Université de Paris VI 2e semestre 2005-2006

Master de Mathématiques (M 20)

THÉORIE DES NOMBRES

Daniel BERTRAND

Envoi 2/ Avril 06

Plan

Sommaire

Ce cours porte sur la théorie algébrique des nombres, certaines de ses applications en algorithmique et en cryptographie, et une introduction à la théorie analytique des nombres.

Bibliographie

H. Cohen: *A course in computational number theory*; Springer, 1993.

M. Demazure: *Cours d'Algèbre*; Cassini, 1997.

G. Hardy and E. Wright: *An introduction to the theory of numbers*; Oxford UP, 1979

P. Samuel: *Théorie algébrique des nombres*; Hermann, 1967.

J-P. Serre: *Cours d'arithmétique*; PUF, 1970.

CHAPITRE IV

QUELQUES ALGORITHMES SUR Z

§1. Modules sur les anneaux principaux.

La notion de module sur un anneau A (utile pour étudier les extensions d'anneaux) est modelée sur celle des espaces vectoriels sur un corps (dont on a vu le rôle pour les extensions de corps). Nous donnons ici un survol de cette théorie, dont nous utiliserons la terminologie générale; les énoncés eux-mêmes ne nous seront utiles que pour $A = \mathbf{Z}$, où elle se réduit à l'étude des groupes abéliens.

Soient A un anneau commutatif et unitaire. Un A-module est la donnée d'un groupe commutatif $(M, +)$, muni d'une loi de composition externe $A \times M \to M : (a, m) \mapsto am$ distributive pour les lois d'addition de A et de M et vérifiant pour tout $a, b \in A, m \in M$: $a(bm) = (ab)m, 1.m = m$. Un homomorphisme $f : M \to M'$ est un homomorphisme de groupe vérifiant $f(am) = af(m)$ pour tout $a \in A, m \in M$. Les notions de famille libre, de famille génératrice, de base, de somme directe, se définissent comme pour les espaces vectoriels. On dit qu'un A-module est de type fini (resp. libre) s'il admet une famille génératrice finie (resp. une base). Le rang d'un A-module est le maximum (fini ou non) des cardinaux de ses familles libres finies. Si un A-module M est libre de type fini, il est de rang n fini, et M est alors isomorphe au A-module A^n.

Pour tout élément x de M, l'*annulateur* $Ann(x) = \{a \in A, ax = 0\}$ est un idéal de A. L'idéal $Ann(M) = \cap_{x \in M} Ann(x)$ s'appelle l'annulateur de M. Les éléments x de M tels que $Ann(x) \neq (0)$ s'appellent les éléments de torsion de M. Si A est intègre, l'ensemble des éléments de torsion de M forme un sous-module M_{tor} de M. Si $M_{tor} = 0$, on dit que M est un module sans torsion; c'est le cas des espaces vectoriels, même sur les corps finis.

On dit qu'un sous-module N de M est facteur direct s'il existe un sous-module N' (qu'on appelle alors un supplémentaire de N) tel que $M = N \oplus N'$.

Proposition 1 : *i) soit N un sous-module d'un A-module M, tel que le quotient M/N soit un A-module* libre. *Alors, N est facteur direct dans M.*

ii) Soit M un module sur un anneau intègre *A. Alors, M/M_{tor} est sans torsion. Si M est libre, alors M est sans torsion.*

Démonstration: i) soit $\mathcal{E}$ un système représentatif dans M d'une base de M/N. On vérifie aisément que le A-module N' engendré par $\mathcal{E}$ dans M est un supplémentaire de N.

ii) est élémentaire. Noter qu'en général, un A-module sans torsion n'est pas forcément libre (exemples: les idéaux non principaux de A; le $\mathbf{Z}$-module sans torsion $\mathbf{Q}$).

Nous nous restreignons désormais au cas des anneaux *principaux*, et même, en ce qui concerne les algorithmes, à $\mathbf{Z}$, ou tout au moins à un anneau euclidien. Le théorème 1.1 (ii) (sous la version équivalente 1.3) ne sera démontré que dans ce cas. (Voir par exemple le livre de P. Samuel *Théorie algébrique des nombres* pour le cas général.)

Théorème 1.1 : *Soient A un anneau principal, $M \simeq A^n$ un A-module libre de type fini, de rang n, et N un sous-A-module de M. Alors*

i) N est libre de type fini, de rang $s \leq n$

ii) il existe une base $\{e_1, \ldots, e_n\}$ de M et des éléments $a_1, \ldots, a_s$ de A tels que a_i divise a_{i+1} pour tout $i = 1, \ldots, s-1$, et que $\{a_1 e_1, \ldots, a_s e_s\}$ soit une base de N.

Les idéaux $\{(a_1), \ldots, (a_s)\}$ ne dépendent que M et N, et s'appellent les facteurs invariants de N dans M. Tout module de type fini étant quotient d'un module libre de type fini, on déduit du théorème 1.1 le corollaire fondamental suivant.

Théorème 1.2 : *Soit M un module de type fini sur un anneau principal A. Alors,*

i) M_{tor} est facteur direct dans M, et M est libre si et seulement s'il est sans torsion;

ii) plus précisément, il existe un entier $r \geq 0$ et des idéaux $(a_s) \subset (a_{s-1}) \subset \ldots \subset (a_1) \neq A$ tels que $M \simeq A^r \oplus A/(a_1) \oplus \ldots \oplus A/(a_s)$. L'entier r est le rang de M, et les idéaux (a_i), qu'on appelle les facteurs invariants de M, ne dépendent que de M; par exemple, $(a_s) = Ann(M_{tor})$.

En voici, pour $A = \mathbf{Z}$, trois applications immédiates:

Éléments primitifs de $\mathbf{Z}^n$: ce sont les vecteurs $x = (x_1, \ldots, x_n)$ de $\mathbf{Z}^n$ vérifiant les propriétés équivalentes suivantes:

i) x est la première colonne d'un élément de $GL_n(\mathbf{Z})$;

ii) les entiers $x_1, \ldots, x_n$ sont premiers entre eux dans leur ensemble;

iii) $\mathbf{Z}^n/\mathbf{Z}x$ est un $\mathbf{Z}$-module sans torsion;

iv) $\mathbf{Z}^n \cap \mathbf{R}x = \mathbf{Z}x$

Groupes abéliens finis : tout groupe abélien $G \neq 0$ fini est isomorphe à un produit de groupes cycliques $\mathbf{Z}/a_1\mathbf{Z} \times \ldots \times \mathbf{Z}/a_s\mathbf{Z}$, où $a_1, \ldots, a_s$ sont des entiers > 1 tels que a_i divise a_{i+1} pour tout $i = 1, \ldots, s-1$. Ces entiers, ainsi que s, ne dépendent que de G (ainsi, leur produit est l'ordre de G; a_s est l'exposant de G.)

Forme normale de Smith: soit B une matrice $m \times n$ (m lignes, n colonnes) à coefficients dans $\mathbf{Z}$, de rang s. On dit qu'elle est sous forme de Smith si tous ses coefficients sont nuls en dehors de ses s premiers élements diagonaux, qui sont positifs et vérifient pour tout $i < s$: $b_{i,i}$ divise $b_{i+1,i+1}$.

Théorème 1.3 : *Soit A une matrice $m \times n$ à coefficients dans $\mathbf{Z}$, de rang s.*

i) Il existe $V \in GL_m(\mathbf{Z})$ et $U \in GL_n(\mathbf{Z})$ telle que $B = VAU$ soit sous forme de Smith.

ii) Pour tout entier $r = 0, 1, ..., s$, soit $\Delta_r(A)$ le pgcd des mineurs d'ordre r de A, avec $\Delta_0 = 1$. Alors, $b_{r,r} = \frac{\Delta_r(A)}{\Delta_{r-1}(A)}$. La matrice B de i) est donc indépendante de U et de V.

Démonstration: i) par récurrence, il suffit de montrer que l'ensemble $\mathcal{A}$ des matrices VAU semblables à A contient une matrice B dont les coefficients $b_{1,j}, b_{i,1}$ sont nuls pour $i, j > 1$. C'est clair si $A = 0$. Sinon, des inversions de lignes et de colonnes montrent que $\mathcal{A}$ contient une matrice B, dont le coefficient $b_{1,1}$ réalise le minimum des valeurs absolues non nulles de tous les coefficients $b'_{i,j}$ de tous les éléments de $\mathcal{A}$. Comme la matrice B' obtenue en ajouant un multiple de la première colonne à la colonne d'indice $j > 1$ de B appartient à $\mathcal{A}$, on voit en effectuant la division euclidienne de $b_{1,j}$ par $b_{1,1}$, puis une nouvelle inversion de colonnes sur B', que tous les coefficients $b_{1,j}$ ($j > 1$) de B sont nuls. De même, $b_{i,1} = 0$ pour tout $i > 1$.

ii) résulte de la formule de Lagrange: soient Y une matrice $q \times t$, Z une matrice $t \times p$, r un entier $\leq inf(p, q, t)$, K une injection croissante: $[1, r] \hookrightarrow [1, q]$, et L une injection croissante: $[1, r] \hookrightarrow [1, p]$; alors,

$$Det(YZ)_{KL} = \Sigma_H Det(Y_{KH}) Det(Z_{HL}),$$

où la sommation porte sur l'ensemble des injections croissantes $H : [1, r] \hookrightarrow [1, t]$.

Nous décrivons maintenant une forme plus simple de réduction des matrices, la mise sous *forme normale d'Hermite*, qui suffit pour de nombreux problèmes: soit B une matrice $m \times n$, à coefficients dans $\mathbf{Z}$, qu'on suppose, pour alléger les énoncés, de rang m (de sorte que $m \leq n$). On dit qu'elle est sous forme d'Hermite si ses $n - m$ dernières colonnes sont nulles, tandis que ses m premières colonnes forment une matrice triangulaire supérieure vérifiant: $\forall 1 \leq i < j$, $0 \leq b_{i,j} < b_{i,i}$.

Théorème 2 : *Soit A une matrice $m \times n$ de rang m, à coefficients dans $\mathbf{Z}$. Alors, il existe une unique matrice B sous forme d'Hermite telle que $B = AU$, où $U \in GL_n(Z)$.*

Démonstration: voir cours d'algèbre du Master. [NB: on notera que les coefficients diagonaux de B ne sont en général pas ceux de la matrice de Smith associée à A.]

Application: soit $A, B = AU$ comme supra. Une base sur $\mathbf{Z}$ du noyau de l'application $\mathbf{Z}$-linéaire attachée à $A : \mathbf{Z}^n \to \mathbf{Z}^m$ est donnée par les $n - m$ dernières colonnes de U.

§2. Géométrie des nombres.

Soit V un espace vectoriel sur $\mathbf{R}$, de dimension n finie. On appelle *réseau* de V tout sous-groupe de V engendré comme $\mathbf{Z}$-module par une base de V sur $\mathbf{R}$. Un réseau L de V est donc discret, et le quotient V/L est compact. Inversement:

Proposition 2 : *Tout sous-groupe discret M de V est un réseau du $\mathbf{R}$-sous-espace vectoriel qu'il engendre dans V. En particulier, le groupe topologique V/M est isomorphe à $(\mathbf{R}/\mathbf{Z})^r \times \mathbf{R}^{n-r}$, où r désigne le rang de M sur $\mathbf{Z}$.*

Démonstration: soient $\{e_1, ..., e_r\}$ un système maximal d'éléments de M linéairement indépendants sur $\mathbf{R}$, W le sous-$\mathbf{R}$-espace vectoriel de V qu'ils engendrent, et $\overline{P}$ la partie compacte $\{\Sigma_{i=1,...,r} x_i e_i, 0 \leq x_i \leq 1\}$ de V. Alors, $\overline{P} \cap M$ est fini (car M est discret), engendre M sur $\mathbf{Z}$ et est contenu dans l'espace vectoriel engendré sur $\mathbf{Q}$ par les e_i. Il existe donc un entier $d > 0$ tel que M soit contenu dans le $\mathbf{Z}$-module libre de rang r engendré par $\frac{1}{d}e_1, ..., \frac{1}{d}e_r$. Le théorème 1.1 entraîne alors que M est engendré sur $\mathbf{Z}$ par r éléments, qui forment encore une base de W sur $\mathbf{R}$.

Fixons un élément de volume sur V, d'où une mesure invariante par translation μ sur V, et soit L un réseau de V. Pour toute base $\{b_1, ..., b_n\}$ de L sur $\mathbf{Z}$, considérons le parallèlépipède $P = \{\Sigma_{i=1,...,n}\ x_i b_i\ ,\ 0 \leq x_i < 1\}$; sa mesure est indépendante de la base choisie, et s'appelle le covolume $\mu(V/L)$ de L. En effet, pour $V = \mathbf{R}^n$, muni de la mesure de Lebesgue μ, $\mu(V/L)$ est donné par la valeur absolue du déterminant de la matrice B représentant $\{b_1, ..., b_n\}$ dans la base canonique de $\mathbf{R}^n$. On l'appelle dans ce cas *déterminant* de L, et on le note $d(L)$. En termes du produit scalaire usuel (.) sur $\mathbf{R}^n$, on peut aussi exprimer $d(L)$ comme la racine carrée du déterminant de la matrice de Gram associée à la base choisie de L:

$$\mu(V/L) = d(L) = |Det(B)| = (det(B^t B))^{1/2} = (det((b_i.b_j)_{1 \leq i,j \leq n}))^{1/2}.$$

(Un changement de base de L sur $\mathbf{Z}$ et un changement de base orthogonale de $\mathbf{R}^n$ transforment B en UBV, où U est une matrice orthogonale, et $V \in GL_n\mathbf{Z}$; cela ne modifie pas $d(L)$.) Enfin, si L est contenu dans le réseau canonique $\mathbf{Z}^n$ de $\mathbf{R}^n$, on peut également voir $d(L)$ comme l'indice $[\mathbf{Z}^n : L]$ de L dans $\mathbf{Z}^n$.

Fixons d'autre part une norme N sur l'espace vectoriel V. Le but de la géométrie des nombres est d'évaluer les éléments de petite norme des réseaux de V. Dans le cas le plus général, N est la jauge d'un corps convexe symétrique par rapport à 0, et on a:

Théorème 2 (Minkowski): *Soient μ une mesure de Haar sur V, $\mathbf{K}$ une partie convexe bornée symétrique par rapport à l'origine de V, et L un réseau de V. On suppose que $\mu(\mathbf{K}) > 2^n \mu(V/L)$. Alors, $\mathbf{K}$ contient un élément non nul de L.*

Démonstration: montrons tout d'abord que si L est un réseau de $\mathbf{R}^n$, muni de la mesure de Lebesgue μ, et si S est une partie μ-intégrable de $\mathbf{R}^n$ telle que $\mu(S) > d(L)$, il existe deux éléments $x \neq y$ de S tels que $x - y \in L$. En effet, soit P un parallèlépipède représentant $\mathbf{R}^n/L$ comme ci-dessus, de sorte que $\mu(P) = d(L)$ et que S est la réunion disjointe des parties $S \cap (h + P)$, où h parcourt L. Supposons que les parties $(-h + S) \cap P$ soient disjointes. Alors,

$$\mu(S) = \Sigma_{h \in L}\ \mu(S \cap (h + P)) = \Sigma_{h \in L}\ \mu((-h + S) \cap P) < \mu(P),$$

ce qui contredit l'hypothèse . Il existe donc $h \neq h' \in L$ et $x, y \in S$ tels que $x - y = h - h' \in L \setminus \{0\}$.

Le théorème 2 s'en déduit en considérant la partie intégrable $S = \frac{1}{2}\mathbf{K}$, qui vérifie par hypothèse $\mu(S) = (\frac{1}{2})^n \mu(\mathbf{K}) > d(L)$. L'élément non nul $z = \frac{1}{2}(2x - 2y)$ de $\mathbf{K} \cap L$ répond alors à la question.

Remarque: supposons $\mathbf{K}$ fermé. Pour tout $i = 1, \ldots, n$, soit λ_i le plus petit nombre réel tel que $L \cap \lambda_i \mathbf{K}$ contient i éléments linéairement indépendants sur $\mathbf{Z}$ (ou sur $\mathbf{R}$ – cela revient au même, puisque L est un réseau). Le théorème 2 équivaut à la majoration: $\lambda_1^n \mu(\mathbf{K}) \leq 2^n \mu(V/L)$. Plus généralement, le *deuxième théorème de Minkowski sur les minima successifs* énonce:

$$\lambda_1 \lambda_2 \ldots \lambda_n \mu(\mathbf{K}) \leq 2^n \mu(V/L).$$

On montre également que $\lambda_1 \lambda_2 \ldots \lambda_n \mu(\mathbf{K}) \geq \frac{2^n}{n!} \mu(V/L)$.

Applications:

i) tout nombre premier $\equiv 1 \bmod 4$ est somme de deux carrés; tout entier positif est somme de 4 carrés.

ii) Supposons que $\mathbf{K}$ soit la boule unité de $\mathbf{R}^n$, muni de la mesure de Lebesgue, de sorte que $\mu(\mathbf{K}) = \frac{\pi^{\frac{n}{2}}}{\Gamma(1+\frac{n}{2})}$. Le théorème 2 entraîne que le carré de la norme euclidienne du plus petit élément non nul de L est majoré par $\gamma_n d(L)^{\frac{2}{n}}$, où γ_n vaut au plus $\frac{4}{\pi}\Gamma(1 + \frac{n}{2})^{\frac{2}{n}}$.

La meilleure valeur possible de γ_n (valable pour tout réseau L de $\mathbf{R}^n$) s'appelle la n-ième constante d'Hermite. La détermination de γ_n est un problème ouvert, mais on en connait les premières valeurs: $\gamma_1 = 1, \gamma_2^2 = \frac{4}{3}, \gamma_3^3 = 2, ..., \gamma_8^8 = 256$. (Et γ_n vaut au plus $(\frac{4}{3})^{\frac{n-1}{2}}$.)

iii) Pour les applications à l'arithmétique des corps de nombres, voir le chapitre 5.

Les algorithmes concernent (comme dans l'application (ii) ci-dessus), le cas où la norme $N = \|.\|$ de V est la racine carrée d'une forme quadratique définie positive, c'est-à-dire où V est une espace euclidien, de produit scalaire (.). Rappelons tout d'abord le procédé d'orthogonalisation de Gram-Schmidt.

Proposition 3 : *Soit $\{b_1, ..., b_n\}$ une base d'un espace euclidien V. Définissons par récurrence sur $i = 1, ..., n$, les vecteurs $b'_i = b_i - \Sigma_{j=1,...,i-1}\mu_{i,j}b'_j$, où $\mu_{i,j} = \frac{(b_i \cdot b'_j)}{(b'_j \cdot b'_j)}$. Pour tout $i = 1, ..., n$, b'_i est la proj. orthogonale de b_i sur l'orthogonal de $\oplus_{j=1,...,i-1}\mathbf{R}b_j = \oplus_{j=1,...,i-1}\mathbf{R}b'_j$ dans $\oplus_{j=1,...,i}\mathbf{R}b_j$, et $\{b'_1, ..., b'_n\}$ est une base orthogonale de V.*

Le corollaire suivant fournit, à l'instar de l'inégalité inverse du deuxième théorème de Minkowski, une minoration du produit des minima successifs de la norme $\|.\|$ sur un réseau de V.

Corollaire (Hadamard) : *Pour tout réseau L de l'espace euclidien V, et toute famille $B = \{b_1, ..., b_n\}$ d'éléments de L linéairement indépendants sur $\mathbf{Z}$: $d(L) \leq \Pi_{i=1,...,n}\|b_i\|$, et ces expressions sont égales si et seulement si B est à la fois une base de L et une base orthogonale de V.*

On s'attend donc à ce que les bases de L formées de 'petits' vecteurs soient presque orthogonales. C'est ce que formalise la notion suivante. [**NB**: la fin de ce §2 ne fait pas partie du programme du cours.]

Définition: soit L un réseau de l'espace euclidien V. On dit qu'une base $\{b_1, ..., b_n\}$ de L est *reduite sous forme LLL* si l'on a, avec les notations du procédé de Gram-Schmidt: $|\mu_{i,j}| \leq \frac{1}{2}$ pour tout $1 \leq j < i \leq n$, et, pour tout $i = 2, ..., n$,

$$\|b'_i + \mu_{i,i-1}b'_{i-1}\|^2 \geq \frac{3}{4}\|b'_{i-1}\|^2,$$

ou de façon équivalente:

$$\|b'_i\|^2 \geq (\frac{3}{4} - \mu_{i,i-1}^2)\|b'_{i-1}\|^2.$$

[Noter que les vecteurs $b'_i + \mu_{i,i-1}b'_{i-1}$ et b'_{i-1} sont les projections orthoganales de b_i et de b'_{i-1} sur l'orthogonal de $\oplus_{j=1,....,i-2}\mathbf{R}b_j$.]

Théorème 3 : *Soit* $\{b_1, ..., b_n\}$ *une base réduite sous forme LLL d'un réseau* L *de* V. *Alors*

i) $d(L) \leq \Pi_{i=1,...,n}\|b_i\| \leq 2^{\frac{n(n-1)}{4}} d(L)$;

ii) $\forall\ 1 \leq j \leq i \leq n\ ,\ \|b_j\| \leq 2^{\frac{i-1}{2}}\|b_i'\|$, *de sorte que* $\|b_1\| \leq 2^{\frac{n-1}{4}} d(L)^{1/n}$;

iii) $\forall\ x \in L \setminus \{0\}\ ,\ \|b_1\| \leq 2^{\frac{n-1}{2}}\|x\|$; *plus généralement, pour tout* t*-uplet* $\{x_1, ...x_t\}$ *d'éléments de* L *lin. indép. sur* $\mathbf{Z}$, *et tout* $j \leq t$, *on a* $\|b_j\| \leq 2^{\frac{n-1}{2}} max(\|x_1\|, ..., \|x_t\|)$.

On trouvera dans les livres de H. Cohen (*A course in computational algebraic number theory*) et de M. Mignotte (*Mathématiques pour le calcul formel*) un algorithme de construction d'une base *LLL* d'un réseau arbitraire L de $\mathbf{R}^n$. Le fait qu'il converge (et par conséquent, que *tout réseau admet des bases réduites sous forme LLL*) repose sur le théorème de Minkowski (sous la version donnée dans sa troisième application). On notera qu'en vertu du Théorème 3.v, l'algorithme *LLL* permet de trouver, si ce n'est les minima successifs du réseau L, du moins des familles d'éléments de L qui ne sont pas loin de les réaliser.

Application: étant donnés n nombres réels non nuls $z_1, ..., z_n$, l'algorithme *LLL* permet souvent de déterminer s'ils sont linéairement dépendants sur $\mathbf{Z}$, et de trouver alors une relation $a_1z_1 + ... + a_nz_n = 0$ à coefficients $(a_1, ..., a_n) = a \in \mathbf{Z}^n$ les liant. Pour cela, on considère, pour tout entier $M > 0$, la forme quadratique $Q_M(a) = a_2^2 + a_3^2 + ... + a_n^2 + M(a_1z_1 + ... + a_nz_n)^2$. Elle est définie positive, et munit donc $\mathbf{R}^n$ d'une structure euclidienne. Si M est très grand, les éléments a du réseau $\mathbf{Z}^n$ tels que $Q_M(a)$ est assez petit sont candidats à fournir de telles relations.

§3 Algorithmes pour les polynômes.

L'algorithme *LLL* a été introduit en vue de factoriser les polynômes $A(X)$ à coefficients dans $\mathbf{Z}$ (cf. A. Lenstra, H. Lenstra, L. Lovász , *Factoring polynomials with rational coefficients*, Math. Ann., 261, 1982, 515-534). Voici une autre méthode, fondée sur l'algorithme de factorisation des polynômes sur les corps finis $\mathbf{F}_p$ donné par la Proposition 4 du Chap. II (Berlekamp).

De $\mathbf{F}_p[X]$ *(pour un ou plusieurs* p*) à* $\mathbf{Z}[X]$.

Un exemple: un polynôme $A(X)$ de degré 4 qui se décompose modulo p_1 (resp. p_2) en produits de deux facteurs irréductibles de degrés 2 (resp. de degrés 1 et 3) est irréductible. Mais on ne trouve pas forcément de tels couples: par exemple, on déduit de la loi de réciprocité quadratique que le polynôme $\Phi_8(X) = X^4 + 1$ se décompose modulo p en

produit de 4 facteurs de degré 1 si $p \equiv 1$ mod. 8 (ou si $p = 2$), et en produit de 2 facteurs irréductibles de degré 2 sinon. On ne peut en déduire l'irréductibilité de Φ_8 dans $\mathbf{Z}[X]$.

Dans la pratique, on combine les informations données par réduction modulo p avec la majoration suivante des valeurs absolues des facteurs eventuels de A.

Soient $A(X) = \Sigma_{i=0,...,n} a_i X^i$, $B(X) = \Sigma_{j=0,...,m} b_j X^j$ deux polynômes non nuls à coefficients dans $\mathbf{Z}$, tels que B divise A. Pour tout $j = 0, ..., m$,

$$|b_j| \leq \binom{n-1}{j}(\Sigma_{i=0,...,n}|a_i|^2)^{\frac{1}{2}} + \binom{n-1}{j-1}|a_n|.$$

Pour d'autres algorithmes, et une étude comparative de leurs performances, voir les livres de H. Cohen et de M. Mignotte cités plus haut. Plutôt que la considération de plusieurs nombres premiers, il est ainsi souvent plus efficace de tâcher de relever aux anneaux (non intègres) $(\mathbf{Z}/p^s\mathbf{Z})[X]$, avec s suffisamment grand, la décomposition donnée par l'algorithme de Berlekamp en un seul nombre premier p.

De $\mathbf{Z}[X]$ à $\mathbf{Q}[X]$ (cf. chap. I, §2).

Pour tout polynôme non nul $A \in \mathbf{Z}[X]$, on rappelle que le contenu de A, noté $cont(A)$, est le pgcd des coefficients de A.

Théorème 4 (lemme de Gauss) : *i) soient P et Q deux polynômes à coefficients dans $\mathbf{Z}$; alors, $cont(PQ) = cont(P)cont(Q)$;*

ii) soient $F \in \mathbf{Z}[X]$ de contenu 1, et $P \in \mathbf{Q}[X], Q \in \mathbf{Q}[X]$ tels que $F = PQ$. Alors, il existe $\lambda \in \mathbf{Q}, \lambda \neq 0$ tel que λP et $\lambda^{-1}Q$ soient des éléments de $\mathbf{Z}[X]$ de contenu 1;

iii) en particulier, les éléments irréductibles de l'anneau $\mathbf{Z}[X]$ sont les nombres premiers (au signe près) et les polynômes de contenu 1 irréductibles dans $\mathbf{Q}[X]$.

iv) $\mathbf{Z}[X]$ est factoriel; plus généralement, pour tout anneau factoriel A, l'anneau $A[X]$ est factoriel.

(Par conséquent, un polynôme unitaire de $\mathbf{Z}[X]$ est irréductible dans $\mathbf{Z}[X]$ si et seulement s'il est irréductible dans $\mathbf{Q}[X]$; et tout algorithme de factorisation dans $\mathbf{Z}[X]$ fournit un algorithme de factorisation dans $\mathbf{Q}[X]$.)

Démonstration: i) Il suffit de prouver la relation lorsque $cont(P) = cont(Q) = 1$. Si $cont(PQ)$ était > 1, il existerait un nombre premier p divisant tous les coefficients de PQ. Si π désigne l'homomorphisme de réduction modulo p, on aurait donc $\pi(P)\pi(Q) = \pi(PQ) = 0$ dans $\mathbf{F}_p[X]$. Mais l'anneau des polynômes à coefficients dans un corps (ou, plus généralement, dans un anneau intègre) est intègre. Contradiction.

ii) soient u (resp. v) un dénominateur commun des coefficients de P (resp. de Q). Alors, uP (resp. vQ) est un élément de $\mathbf{Z}[X]$, dont on note u' (resp. v') le contenu. D'après i), $uvPQ$ a pour contenu $u'v'$. Mais $cont(uvF) = uvcont(F) = uv$, donc $uv = u'v'$, et $\lambda = u/u'$ convient.

iii) tout $F \in \mathbf{Z}[X]$ s'écrit dans $\mathbf{Z}[X]$ sous la forme $cont(F)F'$, où $cont(F') = 1$; et on vient de voir qu'un élément de $\mathbf{Z}[X]$ de contenu 1 est irréductible dans $\mathbf{Z}[X]$ si et seulement s'il l'est dans $\mathbf{Q}[X]$.

iv) pour tout $F \in \mathbf{Z}[X]$, l'existence d'une décomposition en irréductibles de F découle de iii); son unicité du fait que $\mathbf{Z}$ et $\mathbf{Q}[X]$ sont tous deux factoriels. Même démonstration pour un anneau factoriel A quelconque, en remplaçant $\mathbf{Q}$ par le corps des fractions de l'anneau (intègre) A.

Pour conclure, donnons la preuve du critère d'irréductibilité d'Eisentein:

Proposition 5 (critère d'Eisenstein): *soient $A(X) = \Sigma_{i=0,...,n} a_i X^i$ un élément de $\mathbf{Z}[X]$, et p un nombre premier. On suppose que p divise $a_0, a_1, ..., a_{n-1}$ mais ne divise pas a_n, et que p^2 ne divise pas a_0. Alors, P est irréductible dans $\mathbf{Q}[X]$.*

Démonstration: soit $B(X) = \Sigma_{i=0,...,r} b_i X^i$ un facteur non constant de P dans $\mathbf{Z}[X]$. Alors, $p \not| b_r$ et on peut supposer que $p|b_0$. En considérant le plus grand entier t tel que p divise $b_0, ..., b_t$, on voit que $n = t + 1$, d'où $r = n$.

CHAPITRE V

ARITHMÉTIQUE DES CORPS DE NOMBRES

§1. Anneaux d'entiers.

Théorème 1 : *soient B un anneau commutatif et intègre, A un sous-anneau de B, et x un élément de B. Les propriétés suivantes sont équivalentes.*

i) x vérifie une relation de dépendance intégrale sur A (c'est-à-dire : il existe un polynôme unitaire $P \in A[T]$ tel que $P(x) = 0$);

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

iii) il existe un A-module de type fini $M \neq 0$ inclus dans B tel que $xM \subset M$.

Démonstration: *i)* $\Rightarrow$ *ii)* $\Rightarrow$ *iii)* est clair. Écrivons iii) au moyen d'un système générateur de M sur A: $xm_i = \Sigma_{j=1,...,t}\, a_{ij}m_j, i = 1, ..., t$. Par conséquent, $\Delta(x) = \det(xI_t - (a_{i,j}))$ annule la partie $M \neq 0$ de l'anneau intègre B, et $\Delta(x) = 0$ fournit la relation de dépendance intégrale i) recherchée.

Les éléments x de B vérifiant les propriétés équivalentes du thm 1 sont dits *entiers* sur A. Leur ensemble s'appelle la fermeture intégrale A' de A *dans* B; le thm. 1 montre que A' est un sous-anneau de B (pour $x, y \in A'$, considérer $M = A[x, y]$), et que $(A')' = A'$.

Soient A un anneau commutatif intègre, et K son corps de fractions. On dit que A est *intégralement clos* s'il coïncide avec sa fermeture intégrale dans K. Par exemple, tout anneau factoriel, donc tout anneau principal, est intégralement clos.

Soient A et K comme ci-dessus, L une extension algébrique de K de degré n fini, B la fermeture intégrale de A dans L, Ω une clôture algébrique de K, et S l'ensemble des K-homomorphismes de L dans Ω. Pour tout élément x de L, on note η_x l'endomorphisme du K-espace vectoriel L défini par $\{y \in L\} \mapsto \{\eta_x(y) := xy\}$. Le polynôme caractéristique de l'endomorphisme η_x, multiplié par $(-1)^n$, s'appelle le *polynôme caractéristique* de x relativement à l'extension L/K:

$$\mathrm{Car}_{x,L/K}(T) = \det(Tid_L - \eta_x) = T^n - a_{n-1}T^{n-1} + ... + (-1)^n a_0 \in K[T].$$

La trace et la norme de x relativement à L/K sont alors respectivement définies par

$$Tr_{L/K}(x) := a_{n-1} = Tr(\eta_x)\ ,\ N_{L/K}(x) := a_0 = \mathrm{Det}(\eta_x).$$

Proposition 1 : *soit x un élement de L, de degré d sur K (de sorte que d divise n). Alors,*

i) $\mathrm{Car}_{x,L/K}(T) = (\mathrm{Min}_{x,K}(T))^{\frac{n}{d}}$, *de sorte que* $Tr_{L/K}(x) = \frac{n}{d} Tr_{K(x)/K}(x)$, $N_{L/K}(x) = (N_{K(x)/K}(x))^{\frac{n}{d}}$ *;*

ii) si A est intégralement clos, et si x est entier sur A, $Min_{x,K}(T) \in A[T]$, *de sorte que* $Tr_{L/K}(x)$ *et* $N_{L/K}(x)$ *appartiennent à A.*

iii) si L/K est séparable, $Tr_{L/K}(x) = \Sigma_{\sigma \in S} \sigma(x), N_{L/K}(x) = \Pi_{\sigma \in S} \sigma(x)$.

Démonstration: i) si $n = d$, la matrice représentative de η_x dans la base cyclique $1, x = \eta_x(1), ..., x^{d-1} = \eta_x^{d-1}(1)$ est une matrice companion H, dont la dernière colonne est au signe près formée des coefficients de $Min_{x,K}$, et le résultat est bien connu. Dans le cas général, fixons une base $\omega_1, ..., \omega_{n/d}$ de L sur $K(x)$. Dans la base $\omega_j x^i; i = 0, ..., d-1, j = 1, ..., n/d$ de L sur K, la matrice représentative de η_x est composée de blocs diagonaux égaux à H, et son polynôme caractéristique est la puissance $\frac{n}{d}$-ième de celui de H.

ii, iii) Les coefficients de $Min_{x,K}$ sont les fonctions symétriques élémentaires de ses racines, et sont donc à la fois dans K et entiers sur A.

L'application $N_{L/K}$ est un homomorphisme du groupe multiplicatif L^* dans K^*. L'application $Tr_{L/K}$ est une forme K-linéaire sur L, non identiquement nulle si L/K est séparable. Pour simplifier, on suppose désormais que K est de *caractéristique nulle.* Alors, $Tr_{L/K}$ fournit un isomorphisme de K-espaces vectoriels de L vers $Hom_{K-\mathrm{lin}}(L, K)$, et pour toute base $\{\omega_1, \cdots, \omega_n\}$ de L sur K, il existe une unique base $\{\omega'_1, \cdots, \omega'_n\}$ de L sur K telle que $\forall\ i, j \in [1, n]$, $Tr_{L/K}(\omega_i \omega'_j) = \delta_{i,j}$ (symbole de Kronecker).

Définition : soit $\mathbf{B} = \{\omega_1, \cdots, \omega_n\}$ une base de L sur K. On appelle discriminant de $\mathbf{B}$ l'élément

$$disc(\mathbf{B}) = \mathrm{Det}(Tr_{L/K}(\omega_i \omega_j))_{1 \leq i,j \leq n}$$

de K . Comme cette matrice représente une forme bilinéaire non dégénérée, il est non nul.

Proposition 2 : *soient $\mathbf{B}, \mathbf{B}'$ deux bases de L sur K, M, M' les A-modules libres engendrés respectivement par $\mathbf{B}, \mathbf{B}'$ dans L. Alors:*

i) $disc(\mathbf{B}') = disc(\mathbf{B})(\mathrm{Det}P)^2$, *où P désigne la matrice de passage de $\mathbf{B}$ à $\mathbf{B}'$; en particulier,* $disc(\mathbf{B})$ *ne dépend, aux carrés des unités de A près, que de M;*

ii) $disc(\mathbf{B}) = [\mathrm{Det}(\sigma(\omega_i))_{\sigma \in S, 1 \leq i \leq n}]^2$; *en particulier, si* $\mathbf{B} = \{1, x, \cdots, x^{n-1}\}$ *pour un $x \in L$ de polynôme minimal P sur K, alors* $disc(\mathbf{B}) = (-1)^{\frac{n(n-1)}{2}} N_{L/K}(P'(x)) = Disc(P)$;

(iii) on suppose que les éléments de $\mathbf{B}$ appartiennent à l'anneau B, et que A est intégralement clos. Alors, $disc(\mathbf{B})$ *appartient à A. De plus, si $\mathbf{B}' \subset M$, et si* $disc(\mathbf{B}')$ *est sans facteur carré dans A, alors $M' = M$, et $\mathbf{B}'$ est une base de M sur A.*

Démonstration: i) et iii) sont clairs. Pour ii), considérer le produit à gauche de la matrice $(\sigma(\omega_i))_{\sigma,i}$ par sa transposée; si $\mathbf{B} = (x^i), i = 0, ..., n-1$, on obtient un déterminant de van der Monde, égal au signe près au produit des différences des racines de P, c'est-à-dire à son discriminant.

Le théorème suivant montre que quand $A = \mathbf{Z}$, l'anneau B lui-même est un A-module libre de type fini, de rang n.

Théorème 2 : *on suppose que* $A = \mathbf{Z}$, $K = \mathbf{Q}$. *Il existe une base* $\mathbf{B}$ *de* $L/\mathbf{Q}$ *formée d'éléments de* B, *et engendrant* B *sur* $\mathbf{Z}$.

Démonstration: notons tout d'abord que pour tout $x \in L$, il existe un entier $d \neq 0$ tel que dx soit entier sur $\mathbf{Z}$: par exemple, le *ppcm* des dénominateurs des coefficients de $Min_{x,\mathbf{Q}}$ convient. L'ensemble $\mathcal{B}$ des bases de L sur $\mathbf{Q}$ formées d'éléments de B est donc non vide. Leurs discriminants sont des entiers rationnels non nuls, et on peut en choisir une, soit $\mathbf{B}$, de discriminant D minimal en valeur absolue. Alors, les coordonnées de tout élément de B dans $\mathbf{B}$ sont entières, sans quoi on pourrait former, en considérant la partie fractionnaire de l'une d'elles, une base dans $\mathcal{B}$ de discriminant $< D$ en valeur absolue.

Terminologie des corps de nombres.

Dans toute la suite du chapitre, on considère un corps de nombres K, c'est-à-dire une extension de $\mathbf{Q}$, de degré fini $[K : \mathbf{Q}] = n$. On note $S_K = \{\sigma_1, \cdots, \sigma_n\}$ l'ensemble des plongements de K dans le corps $\mathbf{C}$ des nombres complexes, et $\mathbf{O}_K$ la fermeture intégrale de $\mathbf{Z}$ dans K, appelée *anneau des entiers* du corps de nombres K. D'après le théorème 2, il existe une base $\{\omega_1, \cdots, \omega_n\}$ de $\mathbf{O}_K$ sur $\mathbf{Z}$, et puisque les deux unités de l'anneau $\mathbf{Z}$ sont de carré égal à 1, toutes les bases de $\mathbf{O}_K$ sur $\mathbf{Z}$ ont le même discriminant D_K, appelé *discriminant de* K. On note en général U_K le groupe $\mathbf{O}_K^*$ des unités de l'anneau $\mathbf{O}_K$, et on supprime les indices K lorsqu'un seul corps de nombres est en jeu. Par abus de langage, les ideaux et les unités de $\mathbf{O}_K$ sont parfois appelées ideaux et unités de K.

Exemple 1 : les corps *quadratiques* sont les extensions de $\mathbf{Q}$ de degré 2. Ils sont de la forme $K = \mathbf{Q}(\sqrt{d})$, où $d \neq 1$ est un entier rationnel sans facteur carré. Si d est positif (resp. négatif), on dit que K est quadratique réel (resp. imaginaire).

Si $d \equiv 2$ ou 3 mod.4, $\mathbf{O}$ admet $\{1, \sqrt{d}\}$ pour base sur $\mathbf{Z}$, et $D = 4d$;

Si $d \equiv 1$ mod.4, $\mathbf{O}$ admet $\{1, \frac{1+\sqrt{d}}{2}\}$ pour base sur $\mathbf{Z}$, et $D = d$.

On reviendra en détail sur ce cas au chapitre VI.

Exemple 2 : les corps *cyclotomiques*. Ils sont de la forme $K_n = \mathbf{Q}(\zeta_n)$, où n est un entier positif, et $\zeta_n = e^{2i\pi/n}$. Le polynôme cyclotomique Φ_n (cf. chap. I et II) est irréductible sur

$\mathbf{Q}$, de sorte que $K_n/\mathbf{Q}$ est une extension galoisienne, de degré $\phi(n)$, et de groupe de Galois isomorphe à $(\mathbf{Z}/n\mathbf{Z})^*$. L'anneau des entiers $\mathbf{O}_n$ de K_n admet $\{1, \zeta_n, \zeta_n^2, ..., \zeta_n^{\phi(n)-1}\}$ pour base; autrement dit, $\mathbf{O}_n = \mathbf{Z}[\zeta_n] \simeq \mathbf{Z}[T]/\Phi_n(T)$. Pour $n = p \neq 2$ premier, son discriminant vaut $D_p = (-1)^{\frac{p-1}{2}} p^{p-2}$. Le corps K_p contient le corps quadratique $\mathbf{Q}(\sqrt{(-1)^{\frac{p-1}{2}} p})$ (cf. chap II), et aucun autre corps quadratique.

§2 Idéaux des corps de nombres.

Soit K un corps de nombres de degré n, d'anneau d'entiers $\mathbf{O}$. Un idéal $\mathbf{a}$ de $\mathbf{O}$ (on dira aussi: un idéal *entier*) est un $\mathbf{O}$-module contenu dans $\mathbf{O}$. Si $\mathbf{a}$ est non nul, il est, *en tant que* $\mathbf{Z}$*-module*, libre de rang n (d'après le thm. 2 ci-dessus, et le thm. 1.1 du chap. IV). En particulier, l'indice $N(\mathbf{a}) = [\mathbf{O} : \mathbf{a}]$, qu'on appelle la *norme* de $\mathbf{a}$, est *fini*. On en déduit que tout suite croissante d'idéaux de $\mathbf{O}$ est stationnaire (autrement dit, l'anneau $\mathbf{O}$ est *noethérien*). Comme un anneau intègre fini est un corps, on en déduit également:

Proposition 3 : *tout idéal premier non nul* $\mathbf{p}$ *de* $\mathbf{O}$ *est* maximal. *(Par ailleurs, il contient un unique nombre premier: le générateur de* $\mathbf{p} \cap \mathbf{Z} = (p)$*.)*

Les anneaux d'entiers de corps de nombres sont donc noethériens, intégralement clos, et leurs idéaux premiers non nuls sont maximaux. De tels anneaux sont appelés des *anneaux de Dedekind*. Des propriétés générales des anneaux de Dedekind (qu'on trouvera par exemple développées dans le livre de Samuel 'Théorie algébrique des nombres'), on tire les deux énoncés suivants, que nous admettrons.

Définition : soit $\mathbf{O}$ un anneau de Dedekind, de corps de fractions K. Un *idéal fractionnaire* de K est un $\mathbf{O}$-module $\mathbf{a}$ de type fini contenu dans K, ou, de façon équivalente, tel qu'il existe un élément $\gamma \neq 0$ de K pour lequel $\gamma\mathbf{a}$ soit un idéal de $\mathbf{O}$.

Soit $J_K = J$ l'ensemble des idéaux fractionnaires non nuls de K. Si $\mathbf{a}$, $\mathbf{b} \in J$, on pose $\mathbf{ab} := \{\Sigma_{i \in I \text{fini}} a_i b_i, a_i \in \mathbf{a}, b_i \in \mathbf{b}\}$; c'est encore un élément de J.

Théorème 3 : *pour* $\mathbf{O}$ *de Dedekind, ce produit munit* J *d'une structure de groupe abélien, d'élément neutre* $\mathbf{O}$*, où l'inverse d'un élément* $\mathbf{a}$ *de* J *est l'idéal fractionnaire*

$$\mathbf{a}^{-1} := \{x \in K, x\mathbf{a} \subset \mathbf{O}\}.$$

En particulier, pour $\mathbf{a}$ et $\mathbf{b}$ dans J, $\mathbf{b} \subset \mathbf{a}$ si et seulement s'il existe un idéal *entier* $\mathbf{c}$ tel que $\mathbf{b} = \mathbf{ac}$. On dit alors que $\mathbf{a}$ *divise* $\mathbf{b}$, et on note: $\mathbf{a} \mid \mathbf{b}$. Plus généralement, la propriété suivante remplace efficacement la non-factorialité éventuelle de $\mathbf{O}$.

Proposition 4: *soit* $\mathbf{O}$ *un anneau de Dedekind. Tout idéal entier (resp. fractionnaire) non nul et distinct de* $\mathbf{O}$ *admet une décomposition unique en produit de puissances* > 0 *(resp.* > 0 *ou* < 0*) d'idéaux premiers de* $\mathbf{O}$*.*

(Pour l'unicité, noter que si $\mathbf{p}$ est un idéal premier d'un anneau quelconque $\mathbf{O}$, et si $\mathbf{a}$, $\mathbf{b}$ sont des idéaux de $\mathbf{O}$ tels que $\mathbf{p} \supset \mathbf{ab}$, alors, $\mathbf{p}$ contient l'un au moins des idéaux $\mathbf{a}$, $\mathbf{b}$).

Pour $\mathbf{O}$ de Dedekind, on a donc:

$$\mathbf{a} \cap \mathbf{b} = \mathbf{ab} \Leftrightarrow \mathbf{a} + \mathbf{b} = \mathbf{O}.$$

(Rappelons que l'implication $\Rightarrow$ n'est pas correcte dans un anneau quelconque; l'implication $\Leftarrow$ est toujours vraie, cf. le lemme chinois.)

Revenons à l'anneau des entiers $\mathbf{O}$ d'un corps de nombres K, et à la norme $N(\mathbf{a}) = \text{card}(\mathbf{O}/\mathbf{a})$ de ses idéaux $\mathbf{a}$ non nuls.

Proposition 5: *soit* $\mathbf{a}$ *et* $\mathbf{b}$ *deux idéaux non nuls de* $\mathbf{O}$. *Alors:*

i) $N(\mathbf{ab}) = N(\mathbf{a})N(\mathbf{b})$*;*

ii) si $\mathbf{b} \subset \mathbf{a}$, $N(\mathbf{a})$ *divise* $N(\mathbf{b})$ *et* $N(\mathbf{a}) = N(\mathbf{b})$ *si et seulement si* $\mathbf{a} = \mathbf{b}$*;*

iii) $N(\mathbf{a})$ *appartient à* $\mathbf{a}$*; en particulier, pour tout entier naturel* A*, il n'y a qu'un nombre fini d'idéaux de* $\mathbf{O}$ *de norme* A*;*

iv) soit $\{\omega_1, \cdots, \omega_n\}$ *une base de* $\mathbf{a}$ sur $\mathbf{Z}$*; alors* $N(\mathbf{a}) = \mid \frac{Disc(\{\omega_1,\cdots,\omega_n\}}{D_K} \mid^{\frac{1}{2}}$*; en particulier, si* $\mathbf{a} = \alpha\mathbf{O}$ *est un idéal principal,* $N(\mathbf{a}) = \mid N_{K/\mathbf{Q}}(\alpha) \mid$.

Démonstration: i) Grâce à la proposition 4 et au lemme chinois, il suffit de montrer que pour tout idéal premier $\mathbf{p}$, de norme q, et tout entier $m \geq 1$, $N(\mathbf{p}^m) = q^m$. Mais $\mathbf{p}^{m-1}/\mathbf{p}^m$ est naturellement muni d'une structure de module sur $\mathbf{O}/\mathbf{p}$, c'est-à-dire d'espace vectoriel sur le corps $\mathbf{F}_q$, et sa dimension est majorée son rang sur $\mathbf{O}$, donc par 1. Comme elle n'est pas nulle ($\mathbf{p}^{m-1} \neq \mathbf{p}^m$, cf. prop. 4), elle vaut 1. Ainsi, $[\mathbf{p}^{m-1} : \mathbf{p}^m] = q$, et on conclut par récurrence sur m.

ii) et iii) sont clairs ($N(\mathbf{a})$ annule le $\mathbf{Z}$-module $\mathbf{O}/\mathbf{a}$), et iv) résulte de la Prop. 2.

La multiplicativité de l'application 'norme' sur les idéaux entiers permet de l'étendre au groupe J_K tout entier, et montre qu'un idéal de $\mathbf{O}$ est premier dès que sa norme est un nombre premier. La réciproque est fausse, mais si $\mathbf{p}$ est un idéal de $\mathbf{O}$ premier, sa norme, cardinal du corps fini $\mathbf{O}/\mathbf{p}$, est une puissance pure p^f de l'unique nombre premier p que contient $\mathbf{p}$. On en déduit:

Proposition 6: *soient* p *un nombre premier,* $(p) = \mathbf{p}_1^{e_1} \cdots \mathbf{p}_r^{e_r}$ *la décomposition de l'idéal entier* $p\mathbf{O}$ *en produit de puissances d'idéaux premiers, et* p^{f_i} *la norme de* $\mathbf{p}_i$*. Alors, l'ensemble* $\{\mathbf{p}_1, \ldots, \mathbf{p}_r\}$ *coïncide avec l'ensemble des idéaux premiers de* $\mathbf{O}$ *contenant* p*, et* $n = \Sigma_{i=1,\ldots,r} e_i f_i$.

Pour tout i, le nombre e_i (resp. f_i) s'appelle l'*indice de ramification* (resp. le *degré résiduel*) de l'idéal premier $\mathbf{p}_i$ au-dessus de p. La proposition suivante permet de les calculer sous une hypothèse (assez restrictive) sur $\mathbf{O}$.

Proposition 7: *On* suppose *qu'il existe un élément θ de $\mathbf{O}$, de polynôme minimal $P \in \mathbf{Z}[T]$ sur $\mathbf{Q}$ (cf. Prop. 1.ii), tel que $\mathbf{O} = \mathbf{Z}[\theta]$, et on note $P_1, ..., P_s$ des élements de $\mathbf{Z}[T]$ tels que si π désigne la réduction modulo le nombre premier p, la décomposition de $\pi(P)$ en facteurs irréductibles dans $\mathbf{F}_p[T]$ soit donnée par $\pi(P) = \pi(P_1)^{e_1}...\pi(P_r)^{e_r}$. Alors, pour tout $i = 1, ..., r$, l'idéal $\mathbf{p}_i := (p, P_i(\theta))$ de $\mathbf{O}$ est premier, et la décomposition de $p\mathbf{O}$ en idéaux premiers de $\mathbf{O}$ est donnée par $(p) = \mathbf{p}_1^{e_1} \cdots \mathbf{p}_r^{e_r}$.*

Démonstration: si θ_i est une racine de $\pi(P_i)$ dans $\overline{\mathbf{F}}_p$ (de sorte que $\mathbf{F}_p(\theta_i) = \mathbf{F}_p[T]/(\pi(P_i))$), l'application $\pi_i : \mathbf{Z}[\theta] \to \mathbf{F}_p[\theta_i]$ définie par $Q(\theta) \mapsto \pi(Q)(\theta_i)$ a pour image un corps, donc son noyau $Ker(\pi_i)$ est un idéal premier de $\mathbf{O}$. Cet idéal contient clairement $\mathbf{p}_i$, et on vérifie aisément qu'il lui est égal. De plus, $\mathbf{p}_1^{e_1}...\mathbf{p}_r^{e_r}$ est contenu dans $(p, P_1(\theta)^{e_1}....P_r(\theta)^{e_r})$, donc dans $(p, P(\theta) + p\mathbf{O}) = (p)$. Ainsi, $\{\mathbf{p}_1, ..., \mathbf{p}_r\}$ est l'ensemble des idéaux premiers de $\mathbf{O}$ contenant p, et $(p) = \mathbf{p}_1^{e_1'}...\mathbf{p}_r^{e_r'}$ pour des entiers $e_i' \in [1, e_i]$. Or $p^{f_i} = [\mathbf{O} : \mathbf{p}_i] = |\mathbf{F}_p(\theta_i)| = p^{deg(\pi(P_i))}$. On conclut en combinant les relations $\Sigma_i e_i' f_i = n$ et $\Sigma_i e_i deg(\pi(P_i)) = deg(\pi(P)) = deg(P)$.

§3 Les théorèmes de finitude

On reprend les notations de la fin du §1 et du §2. On désigne de plus par s le nombre de plongements réels de K, c'est-à-dire d'éléments σ de S tels que $\sigma(K) \subset \mathbf{R}$. Le nombre de plongements non réels est pair, et noté $2t$, de sorte que $n = s + 2t$. On appelle *constante de Minkowski* de K le nombre

$$M_K := (\frac{4}{\pi})^t \frac{n!}{n^n} \sqrt{D_K}.$$

On estimera à titre d'exercice les constantes de Minkowski des corps quadratiques et des corps cyclotomiques $\mathbf{Q}(\zeta_p)$.

N'étant en général pas factoriels, les anneaux d'entiers des corps de nombres ne sont en général pas principaux . L'énoncé fondamental suivant permet de remédier en grande partie à cette difficulté. Soit Pr_K le sous-groupe de J_K formé par les idéaux fractionnaires *principaux*, c'est-à-dire de la forme $\mathbf{a} = \alpha\mathbf{O}$, pour un élément α de K^*. Le quotient $C\ell_K := J_K/Pr_K$ s'appelle le *groupe des classes* (d'idéaux) de K.

Théorème 4 : *le groupe $C\ell_K$ est un groupe (abélien)* fini. *Son ordre h_K s'appelle le* nombre de classes *du corps de nombres K. Ainsi, pout tout idéal $\mathbf{a}$ de $\mathbf{O}$, $\mathbf{a}^{h_K}$ est un idéal principal, et l'anneau $\mathbf{O}_K$ est principal si et seulement si $h_K = 1$.*

Ce résultat découle de l'énoncé suivant (plus précis, et crucial pour le calcul effectif de h_K), joint à la Prop. 5.ii.

Théorème 5: *tout élément de $C\ell_K$ admet parmi ses représentants dans J_K un idéal entier de norme inférieure ou égal à la constante de Minkowski M_K de K.*

Démonstration: considérons l'application

$$\mathcal{S} : K \to \mathbf{R}^s \times \mathbf{C}^t : x \mapsto (\sigma_i(x), i = 1, ..., s; \sigma_j(x), j = s+1, ..., s+t),$$

où les t derniers plongements représentent les différentes paires $(\sigma_j, \overline{\sigma_j})$ de plongements complexes conjugués. C'est un homomorphisme de groupes (additifs) injectif, appelé plongement canonique de K dans $\mathbf{R}^s \times \mathbf{C}^t \simeq \mathbf{R}^n$ (on fixe ce dernier isomorphisme au moyen de la décomposition $\mathbf{C} = \mathbf{R} \oplus i\mathbf{R}$). La Prop. 2 entraîne que l'image de $\mathbf{O}$ sous $\mathcal{S}$ est un réseau de $\mathbf{R}^n$ de covolume $2^{-t}|D_K|^{1/2}$. Pour tout idéal $\mathbf{a}$ de $\mathbf{O}$, $\mathcal{S}(\mathbf{a})$ est donc un réseau de covolume $2^{-t}|D_K|^{1/2}N(\mathbf{a})$. Considérons alors, pour tout nombre réel $c > 0$, la partie de $\mathbf{R}^s \times \mathbf{C}^t$, convexe et symétrique par rapport à l'origine, $B_c = \{(y_1, ..., y_s, z_{s+1}, ..., z_{s+t}), \Sigma_i|y_i| + 2\Sigma_j|z_j| \leq c\}$. Son volume valant $2^s(\frac{\pi}{2})^t \frac{c^n}{n!}$, le théorème de Minskowski entraîne que dès que $c^n > (\frac{4}{\pi})^t n!|D_K|^{1/2}N(\mathbf{a})$, il existe un élément non nul α de $\mathbf{a}$ tel que $\mathcal{S}(\alpha) \in B_c$. D'après l'inégalité des moyennes arithmétique et géométrique, un tel α vérifie:

$$|N_{K/\mathbf{Q}}(\alpha)| = \Pi_i|\sigma_i(\alpha)|\Pi_j|\sigma_j(\alpha)|^2 \leq [\frac{1}{n}(\Sigma_i|\sigma_i(\alpha)| + 2\Sigma_j|\sigma_j(\alpha)|)]^n \leq \frac{c^n}{n^n}.$$

Ainsi, *tout idéal entier non nul* $\mathbf{a}$ *contient un élément non nul de norme majorée en valeur absolue par* $(\frac{4}{\pi})^t \frac{n!}{n^n}|D_K|^{1/2}N(\mathbf{a}) = M_K N(\mathbf{a})$.

Dans ces conditions, soient C un élément de $C\ell_K$, $\mathbf{a}$ un idéal entier représentant la classe inverse C^{-1} dans J_K, et α un élément non nul de $\mathbf{a}$ de norme $\leq M_K N(\mathbf{a})$. Alors, l'idéal $\alpha\mathbf{a}^{-1}$ est entier, et représente C dans J_K. D'après la Prop. 5, sa norme vaut $|N_{K/\mathbf{Q}}(\alpha)|(N(\mathbf{a}))^{-1}$, qui est bien majoré par M_K.

Corollaire (théorème d'Hermite): $\mathbf{Q}$ *est le seul corps de nombres de discriminant 1 .*

Démonstration: les idéaux entiers non nuls étant de norme ≥ 1, le théorème 5 entraîne l'inégalité $|D_K| \geq \frac{n^{2n}}{(n!)^2}(\frac{\pi}{4})^{2t} \geq \frac{n^{2n}}{(n!)^2}(\frac{\pi}{4})^n$, qui est > 1 pour $n \geq 2$.

Le théorème de Minskowski fournit un autre théorème de finitude fondamental.

Théorème 6 (théorème de Dirichlet): *le groupe U_K des unités de $\mathbf{O}_K$ est le produit direct du groupe fini μ_K (formé par les racines de l'unité dans K) et d'un groupe libre de rang $s + t - 1$.*

En particulier, pour K quadratique réel, il existe une unité u de $\mathbf{O}$ telle que $U_K = \{\pm 1\} \times u^{\mathbf{Z}}$. La détermination d'une telle unité, dite fondamentale, se ramène à la résolution des classiques *équations de Pell-Fermat*. De façon générale, il est clair qu'un élément α de $\mathbf{O}$ est une unité si et seulement si $N_{K/\mathbf{Q}}(\alpha) = \pm 1$.

Le groupe μ_K est le sous-groupe de torsion du $\mathbf{Z}$-module U_K. On déduit facilement de l'irréductibilité des polynômes cyclotomiques qu'il est fini. La partie profonde du théorème est donc la détermination du rang du $\mathbf{Z}$-module libre U_K/μ_K.

Démonstration: considérons l'application

$$\mathcal{L} : U_K \to \mathbf{R}^s \times \mathbf{R}^t : x \mapsto (Log|\sigma_i(x)|, i = 1, ..., s; Log|\sigma_j(x)|, j = s+1, ..., s+t).$$

C'est un homomorphisme de groupes, appelé par abus de langage 'plongement' logarithmique de U_K, dont le noyau coïncide avec μ_K: il n'y a en effet qu'un nombre fini d'éléments de $\mathbf{O}$ dont les images par tous les plongements de K soient bornés, les coefficients de leurs poly. minimaux étant alors bornés. Comme la norme d'une unité vaut ± 1, l'image de U_K sous $\mathcal{L}$ est incluse dans l'hyperplan W de $\mathbf{R}^{s+t}$ d'équation $\Sigma_i x_i + 2\Sigma_j y_j = 0$. La remarque précédente entraîne de plus qu'elle est discrète. D'après IV, Prop. 2, $U_K/\mu_K \simeq \mathcal{L}(U_K)$ est donc un $\mathbf{Z}$-module libre de rang $r \leq s+t-1$. Reste à voir que $\mathcal{L}(U_K)$ engendre W sur $\mathbf{R}$.

Pour alléger l'exposé, nous supposerons que $t = 0$, i.e. $n = s$. Montrons que dès que $s > 1$, il existe une unité η dont tous les conjugués, sauf $\sigma_1(\eta)$, sont de val. absolue < 1 (on dit que η est un nombre de Pisot). Soient $0 < \delta_0 < 1$ et M_0 deux réels tels que $M_0 \delta_0^{n-1} = |D_K|^{1/2}$. D'après Minskowski, il existe $\alpha_0 \neq 0$ dans $\mathbf{O}$ tel que $\sigma_1(\alpha_0) \leq M_0$, $\sigma_i(\alpha_0) \leq \delta_0$ pour $i \geq 2$, et donc $|N(\alpha_0)| \leq |D_K|^{1/2}$. De proche en proche, on construit de même une suite d'entiers $\alpha_n \neq 0$ dans $\mathbf{O}$ tels que $|N(\alpha_n)| \leq |D_K|^{1/2}$ et $sup_{i \geq 2} |\sigma_i(\alpha_n)| < inf_{i \geq 2} |\sigma_i(\alpha_{n-1})| < 1$. Comme il n'y a (d'après la prop. 5 iii) qu'un nombre fini d'éléments de $\mathbf{O}$ de norme bornée non associés, l'un des quotients $\alpha_{n'}/\alpha_n, n' > n \geq 0$, est une unité η répondant à la question. En particulier, $Log|\sigma_i(\eta)| < 0$ pour tout $i \geq 2$.

Supposons que $r < s-1$, i.e. que $\mathcal{L}(U_K)$ soit inclus dans un hyperplan W' distinct de W. Après réindexation, on peut supposer son équation de la forme $\Sigma_i c_i x_i = 0$, avec $c_1 \geq c_i$ pour $i \geq 2$. En retranchant c_1 fois l'équation de W, on voit que $\mathcal{L}(\eta)$ n'appartient pas à W'; contradiction.

CHAPITRE VI

ALGORITHMES QUADRATIQUES

§1. Corps quadratiques.

Soit $d \neq 1$ un entier rationnel sans facteurs carrés. Rappelons (cf. chap. V) que le corps $K = \mathbf{Q}(\sqrt{d})$, admet $\{1, \omega\}$ pour base sur $\mathbf{Z}$ de son anneau d'entiers $\mathbf{O}_K$, avec

$\omega = \sqrt{d}$ si $d \equiv 2$ ou 3 mod.4 ; le discriminant de K vaut alors $D = 4d$;

$\omega = \frac{1+\sqrt{d}}{2}$ si $d \equiv 1$ mod.4; le discriminant de K vaut alors $D = d$.

Les entiers D apparaisant de cette façon s'appellent les *discriminants fondamentaux*. Ils sont congrus à 0 ou 1 mod. 4 . Inversément, tout entier $D \neq 1$ qui est soit $\equiv 1$ mod. 4 et sans facteur carré, soit divisible par 4 et tel que $D/4$ soit $\equiv 2$ ou 3 mod. 4 et sans facteur carré, est un discriminant fondamental. On notera $C_D = C\ell_K$ et $h(D) = h_K$ le groupe de classes et le nombre de classes du corps quadratique K correspondant.

Suivant le type de décomposition de l'idéal (p) qu'il engendre dans $\mathbf{O}_K$, un nombre premier p est dit:

inerte si $(p) = \mathbf{p}$ (autrement dit, si (p) est encore premier);

décomposé si $(p) = \mathbf{pp'}$, où $\mathbf{p'} \neq \mathbf{p}$; dans ce cas, $\mathbf{p'}$ est l'image de $\mathbf{p}$ par l'automorphisme non identique de K, et les classes dans C_D de ces idéaux sont inverses l'une de l'autre;

ramifié si $(p) = \mathbf{p}^2$; dans ce cas, la classe de $\mathbf{p}$ dans C_D est d'ordre 1 ou 2.

On déduit de la proposition 7 du chap. IV, en notant $(\frac{\cdot}{p})$ le symbole de Legendre:

Proposition 1 : *i) Un nombre premier p impair est inerte si $(\frac{d}{p}) = -1$, décomposé si $(\frac{d}{p}) = 1$, et ramifié si p divise d.*

ii) Le nombre premier $p = 2$ est inerte si $d \equiv 5$ mod. 8, décomposé si $d \equiv 1$ mod. 8, et ramifié dans les autres cas.

En particulier, p est ramifié dans K si et seulement si p divise le discriminant D de K. C'est là d'ailleurs une propriété générale des corps de nombres.

L'algorithme de factorisation des entiers dont nous décrivons le principe au §3 repose sur l'énoncé suivant.

Théorème 1 : *Soient $D < 0$ un discriminant fondamental négatif, et t le nombre de facteurs premiers de D distincts. Alors,*

i) le groupe C_D/C_D^2 est isomorphe à $(\mathbf{Z}/2\mathbf{Z})^{t-1}$. En particulier, 2^{t-1} divise le nombre de classes $h(D)$, et $h(D)$ est impair si et seulement si $D = -4, -8$, ou l'opposé d'un nombre premier $\equiv 3$ mod. 4;

ii) plus concrètement, le sous-groupe $C_D[2]$ de C_D formé par les éléments d'ordre 1 ou 2 est engendré par les classes des idéaux premiers divisant D.

[Un énoncé similaire vaut quand $D > 0$, sous réserve de considérer les classes au sens 'restreint'. Sans cette modification, on obtient seulement: $2^{t-2}|h(D)$.]

Nous montrerons seulement que les classes considérées dans ii) engendrent un sous-groupe isomorphe à $(\mathbf{Z}/2\mathbf{Z})^{t-1}$. On se ramène facilement au cas où $D \leq -8$, pour lequel $\mathbf{O}_K^*$ $(= \mu_K$ puisque $D < 0)$ est réduit à $\{\pm 1\}$. Soient $p_1, ..., p_t$ les nombres premiers divisant D, $\mathbf{p_i}$ les idéaux premiers correspondant, et $\mathbf{a}$ le produit de $s \in [1, t]$ d'entre eux. Alors $\mathbf{a}^2 = (p_{i_1}...p_{i_s})$ est principal, mais $\mathbf{a}$ ne peut être principal que s'il existe $\zeta = \pm 1 \in \mathbf{O}_K^*$ tel que $\zeta p_{i_1}...p_{i_s}$ soit un carré dans K^*. Cela se produit si et seulement si $-dp_{i_1}...p_{i_s}$ est un carré dans $\mathbf{Q}^*$, c'est-à-dire ssi $s = t$ lorsque $d \equiv 1$ ou 2 mod. 4 (resp. $s = t-1$ et $2 \neq p_{i_1}, ..., p_{i_s}$ lorsque $d \equiv 3$ mod. 4). Dans chaque cas, les classes de $\mathbf{p}_1, ..., \mathbf{p}_t$ engendrent donc un sous-espace vectoriel de dimension $t-1$ du $\mathbf{F}_2$-espace vectoriel $C_D[2]$. [Contre-exemple dans le cas réel: la classe modulo $\mathbf{O}_K^*$ de $2 = (2-\sqrt{3})(1+\sqrt{3})^2$ est un carré dans $(\mathbf{Q}(\sqrt{3}))^*$, et l'idéal premier $\mathbf{p} = (1+\sqrt{3})$ qui divise 2 est principal.]

Le théorème 1 établit une correspondance entre des diviseurs de D et les éléments d'ordre 2 (appelées traditionellement classes *ambiges*) du groupe de classes C_D. Dans le paragraphe suivant, on montre comment représenter les éléments de C_D par des formes quadratiques de discriminant D, plutôt que par les idéaux de $\mathbf{O}_K$. Les classes ambiges y sont plus facilement reconnaissables, et le passage des formes qui les représentent à une factorisation de D est immédiat (cf. §3). Ce dictionnaire fournit en prime (cf. fin du §2) une majoration très précise du nombre de classes $h(D)$.

§2. Formes quadratiques.

Définition: soient $f(x,y) = ax^2 + bxy + cy^2, f'(x,y) = a'x^2 + b'xy + c'y^2$ deux formes quadratiques binaires à coefficients dans $\mathbf{Z}$. On dit qu'elles sont équivalentes s'il existe un élement $U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbf{Z})$ (= sous-groupe de $GL_2(\mathbf{Z})$ formé des matrices de déterminant $+1$) tel que

$$f(U(x,y)) := f(\alpha x + \beta y, \gamma x + \delta y) = f'(x,y).$$

On vérifie que c'est bien une relation d'équivalence sur l'ensemble des formes quadratiques.

Pour tout entier n, l'étude de l'équation diophantienne $f(x,y) = n$ équivaut alors à celle de $f'(x,y) = n$.

Soit $D = b^2 - 4ac$ le *discriminant* de f. Alors, f' a même discriminant; de même, les pgcd de (a,b,c) et de (a',b',c') coïncident (et on dit que f est *primitive* si ce pgcd vaut 1); enfin, le signe de a' est celui de a si $D < 0$ (et est alors > 0 si et seulement si f est définie positive). Pour tout entier D, on peut donc considérer l'ensemble C'_D des classes d'équivalence de formes quadratiques primitives de discriminant D, auxquelles on demande de plus, si $D < 0$, d'être définies positives. L'ensemble C'_D, dont on note $h'(D)$ le cardinal, est non vide si et seulement si $D \equiv 0$ ou 1 modulo 4 (pour l'existence, considérer respectivement les formes primitives 'fondamentales' $x^2 - \frac{D}{4}y^2$ et $x^2 + xy + \frac{1-D}{4}y^2$). Par ailleurs, si D est un discriminant fondamental au sens du §1, toute forme f représentant un élément de C'_D est primitive.

Proposition 2: *soient $D < 0$ un discriminant fondamental et K le corps quadratique imaginaire $\mathbf{Q}(\sqrt{D})$. Il existe une bijection Ξ, explicitement décrite ci-dessous, entre l'ensemble C'_D des classes d'équivalence de formes quadratiques primitives définies positives de discriminant D, et l'ensemble C_D des classes d'idéaux fractionnaires de K. En particulier, les cardinaux $h(D)$ et $h'(D)$ de ces ensembles coïncident, et l'on peut par transport de structure munir C'_D d'une structure de groupe.*

Remarques: i) Un énoncé similaire vaut quand $D > 0$, sous réserve de considérer les classes d'idéaux au sens 'restreint' du corps quadratique réel K

ii) Soit Φ_D l'ensemble des formes quadratiques primitives de discriminant D (et définies positives si $D < 0$). On peut, suivant Gauss, munir l'ensemble Φ_D lui-même d'une loi de composition interne o . Celle-ci fournit par passage au quotient sous l'action de $SL_2(\mathbf{Z})$ la loi de groupe sur C'_D décrite dans l'énoncé.

Description de Ξ : soit $f(x,y) = ax^2 + bxy + cy^2$ une forme primitive de discriminant $D < 0$, définie positive, de sorte que $(a,b,c) = 1$ et $a > 0$. Soit $\tau = \frac{-b+\sqrt{D}}{2a}$ la racine du polynôme $aT^2 + bT + c$ de partie imaginaire positive. Alors $\mathbf{a} = \mathbf{Z} \oplus \mathbf{Z}\tau$ est un idéal fractionnaire de K, de norme $N(\mathbf{a}) = | \frac{Disc(\{1,\tau\})}{D} |^{\frac{1}{2}} = \frac{1}{a}$. Si $f' = f \circ U$ désigne une forme équivalente à f, avec $U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}^{-1} \in SL_2(\mathbf{Z})$, on aura $\tau' = \frac{\alpha\tau+\beta}{\gamma\tau+\delta}$, et l'idéal fractionnaire $\mathbf{a}' = \mathbf{Z} \oplus \mathbf{Z}\tau' = (\gamma\tau + \delta)^{-1}(\mathbf{Z} \oplus \mathbf{Z}\tau)$ définira dans C_D le même élément que $\mathbf{a}$. D'où une application Ξ : classe de $f \in C'_D \mapsto$ classe de $\mathbf{a} \in C_D$.

Soit N la norme relative à $K/\mathbf{Q}$. Pour $x, y \in \mathbf{Z}$, on a avec les notations précédentes:

$$f(x,y) = a(x^2 + \frac{b}{a}xy + \frac{c}{a}y^2) = \frac{N(x+y\tau)}{N(\mathbf{a})}.$$

On en déduit que l'application qui, à tout idéal fractionnaire non nul $\mathbf{a}$ de K, associe la forme quadratique $\check{f} : \mathbf{a} \to \mathbf{Z} : \check{f}(\xi) = \frac{N(\xi)}{N(\mathbf{a})}$, définit, après choix d'une base orientée de $\mathbf{a}$ sur $\mathbf{Z}$ et passage au quotient par l'action de $SL_2\mathbf{Z}$), une application de C_D dans C'_D, inverse de Ξ. Donc Ξ est bien une bijection.

Définition: soit $f(x,y) = ax^2 + bxy + cy^2$ une forme quadratique, de discriminant D (et définie positive si $D < 0$). On dira *ici* que f est *réduite* si $|b| \leq |a| \leq |c|$; si $D < 0$, et si $a = |b|$ ou c, on demande de plus que $b \geq 0$.

Théorème 2: *Soient D un entier rationnel qui n'est pas un carré, et $f(x,y) = ax^2 + bxy + cy^2$ une forme quadratique de discriminant D (définie positive si $D < 0$).*

i) Si f est réduite, $|a| \leq \sqrt{\frac{|D|}{3}}$.

ii) f admet dans sa classe d'équivalence une forme réduite (et une seule si $D < 0$).

Démonstration: i) si f est réduite, $|D| \geq 4|ac| - |b|^2 \geq 4|a|^2 - |a|^2 = 3|a|^2$.

ii) L'action de $U = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$) (resp. $U = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$) $\in SL_2(\mathbf{Z})$ sur f remplace ses coefficients a, b, c par $a, b-2na, c-nb+n^2a$ (resp. par $c, -b, a$). Par ailleurs, le coefficient a des formes équivalentes à f n'est jamais nul, car D n'est pas un carré. L'algorithme de division euclidienne de b par $2a$ permet donc de supposer que $-|a| \leq b \leq |a|$. Si le nouveau coefficient c obtenu est de valeur absolue $\geq |a|$, on a gagné (aux cas d'égalité près si $D < 0$). Sinon, on remplace a, b, c par $c, -b, a$ avec $|c| < |a|$, et on recommence. On obtient ainsi en un temps fini une forme de la classe de f avec $|a| \geq 1$ minimal, qu'il reste éventuellement à mettre sous forme réduite au moyen d'une dernière division euclidienne.

Pour vérifier l'unicité dans le cas défini positif, on note que le coefficient $a' = a\alpha^2 + b\alpha\gamma + c\gamma^2$ de $f' = f\mathrm{o}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ est $\geq a$ si f est réduite, et égal à a ssi $\gamma = 0$. (Autrement dit, le coefficient a d'une forme réduite f est la plus petite valeur prise par f (et donc par toute f' équivalente à f) sur $\mathbf{Z}^2 \setminus \{0\}$.)

Le théorème 2 entraîne immédiatement que pour tout D non carré, le cardinal $h'(D)$ de C'_D est fini. Plus précisément, désignons par $d(n)$ le nombre de diviseurs d'un entier $n > 0$; par exemple, $d(n) = 2$ ssi n est un nombre premier. Alors, $d(n)$ est une fonction arithmétique multiplicative, qui vérifie:

$$\forall \epsilon > 0, \exists c_\epsilon > 0 \text{ tel que } \forall n \in \mathbf{N}, d(n) < c_\epsilon n^\epsilon$$

(voir Hardy-Wright, *An introduction to the theory of number*, Theorem 315). Puisque les coefficients a, b, c d'une forme réduite de discriminant D vérifient $|b| \leq \sqrt{\frac{|D|}{3}}$ et $4ac = b^2 - D$, on en déduit:

$$h'(D) \leq 2\ \Sigma_{|b|\leq\sqrt{\frac{|D|}{3}}}\ d(|D-b^2|) \leq 4\sqrt{|D|}.c_\epsilon(2|D|)^\epsilon = \ \mathrm{O}(|D|^{\frac{1}{2}+\epsilon}).$$

Par conséquent, d'après la proposition 2:

Corollaire: *Soit K un corps quadratique imaginaire, de discriminant $D<0$. Le nombre de classes $h(D)$ de K est fini, et vérifie $\overline{\lim}_{D\to-\infty}\frac{log(h(D))}{log|D|}\leq\frac{1}{2}$.*

[On démontre que cette limite supérieure est en fait une limite, et qu'elle vaut $\frac{1}{2}$. En particulier, il n'y a qu'un nombre fini de corps quadratiques imaginaires d'anneau d'entiers principal. L'analogue de ce dernier résultat pour les corps quadratiques réels n'est pas connu - et est probablement incorrect.]

§3. Un algorithme de factorisation sur Z.

Voici le principe de cet algorithme, dû à D. Shanks. Soit N un grand entier impair, que, pour simplifier, on supposera ici sans facteurs carrés, et soit D le discriminant du corps $K=\mathbf{Q}(\sqrt{-N})$. Considérons une forme quadratique définie positive $f(x,y)=ax^2+bxy+cy^2$, de discriminant D. Alors l'opposée de $\Xi(f)$ dans C_D est donnée par la forme $ax^2-bxy+cy^2$. Lorsque f est réduite, $\Xi(f)$ est donc une classe ambige (ou triviale) si et seulement si

ou bien $b=0$, auquel cas $D=-4ac$, et $N=ac$;

ou alors $a=b$, auquel cas $D=b(b-4c)$, et $N=b(4c-b)$ pour b impair, $N=\frac{b}{2}(2c-\frac{b}{2})$ pour b pair;

ou enfin $a=c$, auquel cas $D=(b-2a)(b+2a)$, et $N=(2a-b)(b+2a)$ pour b impair, $N=(\frac{b}{2}+a)(a-\frac{b}{2})$ pour b pair.

On retrouve ainsi le fait, établi au §1, que toute classe ambige donne lieu à une factorisation de D; inversément, on déduit des formules précédentes (en distinguant les cas $N\equiv 1,3$ mod. 4), que toute factorisation de D provient d'une forme réduite dans une classe ambige. Autrement dit, la mise sous forme réduite des formes quadratiques fournit une bijection, maintenant *explicite*, entre les factorisations de D et les classes ambiges.
[NB: les formes normales d'Hermite auraient en fait aussi permis de travailler avec les idéaux de $\mathbf{O}_K$.]

Reste à construire quelques classes ambiges. Pour cela, on calcule d'abord le nombre de classes $h(D)=2^sq$, avec q impair. Pour tout $x\in C_D$, l'ordre de x^q est alors une puissance de 2, et si x n'est pas la classe nulle, il existe $r<s$ tel que x^{2^r} soit d'ordre exactement 2. Pour plus de détails sur les algorithmes de Shanks sous-tendant ces constructions, voir le livre d'H. Cohen, §§5.4 et 8.6.