}(x)}$. D'où

$$\mathrm{Tr}(\bar{x}_i . \bar{x}_j) = \overline{\mathrm{Tr}(x_i x_j)},$$

et donc (1) en prenant les déterminants.

LEMME 3. *Soient* K *un corps fini ou de caractéristique* 0, *et* L *une* K*-algèbre de dimension finie sur* K. *Pour que* L *soit réduite, il faut et il suffit que* $\mathfrak{D}_{L/K} \neq (0)$.

Supposons d'abord L non réduite, et soit $x \in L$ un élément nilpotent non nul. On pose $x_1 = x$ et on complète ce début de base en une base $(x_1, \ldots, x_n)$ de L sur K. Alors $x_1 x_j$ est nilpotent, et ainsi la multiplication par $x_1 x_j$ est un endomorphisme nilpotent; donc toutes les valeurs propres de celui-ci sont nulles, d'où $\mathrm{Tr}(x_1 x_j) = 0$. La matrice $(\mathrm{Tr}(x_i x_j))$ a donc une ligne nulle, de sorte que son déterminant $\mathrm{D}(x_1, \ldots, x_n)$ est nul. D'où $\mathfrak{D}_{\mathrm{L/K}} = (0)$.

Réciproquement, supposons L réduite. Alors l'idéal (0) de L est intersection finie d'idéaux premiers, $(0) = \bigcap_{i=1}^{q} \mathfrak{P}_i$ (chap. IV, § 7, lemme). Comme $\mathrm{L}/\mathfrak{P}_i$ est une algèbre intègre de dimension finie sur K, c'est un corps (chap. II, § 1, prop. 3). Donc $\mathfrak{P}_i$ est un idéal maximal de L, de sorte que $\mathfrak{P}_i + \mathfrak{P}_j = \mathrm{L}$ pour $i \neq j$. Ainsi L est isomorphe au produit $\prod_{i=1}^{q} \mathrm{L}/\mathfrak{P}_i$ (chap. I, § 3, lemme 1). On a donc $\mathfrak{D}_{\mathrm{L/K}} = \prod_{i=1}^{q} \mathfrak{D}_{(\mathrm{L}/\mathfrak{P}_i)/\mathrm{K}}$ (lemme 1). Or $\mathfrak{D}_{(\mathrm{L}/\mathfrak{P}_i)/\mathrm{K}} \neq (0)$ car K est fini ou de caractéristique 0 (chap. II, § 7, prop. 3). D'où $\mathfrak{D}_{\mathrm{L/K}} \neq (0)$. CQFD.

DÉFINITION 1. *Soient* K *et* L *deux corps de nombres avec* $\mathrm{K} \subset \mathrm{L}$, A *et* B *les anneaux des entiers de* K et L. *On appelle idéal discriminant de* B *sur* A (*ou de* L *sur* K), *et on note* $\mathfrak{D}_{\mathrm{B/A}}$ *ou* $\mathfrak{D}_{\mathrm{L/K}}$ *l'idéal de* A *engendré par les discriminants des bases de* L *sur* K *qui sont contenues dans* B.

Remarque 1. Si $(x_1, \ldots, x_n)$ est une base de L sur K contenue dans B, on a $\mathrm{Tr}_{\mathrm{L/K}}(x_i x_j) \in \mathrm{A}$ (chap. II, § 6, cor. de la prop. 2), d'où $\mathrm{D}(x_1, \ldots, x_n) \in \mathrm{A}$. Ainsi $\mathfrak{D}_{\mathrm{B/A}}$ est un idéal *entier* de A. Il est *non nul* par le chap. II, § 7, prop. 3.

Remarque 2. Lorsque B est un A-module *libre* (par exemple si A est principal) on a déjà défini l'idéal discriminant $\mathfrak{D}_{\mathrm{B/A}}$ comme étant engendré par $\mathrm{D}(e_1, \ldots, e_n)$ où $(e_1, \ldots, e_n)$ est une base de B sur A (chap. II, § 7, déf. 2). Il coïncide avec celui défini ci-dessus car, pour toute base (x_i) de L sur K contenue dans B, on a $x_i = \sum_i a_{ij} e_j$ avec $a_{ij} \in \mathrm{A}$, d'où $\mathrm{D}(x_1, \ldots, x_n) = \det(a_{ij})^2 \mathrm{D}(e_1, \ldots, e_n)$ (chap. II, § 7, prop. 1).

THÉORÈME 1. *Avec les notations de la déf., pour qu'un idéal premier* $\mathfrak{p}$ *de* A *se ramifie dans* B, *il faut et il suffit qu'il contienne l'idéal discrimiant* $\mathfrak{D}_{\mathrm{B/A}}$. *Les idéaux premiers de* A *qui se ramifient dans* B *sont en nombre fini.*

La seconde assertion résulte de la première car on a vu que $\mathfrak{D}_{\mathrm{B/A}} \neq (0)$. Démontrons celle-ci. Comme $\mathrm{B}/\mathfrak{p}\mathrm{B} \simeq \prod_{i=1}^{q} \mathrm{B}/\mathfrak{P}_i^{e_i}$ (§ 2, prop. 2), « $\mathfrak{p}$ se ramifie » équivaut à « $\mathrm{B}/\mathfrak{p}\mathrm{B}$ non réduit », c'est-à-dire à « $\mathfrak{D}_{(\mathrm{B}/\mathfrak{p}\mathrm{B})/(\mathrm{A}/\mathfrak{p})} = (0)$ » car $\mathrm{A}/\mathfrak{p}$ est un corps fini (lemme 3). Or posons $\mathrm{S} = \mathrm{A} - \mathfrak{p}$, $\mathrm{A}' = \mathrm{S}^{-1}\mathrm{A}$, $\mathrm{B}' = \mathrm{S}^{-1}\mathrm{B}$ et $\mathfrak{p}' = \mathfrak{p}\mathrm{A}'$. Alors A′ est un anneau principal (§ 1, prop. 4), B′ est un A′-module libre, et on a $\mathrm{A}/\mathfrak{p} \simeq \mathrm{A}'/\mathfrak{p}'$ et $\mathrm{B}/\mathfrak{p}\mathrm{B} \simeq \mathrm{B}'/\mathfrak{p}'\mathrm{B}'$ (§ 1, prop. 5). Donc, en désignant par $(e_1, \ldots, e_n)$ une base de B′ sur A′, la relation $\mathfrak{D}_{(B/\mathfrak{p}B)/(A/\mathfrak{p})} = (0)$ équivaut à $D(e_1, \ldots, e_n) \in \mathfrak{p}'$ (lemme 2). Ceci étant, si $D(e_1, \ldots, e_n) \in \mathfrak{p}'$ et si $(x_1, \ldots, x_n)$ est une base de L sur K contenue dans B, on a $x_i = \Sigma a'_{ij} e_j$ avec $a'_{ij} \in A'$ (car $B \subset B'$), d'où $D(x_1, \ldots, x_n) = \det (a'_{ij})^2 D(e_1, \ldots, e_n) \in \mathfrak{p}'$; comme $\mathfrak{p}' \cap A = \mathfrak{p}$ (§ 1, prop. 1, 2), on en déduit $D(x_1, \ldots, x_n) \in \mathfrak{p}$ et $\mathfrak{D}_{B/A} \subset \mathfrak{p}$. Réciproquement, si $\mathfrak{D}_{B/A} \subset \mathfrak{p}$, on a $D(e_1, \ldots, e_n) \in \mathfrak{p}'$ car on peut écrire $e_i = \frac{y_i}{s}$ avec $y_i \in B$ et $s \in S$ pour $1 \leqslant i \leqslant n$; ainsi

$$D(e_1, \ldots, e_n) = s^{-2n} D(x_1, \ldots, x_n) \in A'\mathfrak{D}_{B/A} \subset A'\mathfrak{p} = \mathfrak{p}'. \text{ CQFD.}$$

Exemple des corps quadratiques.

Prenons $K = \mathbf{Q}$ et $L = \mathbf{Q}[\sqrt{d}]$ où d est un entier sans facteurs carrés (chap. II, § 5)

a) Si $d \equiv 2$ ou 3 (mod. 4), $(1, \sqrt{d})$ est une base de l'anneau des entiers de L. Comme $\operatorname{Tr}(1) = 2$, $\operatorname{Tr}(\sqrt{d}) = 0$ et $\operatorname{Tr}(d) = 2d$, on a $D(1, \sqrt{d}) = 4d$. Les nombres premiers qui se ramifient dans L sont donc 2 et les diviseurs premiers de d.

b) Si $d \equiv 1$ (mod. 4), $\left(1, \frac{1+\sqrt{d}}{2}\right)$ est une base de l'anneau des entiers de L. On a

$$\operatorname{Tr}(1) = 2, \quad \operatorname{Tr}\left(\frac{1+\sqrt{d}}{2}\right) = 1$$

et

$$\operatorname{Tr}\left(\left(\frac{1+\sqrt{d}}{2}\right)^2\right) = \operatorname{Tr}\left(\frac{d+1}{4} + \frac{1}{2}\sqrt{d}\right) = \frac{d+1}{2}.$$

D'où $D\left(1, \frac{1+\sqrt{d}}{2}\right) = 2 \cdot \frac{d+1}{2} - 1 = d$. Les nombres premiers qui se ramifient dans L sont donc les diviseurs de d.

On remarquera qu'un corps quadratique $\mathbf{Q}[\sqrt{d}]$ est uniquement déterminé par son discriminant D; en effet $4d = D$ avec $d \equiv 2$ ou 3 (mod. 4) et $D \equiv 1$ (mod. 4) est impossible. On notera aussi le discriminant d'un corps quadratique n'est pas un entier arbitraire.

Exemple des corps cyclotomiques.

Soient p un nombre premier, $z \in \mathbf{C}$ une racine primitive p-ème de l'unité, et $L = \mathbf{Q}[z]$ le corps cyclotomique correspondant. On sait que l'anneau B des entiers de L admet $(1, z \ldots, z^{p-2})$ pour base sur $\mathbf{Z}$ (chap. II, § 9, th. 2), et que le polynôme minimal $F(X)$ de z sur $\mathbf{Q}$ satisfait à $(X-1)F(X) = X^p - 1$ (ibid; th. 1). On va calculer le discriminant $\mathfrak{D}_{B/\mathbf{Z}}$ en utilisant la formule $D(1, z, \ldots, z^{p-2}) = N(F'(z))$ (chap. II, § 7, formule (6)). Par dérivation de $(X-1)F(X) = X^p - 1$, on obtient $(z-1)F'(z) = pz^{p-1}$ (car $F(z) = 0$). Or $N(p) = p^{p-1}$, $N(z) = \pm 1$, $N(z-1) = \pm p$ (chap. II, § 9). On a donc

1. $D(1, z, \ldots, z^{p-2}) = \pm p^{p-2}$.

Il s'ensuit que p est le *seul* nombre premier qui se ramifie dans $\mathbf{Q}[z]$.

Le résultat suivant est quelquefois utile pour déterminer l'anneau des entiers d'un corps de nombres :

PROPOSITION 1. *Soient* L *un corps de nombres de degré* n *sur* $\mathbf{Q}$, *et* $(x_1, \ldots, x_n)$ *des entiers de* L *formant une base de* L *sur* $\mathbf{Q}$. *Si le discriminant* $D(x_1, \ldots, x_n)$ *est sans facteurs carrés, alors* $(x_1, \ldots, x_n)$ *est une base sur* $\mathbf{Z}$ *de l'anneau* B *des entiers de* L.

En effet, si $(e_1, \ldots, e_n)$ est une base de B sur $\mathbf{Z}$, on a $x_i = \sum_{j=1}^{n} a_{ij}e_j$ avec $a_{ij} \in \mathbf{Z}$. D'où $D(x_1, \ldots, x_n) = \det(a_{ij})^2 \, D(e_1, \ldots, e_n)$. Comme $D(x_1, \ldots, x_n)$ est sans facteurs carrés, on en déduit $\det(a_{ij}) = \pm 1$, ce qui implique que $(x_1, \ldots, x_n)$ est aussi une base de B sur $\mathbf{Z}$.

L'exemple des corps cyclotomiques (pour $p \geqslant 5$), ou des corps quadratiques, montre que la condition suffisante ci-dessus n'est nullement nécessaire.

Exemple. Le polynôme $X^3 - X - 1$ (resp. $X^3 + X + 1$, $X^3 + 10X + 1$) est *irréductible* sur $\mathbf{Q}$; sinon, en effet, il aurait un facteur du premier degré, donc une racine $x \in \mathbf{Q}$; on aurait alors $x \in \mathbf{Z}$ car le polynôme est unitaire; comme son terme constant est 1, on aurait même $x = \pm 1$ (car tout facteur de x divise ce terme constant); or ceci n'est pas. Donc, en désignant par $x \in \mathbf{C}$ une racine dudit polynôme, le corps $L = \mathbf{Q}[x]$ est un *corps cubique* (i.e. de degré 3). Ainsi $(1, x, x^2)$ est une base de L sur $\mathbf{Q}$, et x évidemment un entier de L. Or, d'après la formule (7) du § 7, chap. II, on a $D(1, x, x^2) = -4 + 27 = 23$ (resp. 31, 4027), qui est un nombre premier. Donc $(1, x, x^2)$ est une base sur $\mathbf{Z}$ de l'anneau des entiers de L.

5.4. Décomposition d'un nombre premier dans un corps quadratique

Soient $d \in \mathbf{Z}$ un entier sans facteurs carrés, L le corps quadratique $L = \mathbf{Q}[\sqrt{d}]$, B l'anneau des entiers de L, et p un nombre premier. On va étudier la décomposition en idéaux premiers de l'idéal pB.

La formule $\sum_{i=1}^{q} e_i f_i = 2$ (§ 2, th. 1) montre qu'on a $q \leqslant 2$ et que seuls trois cas peuvent se produire :

a) $q = 2$, $e_1 = e_2 = 1$, $f_1 = f_2 = 1$; on dit alors que p est *décomposé* dans L;

b) $q = 1$, $e_1 = 1$, $f_1 = 2$; on dit alors que p est *inerte* dans L;

c) $q = 1$, $e_1 = 2$, $f_1 = 1$; ceci veut dire que p *se ramifie* dans L.

Examinons d'abord le *cas où* p *est impair*. On sait (chap. II, § 5) que $B = \mathbf{Z} + \mathbf{Z}\sqrt{d}$ ou $B = \mathbf{Z} + \mathbf{Z}\left(\dfrac{1 + \sqrt{d}}{2}\right)$ suivant la valeur de d. Mais, si on prend les classes de B modulo Bp, on voit, dans le second cas, que $a+b\left(\frac{1+\sqrt{d}}{2}\right)$ (avec b impair) est congru à $a+(b+p)\left(\frac{1+\sqrt{d}}{2}\right)$, qui est élément de $\mathbf{Z}+\mathbf{Z}\sqrt{d}$. Donc, dans tous les cas, on a

$$B/Bp \simeq (\mathbf{Z}+\mathbf{Z}\sqrt{d})/(p).$$

Or $\mathbf{Z}+\mathbf{Z}\sqrt{d} \simeq \mathbf{Z}[X]/(X^2-d)$. D'où

$$B/Bp \simeq \mathbf{Z}[X]/(p, X^2-d) \simeq (\mathbf{Z}[X]/(p))/(X^2-d) \simeq \mathbf{F}_p[X]/(X^2-\bar{d}),$$

où $\bar{d}$ désigne la classe de d modulo p. Or l'assertion que p est décomposé (resp. est inerte, se ramifie) dans B signifie que B/Bp est produit de deux corps (resp. est un corps, a des éléments nilpotents) (cf. § 2, prop. 2); ceci signifie donc que, dans $\mathbf{F}_p[X]$, le polynôme $X^2-\bar{d}$ est produit de deux facteurs distincts du premier degré (resp. est irréductible, est un carré); or ceci se produit si $\bar{d}$ est un carré non nul dans $\mathbf{F}_p$ (resp. n'est pas un carré dans $\mathbf{F}_p$, est nul dans $\mathbf{F}_p$). Lorsque $\bar{d}$ est un carré non nul dans $\mathbf{F}_p$ (resp. n'est pas un carré dans $\mathbf{F}_p$), on dit que d est un *résidu quadratique* (resp. un *non-résidu*) modulo p.

Traitons maintenant *le cas* $p=2$. Si $d \equiv 2,3 \pmod 4$, on a $B=\mathbf{Z}+\mathbf{Z}\sqrt{d}$, d'où, comme plus haut $B/2B \simeq \mathbf{F}_2[X]/(X^2-\bar{d})$; or $X^2-\bar{d}$ vaut X^2 ou $X^2+1=(X+1)^2$, et est donc un carré; ainsi 2 se ramifie dans B. Si $d \equiv 1 \pmod 4$, $\frac{1+\sqrt{d}}{2}$ admet $X^2-X-\frac{d-1}{4}$ pour polynôme minimal, d'où, comme plus haut, $B/2B \simeq \mathbf{F}_2[X]/(X^2-X-\delta)$ où δ est la classe mod. 2 de $\frac{d-1}{4}$; pour $d \equiv 1 \pmod 8$ on a $\delta=0$ et $X^2-X-\delta=X(X-1)$, de sorte que 2 est décomposé; pour $d \equiv 5 \pmod 8$, on a $\delta=1$ et $X^2-X-\delta=X^2+X+1$ est irréductible dans $\mathbf{F}_2[X]$, de sorte que 2 est inerte.

En résumé, on a démontré les résultats suivants :

PROPOSITION 1. *Soit* $L=\mathbf{Q}[\sqrt{d}]$ *un corps quadratique, où* $d \in \mathbf{Z}$ *est sans facteurs carrés.*

a) Sont décomposés dans L, *les nombres premiers impairs* p *tels que* d *soit résidu quadratique* mod. p, *et* 2 *si* $d \equiv 1$ mod. 8;

b) Sont inertes dans L, *les nombres premiers impairs* p *tels que* d *soit non-résidu* mod. p, *et* 2 *si* $d \equiv 5$ mod. 8;

c) Se ramifient dans L, *les diviseurs premiers impairs de* d, *et* 2 *si* $d \equiv 2$ *ou* 3 (mod. 4)

L'assertion *c*) a déjà été démontrée dans un exemple du § 3.

5.5. Loi de réciprocité quadratique

Étant donnés un nombre premier *impair* p et un entier d premier à p, nous avons introduit au § 4 la locution « d est *un résidu quadratique* mod. p » (resp. « d *est un non-résidu* mod. p ») comme signifiant que la classe de d mod. p est un carré (resp. un non-carré) dans $\mathbf{F}_p^*$. Nous introduisons ici *le symbole de Legendre* $\left(\frac{d}{p}\right)$ ainsi défini.

1. $$\begin{cases} \left(\dfrac{d}{p}\right) = +1 & \text{si } d \text{ est résidu quadratique mod. } p. \\ \left(\dfrac{d}{p}\right) = -1 & \text{si } d \text{ est non-résidu mod. } p. \end{cases}$$

Bien entendu $\left(\frac{d}{p}\right)$ n'est défini que pour d premier à p, c'est-à-dire pour $d \in \mathbf{Z} - p\mathbf{Z}$. Le groupe multiplicatif $\mathbf{F}_p^*$ étant cyclique d'ordre pair $p-1$ (chap. I, § 7, th. 1), les carrés en forment un sous-groupe $\mathbf{F}_p^{*2}$ d'indice 2, et $\mathbf{F}_p^*/\mathbf{F}_p^{*2}$ est isomorphe à $\{+1, -1\}$. Ainsi le symbole de Legendre s'obtient en composant les homomorphismes

$$\mathbf{Z} - p\mathbf{Z} \to \mathbf{F}_p^* \to \mathbf{F}_p^*/\mathbf{F}_p^{*2} \simeq \{+1, -1\}$$

On a donc la formule de multiplicativité

2. $$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Proposition 1 (« critère d'Euler »). *Si p est un nombre premier impair, et si $a \in \mathbf{Z} - p\mathbf{Z}$, on a* $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}$ (mod. p).

En effet notons w une racine primitive mod. p (chap. I, § 7); on a $a \equiv w^j$ (mod. p) avec $0 \leqslant j \leqslant p-2$ car la classe $\overline{w}$ de w est un générateur de $\mathbf{F}_p^*$. Il est clair que « a résidu quadratique » équivaut à « j pair »; on a donc $\left(\frac{a}{p}\right) = (-1)^j$. D'autre part, $\mathbf{F}_p^*$ a un seul élément d'ordre 2, à savoir $\overline{w}^{\frac{p-1}{2}}$, et celui-ci est égal à -1 car son carré est 1; donc, dans $\mathbf{Z}$, on a $-1 \equiv w^{\frac{p-1}{2}}$ (mod. p). Ainsi

$$\left(\frac{a}{p}\right) = (-1)^j \equiv w^{j.\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \pmod{p}. \qquad \text{CQFD.}$$

Nous allons maintenant démontrer un célèbre résultat, qui montre que les propriétés de congruences modulo deux nombres premiers impairs distincts ne sont pas indépendantes.

THÉORÈME 1 (« Loi de réciprocité quadratique de Legendre-Gauss. »)
Si p et q sont deux nombres premiers impairs distincts, on a

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

En effet considérons, dans une extension convenable de $\mathbf{F}_q$, une racine primitive p-ième de l'unité w. Comme $w^p = 1$, la notation w^x a un sens $x \in \mathbf{F}_p$. Nous écrirons aussi le symbole de Legendre $\left(\frac{x}{p}\right)$ pour $x \in \mathbf{F}_p^*$, car $\left(\frac{d}{p}\right)$ ne dépend évidemment que de la classe de d mod. p. Pour $a \in \mathrm{F}_p^*$, considérons la « *somme de Gauss* ».

3. $\tau(a) = \sum_{x \in \mathbf{F}_p^*} \left(\frac{x}{p}\right) w^{ax}$

C'est un élément d'une extension de $\mathbf{F}_q$. Posant $ax = y$, on a

$$\tau(a) = \sum_{y \in \mathbf{F}_p^*} \left(\frac{ya^{-1}}{p}\right) w^y = \left(\frac{a^{-1}}{p}\right) \sum_{y \in {}^*_p} \left(\frac{y}{p}\right) w^y$$

(par (2)), d'où

4. $\tau(a) = \left(\frac{a}{p}\right) \tau(1).$

D'autre part, comme on calcule en caractéristique q et que $\left(\frac{x}{p}\right) \in \mathbf{F}_q$, on a $\tau(1)^q = \sum_{x \in \mathbf{F}_p^*} \left(\frac{x}{p}\right)^q w^{qx}$, d'où, en identifiant q à sa classe mod. p,

5. $\tau(1)^q = \tau(q).$

Calculons maintenant $\tau(1)^2$. On a

$$\tau(1)^2 = \sum_{x, y \in \mathbf{F}_p^*} \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) w^{x+y}.$$

Posant $y = tx$, il vient

$$\tau(1)^2 = \sum_{x, t \in \mathbf{F}_p^*} \left(\frac{x}{p}\right)^2 \left(\frac{t}{p}\right) w^{x(1+t)} = \sum_{x,t} \left(\frac{t}{p}\right) w^{x(1+t)} = \sum_{t \in \mathbf{F}_p^*} \left[\left(\frac{t}{p}\right) \sum_{x \in \mathbf{F}_p^*} w^{x(1+t)}\right].$$

Si $w^{1+t} \neq 1$, on a $\sum_{j=0}^{p-1} (w^{1+t})^j = 0$ par la formule de la progression géométrique, car $(w^{1+t})^p = 1$; d'où $\sum_{x \in \mathbf{F}_p^*} w^{x(1+t)} = -1$. Si $w^{1+t} = 1$, on a $\sum_{x \in \mathbf{F}_p^*} w^{x(1+t)} = p - 1$; ce dernier cas n'a lieu que pour $t = -1$, car w est une racine primitive p-ème de l'unité. On a donc

$$\tau(1)^2 = \left(\frac{-1}{p}\right)(p-1) - \sum_{t \in \mathbf{F}_p^*,\, t \neq -1} \left(\frac{t}{p}\right).$$

Comme il y a autant de carrés que de non-carrés dans $\mathbf{F}_p^*$, on a

$$\sum_{t\in\mathbf{F}_p^*}\left(\frac{t}{p}\right)=0, \quad \text{d'où} \quad \tau(1)^2=\left(\frac{-1}{p}\right)(p-1)+\left(\frac{-1}{p}\right)=\left(\frac{-1}{p}\right)p.$$

Par le critère d'Euler (prop. 1) on a donc

6. $\tau(1)^2=(-1)^{\frac{p-1}{2}}p.$

Enfin, par 4 et 5, on a $\tau(1)^q=\tau(q)=\left(\frac{q}{p}\right)\tau(1)$. Comme $\tau(1)$ est non nul par (6), on simplifie : $\tau(1)^{q-1}=\left(\frac{q}{p}\right)$. Par (6) encore on a

$$\left(\frac{q}{p}\right)=(\tau(1)^2)^{\frac{q-1}{2}}=(-1)^{\frac{(p-1)(q-1)}{4}}p^{\frac{q-1}{2}}.$$

Comme $p^{\frac{q-1}{2}}=\left(\frac{q}{p}\right)$ (prop. 1) et que $\left(\frac{p}{q}\right)=\left(\frac{p}{q}\right)^{-1}$, la loi de réciprocité est démontrée.

Proposition 2 (« formules complémentaires »). *Si p est un nombre premier impair on a*

a) $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$.

b) $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$.

En effet *a*) est un cas particulier du critère d'Euler (prop. 1). Démontrons donc *b*). Notons d'abord que, comme les carrés de 1, 3, 5, 7 mod. 8 sont 1, 1, 1, 1, on a $p^2\equiv 1 \pmod 8$, et la formule écrite a donc un sens. Remarquons ensuite que, dans le groupe $H=\{1, 3, 5, 7\}$ des éléments inversibles de $\mathbf{Z}/8\mathbf{Z}$, $\{1, 7\}$ est un sous-groupe H' d'indice 2; posons $\theta(x)=1$ pour $x\in H'$ et $\theta(x)=-1$ pour $x\in H-H'$, de sorte qu'on a $\theta(xy)=\theta(x)\theta(y)$ pour $x, y\in H$. Soit alors w une racine primitive 8-ième de l'unité dans une extension de $\mathbf{F}_p$. Comme dans le th. 1, considérons, pour $a\in H$, la « *somme de Gauss* ».

7. $\tau(a)=\sum_{x\in H}\theta(x)w^{ax}.$

Comme dans le th. 1 on a $\tau(a)=\theta(a)\tau(1)$ et $\tau(1)^p=\tau(p)$ (en identifiant p à sa classe mod. 8). D'après la définition de $\theta(x)$, on a

$$\begin{aligned}\tau(1)&=w-w^3-w^5+w^7=(1-w^2)(w-w^5)\\&=w(1-w^2)(1-w^4)=2w(1-w^2)\end{aligned}$$

(car $w^8 = 1$ et $w^4 = -1$); d'où

$$\tau(1)^2 = 4w^2(1 - 2w^2 + w^4) = -8w^4 = 8.$$

Comme dans le th. 1, on en déduit $\tau(1)^p = \tau(p) = \theta(p)\tau(1)$; d'où, en simplifiant $\theta(p) = (\tau(1)^2)^{\frac{p-1}{2}} = 8^{\frac{p-1}{2}} = \left(\frac{8}{p}\right)$ (prop. 1) $= \left(\frac{2}{p}\right)^3 = \left(\frac{2}{p}\right)$. On a donc $\left(\frac{2}{p}\right) = \theta(p)$. Or on constate par calcul direct, pour $x = 1$, 3, 5, 7 (ou, plus efficacement, pour $x = 1, 3, -3, -1$) qu'on a $\theta(x) = (-1)^{\frac{x^2-1}{8}}$, et que $\frac{x^2-1}{8}$ ne dépend que de la classe de x mod. 8. CQFD.

Exemple d'application. La loi de réciprocité et les formules complémentaires permettent de calculer le symbole de Legendre par réductions successives. Calculons ainsi $\left(\frac{23}{59}\right)$, sans avoir à écrire la longue table des carrés modulo 59. On a

$$\begin{aligned}\left(\frac{23}{59}\right) &= (-1)^{11\cdot 29}\left(\frac{59}{23}\right) = -\left(\frac{13}{23}\right) = -(-1)^{6\cdot 11}\left(\frac{23}{13}\right) = -\left(\frac{10}{13}\right)\\ &= -\left(\frac{-3}{13}\right) = -\left(\frac{-1}{13}\right)\left(\frac{3}{13}\right) = -(-1)^6\left(\frac{3}{13}\right)\\ &= -(-1)^{6\cdot 1}\left(\frac{13}{3}\right) = -\left(\frac{1}{3}\right) = -1.\end{aligned}$$

Donc 23 n'est pas un carré modulo 59.

5.6. Théorème des deux carrés

Nous allons appliquer la prop. 1 du § 4 au corps $L = \mathbf{Q}[i]$ où $i^2 = -1$. Comme $-1 \equiv 3$ (mod. 4) l'anneau B des entiers de L est $\mathbf{Z} + \mathbf{Z}i$; on l'appelle *l'anneau des entiers de Gauss*; son discriminant est -4 (§ 3, exemple). Si p est un nombre premier impair, et si u est un générateur du groupe cyclique $\mathbf{F}_p^*$, on a $-1 = u^{\frac{p-1}{2}}$. Donc -1 est un carré dans $\mathbf{F}_p$ si et seulement si $\frac{p-1}{2}$ est pair. D'où la classification :

- 2 se ramifie dans $\mathbf{Q}[i]$;
- les nombres premiers de la forme $4k + 1$ sont décomposés;
- les nombres premiers de la forme $4k + 3$ sont inertes.

Le résultat suivant va nous être utile :

Proposition 1.. *L'anneau* $B = \mathbf{Z} + \mathbf{Z}i$ *des entiers de Gauss est principal.*

Écrasons, en effet, cette mouche avec un gros pavé. Avec les notations du chap. IV, § 3, on a $n = 2$, $r_1 = 0$, $r_2 = 1$, $d = -4$. Donc (chap. IV, § 3, cor. de la prop. 1), toute classe d'idéaux de B contient un idéal entier de norme $\leqslant \frac{4}{\pi}\cdot\frac{2}{4}|4|^{1/2} = \frac{4}{\pi}$, donc contient l'idéal unité B (qui est le seul idéal entier de norme 1) car $\frac{4}{\pi} < 2$. Ainsi tout idéal de B est équivalent à l'idéal principal B, et est donc principal. CQFD.

Esquisse de démonstration élémentaire : comme les points de B forment un quadrillage de $\mathbf{C}$, un peu de géométrie montre que, pour tout $x \in \mathbf{Q}[i]$, il existe $z \in \mathrm{B}$ tel que $\mathrm{N}(x - z) = |x - z|^2 \leqslant \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2} < 1$; alors, si $\mathfrak{a}$ est un idéal non nul de B, on choisit dans $\mathfrak{a}$ un élément non nul u de norme minimale (NB : cette norme est un entier > 0); pour $v \in \mathfrak{a}$ on approche $\frac{v}{u}$ par un $z \in \mathrm{B}$ tel que $\mathrm{N}\left(\frac{v}{u} - z\right) < 1$; alors

$$\mathrm{N}(v - zu) < \mathrm{N}(u), \qquad \text{d'où} \qquad v - zu = 0$$

car $v - zu \in \mathfrak{a}$; par conséquent $v \in \mathrm{B}u$ et $\mathfrak{a} = \mathrm{B}u$. On notera l'analogie avec le processus de division euclidienne dans $\mathbf{Z}$.

PROPOSITION 2 (Fermat). *Tout nombre premier* $p \equiv 1 \pmod{4}$ *est somme de deux carrés* (i.e. *est de la forme* $p = a^2 + b^2$ *avec* $a, b \in \mathbf{N}$).

En effet $\mathrm{B}p$ se décompose en un produit $\mathfrak{p}_1\mathfrak{p}_2$ d'idéaux premiers distincts. D'où $p^2 = \mathrm{N}(\mathrm{B}p) = \mathrm{N}(\mathfrak{p}_1)\mathrm{N}(\mathfrak{p}_2)$ (chap. III, § 5, prop. 2). Comme les normes de $\mathfrak{p}_1$ et de $\mathfrak{p}_2$ sont distinctes de 1, on a nécessairement

$$\mathrm{N}(\mathfrak{p}_1) = \mathrm{N}(\mathfrak{p}_2) = p.$$

Or, $\mathfrak{p}_1$ est un idéal principal $\mathrm{B}(a + bi)$ $(a, b \in \mathbf{Z})$ (prop. 1); d'où, en prenant les normes, $p = \mathrm{N}(a + bi) = a^2 + b^2$. CQFD.

THÉORÈME 1. *Soient* x *un entier naturel*, et $x = \prod_p p^{v_p(x)}$ *sa décomposition en facteurs premiers. Pour que* x *soit somme de deux carrés, il faut et il suffit que, pour tout* $p \equiv 3 \pmod{4}$, *l'exposant* $v_p(x)$ *soit pair.*

Pour démontrer la suffisance, remarquons qu'une somme de deux carrés $a^2 + b^2$ est la norme $\mathrm{N}(a + bi)$ d'un élément de B; par la multiplicativité des normes, l'ensemble S des sommes de deux carrés est donc stable par multiplication. Comme $2 = 1^2 + 1^2 \in \mathrm{S}$ et que tout carré est élément de $\mathrm{S}(x^2 = x^2 + 0^2)$, il résulte alors de la prop. 2 que notre condition est suffisante.

Réciproquement soient $x = a^2 + b^2$ une somme de deux carrés $(a, b \in \mathbf{N})$ et p un nombre premier $\equiv 3$ mod. 4. On a vu que l'idéal $\mathrm{B}p$ de B est premier. Or on a $x = a^2 + b^2 = (a + bi)(a - bi)$. Soit n l'exposant de $\mathrm{B}p$ dans la décomposition de $\mathrm{B}(a + bi)$ en facteurs premiers. Comme $\mathrm{B}p$ est stable par l'automorphisme $\sigma : u + iv \mapsto u - iv$ de B, et que $\sigma(a + ib) = a - ib$, l'exposant de $\mathrm{B}p$ dans la décomposition de

$B(a - ib)$ est aussi n; dans celle de $B(a^2 + b^2)$, l'exposant de Bp est donc $2n$. Comme aucun nombre premier distinct de p n'appartient à Bp (car $Bp \cap \mathbf{Z} = p\mathbf{Z}$), on a $v_p(x) = 2n$ et $v_p(x)$ est pair. CQFD.

5.7. Théorème des quatre carrés

Dans ce §, nous nous proposons de démontrer le théorème suivant :

THÉORÈME 1 (Lagrange). *Tout entier naturel est somme de quatre carrés.*

La méthode employée est analogue à celle du § 6 : au lieu de l'anneau des entiers de Gauss, nous travaillerons dans un anneau de *quaternions* convenablement choisi.

Commençons par définir les quaternions. Étant donné un anneau A, nous noterons $(1, i, j, k)$ la base canonique du A-module A^4, et nous définissons une multiplication par :

$$1. \quad \begin{cases} 1 \text{ est élément unité} \\ i^2 = j^2 = k^2 = -1 \\ ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j. \end{cases}$$

Nous étendons cette multiplication aux éléments $a + bi + cj + ck$ de A^4 par linéarité; la distributivité est alors évidente. Quant à l'associativité, il suffit de la vérifier sur les éléments de base : ainsi

$$i(jk) = i^2 = -1 = k^2 = (ij)k;$$

les formules où figure 1 étant évidentes, il reste $3^3 - 1 = 26$ formules à vérifier; le lecteur patient et incrédule en réduira le nombre par permutations, et vérifiera celles qui restent; les autres croiront l'auteur sur parole. Muni de cette multiplication, A^4 est donc un *anneau non nécessairement commutatif*, et même une A-*algèbre*, qu'on appelle *l'anneau des quaternions* sur A, et qu'on note $\mathbf{H}(A)$ ($\mathbf{H}$ en honneur de W. R. Hamilton, inventeur des quaternions).

Étant donné un quaternion $z = a + bi + cj + dk$ sur A (on écrit a au lieu de $a.1$), on appelle *quaternion conjugué* de z, et on note $\bar{z}$ le quaternion $\bar{z} = a - bi - cj - dk$.

LEMME 1. *On a* $\overline{z + z'} = \bar{z} + \bar{z}'$, $\overline{zz'} = \bar{z}'.\bar{z}$ *et* $\bar{\bar{z}} = z$; *en termes plus savants,* $z \mapsto \bar{z}$ *est un antiautomorphisme involutif de* $\mathbf{H}(A)$.

La première et la troisième formule sont évidentes. Pour la seconde on est ramenés par linéarité à montrer qu'on a $\overline{xy} = \bar{y}.\bar{x}$ lorsque $x, y \in \{1, i, j, k\}$. Or c'est clair si $x = 1$ ou si $y = 1$. Si $x = y = i$ on a $\overline{xy} = \overline{-1} = -1$ et $\bar{y}.\bar{x} = (-i)(-i) = i^2 = -1$. Si $x = i$ et $y = j$ on a

$$\overline{xy} = \bar{k} = -k \quad \text{et} \quad \bar{y}.\bar{x} = (-j)(-i) = ji = -k.$$

Les autres vérifications s'en déduisent par permutation. CQFD.

Étant donné un quaternion z sur A, on appelle *norme réduite* de z, et on note $N(z)$ le quaternion $z\bar{z}$.

Lemme 2 a) *Étant donné un quaternion* $z = a + bi + cj + dk$ *sur* A, *on a* $N(z) = a^2 + b^2 + c^2 + d^2$ (quatre carrés!), *donc* $N(z) \in A$.

b) *Étant donnés deux quaternions* z, z' *sur* A, *on a* $N(zz') = N(z)N(z')$.

Pour *a*), on développe $(a + bi + cj + dk)\ (a - bi - cj - dk)$: par (1) les termes « rectangles » disparaissent, et il reste $a^2 + b^2 + c^2 + d^2$. On voit aussi que $z\bar{z} = \bar{z}z$. Alors

$$N(zz') = zz'.\overline{zz'} = zz'\bar{z}'\bar{z} = zN(z')\bar{z} = z\bar{z}N(z')$$

(car l'élément $N(z')$ de A est permutable à tout quaternion); d'où $N(zz') = N(z).N(z')$. CQFD.

Le lemme 2 montre que, dans un anneau A (commutatif), l'ensemble des normes réduites de quaternions, c'est-à-dire des sommes de 4 carrés, est stable pour la multiplication.

Celà étant nous considérerons, dans $\mathbf{H}(\mathbf{Q})$, le sous-anneau non-commutatif $\mathbf{H}(\mathbf{Z})$ et l'ensemble $\mathbf{H}$ des « *quaternions d'Hurwitz* » $a + bi + cj + dk$ où a, b, c, d sont, ou bien tous les quatre dans $\mathbf{Z}$, ou bien tous les quatre dans $\frac{1}{2} + \mathbf{Z}$.

Lemme 3 a) *L'ensemble* $\mathbf{H}$ *des quaternions d'Hurwitz est un sous-anneau non commutatif de* $\mathbf{H}(\mathbf{Q})$ *contenant* $\mathbf{H}(\mathbf{Z})$, *et stable par* $z \mapsto \bar{z}$

b) *Pour tout* $z \in \mathbf{H}$ *on a* $z + \bar{z} \in \mathbf{Z}$ *et* $N(z) = z\bar{z} \in \mathbf{Z}$

c) *Pour que* $z \in \mathbf{H}$ *soit inversible, il faut et il suffit que* $N(z) = 1$

d) *Tout idéal à gauche* (resp. *à droite*) $\mathfrak{a}$ *de* $\mathbf{H}$ *est principal* (i.e. *est de la forme* $\mathbf{H}z$ (reps. $z\mathbf{H}$)).

Pour *a*), toutes les assertions sont évidentes, sauf la stabilité de $\mathbf{H}$ pour la multiplication. Pour celle-ci il suffit de vérifier que, si on pose

$$u = \frac{1}{2}(1 + i + j + k),$$

on a $u.1$, $u.i$, $u.j$, $u.k$ et $u^2 \in \mathbf{H}$; or $u.1 = \frac{1}{2}(1 + i + j + k)$, $u.i = \frac{1}{2}(-1 + i + j - k)$, $u.j = \frac{1}{2}(-1 - i + j + k)$,

$$u.k = \frac{1}{2}(-1 + i - j + k);$$

d'où, par addition $2u^2 = \frac{1}{2}(-2 + 2i + 2j + 2k)$ et $u^2 \in \mathbf{H}$.

Pour b), si

$$z = \frac{1}{2} + a + \left(\frac{1}{2} + b\right)i + \left(\frac{1}{2} + c\right)j + \left(\frac{1}{2} + d\right)k (a, b, c, d \in \mathbf{Z}),$$

on a $z + \bar{z} = 1 + 2a \in \mathbf{Z}$, et

$$z\bar{z} = \left(\frac{1}{2} + a\right)^2 + \left(\frac{1}{2} + b\right)^2 + \left(\frac{1}{2} + c\right)^2 + \left(\frac{1}{2} + d\right)^2 \in \frac{4}{4} + \mathbf{Z} \subset \mathbf{Z}$$

(lemme 2, b).

Si z est inversible dans $\mathbf{H}$, et si z' est son inverse, on a

$$\mathrm{N}(z)\mathrm{N}(z') = \mathrm{N}(zz') = 1;$$

comme $\mathrm{N}(z)$ et $\mathrm{N}(z')$ sont des entiers > 0 ((b) et lemme 2, a)), on a nécessairement $\mathrm{N}(z) = 1$. Réciproquement si $z \in \mathbf{H}$ et si $\mathrm{N}(z) = 1$, on a $z\bar{z} = \bar{z}.z = \mathrm{N}(z) = 1$ et z est inversible car $\bar{z} \in \mathbf{H}$ par a). Ceci démontre c).

Démontrons enfin d). Étant donné un quaternion

$$x = a + bi + cj + dk \in \mathbf{H}(\mathbf{Q}),$$

il existe quatre entiers $a', b', c', d' \in \mathbf{Z}$ tels que

$$|a - a'| \leqslant \frac{1}{2}, \quad |b - b'| \leqslant \frac{1}{2}, \quad |c - c'| \leqslant \frac{1}{2}, \quad |d - d'| \leqslant \frac{1}{2};$$

posons $z = a' + b'i + c'j + d'k$; on a alors

$$\mathrm{N}(x - z) = (a - a')^2 + (b - b')^2 + (c - c')^2 + (d - d')^2 \leqslant 4 \cdot \frac{1}{4} = 1.$$

Il y a même inégalité stricte, sauf dans le cas où a, b, c, d sont tous dans $\frac{1}{2} + \mathbf{Z}$; mézalor on a $x \in \mathbf{H}$. Donc, pour tout quaternion $x \in \mathbf{H}(\mathbf{Q})$, il existe un quaternion d'Hurwitz $z \in \mathbf{H}$ tel que $\mathrm{N}(x - z) < 1$ (c'est justement pour avoir l'inégalité stricte qu'on a introduit les quaternions d'Hurwitz, ceux de $\mathbf{H}(\mathbf{Z})$ n'auraient pas suffi). Ceci étant, soit $\mathfrak{a}$ un idéal à gauche de $\mathbf{H}$; pour montrer qu'il est principal, on peut supposer $\mathfrak{a} \neq (0)$. Choisissons, dans $\mathfrak{a}$, un élément non nul u de norme réduite minimale (il en existe, car ces normes sont des entiers > 0 par b); alors u est inversible dans $\mathbf{H}(\mathbf{Q})$, car son inverse est $\bar{u}\mathrm{N}(u)^{-1}$ (ceci montre d'ailleurs que $\mathbf{H}(\mathbf{Q})$ est un corps non-commutatif). Pour $y \in \mathfrak{a}$, formons $yu^{-1} \in \mathbf{H}(\mathbf{Q})$ et prenons un élément $z \in \mathbf{H}$ tel que $\mathrm{N}(yu^{-1} - z) < 1$. Alors, par le lemme 2, b, on a $\mathrm{N}(y - zu) = \mathrm{N}((yu^{-1} - z)u) < \mathrm{N}(u)$. Comme $y - zu \in \mathfrak{a}$ et que $\mathrm{N}(u)$ est minimal, on en déduit $y - zu = 0$, $y \in \mathbf{H}u$ et $\mathfrak{a} = \mathbf{H}u$. CQFD.

Ceci étant, comme l'ensemble des sommes de quatre carrés dans $\mathbf{Z}$ est multiplicativement stable (cf. lemme 2), le th. 1 se ramène à la :

PROPOSITION 1. *Tout nombre premier* p *est somme de quatre carrés.*

Comme $2 = 1^2 + 1^2 + 0^2 + 0^2$, on peut supposer p impair. Comme p est permutable à tout quaternion, l'idéal à gauche $\mathbf{H}p$ est bilatère; on peut donc former l'anneau quotient $\mathbf{H}/\mathbf{H}p$. Comme p est impair, tout $z \in \mathbf{H}$ est congru mod. $\mathbf{H}p$ à un élément de $\mathbf{H}(\mathbf{Z})$ (si les composantes de z sont toutes dans $\frac{1}{2} + \mathbf{Z}$, on forme $z + p \cdot \frac{1}{2}(1 + i + j + k)\Big)$; donc $\mathbf{H}/\mathbf{H}p$ est isomorphe au quotient correspondant de $\mathbf{H}(\mathbf{Z})$, c'est-à-dire à $\mathbf{H}(\mathbf{F}_p)$.

Or, comme la forme $a^2 + b^2 + c^2 + d^2$ représente 0 dans $\mathbf{F}_p$ (chap. I, § 7, th. 2; voir en remarque ci-dessous une démonstration directe), $\mathbf{H}(\mathbf{F}_p)$ admet des éléments non nuls de norme réduite nulle; un tel élément n'est pas inversible (lemme 2, b), donc engendre un idéal à gauche non trivial. En revenant à $\mathbf{H}$, on voit que $\mathbf{H}p$ est contenu dans un idéal à gauche $\mathbf{H}z$ distinct de $\mathbf{H}$ et de $\mathbf{H}p$. Par conséquent on a $p = z'z$ avec $z, z' \in \mathbf{H}$ non inversibles. Alors $p^2 = \mathrm{N}(p) = \mathrm{N}(z)\mathrm{N}(z')$, et, comme $\mathrm{N}(z)$ et $\mathrm{N}(z')$ sont des entiers > 1 (lemme, 3, b) et c)), on a $\mathrm{N}(z) = \mathrm{N}(z') = p$.

Posons $z = a + bi + cj + dk$ $\left(a, b, c, d \in \mathbf{Z} \text{ ou } \in \frac{1}{2} + \mathbf{Z}\right)$. Si $a, b, c, d \in \mathbf{Z}$, on a $p = \mathrm{N}(z) = a^2 + b^2 + c^2 + d^2$, et on a gagné. Reste à montrer que, si $a, b, c, d \in \frac{1}{2} + \mathbf{Z}$, on peut se ramener au cas précédent en multipliant z par un élément de norme réduite 1 de $\mathbf{H}$, plus précisément par un élément de la forme $\frac{1}{2}(\pm 1 \pm i \pm j \pm k)$. En effet considérons la classe η de $2z$ dans $\mathbf{H}(\mathbf{Z})/4\mathbf{H}(\mathbf{Z}) \simeq \mathbf{H}(\mathbf{Z}/4\mathbf{Z})$; comme $\mathrm{N}(z) \in \mathbf{Z}$, on a $\mathrm{N}(2z) \in 4\mathbf{Z}$, d'où $\mathrm{N}(\eta) = 0$ et $\eta\bar{\eta} = 0$; or $\bar{\eta}$ est la classe d'un quaternion z' de la forme $\pm 1 \pm i \pm j \pm k$; alors $u = \frac{1}{2}z' \in \mathbf{H}$, u est de norme réduite 1, et, comme la classe de $(2z).(2u)$ est nulle mod. 4, on a $zu \in \mathbf{H}(\mathbf{Z})$. Comme $p = \mathrm{N}(z) = \mathrm{N}(zu)$, notre assertion est démontrée. CQFD.

Remarque. Voici une démonstration très élémentaire du fait que, sur un corps fini K, la forme quadratique $a^2 + b^2 + c^2 + d^2$ *représente* 0 (i.e. a un zéro non trivial dans K^4). En prenant $c = 1$, $d = 0$, il suffit de montrer que l'équation $a^2 + b^2 + 1 = 0$ a une solution dans K^2. Écrivons la $b^2 + 1 = -a^2$. En caractéristique 2, on peut prendre $b = 0$ et $a = 1$. Sinon, si q est le cardinal de K, il y a $\frac{q+1}{2}$ carrés dans K $\left(0 \text{ et les } \frac{q-1}{2}\right.$ carrés non nuls); donc l'ensemble T (resp. T′) des éléments de K de la forme $b^2 + 1$ avec $b \in \mathrm{K}$ (resp. de la forme $-a^2$ avec $a \in \mathrm{K}$) a $\frac{q+1}{2}$ éléments par translation (resp. symétrie). Comme $\frac{q+1}{2} + \frac{q+1}{2} > q$, on a $\mathrm{T} \cap \mathrm{T}' \neq \emptyset$, ce qui signifie que $b^2 + 1 = -a^2$ a une solution CQFD.

Extensions galoisiennes
des corps de nombres

6.1. Théorie de Galois

Ce § est un complément à la théorie générale des corps commutatifs cf. chap. II, §§ 3, 4, 6 et 7). Étant donnés un corps L et un ensemble G d'automorphismes de L, l'ensemble des $x \in \mathrm{L}$ tels que $\sigma(x) = x$ pour tout $\sigma \in \mathrm{G}$ est, comme on le voit aussitôt, un *sous-corps* de L, qu'on appelle le *corps des invariants* de G. D'autre part, étant donnée une extension L d'un corps K, l'ensemble des K-automorphismes de L est un *groupe* pour la composition des applications.

THÉORÈME 1. *Soit* L *une extension de degré fini* n *d'un corps* K *fini ou de caractéristique* 0. *Les conditions suivantes sont équivalentes:*

a) K *est le corps des invariants du groupe* G *des* K-*automorphismes de* L*;*

b) *pour tout* $x \in \mathrm{L}$, *le polynôme minimal de* x *sur* K *a toutes ses racines dans* L*;*

c) L *est engendrée par les racines d'un polynôme sur* K.

Dans ces conditions le groupe G *des* K-*automorphismes de* L *a* n *éléments.*

Montrons que *a*) implique *b*). En effet, pour $x \in \mathrm{L}$, le polynôme $\prod_{\sigma \in \mathrm{G}} (\mathrm{X} - \sigma(x))$ est invariant par G (car tout $\tau \in \mathrm{G}$ permute entre eux ses facteurs) (1). Donc ses coefficients appartiennent à K. Comme il admet x pour racine ($1 \in \mathrm{G}$), c'est un multiple du polynôme minimal de x sur K (chap. II, § 3, (4)). D'où *b*).

Pour voir que *b*) implique *c*), on prend un élément primitif x de L sur K (chap. II, § 4, cor. du th. 1). Son polynôme minimal sur K a toutes ses racines dans L par *b*), et celles-ci engendrent évidemment L sur K.

Prouvons enfin que *c*) implique *a*). Par hypothèse L est engendrée sur K par un nombre fini d'éléments $(x^{(1)}, \ldots, x^{(q)})$ et par tous leurs conjugués $(x_j^{(i)})$ (chap. II, § 4). Alors tout K-isomorphisme σ de L dans une extension de L envoie chacun de ces générateurs sur un autre; on a donc $\sigma(\mathrm{L}) \subset \mathrm{L}$, d'où $\sigma(\mathrm{L}) = \mathrm{L}$ par l'algèbre linéaire car σ est une application K-linéaire injective; autrement dit σ est un K-*automorphisme* de L.

(1) La finitude de G résulte du chap. II, § 4, th. 1.

Ainsi le groupe G des K-automorphismes de L à n éléments (chap. II, § 4, th. 1 et cor.). Soit alors $x \in L$ invariant par G; alors tout $\sigma \in G$ est un $K[x]$-automosphisme de L; or (chap. II, § 4) il y a exactement $[L : K[x]]$ $K[x]$-isomorphismes de L dans une extension de L; on a donc $n \leqslant [L : K[x]]$, d'où $n = [L : K[x]]$, $K[x] = K$ et $x \in K$. Ceci démontre *a*). L'assertion card (G) $= n$ a été démontrée en cours de route. CQFD.

DÉFINITION 1. *Si les conditions du th.* 1 *sont satisfaites, on dit que* L *est une extension galoisienne de* K, *et que* G *est le groupe de Galois de* L *sur* K. *Si* G *est abélien* (resp. *cyclique*) *on dit que* L *est une extension abélienne* (resp. *cyclique*) *de* K.

COROLLAIRE DU THÉORÈME 1. *Soient* K *un corps fini ou de caractéristique* 0, L *une extension de degré fini* n *de* K, *et* H *un groupe d'automorphismes de* L *admettant* K *pour corps d'invariants. Alors* L *est extension galoisienne de* K, *et* H *est son groupe de Galois.*

En effet, pour $x \in L$, le polynôme $\prod_{\sigma \in H} (X - \sigma(x))$ est invariant par H, donc a ses coefficients dans K, et est par conséquent multiple du polynôme minimal de x sur K; ainsi, par le th. 1, *b*), L est extension galoisienne de K. Si G désigne son groupe de Galois, on a $H \subset G$ et card (G) $= n$ (th. 1). Prenons alors un élément primitif x de L sur K (chap. II, § 4, cor. du th. 1) et considérons le polynôme

$$P(X) = \prod_{\sigma \in H} (X - \sigma(x));$$

comme plus haut il a ses coefficient dans K et est multiple du polynôme minimal de x sur K; d'où $n \leqslant d^o(P)$. Comme

$$d^o(P) = \text{card}\,(H) \leqslant \text{card}\,(G) = n,$$

on en déduit $H = G$. CQFD.

THÉORÈME 2. *Soient* K *un corps fini ou de caractéristique* 0, L *une extension galoisienne de* K, *et* G *son groupe de Galois. A tout sous-groupe* G' *de* G *associons le corps des invariants* $k(G')$ *de* G', *et à tout sous-corps* K' *de* L *contenant* K *associons le sous-groupe* $g(K') \subset G$ *des* K'*-automorphismes de* L.

a) *Les applications* g *et* k *sont des bijections réciproques l'une de l'autre, décroissantes pour les relations d'inclusion. De plus* L *est l'extension galoisienne de tout corps intermédiaire* K' (i.e. $K \subset K' \subset L$)

b) *Pour qu'un corps intermédiaire* K' *soit extension galoisienne de* K, *il faut et il suffit que* $g(K')$ *soit un sous-groupe invariant de* G; *alors le groupe de Galois de* K' *sur* K *s'identifie au groupe quotient* $G/g(K')$.

En effet, pour tout corps intermédiaire K' et tout $x \in L$, le polynôme minimal de x sur K' divise le polynôme minimal de x sur K; il a donc toutes ses racines dans L par le th. 1, *b*), de sorte que L est extension *galoisienne* de K' par le th. 1, *b*) encore. Ainsi K' est le corps des invariants du groupe $g(K')$ des K'-automorphismes de L (th. 1, *a*)); autrement dit $k(g(K')) = K'$. Soit maintenant G' un sous-groupe de G; alors G' est le groupe de Galois de L sur $k(G')$ (cor. du th. 1); autrement dit on a $G' = g(k(G'))$. Les formules $k(g(K')) = K'$ et $g(k(G')) = G'$ montrent que k et g des bijections réciproques l'une de l'autre. Leur décroissance est évidente. Ceci démontre *a*).

Prouvons maintenant *b*). Soient K' un corps intermédiaire $(K \subset K' \subset L)$ Pour $x \in K'$, les racines du polynôme minimal de x sur K sont les $\sigma(x)$ $(x \in G)$; d'après le th. 1, *b*), pour que K' soit extension galoisienne de K, il faut et il suffit que $\sigma(x) \in K'$ pour tout $x \in K'$ et tout $\sigma \in G$, c'est-à-dire que $\sigma(K') \subset K'$ pour tout $\sigma \in G$. Or, si $\sigma(K') \subset K'$, si $\tau \in g(K')$ et si $x \in K'$, on a $\sigma^{-1}\tau\sigma(x) = \sigma^{-1}\sigma(x) = x$, d'où $\sigma^{-1}\tau\sigma \in g(K')$; autrement dit « K' galoisienne sur K » implique « $g(K')$ invariant dans G ». Inversement, supposons $g(K')$ invariant dans G; si $x \in K'$, si $\sigma \in G$ et si $\tau \in g(K')$, on a $\tau\sigma(x) = \sigma.\sigma^{-1}\tau\sigma(x) = \sigma(x)$ car $\sigma^{-1}\tau\sigma \in g(K')$ et car $x \in K'$; ainsi $\sigma(x)$ est invariant par tout élément τ de $g(K')$, de sorte que $\sigma(x) \in K'$; par conséquent « $g(K')$ invariant dans G » implique « $\sigma(K') \subset K'$ », et donc que K' est galoisienne sur K.

Déterminons enfin dans ce cas, le groupe de Galois de K' sur K. Comme on a $\sigma(K') \subset K'$ pour tout $\sigma \in G$ (et même $\sigma(K') = K'$ par l'algèbre linéaire), la restriction $\sigma|K'$ de σ à K' est un K-automorphisme de K'. On a alors un « homomorphisme de restriction » $\sigma \mapsto \sigma|K'$ de G dans le groupe de Galois H de K' sur K; son noyau est évidemment $g(K')$. Comme on a

$$\begin{aligned}\text{card }(H) &= [K' : K] = [L : K]\,[L : K']^{-1} = \text{card }(G).\text{card }(g(K'))^{-1}\\ &= \text{card }(G/g(K')),\end{aligned}$$

cet homomorphisme est surjectif, et $H \simeq G/g(K')$. CQFD.

Exemple 1. *Extensions quadratiques.*

Soient K un corps de caractéristique 0, et L une extension quadratique (i.e. de degré 2) de K. Comme au début du § 5, chap. II on voit que L est de la forme $K[x]$ où x est racine d'un polynôme $X^2 - d (d \in K$, d non carré dans $K)$. Comme l'autre racine de ce polynôme est $-x$, L admet un K-automorphisme non trivial σ défini par $\sigma(x) = -x$, i.e.

$$\sigma(a + bx) = a - bx \qquad (a,\ b \in K)$$

On a $\sigma^2 = 1$ et K est le corps des invariants de σ. Donc L est extension *galoisienne* de K, avec le groupe *cyclique* $\{1, \sigma\}$ pour groupe de Galois (th. 1 et cor. du th. 1).

Exemple 2. *Extensions cyclotomiques.*

Soient K un corps de caractéristique 0, z une racine primitive n-ème de l'unité dans une extension de K, et $L = K(z)$; on dit alors que L est une extension *cyclotomique* de K. Le polynôme minimal F(X) de z sur K divise $X^n - 1$ (chap. II, § 3, (4)), donc ses racines sont des racines n-èmes de l'unité et donc des puissances de z (chap. I, § 6). Ainsi L est extension *galoisienne* de K par le th. 1, *c*).

Soit G son groupe de Galois; tout $\sigma \in G$ est déterminé par $\sigma(z)$, qui est une puissance $z^{j(\sigma)}$ de z où $j(\sigma)$ est bien déterminé mod. n. Pour $\sigma, \tau \in G$ on a $\sigma\tau(z) = \sigma(z^{j(\tau)}) = \sigma(z)^{j(\tau)} = z^{j(\sigma)j(\tau)}$ d'où

$$j(\sigma\tau) \equiv j(\sigma)j(\tau)$$

(mod. n). Autrement dit, on peut considérer $\sigma \mapsto j(\sigma)$ comme un *homomorphisme* $G \to (\mathbf{Z}/n\mathbf{Z})^*$. Comme $j(\sigma)$ détermine σ de façon unique, cet homomorphisme est *injectif* et G est abélien. Ainsi *toute extension cyclotomique est abélienne.* Si n est premier, cette extension est même *cyclique,* car G est isomorphe à un sous-groupe de $(\mathbf{Z}/n\mathbf{Z})^* = \mathbf{F}_n^*$ (chap. I, § 7, th. 1, *b*)).

Comme tout sous-groupe d'un groupe abélien est invariant, tout corps intermédiaire K′ d'une extension cyclotomique L de K est extension galoisienne (et même abélienne) de K (th. 2, *b*)). En particulier tout sous-corps d'un corps cyclotomique est extension abélienne de $\mathbf{Q}$. Réciproquement on démontre (théorème de Kronecker-Weber) que toute extension abélienne de $\mathbf{Q}$ est un sous-corps d'un corps cyclotomique.

On notera que, avec les notations précédentes, l'automorphisme σ *élève toutes les racines n-èmes de l'unité à la puissance* $j(\sigma)$, car celles-ci sont des puissances de z. Ainsi $\sigma \mapsto j(\sigma)$ est indépendant du choix de z.

Exemple 3. *Corps finis.*

Soit $\mathbf{F}_q$ un corps *fini* ($q = p^s$ avec p premier); toute extension de degré fini de $\mathbf{F}_q$ est de la forme $\mathbf{F}_{q^n}$; son degré est n (chap. I, § 7). Or on sait que $\sigma : x \mapsto x^q$ est un automorphisme de $\mathbf{F}_{q^n}$ (*ibid.*, prop. 1), et que $\mathbf{F}_q$ est son corps des invariants (*ibid*, th. 1, *c*)). Pour tout $x \in \mathbf{F}_{q^n}$, on a $\sigma^j(x) = x^{q^j}$, d'où $\sigma^n = 1$ car $\mathbf{F}_{q^n}$ est l'ensemble des x tels que $x^{q^n} = x$ (*ibid.*, th. 1, *c*)). D'autre part, pour $1 \leqslant j \leqslant n - 1$, on a $\sigma^j \neq 1$ car $\mathbf{F}_{q^j} \neq \mathbf{F}_{q^n}$. Donc $\{1, \sigma, \ldots, \sigma^{n-1}\}$ est un groupe cyclique d'ordre n. Ainsi. d'après le cor. à la prop. 1, $\mathbf{F}_{q^n}$ *est une extension cyclique de degré* n *de* $\mathbf{F}_q$, *et son groupe de Galois a un générateur privilégié, à savoir* $x \mapsto x^q$, *qu'on appelle l'automorphisme de Frobenius.*

6.2. Groupe de décomposition et groupe d'inertie

Dans ce §, A *désigne un anneau de Dedekind,* K *son corps des fractions qu'on suppose de caractéristique* 0, K′ *une extension galoisienne de* K, n *son degré,* G *son groupe de Galois, et* A′ *la fermeture intégrale de* A *dans* K′.

En appliquant $\sigma \in G$ à une équation de dépendance intégrale (sur A) d'un élément $x \in A'$, on voit que $\sigma(x) \in A'$; donc :

1. A' *est stable par* G, *i.e.* $\sigma(A') = A'$ *pour tout* $\sigma \in G$.

En fait on a seulement démontré $\sigma(A') \subset A'$; mais on a alors aussi $\sigma^{-1}(A') \subset A'$ d'où $A' = \sigma\sigma^{-1}(A') \subset \sigma(A')$. Nous omettrons souvent dans la suite ce facile complément de raisonnement.

D'autre part, si $\mathfrak{p}$ est un idéal maximal de A et $\mathfrak{p}'$ un idéal maximal de A' tel que $\mathfrak{p}' \cap A = \mathfrak{p}$ (c'est-à-dire figurant dans la décomposition de $A'\mathfrak{p}$ en idéaux premiers; cf. chap. V, § 2, prop. 1), on a évidemment $\sigma(\mathfrak{p}') \cap A = \mathfrak{p}$, et $\sigma(\mathfrak{p}')$ figure dans la décomposition de $A'\mathfrak{p}$ avec le *même* exposant que $\mathfrak{p}'$. Nous dirons que $\mathfrak{p}'$ et $\sigma(\mathfrak{p}')$ sont des idéaux premiers *conjugués* de A'. Nous allons montrer qu'il n'y en a pas d'autres dans la décomposition de $A'\mathfrak{p}$:

PROPOSITION 1. *Si* $\mathfrak{p}$ *est un idéal maximal de* A, *les idéaux maximaux* $\mathfrak{p}'_i$ *de* A' *figurant dans la décomposition de* $A'\mathfrak{p}$ (i.e. *tels que* $\mathfrak{p}'_i \cap A = \mathfrak{p}$) *sont deux à deux conjugués, et ont le même degré résiduel* f *et le même indice de ramification* e; *ainsi* $A'\mathfrak{p} = \left(\prod_{i=1}^{g} \mathfrak{p}'_i\right)^e$, et $n = efg$.

L'assertion sur l'indice de ramification et le degré résiduel est évidente, car un automorphisme σ conserve *toutes* les relations algébriques. La formule $n = efg$ est alors un cas particulier de $\Sigma e_i f_i = n$ (chap. V, § 2, th. 1). Ceci étant, soit $\mathfrak{p}'$ l'un des $\mathfrak{p}'_i$, et supposons qu'un autre des $\mathfrak{p}'_i$, que nous noterons $\mathfrak{q}'$, ne soit pas conjugué de $\mathfrak{p}'$. Comme $\mathfrak{q}'$ et $\sigma(\mathfrak{p}')$ $(\sigma \in G)$ sont maximaux et distincts, on a $\sigma(\mathfrak{p}') \not\subset \mathfrak{q}'$. Or on a le lemme suivant

LEMME 1 (« lemme d'évitement des idéaux premiers »). *Soient* R *un anneau,* $\mathfrak{p}_1, \ldots, \mathfrak{p}_q$ *une famille finie d'idéaux premiers de* R, *et* $\mathfrak{b}$ *un idéal de* R *tel que* $\mathfrak{b} \not\subset \mathfrak{p}_i$ *pour tout* i. *Alors il existe* $b \in \mathfrak{b}$ *tel que* $b \notin \mathfrak{p}_i$ *pour tout* i.

En effet, en supprimant les $\mathfrak{p}_i$ non maximaux dans $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_q\}$, on peut supposer qu'on a $\mathfrak{p}_j \not\subset \mathfrak{p}_i$ pour $i \neq j$; soit alors $x_{ij} \in \mathfrak{p}_j$ tel que $x_{ij} \notin \mathfrak{p}_i$. D'autre part, comme $\mathfrak{b} \not\subset \mathfrak{p}_i$, il exixte $a_i \in \mathfrak{b}$ tel que $a_i \notin \mathfrak{p}_i$. Posons alors $b_i = a_i \prod_{j \neq i} x_{ij}$; on a $b_i \in \mathfrak{b}, b_i \in \mathfrak{p}_j$ pour $j \neq i$, et $b_i \notin \mathfrak{p}_i$ car $\mathfrak{p}_i$ est premier. Alors $b = b_1 + \cdots + b_q$ répond à la question, car $b \in \mathfrak{b}$ et que, pour tout i, on a $\sum_{j \neq i} b_j \in \mathfrak{p}_i$, $b_i \notin \mathfrak{p}_i$ et donc $b \notin \mathfrak{p}_i$. CQFD.

Ceci étant, le lemme montre qu'on a un élément $x \in \mathfrak{q}'$ tel que $x \notin \sigma(\mathfrak{p}')$ pour tout $\sigma \in G$. Considérons alors $N(x) = \prod_{\tau \in G} \tau(x)$ (chap. II, § 6, prop. 1); comme $\tau(x) \in A'$ pour tout $\tau \in G$ (par (1)) on a $N(x) \in \mathfrak{q}'$, d'où

$$N(x) \in \mathfrak{q}' \cap A = \mathfrak{p};$$

d'autre part on a $x \notin \tau^{-1}(\mathfrak{p}')$, d'où $\tau(x) \notin \mathfrak{p}'$ pour tout $\tau \in G$; comme $\mathfrak{p}'$ est premier, on en déduit $N(x) \notin \mathfrak{p}'$, ce qui contredit $N(x) \in \mathfrak{p}$. CQFD.

Ceci étant, soit $\mathfrak{p}'$ l'un des idéaux maximaux de A' tels que $\mathfrak{p}' \cap A = \mathfrak{p}$. Les $\sigma \in G$ tels que $\sigma(\mathfrak{p}') = \mathfrak{p}'$ forment un sous groupe D de G, qu'on appelle le *groupe de décomposition de* $\mathfrak{p}'$. Si g est le nombre des conjugués de $\mathfrak{p}'$ on a donc

2. $g = \text{card}\,(G).\text{card}\,(D)^{-1}$ ou $\text{card}\,(D) = n/g = ef.$

Pour $\sigma \in D$, les relations $\sigma(A') = A'$ et $\sigma(\mathfrak{p}') = \mathfrak{p}'$ montrent que σ définit, par passage au quotient, un automorphisme $\bar{\sigma}$ de $A'/\mathfrak{p}'$ (en effet $x \equiv y \pmod{\mathfrak{p}'}$ entraîne $\sigma(x) \equiv \sigma(y) \pmod{\mathfrak{p}'}$). Il est clair que $\bar{\sigma}$ est un $(A/\mathfrak{p})$-automorphisme. L'application $\sigma \mapsto \bar{\sigma}$ est un *homomorphisme* de groupes, dont le *noyau* est l'ensemble I des $\sigma \in D$ tels que $\sigma(x) - x \in \mathfrak{p}'$ pour tout $x \in A'$; ainsi I est un *sous-groupe invariant* de D, qu'on appelle le *groupe d'inertie* de $\mathfrak{p}'$.

Proposition 2. *Avec les mêmes notations, on suppose* $A/\mathfrak{p}$ *fini ou de caractéristique* 0. *Alors* $A'/\mathfrak{p}'$ *est extension galoisienne de degré* f *de* $A/\mathfrak{p}$, *et* $\sigma \mapsto \bar{\sigma}$ *est un homomorphisme surjectif de* D *sur son groupe de Galois. De plus* $\text{card}\,(I) = e$.

En effet soient K_D le corps des invariants de D, $A_D = A' \cap K_D$ la fermeture intégrale de A dans K_D et $\mathfrak{p}_D$ l'idéal premier $\mathfrak{p}' \cap A_D$. D'après la prop. 1 et la définition de D, $\mathfrak{p}'$ est le seul facteur premier de $A'\mathfrak{p}_D$; posons $A'\mathfrak{p}_D = \mathfrak{p}'^{e'}$, et notons f' le degré résiduel $[A'/\mathfrak{p}' : A_D/\mathfrak{p}_D]$. D'après le th. 1 du § 2, chap. V, le th. 2 du § 1, et (2) on a

$$e'f' = [K' : K_D] = \text{card}\,(D) = ef.$$

Comme $A/\mathfrak{p} \subset A_D/\mathfrak{p}_D \subset A'/\mathfrak{p}'$ on a $f' \leqslant f$; comme $\mathfrak{p}A_D \subset \mathfrak{p}_D$, on a $e' \leqslant e$; joint à $e'f' = ef$, ceci montre qu'on a $e = e'$ et $f = f'$, d'où :

3. $A/\mathfrak{p} \simeq A_D/\mathfrak{p}_D$.

Ceci étant, soit $\bar{x}$ un élément primitif de $A'/\mathfrak{p}'$ sur $A/\mathfrak{p}$, et soit $x \in A'$ un représentant de $\bar{x}$. Soit $X^r + a_{r-1}X^{r-1} + \cdots + a_0$ le polynôme minimal de x *sur* K_D; on a $a_i \in A_D$ (chap. II, § 6, cor. de la prop. 2); l'ensemble de ses racines est celui des $\sigma(x)$ avec $\sigma \in D$. Le polynôme « réduit » $X^r + \bar{a}_{r-1}X^{r-1} + \cdots + \bar{a}_0$ a ses coefficients dans $A/\mathfrak{p}$ (par (3)) et l'ensemble de ses racines est celui des $\bar{\sigma}(\bar{x})$ avec $\sigma \in D$. Il en résulte d'abord que $A'/\mathfrak{p}'$ contient tous les conjugués de $\bar{x}$ sur $A/\mathfrak{p}$, et $A'/\mathfrak{p}'$ est donc extension *galoisienne* de $A/\mathfrak{p}$ (§ 1, th. 1, *c*)). Il en résulte d'autre part que, comme tout conjugué de $\bar{x}$ sur $A/\mathfrak{p}$ est un $\bar{\sigma}(\bar{x})$, tout $(A/\mathfrak{p})$-automorphisme de $A'/\mathfrak{p}'$ est un $\bar{\sigma}$. Ainsi le groupe de Galois de $A'/\mathfrak{p}'$ sur $A/\mathfrak{p}$ s'identifie à D/I; comme son ordre est $[A'/\mathfrak{p}' : A/\mathfrak{p}] = f$, on a $\text{card}\,(D)/\text{card}\,(I) = f$, d'où $\text{card}\,(I) = e$ d'après (2). CQFD.

COROLLAIRE. *Pour que* $\mathfrak{p}$ *ne se ramifie pas dans* A', *il faut et il suffit que le groupe d'inertie* I *soit réduit à l'identité.*

Remarque. Si on note $D_{\mathfrak{p}'}$ et $I_{\mathfrak{p}'}$ les groupes de décomposition et d'inertie de l'idéal maximal $\mathfrak{p}'$, ceux du *conjugué* $\sigma(\mathfrak{p}')$ $(\sigma \in G)$ sont

4. $D_{\sigma(\mathfrak{p}')} = \sigma D_{\mathfrak{p}'}\sigma^{-1}, \quad I_{\sigma(\mathfrak{p}')} = \sigma I_{\mathfrak{p}'}\sigma^{-1}$

En effet, pour $\tau \in D_{\mathfrak{p}'}$, on a $\sigma\tau\sigma^{-1}.\sigma(\mathfrak{p}') = \sigma\tau(\mathfrak{p}') = \sigma(\mathfrak{p}')$, d'où $\sigma D_{\mathfrak{p}'}\sigma^{-1} \subset D_{\sigma(\mathfrak{p}')}$; en appliquant ceci à σ^{-1} et à $\sigma(\mathfrak{p}')$, on obtient l'inclusion opposée. De même, pour $\tau \in I_{\mathfrak{p}'}$ et $x \in A'$, on a

$$\sigma\tau\sigma^{-1}(x) - x = \sigma\tau(\sigma^{-1}(x)) - \sigma\sigma^{-1}(x) = \sigma(\tau(\sigma^{-1}(x)) - \sigma^{-1}(x)) \in \sigma(\mathfrak{p}'),$$

d'où $\sigma I_{\mathfrak{p}'}\sigma^{-1} \subset I_{\sigma(\mathfrak{p}')}$, et l'égalité par application à σ^{-1} et $\sigma(\mathfrak{p}')$.
Lorsque K' est une extension *abélienne* de K, les groupes $D_{\sigma(\mathfrak{p}')}$ (resp. $I_{\sigma(\mathfrak{p}')}$) $(\sigma \in G)$ sont donc tous *égaux*, et ne dépendent que de l'idéal $\mathfrak{p}$ du petit anneau (prop. 1).

6.3. Cas des corps de nombres. L'automorphisme de Frobenius

Ce qui précède s'applique aux corps de nombres et à leurs anneaux d'entiers; en effet ces corps sont de caractéristique 0, et les corps résiduels de ces anneaux sont finis.

Conservons les notations précédentes ($K \subset K'$ corps de nombres, K' galoisien sur K, groupe G, anneaux A et A'). Soit $\mathfrak{p}$ un idéal maximal de A qui *ne se ramifie pas* dans A', et soit $\mathfrak{p}'$ un facteur premier de $A'\mathfrak{p}$. Alors le groupe d'inertie de $\mathfrak{p}'$ est réduit à l'identité (§ 2, cor. de la prop. 2), et son groupe de décomposition D est donc canoniquement isomorphe au groupe de Galois de $A'/\mathfrak{p}'$ sur $A/\mathfrak{p}$ (§ 2, prop. 2). Mais ce dernier est cyclique, avec un générateur privilégié $\bar{\sigma} : \bar{x} \mapsto \bar{x}^q$ où $q = \text{card}\,(A/\mathfrak{p})$ (§ 1, ex. 3). Donc D est lui aussi *cyclique*, avec un générateur privilégié σ tel que $\sigma(x) \equiv x^q \pmod{\mathfrak{p}'}$ pour tout $x \in A'$. Ce générateur s'appelle encore *l'automorphisme de Frobenius* de $\mathfrak{p}'$; on le note souvent $(\mathfrak{p}', K'/K)$

Pour $\tau \in G$ on a, comme dans la remarque à la fin du § 2,

1. $(\tau(\mathfrak{p}'), K'/K) = \tau.(\mathfrak{p}', K'/K).\tau^{-1}$.

En particulier, si K' est extension *abélienne*, $(\mathfrak{p}', K'/K)$ ne dépend que de l'idéal $\mathfrak{p}$ de A; alors on le note parfois $\left(\dfrac{K'/K}{\mathfrak{p}}\right)$.

PROPOSITION 1. *Avec les hypothèses et notations précédentes, soit* F *un corps intermédiaire* $(K \subset F \subset K')$; *notons* f *le degré résiduel de* $\mathfrak{p}' \cap F$ *sur* K. *Alors*

a) *on a* $(\mathfrak{p}', K'/F) = (\mathfrak{p}', K'/K)^f$

b) *si* F *est galoisien sur* K, *la restriction de* $(\mathfrak{p}', K'/K)$ *à* F *est égale à* $(\mathfrak{p}' \cap F, F/K)$.

En effet, posons $\sigma = (\mathfrak{p}', K'/K)$. Par définition on a $\sigma(\mathfrak{p}') = \mathfrak{p}'$ et $\sigma(x) \equiv x^q$ (mod. $\mathfrak{p}'$) pour tout $x \in A'$ (ici $q = \text{card}(A/\mathfrak{p})$). On a donc

$$\sigma^f(\mathfrak{p}') = \mathfrak{p}' \qquad \text{et} \qquad \sigma^f(x) \equiv x^{q^f}$$

(mod. $\mathfrak{p}'$) pour tout $x \in A'$; par définition de f, q^f est le cardinal du corps résiduel $(A' \cap F)/(\mathfrak{p}' \cap F)$. De plus le groupe de décomposition de $\mathfrak{p}'$ sur F est évidemment un sous-groupe du groupe de décomposition D de $\mathfrak{p}'$ sur K, et est d'ordre

$$[A'/\mathfrak{p}' : (A' \cap F)/(\mathfrak{p}' \cap F)] = f^{-1}[A'/\mathfrak{p}' : A/\mathfrak{p}] = f^{-1}. \text{ card}(D)$$

par (2) du § 2; comme D est cyclique et engendré par σ, son seul sous-groupe d'ordre f^{-1}. card (D) est engendré par σ^f. Ceci démontre *a*).

Supposons maintenant F galoisien sur K, et notons σ' la restriction de σ à F (§ 1, th. 1, *b*)). Comme $\sigma'(\mathfrak{p}') = \mathfrak{p}'$, on a $\sigma'(\mathfrak{p}' \cap F) = \mathfrak{p}' \cap F$ et σ' appartient au groupe de décomposition de $\mathfrak{p}' \cap F$ sur K. De plus on a évidemment $\sigma'(x) \equiv x^q$ pour tout $x \in A' \cap F$, avec $q = \text{card}(A/\mathfrak{p})$. Ceci démontre *b*).

6.4. Application aux corps cyclotomiques

Nous allons utiliser ce qui précède pour démontrer un résultat qui généralise l'irréductibilité du polynôme cyclotomique, et en donne une troisième démonstration (cf. chap. II, § 9, th. 1, et chap. V, § 2, ex.)

THÉORÈME 1. *Soit* z *une racine primitive n-ème de l'unité dans* $\mathbf{C}$. *Alors*

a) *Aucun nombre premier* p *qui ne divise pas* n *ne se ramifie dans* $\mathbf{Q}[z]$;

b) $\mathbf{Q}[z]$ *est extension abélienne de* $\mathbf{Q}$, *de degré* $\varphi(n)$ *et de groupe de Galois isomorphe à* $(\mathbf{Z}/n\mathbf{Z})^*$.

En effet soient $F(X)$ le polynôme minimal de z sur $\mathbf{Q}$, et d son degré (on a $d = [\mathbf{Q}[z] : \mathbf{Q}]$). Le polynôme $F(X)$ est un diviseur de $X^n - 1$, soit $X^n - 1 = F(X)G(X)$. On a $D(1, z, \ldots, z^{d-1}) = N(F'(z))$ (chap. II, § 7, (6)); or de $nX^{n-1} = F'(X)G(X) + F(X)G'(X)$, on tire $nz^{n-1} = F'(z)G(z)$; comme z est une unité de $\mathbf{Q}[z]$ et est donc de norme ± 1, on en déduit en prenant les normes que $N(F'(z))$ divise n^d. Enfin, comme z est un entier de $\mathbf{Q}[z]$, le discriminant absolu de $\mathbf{Q}[z]$ divise $D(1, z, \ldots, z^{d-1})$ et donc n^d. Ainsi, d'après le chap. V, § 3, th. 1, aucun nombre premier p qui ne divise pas n ne se ramifie dans $\mathbf{Q}[z]$. Ceci démontre *a*).

Pour *b*) rappelons (§ 1, ex. 2) que $\mathbf{Q}[z]$ est extension abélienne de $\mathbf{Q}$ et qu'on a un homomorphisme injectif j du groupe de Galois G de $\mathbf{Q}[z]$ sur $\mathbf{Q}$ dans $(\mathbf{Z}/n\mathbf{Z})^*$; plus précisément l'élément $\sigma \in G$ élève toutes les racines n-èmes de l'unité à la puissance $j(\sigma)$. Soit alors p un nombre premier qui ne divise pas n; par *a*), l'automorphisme de Frobenius $\left(\frac{\mathbf{Q}[z]/\mathbf{Q}}{p}\right)$ est défini; notons le σ_p. En notant A l'anneau des entiers de $\mathbf{Q}[z]$ et $\mathfrak{p}$ un facteur premier quelconque de Ap, on a par définition $\sigma_p(x) \equiv x^p$ mod. $\mathfrak{p}$ pour tout $x \in A$. En particulier, en posant $j = j(\sigma_p)$, on a $z^j \equiv z^p$ mod. $\mathfrak{p}$. Or on a

$$\prod_{\substack{0 \leqslant r \leqslant n-1 \\ r \not\equiv p \,(\mathrm{mod.}\, n)}} (z^p - z^r) = P'(z^p) = nz^{p(n-1)},$$

où $P(X) = X^n - 1 = \prod_{0 \leqslant r \leqslant n-1} (X - z^r)$; comme n est premier à p, que $\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$, et que z est inversible, on en déduit qu'on a

$$\prod_{\substack{0 \leqslant r \leqslant n-1 \\ r \not\equiv p \,(\mathrm{mod.}\, n)}} (z^p - z^r) \notin \mathfrak{p}.$$

La relation $z^j \equiv z^p$ (mod. $\mathfrak{p}$) implique donc que j est la classe de p mod. n. Ainsi $j(G)$ contient les classes mod. n de tous les nombres premiers p qui ne divisent pas n, et donc, par multiplicativité, les classes de tous les entiers premiers à n; autrement dit $j(G) = (\mathbf{Z}/n\mathbf{Z})^*$ et ceci démontre *b*).

6.5. Nouvelle démonstration de la loi de réciprocité quadratique

Soient q un nombre premier *impair*, et K le corps cyclotomique engendré par une racine primitive q-ème de l'unité dans $\mathbf{C}$. Le groupe de Galois G de K sur $\mathbf{Q}$ est isomorphe à $\mathbf{F}_q^*$ (§ 4, th. 1, *b*)), donc est *cyclique* d'ordre pair $q - 1$. Il admet donc un sous-groupe H d'indice 2 et un seul, qui correspond au sous-groupe des carrés $(\mathbf{F}_q^*)^2$. Ainsi K contient un sous-corps *quadratique* F et un seul (§ 1, th. 2, *b*)). Aucun nombre premier $p \neq q$ ne se ramifie dans F, car, sinon, il se ramifierait dans K contrairement au th. 1, *a*) du § 4. Le calcul du discriminant d'un corps quadratique (chap. V, § 3, ex.) montre qu'on a nécessairement $F = \mathbf{Q}[\sqrt{q}]$ si $q \equiv 1$ mod. 4, et $F = \mathbf{Q}[\sqrt{-q}]$ si $q \equiv 3$ mod. 4; en posant $q^* = (-1)^{\frac{q-1}{2}} q$, on a en tous cas $F = \mathbf{Q}[\sqrt{q^*}]$.

Soit p un nombre premier distinct de q. Notons σ_p l'automorphisme de Frobenius $\left(\frac{K/\mathbf{Q}}{p}\right)$ (cf. § 4). Sa restriction à F est $\left(\frac{F/\mathbf{Q}}{p}\right)$ (§ 3, prop. 1, *b*); c'est l'identité si $\sigma_p \in H$, c'est-à-dire si l'exposant $j(\sigma_p)$ = classe de p mod. q (cf. § 4) est un *carré* dans $\mathbf{F}_q^*$; c'est l'automorphisme non identique dans le cas contraire. Autrement dit, en identifiant le groupe de Galois G/H de F sur $\mathbf{Q}$ à $\{+1, -1\}$, on a

1. $\left(\frac{F/\mathbf{Q}}{p}\right) = \left(\frac{p}{q}\right)$

par définition du symbole de Legendre $\left(\frac{p}{q}\right)$ (chap. V, § 5).

D'autre part les résultats sur le décomposition du nombre premier p dans $F = \mathbf{Q}[\sqrt{q^*}]$ (chap. V, § 4) donnent d'autres renseignements sur $\left(\frac{F/\mathbf{Q}}{p}\right)$. Par définition c'est l'identité si p est décomposé dans F, et l'automorphisme non identique si p est inerte. D'après la prop. 1 du § 4, chap. V, on a donc, si p est *impair*

2. $\left(\frac{F/\mathbf{Q}}{p}\right) = \left(\frac{q^*}{p}\right)$

En comparant (1) et (2) on obtient $\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right) = \left(\frac{-1}{p}\right)^{\frac{q-1}{2}} \left(\frac{q}{p}\right)$; or $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-2}{2}}$ par le très élémentaire critère d'Euler (chap. V, § 5, prop. 1). D'où $\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right)$ et on retrouve la loi de réciprocité quadratique (chap. V, § 5, th. 1)

Pour $p = 2$, rappelons que 2 est décomposé dans F si $q^* \equiv 1 \pmod 8$, et est inerte si $q^* \equiv 5 \pmod 8$ (chap. V, § 4, prop. 1). Or

$$(-1)^{\frac{q^2-1}{8}} = (-1)^{\frac{q^{*2}-1}{8}}$$

vaut 1 si $q^* \equiv 1 \pmod 8$ et -1 si $q^* \equiv 5 \pmod 8$. On a donc

3. $\left(\frac{F/\mathbf{Q}}{2}\right) = (-1)^{\frac{q^2-1}{8}}$

En comparant 1 et 3, on obtient $\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}}$, ce qui est la « formule complémentaire » difficile (chap. V, § 5, prop. 2, *b*)).

Compléments sans démonstrations

Nous donnons ici, sans démonstration, quelques compléments à ce qui a été fait dans le texte. Il s'agit de questions très liées à celles traitées dans le texte, et dont le degré de profondeur et de difficulté est tout à fait analogue ; elles n'ont pas été incluses afin de garder à ce livre une taille raisonnable, et aussi parce qu'on les trouve traitées dans d'autres ouvrages (voir p. ex. le chap. V de [9], directement lisible après ce livre).

L'auteur a reculé devant la tâche consistant à donner, sans démonstration, une description du développement ultérieur de la théorie des nombres (adèles, corps de classes, fonctions zéta et séries L, arithmétiques des algèbres simples, théorie analytique, formes quadratiques etc.). Il renvoie par cela aux ouvrages cités dans la première partie de la Bibliographie (titres non numérotés).

Formules de transitivité

Étant donnés 3 corps emboîtés, $K \subset L \subset M$, chacun extension de *degré fini* du précédent, on a les applications « trace »

$$\mathrm{Tr}_{L/K} : L \to K, \qquad \mathrm{Tr}_{M/L} : M \to L, \qquad \mathrm{Tr}_{M/K} : M \to K,$$

et les applications « normes » analogues (chap. II, § 6). Alors, pour x $x \in M$, on a

$$1. \quad \begin{cases} \mathrm{Tr}_{M/K}(x) = \mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(x)) \\ \mathrm{N}_{M/K}(x) = \mathrm{N}_{L/K}(\mathrm{N}_{M'L}(x)) \end{cases}$$

Norme relative d'un idéal

Étant donnés deux corps de nombres emboîtés, $K \subset K'$, et un idéal (entier ou fractionnaire) $\mathfrak{a}'$ de K', l'idéal de K engendré par les $\mathrm{N}_{K'/K}(x)$ $(x \in \mathfrak{a}')$ s'appelle la *norme relative* de $\mathfrak{a}'$, et se note $\mathrm{N}_{K'/K}(\mathfrak{a}')$ (ou $\mathrm{N}(\mathfrak{a}')$). Si $\mathfrak{a}'$ est un idéal principal (a') on a

$$2. \quad \mathrm{N}_{K'/K}((a')) = (\mathrm{N}_{K'/K}(a'))$$

Si $K = \mathbf{Q}$ on retrouve la notion exposée au chap. III, § 5 : si $\mathfrak{a}'$ est un idéal entier de K', et si A' est l'anneau des entiers de K', on a

3. $N_{K'/Q}(\mathfrak{a}') = \text{card}\,(A'/\mathfrak{a}')\mathbf{Z}$.

Revenons au cas général; si $\mathfrak{a}$ est un idéal de K, et si $n = [K' : K]$ on a

4. $N_{K'/K}(A'\mathfrak{a}) = \mathfrak{a}^n$

Si $\mathfrak{a}'$ et $\mathfrak{b}'$ sont des idéaux de K', on a la formule de multiplicativité :

5. $N_{K'/K}(\mathfrak{a}'\mathfrak{b}') = N_{K'/K}(\mathfrak{a}')N_{K'/K}(\mathfrak{b}')$

Enfin, si $\mathfrak{p}'$ est un idéal premier de K', si $\mathfrak{p} = \mathfrak{p}' \cap K$, et si f est le degré résiduel de $\mathfrak{p}'$ sur K, on a

6. $N_{K'/K}(\mathfrak{p}') = \mathfrak{p}^f$

Avec trois corps de nombres emboîtés $K \subset K' \subset K''$, on a la formule de transitivité suivante, où $\mathfrak{a}''$ désigne un idéal de K'' :

7. $N_{K''/K}(\mathfrak{a}'') = N_{K'/K}(N_{K''/K'}(\mathfrak{a}''))$

Dans la même situation, la notion de norme relative d'un idéal permet de donner une formule de transitivité des discriminants (où $\mathfrak{D}_{K'/K}$ désigne le discriminant de K' sur K; cf. chap. V, § 3, déf. 1)

8. $\mathfrak{D}_{K''/K} = N_{K'/K}(\mathfrak{D}_{K''/K'}).\mathfrak{D}_{K'/K}^{[K'':K']}$

Tout ceci se généralise à un anneau de Dedekind A et à sa fermeture intégrale A' dans une extension de degré du corps des fractions de A.

La différente

Ce qui suit s'applique à un anneau de Dedekind A et à la fermeture intégrale de A dans une extension de degré fini de son corps des fractions. Pour alléger, nous nous bornerons au cas des corps de nombres.

Soient $K \subset K'$ deux corps de nombres emboîtés, A et A' leurs anneaux d'entiers. On dit qu'un idéal maximal $\mathfrak{p}'$ de A' *est ramifié* sur A (ou sur K) si son indice de ramification sur A est > 1. Alors l'idéal maximal $\mathfrak{p} = \mathfrak{p}' \cap A$ de A *se ramifie* dans A' (chap. V, § 3). Il résulte aisément du chap. V, § 3, th. 1 que les idéaux maximaux de A' qui sont ramifiés sur A sont *en nombre fini*. Nous allons caractériser un idéal $\mathfrak{d}_{K'/K}$ de A', la « *différente* » de K' sur K, tel que ces idéaux maximaux soient exactement ceux qui contiennent $\mathfrak{d}_{K'/K}$ (noter l'analogie avec le chap. V, § 3, th. 1)

On démontre d'abord que l'ensemble des $x \in K'$ tels que

9. $\mathrm{Tr}_{K'/K}(xA') \subset A$

est un idéal fractionnaire $\mathfrak{C}$ de A'; on l'appelle la *codifférente* de K' sur K; par définition la *différente* $\mathfrak{d}_{K'/K}$ est l'idéal inverse $\mathfrak{C}^{-1}$. C'est un idéal *entier* non nul de A'. On démontre qu'il est *engendré par les* $F'(x)$, où x parcourt A' et où F désigne le polynôme minimal de x sur K. En particulier, si A' est de la forme $A[y]$ (ce qui n'est pas toujours le cas), et si G est le polynôme minimal de y sur K, alors la différente $\mathfrak{d}_{K'/K}$ est l'idéal principal de A' engendré par $G'(y)$.

Les idéaux premiers non nuls de A' qui sont ramifiés sur A sont ceux qui contiennent $\mathfrak{d}_{K'/K}$. Plus précisément soit

10. $\mathfrak{d}_{K'/K} = \prod_i \mathfrak{p}_i'^{m_i} \quad (m_i > 0)$

la décomposition de la différente en idéaux premiers, et soit e_i l'indice de ramification de $\mathfrak{p}_i'$ sur A. Alors les idéaux premiers non nuls de A' qui sont ramifiés sur A sont les $\mathfrak{p}_i'$, et on a $m_i \geqslant e_i - 1$ pour tout i. De plus on a $m_i = e_i - 1$ si et seulement si e_i est premier à la caractéristique du corps résiduel $A'/\mathfrak{p}'_i$

La différente $\mathfrak{d}_{K'/K}$ (idéal de A') et le discriminant $\mathfrak{D}_{K'/K}$ (idéal de A) sont liés par la relation suivante :

11. $\mathfrak{D}_{K'/K} = N_{K'/K}(\mathfrak{d}_{K'/K})$

(cf. chap. II, § 7, formule (6)). Ainsi la donnée de la différente est plus précise que celle du discriminant.

Enfin, étant donnés trois corps de nombres emboîtés, $K \subset K' \subset K''$, on a la formule de transitivité suivante pour les différentes :

12. $\mathfrak{d}_{K''/K} = \mathfrak{d}_{K''/K'} . \mathfrak{d}_{K'/K}$.

Exercices

Les exercices marqués A sont des exercices « de réflexion immédiate », destinés au contrôle direct des connaissances. Les exercices marqués B sont plus élaborés. Les « problèmes de revision » (à la fin) sont des problèmes d'examen, où l'on est parfois mieux guidé que dans certains exercices marqués B.

Chapitre I

1 B. Soient p un nombre premier et $r \in \mathbf{N}$. Montrer que le groupe multiplicatif $(\mathbf{Z}/p^r\mathbf{Z})^*$ est cyclique, sauf si $p = 2$ et $r \geqslant 3$ (pour p impair, on montrera que la classe de $1 + p$ est d'ordre p^{r-1}; pour $p = 2$ on étudiera l'ordre de la classe de 5; utiliser alors le cor. 4 du th. 1, § 5)

2 B. *a*) Montrer que l'équation diophantienne $x^2 + y^2 = 3z^2$ n'a pas de solution entière non triviale (i.e. $\neq (0, 0, 0)$ (réduire mod. 3). Question analogue pour $x^2 + y^2 = 7z^2$ et $x^2 + y^2 = 11z^2$.

b) Montrer que $x^2 + y^2 = 5z^2$ et $x^2 + y^2 = 13\, z^2$ ont des solutions entières non triviales.

c) Essayer de généraliser *a*) à certaines équations $x^2 + y^2 = pz^2$, p premier donné (on étudiera à quelle condition -1 est un carré dans $\mathbf{F}_p^*$).

3 B. Retrouver la démonstration classique du fait qu'il y a une infinité de nombres premiers. En s'inspirant de celle-ci, montrer qu'il y a une infinité de nombres premiers de la forme $4k - 1 (k \in \mathbf{N})$.

4 B. Pour que $n \in \mathbf{N}$ soit premier, il faut et il suffit que n divise $(n-1)! + 1$ (Si n est premier, calculer le produit des éléments de $\mathbf{F}_n^*$; examiner ensuite le cas où n n'est pas premier)

5 B. Montrer que, dans un corps fini K, tout élément est somme de deux carrés (traiter d'abord le cas où $q = \text{card (K)}$ est pair; si q est impair, calculer les nombres de valeurs prises par les fonctions $x \mapsto x^2$ et $y \mapsto a - y^2$, $x, y \in \mathrm{K}$, $a \in \mathrm{K}$ donné)

6 B. Décomposer le polynôme $X^3 - X + 1$ sur $\mathbf{F}_{23}$ et le polynôme $X^3 + X + 1$ sur $\mathbf{F}_{31}$ (chacun a une racine double et une racine simple)

7 A. Donner un exemple de deux idéaux $\mathfrak{a}, \mathfrak{b}$ d'un anneau A tels que $\mathfrak{a} \cap \mathfrak{b} \neq \mathfrak{a}\mathfrak{b}$. Montrer qu'on a toujours $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$.

8 B. Soient A un anneau intègre, a, $b \in A$, et $B = A[X]/(aX + b)$. Montrer que, si $Aa \cap Ab = Aab$, alors B est intègre (considérer l'élément $-b/a$ du corps des fractions K de A, et montrer que l'homomorphisme $\varphi : A[X] \to K$ défini par $\varphi(X) = -b/a$ et $\varphi(y) = y$ pour $y \in A$ a exactement $(aX + b)$ pour noyau).

9 B. Soient A un anneau intègre et i, j des entiers $\geqslant 1$ premiers entre eux. Montrer que l'idéal $(X^i - Y^j)$ de l'anneau de polynômes $A[X, Y]$ est premier (définir un homomorphisme $A[X, Y] \to A[X]$ ayant cet idéal pour noyau).

10 B. *a*) Soient A un anneau intègre, K son corps des fractions et b un élément non nul de A. Montrer que le A-module Hom $(A/Ab, K/A)$ est isomorphe à A/Ab (on rappelle que, étant donnés deux A-modules E, F, on note Hom (E, F) l'ensemble des homomorphismes, ou applications A-linéaires de E dans F; de plus Hom (E, F) est un A-module; on notera qu'un homomorphisme $\varphi : A/Ab \to K/A$ est déterminé par sa valeur sur la classe $\bar{1}$ de 1).

b) Pour tout A-module, E, on pose $E' = \mathrm{Hom}(E, K/A)$ et

$$E'' = \mathrm{Hom}\,(E', K/A).$$

Définir un homomorphisme canonique $E \to E''$.

c) On suppose A principal. Soit E un A-module de type fini et de torsion (i.e. tel que, pour tout $x \in E$, il existe $a \in A$ non nul pour lequel $ax = 0$). Déterminer la structure de E, et déduire de *a*) que E est isomorphe à $E' = \mathrm{Hom}\,(E, K/A)$. En déduire que l'homomorphisme canonique $E \to E''$ de *b*) est un isomorphisme.

Chapitre II

1 A. Le th. 1 du § 7 reste vrai si, au lieu d'y supposer K de caractéristique 0, on suppose K fini; dire pourquoi. Le cas où K est fini est-il intéressant?

2 B. Soient A un anneau intégralement clos, K son corps des fractions, et $P(X) \in A[X]$ un polynôme unitaire. Si $P(X)$ est réductible dans $K[X]$, montrer qu'il est réductible dans $A[X]$ (considérer les racines de $P(X)$ dans une extension de K).

3 B. Pour tout $n \geqslant 1$, on désigne par $f(n)$ le nombre de polynômes unitaires irréductibles de degré n sur $\mathbf{F}_q$. Montrer qu'on a $\sum\limits_{d \mid n} d f(d) = q^n$

(classifier les éléments de $\mathbf{F}_{q^n}$ suivant leurs polynômes minimaux sur $\mathbf{F}_q$, et noter que $\mathbf{F}_{q^d} \subset \mathbf{F}_{q^n}$ équivaut à $d|n$). En déduire les valeurs de $f(1)$, $f(2)$, $f(3)$, $f(4)$ et $f(p)$ pour p premier.

4 A. Donner un exemple d'anneau intègre qui n'est pas intégralement clos (penser au § 5).

5 B. Soient R un anneau, A un sous-anneau de R et x un élément inversible de R. Montrer que tout $y \in A[x] \cap A[x^{-1}]$ est entier sur A (on montrera qu'il existe un entier n tel que le A-module

$$M = A + Ax + \cdots + Ax^n$$

soit stable par la multiplication par y, i.e. que $yM \subset M$; on s'inspirera alors de la fin de la démonstration du th. 1, § 1).

Chapitre III

1 A. Pourquoi un corps est-il un anneau de Dedekind?

2 A. Comment pourrait-on modifier l'énoncé du th. 2, § 4 de façon que l'hypothèse que A n'est pas un corps, soit superflue.

3 B. Dans un anneau nœthérien A il est clair que tout idéal $\neq$ A est contenu dans un idéal maximal. Montrer que cette conclusion reste vraie si on ne suppose pas A nœthérien (utiliser le théorème de Zorn).

4 A. Donner un exemple d'un anneau intègre A, d'un idéal premier $\mathfrak{p} \neq (0)$ de A et d'un sous-anneau $A' \subset A$ tels que $\mathfrak{p} \cap A' = (0)$.

5 A. Soit K un corps. L'anneau K[X, Y] des polynômes à deux variables sur K est-il un anneau de Dedekind?

6 B. Soient K un corps et A le sous-anneau $K[X^2, X^3]$ de l'anneau de polynômes K[X].

a) En utilisation les inclusions $K[X^2] \subset A \subset K[X]$, montrer que A est nœthérien et que tout idéal premier non-nul de A est maximal.

b) Montrer que A n'est pas un anneau de Dedekind (considérer l'élément X).

Chapitre IV

1 B. Montrer que l'anneau A des entiers du corps cubique $\mathbf{Q}[x]$ avec $x^3 = 2$ est principal (majorer le discriminant de A par $D(1, x, x^2)$ et appliquer le cor. 1 de la prop. 1, § 3; en fait on a $A = \mathbf{Z}[x]$, voir ci-dessous un problème de révision).

2 B. Déterminer les unités de l'anneau $A = \mathbf{Z}[X]/(X^3)$, et la structure du groupe A^*.

3 B. Soit K un corps cubique tel que $r_1 = r_2 = 1$. On suppose K plongé dans $\mathbf{R}$.

a) Montrer que les unités positives de K forment un groupe isomorphe à $\mathbf{Z}$, et que toute unité positive de K est de norme 1.

b) Soient d le discriminant absolu de K et u une unité > 1. Montrer qu'on a $|d| \leqslant 4u^3 + 20$ (poser $u = x^2$ avec $x \in \mathbf{R}$, $x > 0$; noter que les conjugués de u sont de la forme $x^{-1}e^{iy}$ et $x^{-1}e^{-iy}$ avec $y \in \mathbf{R}$; calculer le discriminant $d' = \mathrm{D}(1, u, u^2)$ en fonction de x et y, soit $|d'|^{1/2} = \varphi(x, y)$; évaluer le maximum de $\varphi(x, y)$ par x fixé, et en déduire que

$$|d'| \leqslant 4u^3 + 20;$$

conclure en notant que d divise d').

c) Montrer que le polynôme $X^3 + 10X + 1$ est irréductible sur $\mathbf{Q}$ (cf. chap. V, § 3, exemple vers la fin). Soit x une de ses racines dans $\mathbf{R}$. Montrer que l'anneau des entiers du corps cubique $\mathbf{Q}[x]$ est $\mathbf{Z}[x]$ (*ibid*). Montrer que $u = -\dfrac{1}{x}$ est un générateur du groupe des unités positives de $\mathbf{Q}[x]$.

4 B. Soient K un corps de nombres, A l'anneau des entiers de K et P l'ensemble des idéaux maximaux de A. Pour $\mathfrak{p} \in \mathrm{P}$ et $x \in \mathrm{K}^*$ on note $v_{\mathfrak{p}}(x)$ l'exposant de $\mathfrak{p}$ dans la décomposition de $\mathrm{A}x$ en produit d'idéaux premiers; on pose $v_{\mathfrak{p}}(0) = +\infty$.

a) Montrer que, pour $x, y \in \mathrm{K}$ on a $v_{\mathfrak{p}}(xy) = v_{\mathfrak{p}}(x) + v_{\mathfrak{p}}(y)$ et

$$v_{\mathfrak{p}}(x + y) \geqslant \min\,(v_{\mathfrak{p}}(x),\ v_{\mathfrak{p}}(y)).$$

b) Soit P′ une partie de P. Montrer que l'ensemble A(P′) des $x \in \mathrm{K}$ tels que $v_{\mathfrak{p}}(x) \geqslant 0$ pour tout $\mathfrak{p} \in \mathrm{P}'$ est un sous-anneau de K. Examiner les cas $\mathrm{P}' = \mathrm{P}$, $\mathrm{P}' = \emptyset$.

c) On prend pour P′ le complémentaire d'une partie *finie* S de P. Montrer que le groupe U des unités de A(P′) est de type fini, et que U/A^* est un $\mathbf{Z}$-module libre de rang card (S) (considérer l'application $x \mapsto (v_{\mathfrak{p}}(x))_{\mathfrak{p} \in \mathrm{S}}$ de U dans $\mathbf{Z}^{\mathrm{S}}$; déterminer son noyau; déterminer son image en notant que tout idéal de A a une puissance qui est un idéal principal).

Chapitre V

1 B. Soient A un anneau principal et K son corps des fractions.

a) Montrer que tout anneau intermédiaire B ($\mathrm{A} \subset \mathrm{B} \subset \mathrm{K}$) est un anneau de fractions de A $\left(\text{si } \dfrac{a}{b} \in \mathrm{B} \text{ avec } a, b \in \mathrm{A} \text{ premiers entre eux, on montrera en utilisant une identité de Bezout que } \dfrac{1}{b} \in \mathrm{B}\right)$.

b) Classifier les anneaux de fractions de A (considérer les éléments premiers de A qui sont inversibles dans $\mathrm{S}^{-1}\mathrm{A}$).

c) Montrer que tout anneau de fractions de A est principal.

2 A. Montrer qu'aucun entier $\equiv 7$ modulo 8 n'est somme de trois carrés (réduire mod. 8).

3 B. Soient K un corps et A une K-algèbre réduite de dimension finie sur K.

a) S'inspirer du § 3, lemme 3 pour montrer que A est isomorphe à un produit fini $\prod_{i=1}^{n} L_i$ d'extensions de degré fini de K.

b) Montrer que, si K est de caractéristique 0, A est monogène, c-à-d de la forme $K[x]$ avec $x \in A$ (on construira des éléments primitifs x_i des L_i sur K dont les polynômes minimaux sur K sont deux à deux distincts; prendre alors $x = (x_1, \ldots, x_n)$).

4 B. Soit p un nombre premier $\equiv 1$ mod. 4. Montrer qu'il y a exactement 8 couples $(a, b) \in \mathbf{Z} \times \mathbf{Z}$ tels que $p = a^2 + b^2$ (autrement dit, l'équation diophantienne $p = a^2 + b^2$ n'a qu'une seule solution, à des transformations triviales près).

5 B. Soient K un corps, A une algèbre de dimension finie sur K. Donner des exemples où A n'est pas monogène. (i.e. pas de la forme $K[x]$) :

a) lorsque A n'est pas réduite;

b) lorsque A est réduite et K fini (cf. exer. 3).

6 B. *a*) Montrer que le polynôme $X^5 - X + 1$ est irréductible sur $\mathbf{Q}$ (on pourra étudier sa réduction mod. 5). Soit x une de ses racines. Calculer les entiers r_1 et r_2 du corps $\mathbf{Q}[x]$.

b) Calculer la discriminant de $(1, x, \ldots, x^4)$ (sur $\mathbf{Z}$; cf. chap. II, § 7, formule (7)). Montrer qu'il est sans facteurs carrés, et en déduire que $\mathbf{Z}[x]$ est l'anneau des entiers de $\mathbf{Q}[x]$ (§ 3, prop. 1).

c) Montrer que l'anneau $\mathbf{Z}[x]$ est principal (utiliser le cor. 1 de la prop. 1 du § 3, chap. IV, et noter, par réduction de $X^5 - X + 1$ mod. 2 et mod. 3, que $\mathbf{Z}[x]$ n'admet pas d'idéaux de norme 2 ni 3).

7 B. Soit $K = \mathbf{Q}[\sqrt{d}]$ un corps quadratique, où d est un entier sans facteurs carrés, et soit A l'anneau des entiers de K.

a) Par utilisation directe du cor. à la prop. 1, § 3, chap. IV, montrer que A est principal pour $d = 2, 3, 5, 13, -1, -2, -3, -7$.

b) Par la même méthode montrer que tout idéal 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 lesquels 2 est inerte (on trouve $d = 21, 29, -11, -19$; cf. § 4, prop. 1), et montrer que leurs anneaux d'entiers sont principaux.

c) On suppose $d \equiv 2$ ou 3 mod. 4. Montrer que K admet un idéal principal de norme 2 si et seulement si il existe $a, b \in \mathbf{Z}$ tels que

$a^2 - db^2 = \pm 2$. En déduire que A est principal pour $d = 6, 7$, et qu'il admet deux classes d'idéaux pour $d = -5$ (on notera que 2 est ramifié dans ce corps).

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

e) Montrer que, pour $d = 10$ et $d = -6$, A admet deux classes d'idéaux (noter que tout idéal de K est équivalent à un idéal entier de norme 1, 2 ou 3; étudier les décompositions de 2 et de 3 dans K, et noter qu'on a $(2 + \sqrt{10})(2 - \sqrt{10}) = -2.3$ et $(\sqrt{-6})^2 = -2.3$).

f) Montrer que, pour $d = -23$, A admet trois classes d'idéaux (procéder comme dans *e*); en déduire qu'on a des idéaux premiers non principaux $\mathfrak{p}, \mathfrak{p}', \mathfrak{q}, \mathfrak{q}'$ de A tels que $2A = \mathfrak{p}\mathfrak{p}'$, $3A = \mathfrak{q}\mathfrak{q}'$; remarquer que $x = \frac{1}{2}(3 + \sqrt{-23})$ et $y = \frac{1}{2}(1 + \sqrt{-23})$ sont des éléments de normes 8 et 6 de A, et étudier les décompositions de Ax et Ay en idéaux premiers).

8 A. Soient $K \subset K' \subset K''$ trois corps de nombres emboîtés, $\mathfrak{p}''$ un idéal maximal de K'' et $\mathfrak{p}' = \mathfrak{p}'' \cap K'$. On note e (resp. e', e'') l'indice de ramification de $\mathfrak{p}''$ sur K (resp. $\mathfrak{p}'$ sur K, $\mathfrak{p}''$ sur K'); on note f (resp. f', f'') le degré résiduel de $\mathfrak{p}''$ sur K (resp. $\mathfrak{p}'$ sur K, $\mathfrak{p}''$ sur K'). Montrer qu'on a $e = e'e''$ et $f = f'f''$.

9 B. *a*) Montrer que le polynôme $X^3 + X^2 - 2X + 8$ est irréductible sur $\mathbf{Q}$ (noter qu'il n'a pas de racine dans $\mathbf{Z}$, ni donc dans $\mathbf{Q}$). On note x une de ses racines, K le corps cubique $\mathbf{Q}[x]$ et A l'anneau des entiers de K.

b) Montrer qu'on a $D(1, x, x^2) = -4.503$ et que 503 est premier.

c) Montrer que $y = \frac{4}{x}$ est un entier de K, que $y \notin \mathbf{Z}[x]$, et que $A' = \mathbf{Z} + \mathbf{Z}x + \mathbf{Z}y$ est un sous-anneau de K contenant strictement $\mathbf{Z}[x]$. Montrer que le discriminant de A' sur $\mathbf{Z}$ est 503 (comparer les discriminants de A et de A', ou calculer directement $D(1, x, y)$). En déduire que $A = A'$.

d) Montrer que 2A est produit de 3 idéaux premiers distincts (écrire la table de multiplication des éléments $1, x, y$ et réduire modulo 2). En déduire qu'il n'existe aucun élément u de A tel que $A = \mathbf{Z}[u]$ (noter que $A/2A$ n'est pas monogène sur $\mathbf{F}_2$).

e) Montrer que, si u est un élément primitif de K contenu dans A, le groupe $A/\mathbf{Z}[u]$ admet un quotient d'ordre 2 (noter que deux des trois homomorphismes de A sur $\mathbf{F}_2$ donnés par *d*) coïncident sur $\mathbf{Z}[u]$, et considérer leur différence). En déduire que $D(1, u, u^2)$ est un multiple de 4.503 (noter que $D(1, u, u^2) = -503.\text{card}\,(A/\mathbf{Z}[u])^2$). Ainsi les $D(1, u, u^2)$ n'engendrent pas l'idéal discriminant de K sur $\mathbf{Q}$.

f) Montrer que l'anneau A est principal (par le chap. IV, § 3, cor. 1 à la prop. 1 on est ramené à montrer que tout idéal premier de norme $n \leqslant 6$ est principal; exclure $n = 6$ et, par utilisation de *d*), $n = 4$; étudier les normes et les décomposition de $x, y, x - 1, x + 2$ et $x + 3$ dans A; constater que $\dfrac{x-2}{x+2}$ et $\dfrac{x-1}{x+3}$ engendrent deux des trois idéaux premiers de norme 2, ce qui règle le cas de $n = 2$; pour $n = 3$, montrer que 3A est premier; pour $n = 5$, 5A est produit d'un idéal premier de norme 5 et d'un autre de norme 25, et on compare les décompositions et les normes de 5A et de $(x + 1)A$).

10 B. *a*) Soient p, q deux nombres premiers $\geqslant 5$, distincts, et tels que $pq^2 \not\equiv 1$ (mod. 9). Soit K le corps cubique $\mathbf{Q}[u]$ où $u^3 = p^2q$. Montrer que u et $v = pqu^{-1}$ sont des entiers de K, que $D(1, u, v) = -27p^2q^2$, et que $B = \mathbf{Z} + \mathbf{Z}u + \mathbf{Z}v$ est un sous-anneau de l'anneau A des entiers de K (noter que $u^2 = qv$ et $v^2 = pu$).

b) Soit $\mathfrak{q}$ un idéal premier de A contenant Aq; déduire de $u^3 = p^2q$ que l'exposant de $\mathfrak{q}$ dans la décomposition de Aq est 3, et que $Aq = \mathfrak{q}^3$. Montrer que $B \cap \mathfrak{q}$ est l'idéal de B engendré par u, v, q, que

$$A/\mathfrak{q} = B/B \cap \mathfrak{q}$$

et que $A = B + \mathfrak{q}$. En déduire que $A = B + qA$. Montrer de même qu'on a $Ap = \mathfrak{p}^3$ avec $\mathfrak{p}$ premier et que $A = B + pA$.

c) Par considération de $(u \pm 1)^3$ (suivant la classe de p^2q mod. 3), montrer que 3A est le cube d'un idéal premier de A, et que (comme dans *b*)) on a $A = B + 3A$.

d) Soit $x = a + bu + cv$ $(a, b, c \in \mathbf{Q})$ un entier de K. Déduire d'un calcul de traces qu'on a $3pqx \in B$, d'où $3pqA \subset B$. Utiliser *b*) et *c*) pour montrer que $A = B + 3pqA$. En conclure que $A = B$.

e) Montrer que, pour $x = a + bu + cv$ $(a, b, c \in \mathbf{Z})$, on a

$$D(1, x, x^2) = 3p^2q^2(b^3q - c^3p)^2.$$

f) Déduire que *e*) que, si on a $p \equiv 1$ (mod. 3) et $q^{\frac{p-1}{3}} \equiv 1$ (mod. p), A n'admet aucune base (sur $\mathbf{Z}$) de la forme $(1, x, x^2)$ $(x \in A)$. Montrer que ceci a lieu pour $p = 7$ et $q = 5$ (alors $K = \mathbf{Q}[\sqrt[3]{175}] = \mathbf{Q}[\sqrt[3]{245}]$); montrer que, dans ce cas, le discriminant absolu de K est le pgcd des $D(1, x, x^2)$ pour $x \in A$.

Chapitre VI

1. *a*) Montrer que le corps $L = \mathbf{Q}[\sqrt{5}, \sqrt{-1}]$ est une extension galoisienne de degré 4 de $\mathbf{Q}$. Calculer son groupe de Galois.

b) Montrer que l'anneau A des entiers de L est $\mathbf{Z}\left[\sqrt{-1}, \frac{1+\sqrt{5}}{2}\right]$ (noter que le discriminant de $\left(1, \frac{1+\sqrt{5}}{2}\right)$ sur l'anneau des entiers de Gauss est sans facteurs carrés dans cet anneau; s'inspirer alors du chap. V, § 3, prop. 1). Calculer le discriminant absolu de L. Montrer que les seuls nombres premiers qui se ramifient dans L sont 2 et 5, et que les indices de ramification correspondants sont égaux à 2 (utiliser $n = efg$, cf. § 2, prop. 1).

c) Calculer les automorphismes de Frobenius $\left(\frac{L/\mathbf{Q}}{p}\right)$ pour p premier, distinct de 2 et 5 (cf. § 3). Calculer les groupes de décomposition et d'inertie de 2 et 5.

d) Montrer qu'on a $\mathbf{Q}[\sqrt{-5}] \subset L$, et qu'aucun idéal premier de $\mathbf{Q}[\sqrt{-5}]$ ne se ramifie dans L.

e) Montrer, de même, qu'on a $\mathbf{Q}[\sqrt{10}] \subset \mathbf{Q}[\sqrt{2}, \sqrt{5}]$, et qu'aucun idéal premier de $\mathbf{Q}[\sqrt{10}]$ ne se ramifie dans $\mathbf{Q}[\sqrt{2}, \sqrt{5}]$.

On notera que $K = \mathbf{Q}[\sqrt{-5}]$ et $K = \mathbf{Q}[\sqrt{10}]$ admettent ainsi chacun une extension abélienne « non ramifiée « (i.e. où aucun idéal premier de K ne se ramifie) dont le groupe de Galois (cyclique d'ordre 2) est isomorphe au groupe des classes d'idéaux de K. Ceci est un cas très particulier de la célèbre « théorie du corps de classes ».

2 B. Soient x la racine réelle du polynôme $X^3 - X + 1$, y et $\bar{y}$ ses deux autres racines dans C, et K le corps cubique $\mathbf{Q}[x]$ (cf. chap. V, § 3, exemple).

a) Montrer qu'on a $y + \bar{y} = -x$, $y\bar{y} = -\frac{1}{x}$ et

$$[(y-x)(\bar{y}-x)(y-\bar{y})]^2 = -23$$

(cf. chap. II, § 7, formules (6) et (7). En déduire que $K[\sqrt{-23}] = \mathbf{Q}[x, y, \bar{y}]$ et que ce corps L est une extension galoisienne de degré 6 de $\mathbf{Q}$. Déterminer son groupe de Galois G (noter qu'un $\mathbf{Q}$-automorphisme de L est déterminé par son effet sur $x, y, \bar{y}$).

b) Quels sont les sous-groupes de G? Déterminer les sous-corps de L correspondants (cf. § 1, th. 2). Quels sont les sous-corps de L galoisiens sur $\mathbf{Q}$?

c) On rappelle que l'anneau des entiers de K est $\mathbf{Z}[x]$ (chap. V, exemple à la fin du § 3). Montrer qu'il est principal (chap. IV, § 3, cor. 1 de la prop. 1).

d) Montrer que 23 est le seul nombre premier ramifié dans L, et que l'indice de ramification correspondant est 2 (noter que la décomposition en facteurs premiers de 23 dans l'anneau des entiers de K, est de la forme $\alpha\beta^2$; en désignant par e, f, g les nombres relatifs à la décomposition de 23 dans L définis dans la prop. 1 du § 2, en déduire que $g \geqslant 2$ et que e est pair (cf. exer. 8 sur le chap. V); utiliser $efg = 6$ pour conclure que $e = 2, f = 1, g = 3$).

e) Montrer que $\mathbf{Q}[\sqrt{-23}] \subset \mathrm{L}$ et qu'aucun idéal premier de

$$\mathbf{Q}[\sqrt{-23}]$$

ne se ramifie dans L.

On remarquera que L est une extension cyclique non ramifiée de degré 3 de $\mathbf{Q}[\sqrt{-23}]$, et que le groupe des classes d'idéaux de $\mathbf{Q}[\sqrt{-23}]$ est cyclique d'ordre 3 (cf. exerc. 7, *b*) sur le chap. V). Nouveau cas particulier de la théorie du corps de classes.

3 B. Transposer l'exer. 2 au polynôme $X^3 + X + 1$ (au lieu de $X^3 - X + 1$) et à -31 (au lieu de -23). Transposer à $\mathbf{Q}[\sqrt{-31}]$ l'exer. 7, *f*) sur le chap. V.

4 B. Soient K un corps de nombres, et L le plongement logarithmique de K^* dans $\mathbf{R}^{r_1+r_2}$ (chap. IV, § 4, th. 1). On note U le groupe des unités de K et on appelle *régulateur* de K le volume du réseau L(U) de l'hyperplan W considéré au chap. IV, § 4, th. 1 (pour la mesure sur W obtenue en transportant par $W \to \mathbf{R}^{r_1+r_2-1}$ la mesure de Lebesgue).

a) Calculer les régulateurs des corps quadratiques réels donnés comme exemples explicites au chap. IV, § 6.

b) Soient z une racine primitive n-ème de l'unité dans $\mathbf{C}$, K le corps cyclotomique $\mathbf{Q}[z]$, σ l'automorphisme de K défini par $\sigma(z) = z^{-1}$ et K′ le corps des invariants de σ. Calculer $[K : K']$ et les rangs des groupes des unités U et U′ de K et K′; montrer que ces rangs sont égaux à un même entier r. Montrer qu'il existe un entier m tels que les régulateurs ρ et ρ' de K et K′ soient liés par la relation $\rho' = m\rho$. Calculer le nombre des racines de l'unité contenues dans K (resp. K′) $\left(\text{on pourra prendre } z = e^{\frac{2i\pi}{n}}\right)$. En déduire l'indice de U′ dans U.

c) avec les notations de *b*), on suppose que $n = p^s$ avec p premier, $p \neq 2$. Montrer que, pour $u \in U$, on a $\sigma(u) = \pm z^{2j}u$ (noter que $\sigma(u).u^{-1}$ est de module 1 pour tout plongement de K dans $\mathbf{C}$, donc est une racine de l'unité), d'où $\sigma(z^j u) = \pm z^j u$.

Montrer qu'on a $\sigma(z^j u) = z^j u$ (exclure le signe — en considérant les conjugués de $z^j u$ sur K'). En déduire qu'on a $U = V.U'$ où V est le groupe des racines n-èmes de l'unité contenues dans K. Montrer que l'entier m de *b*) est alors égal à 1.

5 B. *a*) Soit K le corps cyclotomique engendré sur $\mathbf{Q}$ par une racine $9^{\text{ème}}$ de l'unité z. Montrer que c'est une extension cyclique de degré 6 de $\mathbf{Q}$ (cf. § 4). Soit G son groupe de Galois.

b) En utilisant le sous-groupe H d'indice 3 de G, construire une extension galoisienne K' de degré 3 de $\mathbf{Q}$ (cf. § 1, th. 2); on montrera que $K' = \mathbf{Q}\left[\cos\frac{2\pi}{9}\right]$, et on déterminera le polynôme minimal de $2\cos\frac{2\pi}{9}$ sur $\mathbf{Q}$ (il a pour racines $z + z^8$, $z^2 + z^7$ et $z^4 + z^5$).

PROBLÈMES DE RÉVISION

I

Dans le corps $\mathbf{C}$ des nombres complexes, on pose $z = {}^{2i\pi/5}$ et on note K le corps cyclotomique $\mathbf{Q}(z)$.

1) Trouver le degré, l'anneau des entiers et le discriminant absolu de K (pour ce dernier point il pourra être commode de calculer les nombres $\mathrm{Tr}(z^j)$). Quels nombres premiers se ramifient dans A?

2) On note $\mathbf{R}$ le corps des réels, et on pose $K' = K \cap \mathbf{R}$. Montrer que K' est un corps quadratique et préciser lequel. Décrire l'anneau A' des entiers de K' et le groupe A'^* des unités de A'.

3. Montrer que K' est le seul corps quadratique contenu dans K (on pourra noter que, si K'' est un sous-corps de K, tout nombre premier qui se ramifie dans K'' se ramifie dans K).

4. Montrer que K ne contient d'autres racines de l'unité que les racines 10^{e} de l'unité (on pourra fixer son attention sur les racines de l'unité dont l'ordre est premier ou est une puissance de 2, et utiliser 3)). On note G le groupe des racines 10^{e} de l'unité.

5. *a*) En utilisant le plongement logarithmique de K, montrer que, si a est une unité de module 1 de l'anneau A des entiers de K, alors a est une racine de l'unité.

b) Soit $a = re^{i\theta}$ une unité de A $(r > 0)$. Montrer qu'on a $r^2 \in A'^*$ et $e^{2i\theta} \in G$, et que les relations $r \in A'^*$ et $e^{i\theta} \in G$ sont équivalentes.

c) On rappelle que $A(1 - z) = A(1 - z^2) = A(1 - z^3) = A(1 - z^4)$ est un idéal premier $\mathfrak{p}$ de A et qu'on a $5A = \mathfrak{p}^4$. En déduire qu'aucun élément de $(1 - z^3)K'$ n'est une unité de A, que A n'admet aucune unité d'argument $\pi/10$, et que le groupe A^* des unités de A est composé direct de G et du groupe U des unités positives de A'.

6. On rappelle que, avec les notations classiques, toute classe d'idéaux d'un corps de nombres contient un idéal entier de norme $\leqslant (4/\pi)^{r_2}.n!n^{-n}|d|^{\frac{1}{2}}$. Montrer que l'anneau A est principal.

II

Soient $\mathbf{Q}$ le corps des nombres rationnels, x le nombre réel tel que $x^3 = 2$, et K le corps $\mathbf{Q}(x)$.

1. Montrer que le polynôme $X^3 - 2$ est irréductible sur $\mathbf{Q}$, et que K est une extension de degré 3 de $\mathbf{Q}$. Quels sont, dans le corps $\mathbf{C}$ des complexes, les corps conjugués de K?

2. Soit $z = a + bx + cx^2$ $(a, b, c \in \mathbf{Q})$ un élément de K. Calculer soigneusement la trace, la norme, et le polynôme caractéristique de z sur $\mathbf{Q}$.

3. Soient $\mathbf{Z}$ l'anneau des entiers rationnels et B le sous-anneau $\mathbf{Z}[x]$ de K. Dans ce n° on se propose de montrer que l'anneau A des entiers de K est égal à B.

a) Montrer qu'on a $B \subset A$, et trouver une base du $\mathbf{Z}$-module B.

b) Soit $z = a + bx + cx^2$ $(a, b, c \in \mathbf{Q})$ un entier de K; déduire du calcul des traces de z, xz et x^2z qu'on a $6A \subset B$.
A partir de là on pourra, soit utiliser 2) pour montrer que les entiers $6a$, $6b$, $6c$ définis dans *b*) sont multiples de 6 (le raisonnement est assez long, mais élémentaire), soit procéder moins élémentairement de la façon suivante :

c) Montrer que les idéaux xA et xB sont premiers (pour xA on pourra considérer la décomposition de l'idéal 2A dans A), qu'on a $xB = B \cap xA$, et que les corps A/xA et B/xB sont égaux; en déduire qu'on a $A = B + xA$, et ensuite qu'on a $A = B + 2A$.

d. Démontrer qu'on a $3 = (x - 1)(x + 1)^3$ et que $x - 1$ est inversible dans B; procéder comme dans *c*), avec $x + 1$ à la place de x et 3 à la place de 2, pour montrer qu'on a $A = B + (x + 1)A$, et ensuite que $A = B + 3A$.

e). Déduire de *c*) et *d*) qu'on a $A = B + 6A$, et terminer la démonstration de $A = B$.

4. Calculer la différente et le discriminant de K.

5. *a*) Quelle est la structure du groupe (multiplicatif) des unités de A? Montrer que toute unité positive (resp. négative) de A est de norme 1 (resp. -1). Montrer que $x^2 + x + 1$ est une unité de A.

b) On rappelle que, si u est une unité > 1 de A et si D est le discriminant de K, on a $|D| < 4u^3 + 20$ (cf. exerc. 3 sur le chap. IV) En déduire que $x^2 + x + 1$ est un générateur du groupe des unités positives de K (des valeurs approchées de x et x^2 sont 1,26 et 1,58).

c) Calculer 3 ou 4 solutions en nombres entiers a, b, c, de l'équation

$$a^3 + 2b^3 + 4c^3 - 6abc = 1.$$

Expliquer comment on peut trouver toutes ses solutions en nombres entiers, ainsi que toutes ses solutions en nombres entiers positifs.

III

1. Montrer que le polynôme $X^3 - 3X + 1$ n'a pas de racine dans $\mathbf{Q}$ et est irréductible sur $\mathbf{Q}$. Montrer que ses trois racines dans $\mathbf{C}$ sont réelles; soit x l'une d'elles.

On note K le corps cubique $\mathbf{Q}[x]$ et A l'anneau des entiers de K.

2. Calculer le discriminant $D(1, x, x^2)$. En déduire que, si

$$a + bx + cx^2 \ (a,\ b,\ c \in \mathbf{Q})$$

est un entier de K, on a $a, b, c \in S^{-1}\mathbf{Z}$ où S est l'ensemble des $3^n (n \geqslant 0)$ (considérer $S^{-1}\mathbf{Z} \subset S^{-1}A$).

3. On pose $A' = \mathbf{Z}[x]$. Démontrer que x et $x + 2$ sont des unités de A' et de A, et qu'on a $(x + 1)^3 = 3x(x + 2)$. En déduire que $(x + 1)A$ est un idéal premier de A, qu'on a $(x + 1)A \cap A' = (x + 1)A'$ et que $A/(x + 1)A = A'/(x + 1)A'$. Montrer alors qu'on a $A = A' + (x + 1)A$ et $A = A' + 3A$. Conclure de ceci et de 2) qu'on a $A = A' = \mathbf{Z}[x]$.

4. Montrer que 2A est un idéal premier de A (noter que $X^3 - 3X + 1$ est irréductible mod. 2). En déduire que A est un anneau principal (on rappelle que toute classe d'idéaux de A contient un idéal entier de norme $\leqslant \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |d|^{\frac{1}{2}}$, avec les notations usuelles).

5. Montrer que $x^2 - 2$ est racine du polynôme $X^3 - 3X + 1$. Quels sont les corps conjugués de K sur $\mathbf{Q}$, et les $\mathbf{Q}$-isomorphismes de K dans $\mathbf{C}$?

6. On rappelle que $\cos 3u = 4\cos^3 u - 3\cos u$. Posant $x = 2\cos u$, calculer les valeurs possibles de l'angle u. En déduire que K est de la forme $L \cap \mathbf{R}$, où L est un corps cyclotomique qu'on précisera.

N.B. — Les questions 5 et 6 sont indépendantes des questions 2, 3 et 4.

Bibliographie *

E. Artin. *Theory of algebraic numbers* (G. Striker, Schildweg 12, Göttingen, Allemagne-1957) (Donne le pas à la théorie des valuations; très élégant; nombreux exemples).

H. Hasse. *Zahlentheorie* (Akademie Verlag, Berlin, 1949) (massif et très complet).

H. Hasse, *Vorlesungen über Zahlen theorie* (Springer, 1964) (décrit de multiples aspects de la théorie des nombres).

G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers* (Clarendon Press-Oxford, 1965) (profond et attrayant; remarquable sens esthétique dans le choix des sujets).

E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen* (Chelsea, New York, 1948) (un classique, très efficace et complet).

S. Lang, *Algebraic Numbers,* (Addison-Wesley, 1964) (petit livre très dense et concentré).

S. Lang, *Diophantine Geometry* (Interscience Tract nº 11, J. Wiley, New York, 1962) (orienté vers les équations diophantiennes; expose très nettement leur lien avec la Géométrie algébrique).

O'Meara, *Introduction to quadratic formes* (Springer, 1963) (exposé très efficace de la théorie des nombres algébriques, suivi d'une de ses plus belles applications et motivations).

J. P. Serre, *Corps locaux* (Hermann, Paris, 1962) (l'accent porte ici sur les corps *p*-adiques; exposé très clair et lucide des méthodes algébriques les plus récentes de la Théorie des nombres; très riche de contenu; nombreux exemples).

* Les références précédées d'un chiffre entre crochets se rapportent aux appels du texte.

E. Artin and J. Tate. *Class-field theory* (Math. Dept. Harvard University) (l'exposé le plus moderne de la fameuse théorie du « corps de classes », c'est-à-dire des extensions abéliennes des corps de nombres).

A. Weil, *Basic number theory* (Springer, 1967) (utilise la fructueuse méthode des adèles, et traite parallèlement corps de nombres et corps de fonctions).

Z. I. Borovic et I. R. Safarevic. *Théorie des nombres* (Gauthiers Villars, 1966) (très complet; excellents chapitres sur les méthodes analytiques, complexes et p-adiques; nombreuses tables numériques).

[1] N. Bourbaki. *Algèbre* (Paris, Hermann). Surtout chap. V en ce qui concerne les corps, chap. VI en ce qui concerne la divisibilité, et chap. VII en ce qui concerne les modules sur les anneaux principaux.

[2] N. Bourbaki. *Algèbre commutative* (*ibid*). Surtout chap. V en ce qui concerne les éléments entiers, et chap. VII en ce qui concerne les anneaux de Dedekind et factoriels. Théorie très complète et générale des anneaux de fractions au chap. II. Bon exposé de la théorie des valuation au chap. VI.

[3] H. Cartan. *Théorie élémentaire des fonctions analytiques...* (Paris, Hermann, 1962).

[4] G. Choquet. *Cours d'analyse* (Paris, Masson, 1963).

[5] S. Lang. *On quasi-algebraic closure* (Ann. of math., 55 (1962), 373-390).

[6] P. Samuel. *A propos du théorème des unités* (Bull. Sci. math., 90, (1966) 89-96).

[7] P. Samuel. *Anneaux factoriels* (Publ. Soc. mat. São Paulo, 1964).

[8] G. Terjanian, *Sur une conjecture de* M. *Artin* (C.R. Acad. Sci. Paris, (1966)).

[9] O. Zariski and P. Samuel, *Commutative Algebra*, Vol. I (Van Nostrand, Princeton, 1958). Chap. II sur les corps, chap. IV sur les anneaux nœthériens, chap. V sur les éléments entiers et les anneaux de Dedekind.

Index

La notation V.2 signifie chapitre V, § 2.

The index, I copied from old
Vladivostok telephone directory
Tom Lehrer