Université P. et M. Curie (Paris VI),
Deuxième semestre 2006/2007

Michel Waldschmidt
date de mise à jour: 24/04/2007

Master de sciences et technologies 1ère année -
Spécialité : Mathématiques Fondamentales

Mention : Mathématiques et applications
MO11 : Théorie des nombres (12 ECTS)

Table des matières

Université P. et M. Curie (Paris VI),
Deuxième semestre 2006/2007

Michel Waldschmidt
date de mise à jour: 24/04/2007

Master de sciences et technologies 1ère année -
Spécialité : Mathématiques Fondamentales

Mention : Mathématiques et applications
MO11 : Théorie des nombres (12 ECTS)

Première partie: Théorie des Corps

Fascicule 1 : introduction + sections 1.1 à 1.4 (10 pages)

Introduction : équations Diophantiennes

Historiquement, la principale source du développement de la théorie algébrique des nombres est le problème de la résolution des équations en nombres entiers ou rationnels. Traditionnellement, on appelle *équation Diophantienne* une équation polynomiale $f(x_1, \ldots, x_n) = 0$, où f est un polynôme à coefficients rationnels, que l'on cherche à résoudre en nombres entiers ou rationnels. *Résoudre* une telle équation signifie d'abord décider si elle a ou non des solutions, quand elle en a il faut ensuite dire si leur ensemble est fini ou non, et pour la résoudre complètement il faut enfin déterminer toutes les solutions.

Un exemple simple est l'équation $y(y-1) = x^2$. Elle a 2 solutions en nombres entiers, à savoir $(x, y) = (0, 0)$ et $(0, 1)$, tandis qu'elle a une infinité de solutions en nombres rationnels : pour chaque nombre rationnel t distinct de ± 1 le couple

$$(x, y) = (t/(t^2-1)\ ,\ t^2/(t^2-1)) \in \mathbf{Q} \times \mathbf{Q}$$

est solution, et on les obtient toutes ainsi à part $(0, 1)$ (qu'on retrouverait en passant en coordonnées projectives, ce qui revient à prendre $t = \infty$).

Un des premiers mathématiciens à avoir considéré ce genre de question est Diophante d'Alexandrie (325–409). La traduction, par Bachet de Méziriac (1581–1638) de la partie de ses œuvres qui était parvenue dans le monde occidental grâce aux mathématiciens arabes a été la source d'inspiration de Fermat (1601–1665). Beaucoup d'énoncés formulés par Fermat, et bien d'autres, ont été démontrés par Euler (1707–1783). La théorie des équations quadratiques fait l'objet de nombreux travaux à partir du XVIIIè siècle, notamment par Lagrange (1736–1813) et Gauss (1777-1855). Le "dernier théorème de Fermat", selon lequel l'équation $x^n + y^n = z^n$ n'a pas de solution en nombres rationnels non nuls x, y, z dès que l'entier n est supérieur ou égal à 3, reste un défi jusqu'en 1994 où A. Wiles en donnera enfin une démonstration complète. Il motive les recherches de Kummer (1810–1893), Dedekind (1831–1916), Dirichlet (1805–1859) et bien d'autres ; c'est ce problème qui est à l'origine des principaux concepts dont il sera question dans ce cours.

Jusque vers la fin du XIXème siècle les méthodes employées seront spécifiques aux équations considérées. Il faudra attendre les contributions de Hurwitz (1859–1919) et Poincaré (1854–1912) pour disposer d'énoncés portant sur des classes générales d'équations. Le début du XXème siècle verra apparaître d'abord les méthodes d'approximation diophantienne avec les travaux de Thue

(1863–1922), puis grâce à ces outils puissants les résultats de Siegel (1896–1981) sur les points entiers sur des courbes algébriques (il s'agit de décider si une équation $f(x,y)=0$ a une infinité de solution entières, Siegel donne en 1929 des conditions nécessaires et suffisantes sur le polynôme $f \in \mathbf{Z}[X]$). Un énoncé semblable pour les points rationnels a été proposé par Mordell (1888–1972) et démontré par G. Faltings en 1983. On sait maintenant dire si une équation Diophantienne $f(x,y)=0$ a une infinité de solution rationnelles ou non, mais quand il y en a seulement un nombre fini on ne sait pas encore les déterminer toutes : on sait cependant en majorer le nombre.

Pour les équations Diophantiennes faisant intervenir un plus grand nombre de variables, Yu.V. Matiyasevich a résolu par la négative en 1970 une question posée par Hilbert en 1900 : *il n'y a pas d'algorithme général permettant de déterminer si une équation en nombres entiers $f(x_1,\dots,x_n)$ a ou non une infinité de solutions dans $\mathbf{Z}^n$.*

Une extension de la notion d'équation Diophantienne est celle *d'équation Diophantienne exponentielle*, dans laquelle certains exposants sont considérés comme des inconnues. Une des plus connues est celle proposée en 1844 par Catalan $x^p - y^q = 1$, où les inconnues (x,y,p,q) sont des entiers tous ≥ 2. Catalan (1814-1894) a conjecturé que la seule solution était $(3,2,2,3)$ correspondant à $3^2 - 2^3 = 1$. Cette conjecture a été démontrée en 2003 par Preda Mihailescu. Une démonstration complète et détaillée est donnée par H. Cohen [1].

Une question plus vaste que celle de Catalan a été posée par S.S. Pillai (1901–1950) en 1945 : *pour chaque entier $k > 0$, l'équation $x^p - y^q = k$ n'a qu'un nombre fini de solutions en entiers (x,y,p,q) tous ≥ 2.* Il n'y a que le cas $k=1$ qui soit résolu. La conjecture de Pillai signifie que la distance entre deux termes consécutifs de la suite

$$1, 4, 8, 9, 16, 25, 27, 32, 36, 49, 64, 81, 100, 121, 125, 128, 144, \dots$$

des puissance parfaites tend vers l'infini.

Remarque : On trouve des informations biographiques concernant les différents mathématiciens cités sur le site internet
The MacTutor History of Mathematics archive
http ://www-gap.dcs.st-and.ac.uk/∼history/

Considérons pour commencer la plus simple des équations Diophantiennes en deux variables : on fixe deux entiers a et b et on cherche à résoudre l'équation $ax + by = 0$ où les inconnues x, y sont dans $\mathbf{Z}$. Si on note d le pgcd de a et b, et $a' = a/d$, $b' = b/d$, alors la solution générale est $(x,y) = (tb', -ta')$, $t \in \mathbf{Z}$. Cet exemple élémentaire se généralise aisément aux systèmes de m équations en n inconnues : on se donne une matrice de format $m \times n$ à coefficients entiers et on cherche les vecteurs colonnes $X = {}^t(x_1,\dots,x_n)$ à coefficients dans $\mathbf{Z}$ qui satisfont $AX = 0$. L'algèbre linéaire permet de résoudre la question.

Si maintenant on se donne, en plus, un vecteur colonne B (matrice $m \times 1$) et que l'on veut résoudre $AX = B$, pour en obtenir la solution générale il suffit d'ajouter à une solution particulière de cette équation la solution générale de l'équation homogène associée $AX = 0$.

Revenant au cas particulier d'une équation en deux inconnues ($m=1$, $n=2$), pour résoudre l'équation de Bézout $ax + by = c$ on utilise l'algorithme d'Euclide : cette équation a une solution $(x,y) \in \mathbf{Z} \times \mathbf{Z}$ si et seulement si le pgcd de a et b divise c.

Passons aux équations quadratiques. La plus célèbre est sans doute celle de Pythagore (VIème siècle avant J.-C) : $x^2 + y^2 = z^2$. Comme elle est homogène, la résoudre en nombres entiers revient à résoudre en nombres rationnels l'équation $x^2 + y^2 = 1$, c'est-à-dire à déterminer les

points rationnels sur un cercle. La méthode géométrique, qui permet plus généralement de trouver les points rationnels sur une conique (c'est-à-dire de résoudre en nombres rationnels une équation $f(x,y)=0$ où f est un polynôme en deux variables de degré 2), consiste à tracer une droite passant par un point rationnel : elle coupe la courbe en question en un autre point et cela fournit une paramétrisation des solutions. Pour le cercle on peut partir par exemple du point $(x,y)=(-1,0)$ et considérer la droite $y=t(x+1)$ de pente $t\in\mathbf{Q}$. Le second point d'intersection est obtenu en résolvant l'équation

$$x^2+t^2(x+1)^2-1=0$$

qui possède bien entendu la solution $x=-1$. On peut donc mettre $x+1$ en facteur dans le membre de gauche : si $x\neq -1$ alors on peut diviser par $x+1$ et l'équation devient linéaire

$$x-1+t^2(x+1)=0,$$

ce qui donne

$$x=\frac{1-t^2}{1+t^2},\quad y=\frac{2t}{1+t^2}.$$

Pour chaque $t\in\mathbf{Q}$ ces formules donnent un point rationnel (x,y) sur le cercle, et inversement tout point rationnel sur le cercle distinct de $(-1,0)$ est de cette forme. On retrouve le point exceptionnel $(-1,0)$ en autorisant $t=+\infty$, c'est-à-dire en passant en coordonnées projectives. En écrivant $t=a/b$ on retrouve les formules

$$x=\frac{b^2-a^2}{b^2+a^2},\quad y=\frac{2ab}{b^2+a^2}$$

qui conduisent à la solution générale en nombres entiers de l'équation de Pythagore $x^2+y^2=z^2$. On remarque d'abord que si x, y, z sont des entiers positifs qui satisfont $x^2+y^2=z^2$, et si d est leur pgcd, alors le triplet (x',y',z') défini par $x'=x/d$, $y'=y/d$, $z'=z/d$ satisfait encore l'équation de Pythagore, et en plus ces trois entiers x', y', z' sont premiers entre eux dans leur ensemble (ils sont même premiers entre eux deux-à-deux). De plus z' est impair. On en déduit facilement que l'un des deux nombres x', y' est pair, l'autre bien entendu est impair. Voici l'énoncé auquel on aboutit (voir par exemple [3], § 1.2, Th.1 ou [2], Th. 5.9).

Théorème 0.1. *Si x, y, z sont des entiers positifs premiers entre eux dans leur ensemble avec y pair qui vérifient l'équation de Pythagore $x^2+y^2=z^2$, alors il existe des entiers a et b premiers entre eux tels que*

$$x=b^2-a^2,\quad y=2ab,\quad z=b^2+a^2.$$

Le procédé géométrique de la corde et de la tangente que nous venons de voir est utile aussi pour les équations cubiques : si on dispose d'un point rationnel sur une courbe $f(x,y)=0$ où f est un polynôme de degré 3, la tangente à la courbe en ce point coupe généralement la cubique en un autre point, si le premier est rationnel alors le second l'est aussi (on est amené à résoudre une équation de degré 3 en x, qui a une racine double, donc se décompose en un produit d'un terme linéaire au carré par un autre terme linéaire). De même si on dispose de deux points rationnels sur la courbe, la droite joignant ces deux points coupe généralement la cubique en un autre point rationnel. C'est la base de la théorie des courbes elliptiques.

Le processus géométrique permet de paramétrer les solutions rationnelles d'une équation de degré 2 en 2 inconnues. Il ne donne pas forcément d'information sur les solutions entières. Par

exemple si d est un entier qui n'est pas un carré, les points rationnels $\neq (0,0)$ sur la courbe $x^2 - dy^2 = 1$ sont paramétrés par

$$x = \frac{dt^2+1}{dt^2-1}, \quad y = \frac{2t}{dt^2-1}.$$

Quand d est un entier positif qui n'est pas un carré, l'équation $x^2 - dy^2 = \pm 1$, où les inconnues x et y sont dans $\mathbf{Z}$, porte le nom de Pell–Fermat. Pourtant elles ont été étudiées par le mathématicien indien Brahmagupta (598–670) bien avant Pell (1611–1685) et Fermat. Il a trouvé la plus petite solution en entiers positifs de l'équation $x^2 - 92y^2 = 1$, qui est $(x, y) = (1151\ ,\ 120)$. On peut noter que l'équation $x^2 - 23y^2$ possède la solution $(x, y) = (24, 5)$, puisque $24^2 = 576$ et $5^2 \cdot 23 = 575$. En développant $(24 + 5\sqrt{23})^2 = 1151 + 120\sqrt{23}$ on retrouve la solution donnée par Brahmagupta.

Au XIIème siècle Bhaskara II a trouvé pour l'équation $x^2 - 61y^2 = 1$ (qui sera plus tard considérée par Fermat) la solution

$$(x, y) = (1\,766\,319\,049\ ,\ 226\,153\,980).$$

Plus tard Narayana (∼1340–∼1400) a obtenu pour $x^2 - 103y^2 = 1$ la solution $(x, y) = (227\,528\ ,\ 22\,419)$.

Un algorithme pour résoudre une équation de Pell–Fermat consiste à développer $\sqrt{d}$ en *fraction continue* (voir par exemple [2] Chap. 3 et 4). La résolution de l'équation $x^2 - dy^2 = \pm 1$ est étroitement liée à la recherche des *unités* du corps quadratique $\mathbf{Q}(\sqrt{d})$. Nous allons voir de quoi il s'agit (l'algèbre classique enseigne que les unités d'un corps sont les éléments non nuls du corps, mais en théorie algébrique des nombres ce que l'on appelle *unité d'un corps de nombres* est autre chose).

Quelques rappels

Consulter [3] (§ 1.1) et [2] (notamment le chapitre 5) pour revoir les notions de base sur la divisibilité dans les anneaux (on les suppose toujours commutatifs unitaires), sur les unités (= éléments inversibles), les éléments irréductibles, les éléments premiers (dans un anneau intègre tout premier est irréductible), les idéaux, ainsi que les notions d'anneau principal, factoriel et euclidien.

1 Extensions Algébriques

Tous les corps sont supposés commutatifs.

Quand K est un corps, l'intersection de tous les sous-corps de K est un sous-corps de K, c'est le plus petit d'entre eux, on l'appelle le *sous-corps premier de* K. Ce sous-corps est isomorphe (de manière unique) soit à $\mathbf{Q}$, soit à un corps $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ avec p nombre premier. On dit que K est de caractéristique 0 dans le premier cas, p dans le second.

1.1 Extensions de corps

Soient L un corps et K un sous-corps de L. On dit alors que L est une *extension* de K. On écrit aussi une telle extension L/K. Dans ces conditions L est un K-espace vectoriel. On dit que

l'extension est *finie* si le K-espace vectoriel L est de dimension finie sur K. Cette dimension est notée $[L : K]$ et appelée le *degré* de l'extension L/K.

Quand L/K est une extension et E une partie de L, on note $K[E]$ le sous-anneau de L engendré par $K \cup E$ et par $K(E)$ le sous-corps de L engendré par $K \cup E$. Ainsi $K(E)$ est le corps des fractions de $K[E]$, c'est l'intersection des sous-corps de L qui contiennent E et K, on l'appelle *sous-corps de L engendré par E sur K*. C'est encore l'ensemble des éléments de L de la forme $R(\alpha_1, \ldots, \alpha_n)$ quand $\{\alpha_1, \ldots, \alpha_n\}$ décrit les familles finies d'éléments de E et R l'ensemble des fractions rationnelles dans $K(X_1, \ldots, X_n)$ dont le dénominateur ne s'annule pas au point $(\alpha_1, \ldots, \alpha_n)$.

On écrit encore $K(E, E')$ au lieu de $K(E \cup E')$ et $K(\alpha)$ au lieu de $K(\{\alpha\})$. Une extension L/K est *de type fini* s'il existe un ensemble fini E tel que $L = K(E)$. Elle est *monogène* s'il existe $\alpha \in L$ tel que $L = K(\alpha)$; dans ce cas α est un *générateur* de l'extension L/K.

Lemme 1.1. *Soient $K \subset L \subset F$ trois corps. L'extension F/K est finie si et seulement si les deux extensions L/K et F/L sont finies. Dans ce cas*

$$[F : K] = [F : L][L : K].$$

Démonstration. Si $\{\alpha_i \ ; \ i \in I\}$ est une base de L/K et $\{\beta_j \ ; \ j \in J\}$ est une base de F/L, alors $\{\alpha_i \beta_j \ ; \ (i, j) \in I \times J\}$ est une base de F/K.

□

Avec les notations du lemme 1.1, on a les équivalences

$$[L : K] = 1 \Longleftrightarrow [F : L] = [F : K] \Longleftrightarrow L = K$$

et

$$[F : L] = 1 \Longleftrightarrow [L : K] = [F : K] \Longleftrightarrow L = F.$$

1.2 Extensions algébriques et extensions transcendantes

Soient A un anneau, K un sous-corps de A et α un élément de A. Considérons l'homomorphisme de K-algèbres $\Phi : K[X] \to A$ qui envoie X sur α. Son image $K[\alpha]$ est le sous anneau de A engendré par $K \cup \{\alpha\}$, son noyau $\ker \Phi$ est un idéal de $K[X]$. Les deux anneaux $K[X]/\ker \Phi$ et $K[\alpha]$ sont isomorphes.

Si $\ker \Phi = \{0\}$, c'est-à-dire si Φ est injectif, on dit que α est *transcendant* sur K. Alors les anneaux $K[X]$ et $K[\alpha]$ sont isomorphes et le corps des fractions $K(\alpha)$ de $K[\alpha]$ est isomorphe au corps des fractions rationnelles $K(X)$.

Supposons $\ker \Phi \neq \{0\}$. On dit alors que α est *algébrique* sur K. Comme l'anneau $K[X]$ est principal, il existe un unique polynôme unitaire $f \in K[X]$ qui engendre l'idéal $\ker \Phi$. C'est le polynôme de degré *minimal* qui s'annule en α : on l'appelle le *polynôme minimal de α sur K*. Si $K[\alpha]$ est intègre (ce qui est le cas par exemple quand A lui-même est intègre), alors le polynôme minimal f de α sur K est irréductible dans l'anneau $K[X]$; on dit encore que f est *le polynôme irréductible de α sur K*. L'idéal $\ker \Phi$ est alors maximal, le quotient $K[X]/\ker \Phi$ est un corps, donc $K[\alpha] = K(\alpha)$. L'extension $K(\alpha)/K$ est finie, de degré $[K(\alpha) : K]$ le degré du polynôme f, qu'on appelle encore le *degré* de α sur K. Une base de $K(\alpha)$ comme K-espace vectoriel est $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$.

Une extension L/K est dite *algébrique* si tout élément de L est algébrique sur K. Dans le cas contraire on dit qu'elle est *transcendante*.

Lemme 1.2. *Si L/K est une extension finie, alors c'est une extension algébrique et, pour tout $\alpha \in L$, le degré $[K(\alpha) : K]$ de α sur K divise le degré $[L : K]$ de L sur K.*

Démonstration. L'extension L/K étant finie, pour tout $\alpha \in L$ les éléments

$$1, \alpha, \alpha^2, \ldots, \alpha^n, \ldots$$

sont liés dans le K-espace vectoriel L, donc α est algébrique sur K. Comme $K(\alpha)$ est un sous-corps de L contenant K, son degré $[K(\alpha) : K]$ sur K divise $[L : K]$, d'après le lemme 1.1.

□

Lemme 1.3. *Soit L/K une extension et soient $\alpha_1, \ldots, \alpha_m$ des éléments de L qui sont algébriques sur K. Alors $K(\alpha_1, \ldots, \alpha_m)$ est une extension finie de K.*

Démonstration. On peut démontrer ce résultat par récurrence sur m. Pour $m = 1$ l'extension $K(\alpha_1)/K$ est finie car α_1 est algébrique sur K. Comme α_m est algébrique sur K, il l'est sur le corps $K(\alpha_1, \ldots, \alpha_{m-1})$ et le lemme 1.1 joint à l'hypothèse de récurence permet de conclure. □

Il est évident qu'une extension finie est de type fini et, d'après le lemme 1.2, elle est aussi algébrique ; le lemme 1.3 montre que, réciproquement, une extension algébrique de type fini est finie.

Lemme 1.4. *Soient $K \subset L \subset E$ trois corps. L'extension E/K est algébrique si et seulement si les deux extensions L/K et E/L sont algébriques.*

Démonstration. Si l'extension E/K algébrique, il est clair que chacune des deux extensions L/K et E/L est algébrique. Inversement, supposons les deux extensions L/K et E/L algébriques. Soit $\alpha \in E$. Comme E est algébrique sur L, il existe un polynôme non nul de $L[X]$ qui s'annule en α. Soient $a_0, \ldots, a_m$ ses cœfficients ; chacun d'eux est un élément de L, donc est algébrique sur K. Maintenant α est algébrique sur $K(a_0, \ldots, a_m)$. Le lemme 1.1 montre que l'extension $K(a_0, \ldots, a_m, \alpha)/K$ est finie, donc (lemme 1.2) algébrique et ainsi α est algébrique sur K.

□

Lemme 1.5. *Soit L/K une extension et soit A une partie de L. On suppose que tous les éléments de A sont algébriques sur K. Alors $K(A)$ est une extension algébrique de K et on a $K[A] = K(A)$.*

Démonstration. Soit $\beta \in K(A)$. Il existe une partie finie $\{\alpha_1, \ldots, \alpha_m\}$ de A telle que $\beta \in K(\alpha_1, \ldots, \alpha_m)$. Le lemme 1.4 montre que β est algébrique sur K. Il reste à vérifier que $K[A]$ est un corps. Soit $\gamma \in K[A]$, $\gamma \neq 0$. Alors $K[\gamma] \subset K[A]$ et comme γ est algébrique sur K on a $K(\gamma) = K[\gamma]$, d'où $\gamma^{-1} \in K[A]$.

□

Soient E et F deux sous-corps d'un corps Ω. L'intersection de tous les sous-corps de Ω qui contiennent $E \cup F$ est le plus petit sous-corps de Ω qui contienne E et F, c'est à la fois $E(F)$ et $F(E)$. On le note EF et on l'appelle *le composé* (ou *compositum*) de E et F.

Quand K est un sous corps de $E \cap F$, on a $EF = K(E, F)$; de plus l'extension EF/K est finie (resp. algébrique) si et seulement si les deux extensions E/K et F/K sont finies (resp. algébriques).

Lemme 1.6. *Soient L/K une extension de corps, E et F deux sous-corps de L qui contiennent K. Si l'extension F/K est algébrique, alors l'extension EF/E est aussi algébrique.*

Démonstration. Soit $\alpha \in F$. Par hypothèse α est algébrique sur K, donc sur E. Le lemme 1.5 montre que $E[F] = E(F)$ et que l'extension $E(F)/E$ est algébrique. □

Soit L/K une extension de corps. On dit que K est *algébriquement fermé* dans L si tout élément de L algébrique sur K appartient à K.

Exemple. On peut montrer que le corps $\mathbf{C}(z)$ des fractions rationnelles est algébriquement fermé dans le corps des fonctions méromorphes sur $\mathbf{C}$.

Lemme 1.7. *Soit L/K une extension. L'ensemble E des éléments de L algébriques sur K est un corps, algébriquement fermé dans L.*

Ce corps E, qui est la plus grande extension algébrique de K contenue dans L, est la *fermeture algébrique de K dans L*. C'est aussi la plus petite extension de K contenue dans L qui soit algébriquement fermée dans L.

On désignera par $\overline{\mathbf{Q}}$ l'ensemble des nombres complexes algébriques sur $\mathbf{Q}$; c'est le *corps des nombres algébriques*. La fermeture algébrique de $\mathbf{Q}$ dans $\mathbf{R}$ est le corps $\overline{\mathbf{Q}} \cap \mathbf{R}$ des nombres algébriques réels.

Un corps Ω est dit *algébriquement clos* s'il vérifie les propriétés équivalentes suivantes :
(i) tout polynôme non constant de $\Omega[X]$ a au moins une racine dans Ω
(ii) tout polynôme non constant de $\Omega[X]$ se décompose complètement dans $\Omega[X]$
(iii) les éléments irréductibles de l'anneau $\Omega[X]$ sont les polynômes de degré 1.

Un corps algébriquement clos est algébriquement fermé dans toute extension.

Si K est un corps, une extension Ω de K est appelée *clôture algébrique de K* si Ω est un corps algébriquement clos et Ω/K est une extension algébrique.

Quand Ω est un corps algébriquement clos et K un sous-corps de Ω, la fermeture algébrique de K dans Ω est une clôture algébrique de K.

Exemple. Le corps $\mathbf{C}$ est algébriquement clos et $\overline{\mathbf{Q}}$ est une clôture algébrique de $\mathbf{Q}$.

Nous admettrons l'existence, pour tout corps K, d'un corps Ω algébriquement clos contenant K.

Théorème 1.8. *Tout corps K admet une clôture algébrique.*

Démonstration. Soit Ω un corps algébriquement clos contenant K. Soit $\overline{K}$ la fermeture algébrique de K dans Ω. Alors $\overline{K}$ est une clôture algébrique de K. □

Remarque. On peut aussi montrer que si $\overline{K}_1$ et $\overline{K}_2$ sont deux clôtures algébriques de K, alors il existe un isomorphisme de $\overline{K}_1$ sur $\overline{K}_2$ dont la restriction à K est l'identité.

Étant donné que tout homomorphisme d'un corps dans un anneau est injectif, se donner une extension revient à se donner un homomorphisme d'un corps dans un autre. Plus précisément, si $\sigma : K \to L$ est un homomorphisme de corps, alors le corps $\sigma(K)$ est isomorphe à K et L est une extension de $\sigma(K)$. Dans ces conditions on dit que σ est un isomorphisme de K *dans* L. On étend σ en l'unique homomorphisme (encore noté σ) de $K[X]$ dans $L[X]$ qui envoie X sur X et coïncide avec σ sur K :

$$\sigma\big(a_0 + a_1X + \cdots + a_nX^n\big) = \sigma(a_0) + \sigma(a_1)X + \cdots + \sigma(a_n)X^n.$$

Soient E et L deux extensions d'un même corps K et soit $\sigma : E \to L$ un isomorphisme de E dans L. On dit que σ est un *K-isomorphisme* si la restriction de σ à K est l'identité.

Si E_1 et E_2 sont deux corps entre lesquels il existe un homomorphisme de corps $\sigma : E_1 \to E_2$, alors E_1 et E_2 ont la même caractéristique et le même sous-corps premier F (plus précisément, il y a un isomorphisme unique entre leurs sous-corps premiers, ce qui nous autorise à les identifier). Dans ce cas σ est un F-isomorphisme de E_1 dans E_2.

Soit L/K une extension. Deux éléments α et β de L sont dits *conjugués* sur K s'il existe un K-isomorphisme σ de $K(\alpha)$ dans $K(\beta)$ tel que $\sigma(\alpha) = \beta$. Dans ce cas σ est unique et surjectif. La conjugaison définit une relation d'équivalence sur L.

Lemme 1.9. *Soient L/K une extension et α, β deux éléments de L. Si α est transcendant sur K, alors β est conjugué de α sur K si et seulement si β est aussi transcendant. Si α est algébrique sur K, alors β est conjugué de α si et seulement si β est algébrique sur K avec le même polynôme irréductible que α sur K.*

Démonstration. Si α est transcendant sur K, alors $K(\alpha)$ est isomorphe au corps $K(X)$ des fractions rationnelles sur X, donc à tout $K(\beta)$ avec β transcendant sur K. Dans ces conditions, comme $K(\alpha)$ n'est pas de degré fini sur K, il ne peut pas être isomorphe à $K(\beta)$ quand β est algébrique sur K.

Supposons maintenant α et β algébriques sur K et conjugués. Soit $\sigma : K(\alpha) \to K(\beta)$ un K-isomorphisme tel que $\sigma(\alpha) = \beta$. Notons $f \in K[X]$ le polynôme irréductible de α sur K. On a $f(\alpha) = 0$, donc $\sigma\big(f(\alpha)\big) = 0$. Mais, comme la restriction à K de σ est l'identité et que les coefficients de f sont dans K, on a

$$\sigma\big(f(\alpha)\big) = f\big(\sigma(\alpha)\big) = f(\beta).$$

Donc β est racine de f.

Enfin si α et β sont algébriques racines du même polynôme irréductible $f \in K[X]$, alors $K(\alpha)$ et $K(\beta)$ sont tous deux isomorphes au corps $K[X]/(f)$. En effet le morphisme d'anneaux $K[X] \to K[\alpha]$ qui envoie X sur α et laisse fixe les éléments de K a pour image $K[\alpha] = K(\alpha)$ et pour noyau l'idéal (f) de $K[X]$. L'isomorphisme de corps de de $K(\alpha)$ sur $K(\beta)$ qui rend commutatif le diagramme

$$\begin{array}{ccc} K[X] & \to & K[\beta] \\ \downarrow & \nearrow_{\sigma} & \\ K[\alpha] & & \end{array}$$

n'est autre que l'application K-linéaire σ de $K(\alpha)$ dans $K(\beta)$ définie sur la base $\{1, \alpha, \ldots, \alpha^{n-1}\}$ (où n désigne le degré de α) par $\sigma(\alpha^i) = \beta^i$ $(0 \leq i \leq n-1)$. □

1.3 Corps de rupture d'un polynôme

Soient K un corps et $f \in K[X]$ un polynôme irréductible. Une extension L/K est un *corps de rupture de f sur K* s'il existe une racine α de f dans L telle que $L = K(\alpha)$.

Exemple. Si 1, j et j^2 désignent les trois racines cubiques de l'unité dans $\mathbf{C}$, chacun des trois corps $\mathbf{Q}(\sqrt[3]{2})$, $\mathbf{Q}(j\sqrt[3]{2})$ et $\mathbf{Q}(j^2\sqrt[3]{2})$ est un corps de rupture sur $\mathbf{Q}$ du polynôme $X^3 - 2$.

L'existence d'un corps de rupture est donnée par le lemme suivant :

Lemme 1.10. *Soient K un corps et f un polynôme irréductible de $K[X]$. L'idéal principal (f) de $K[X]$ est maximal, le quotient $L = K[X]/(f)$ contient (un sous-corps isomorphe à) K et L est un corps de rupture de f sur K.*

Démonstration. Soit j l'injection naturelle de K dans $K[X]$ et soit $s : K[X] \to K/(f)$ la surjection canonique de noyau l'idéal (f) engendré par f. Alors $\sigma = s \circ j$ est un isomorphisme de K dans L. Soit $\alpha \in L$ la classe de X modulo f et soit $g = \sigma(f) \in \sigma(K)[X]$. On a

$$g(\alpha) = s(f) = 0.$$

Ainsi on voit que L est un corps de rupture sur $\sigma(K)$ du polynôme $g = \sigma(f)$. Comme $\sigma(K)$ est un corps isomorphe à K on peut l'identifier avec K et alors $g = f$. □

Un corps de rupture est unique à isomorphisme près :

Lemme 1.11. *Soient K un corps, f un polynôme irréductible de $K[X]$, $\varphi : K \to K'$ un isomorphisme de K sur un corps K', L un corps de rupture de f sur K, α une racine de f dans L, L' un corps de rupture de φf sur K' et α' une racine de φf dans L'. Alors il existe un unique isomorphisme ψ de L sur L' dont la restriction à K soit φ et tel que $\psi(\alpha) = \alpha'$.*

Démonstration. Comme $L = K(\alpha)$ et $L' = K(\alpha')$, l'unicité de ψ est claire. Pour l'existence, on reprend l'argument de la démonstration du lemme 1.9.

□

1.4 Corps de décomposition d'un polynôme

Comme nous venons de le voir dans le §1.3, un corps de rupture d'un polynôme f irréductible sur un corps K est une extension de K qui contient au moins une racine de f (et qui est minimale pour cette propriété). Nous recherchons maintenant une extension qui contienne toutes les racines de f - il n'est alors plus nécessaire de supposer f irréductible pour étudier la question.

Soient K un corps et f un polynôme non constant de $K[X]$. Quand L est une extension de K, on dit que le polynôme f est *complètement décomposé* dans L si f est produit de facteurs linéaires de $L[X]$. On dit que L est un *corps de décomposition de f sur K* si f est complètement décomposé dans L et s'il existe des racines $\alpha_1, \ldots, \alpha_m$ de f dans L telles que $L = K(\alpha_1, \ldots, \alpha_m)$. Ainsi, f est complètement décomposé dans une extension L de K si et seulement si on peut écrire

$$f(X) = a_0(X - \alpha_1) \cdots (X - \alpha_d)$$

avec $\alpha_1, \ldots, \alpha_d$ dans L (ici d est le degré de f et $a_0 \in K$ est le coefficient directeur de f). Alors *le* corps de décomposition de f dans L est $K(\alpha_1, \ldots, \alpha_d)$.

L'énoncé suivant assure l'existence d'un corps de décomposition.

Lemme 1.12. *Soient K un corps et f un polynôme non constant de $K[X]$. Alors il existe un corps de décomposition L de f sur K.*

Démonstration. On démontre le résultat par récurrence sur le degré d de f. Si $d = 1$ on prend $L = K$. Supposons le résultat vrai pour tous les corps et pour les polynômes de degré $< d$. Soit g un facteur irréductible de f, soit E un corps de rupture sur K de g et soit $\alpha \in E$ une racine de g dans E telle que $E = K(\alpha)$. Alors dans $E[X]$ on a $f(X) = (X - \alpha)h(X)$ avec h de degré $d-1$. Il suffit maintenant de prendre pour L un corps de décomposition de $h(X)$ sur E en utilisant l'hypothèse de récurrence. □

Voici maintenant l'unicité :

Lemme 1.13. *Soient K un corps, f un polynôme non constant de $K[X]$, $\varphi : K \to K'$ un isomorphisme de K sur un corps K', L un corps de décomposition de f sur K et L' un corps de décomposition de φf sur K'. Alors il existe un isomorphisme ψ de L sur L' dont la restriction à K soit φ.*

Démonstration. On va démontrer le résultat par récurrence sur le degré d de f, le cas $d = 1$ étant banal. Supposons le résultat vrai pour tous les corps et tous les polynômes de degré $< d$. Soient g un facteur irréductible de f dans $K[X]$, α une racine de g dans L, α' une racine de $\varphi \circ g$ dans L'. Le lemme 1.11 montre qu'il existe un isomorphisme θ de $K(\alpha)$ sur $K(\alpha')$ qui envoie α sur α' et dont la restriction à K soit φ. On remarque que L est un corps de décomposition sur $K(\alpha)$ du polynôme $h(X) = f(X)/(X - \alpha)$ et L' est un corps de décomposition sur $K'(\alpha')$ du polynôme $\theta\big(h(X)\big) = \varphi\big(f(X)\big)/(X - \alpha')$. L'hypothèse de récurrence permet de conclure.

□

L'isomorphisme ψ qui étend φ n'est en général pas unique. Si on en choisit un, on obtient tous les autres en le composant avec un K-automorphisme de L. Un tel automorphisme est déterminé par son action sur les racines de f, qui est une permutation. La théorie de Galois a pour but d'étudier ces permutations.

Nous allons voir maintenant qu'un corps de décomposition contenu dans une extension E de K est stable sous tout K-automorphisme de E :

Lemme 1.14. *Soit L un corps de décomposition d'un polynôme de $K[X]$, soit E une extension de L et soit σ un K-isomorphisme de L dans E. Alors $\sigma(L) = L$.*

Démonstration. Soient $\alpha_1, \ldots, \alpha_d$ les racines dans L du polynôme considéré. On a $L = K(\alpha_1, \ldots, \alpha_d)$ et σ permute les α_i, donc $\sigma(L) = K(\alpha_1, \ldots, \alpha_d) = L$.

□

Références

[1] H. Cohen – *Démonstration de la conjecture de Catalan*, http ://www.math.polytechnique.fr/xups/xups05-01.pdf

[2] D. Duverney – *Théorie des nombres : cours et exercices corrigés*, Paris : Dunod. viii, 244 p., 1998.

[3] P. Samuel – *Théorie algébrique des nombres*, Hermann, Paris, 1967.

De nombreux documents sont disponibles sur internet. Voir notamment la liste disponible sur la page `Online number theory lecture notes`
http ://www.numbertheory.org/ntw/lecture_notes.html
du site du `réseau de théorie des nombres`
http ://www.numbertheory.org/ntw/web.html

Université P. et M. Curie (Paris VI),
Deuxième semestre 2006/2007

Michel Waldschmidt
date de mise à jour: 24/04/2007

Master de sciences et technologies 1ère année -
Spécialité : Mathématiques Fondamentales

Mention : Mathématiques et applications
MO11 : Théorie des nombres (12 ECTS)

Première partie: Théorie des Corps

Fascicule 2 : sections 1.5 à 1.8 (10 pages) [1]

1.5 Extensions normales

Une extension L/K est dite *normale* si elle est algébrique et si tout polynôme irréductible de $K[X]$ ayant une racine dans L est complètement décomposé dans L.

Théorème 1.15. *Une extension finie L/K est normale si et seulement s'il existe un polynôme non constant f tel que L soit le corps de décomposition de f sur K.*

Démonstration. Supposons dans un premier temps que L est le corps de décomposition sur K du polynôme $f \in K[X]$. Soit $\beta \in L$, soit g le polynôme irréductible de β sur K, soit E un corps de décomposition sur L de g et soit β' une racine de g dans E. Il s'agit de vérifier que β' est dans L. Comme $K(\beta)$ et $K(\beta')$ sont deux corps de rupture sur K du polynôme g, il existe un K-isomorphisme de $K(\beta)$ sur $K(\beta')$ qui envoie β sur β'. Le corps de décomposition sur $K(\beta)$ de f est L et le corps de décomposition sur $K(\beta')$ de f est $L(\beta')$. D'après le lemme 1.13 il existe un isomorphisme ψ de L sur $L(\beta')$ dont la restriction à $K(\beta)$ est σ. Le lemme 1.14 implique $\psi(L) = L$, donc $L(\beta') = L$ et $\beta' \in L$.

Inversement supposons l'extension L/K finie et normale. Comme L/K est une extension de type fini il existe des éléments $\alpha_1, \ldots, \alpha_m$ de L tels que $L = K(\alpha_1, \ldots, \alpha_m)$. Pour $1 \leq i \leq m$ soit f_i le polynôme irréductible de α_i sur K et soit $f = f_1 \cdots f_m$. Toute racine de f_i est un conjugué de α_i, donc est dans L. Ainsi L est le corps de décomposition de f sur K.

□

Remarque. Si une extension L/K est normale et si E est un corps intermédiaire, $K \subset E \subset L$, alors l'extension L/E est encore normale.

Quand E/K est une extension finie, il existe une extension finie L/E telle que l'extension L/K soit normale : il suffit d'écrire $E = K(\alpha_1, \ldots, \alpha_m)$ et de prendre pour L un corps de décomposition de $f_1 \cdots f_m$ sur K, où f_i est le polynôme irréductible de α_i sur K. Si Ω est un corps algébriquement clos qui contient E, on définit la *clôture normale de l'extension E/K dans Ω* comme l'intersection (= le plus petit) des sous-corps L de Ω contenant E tels que l'extension L/K soit normale.

De même quand $E_1, \ldots, E_n$ sont des extensions finies de K, il existe une extension normale N de K et des isomorphismes de chacun des E_i dans N.

[1] Ce texte est téléchargeable à partir de la page http ://www.math.jussieu.fr/∼miw/enseignement.html

Proposition 1.16. *Soient $K \subset E \subset N$ trois corps. On suppose l'extension N/K finie et normale. Soit σ un K-isomorphisme de E dans N. Alors il existe un K-automorphisme τ de N dont la restriction à E est σ.*

Démonstration. D'après le théorème 1.15 il existe un polynôme $f \in K[X]$ dont le corps de décomposition sur K est N. Alors N est encore un corps de décomposition de f sur E et sur $\sigma(E)$. Comme $\sigma(f) = f$ le lemme 1.13 montre qu'il existe un isomorphisme de N sur N dont la restriction à E est σ.

□

Un tel automorphisme τ en général n'est pas unique.

La proposition 1.16 permet de donner une caractérisation des extensions normales :

Corollaire 1.17. *Soit L/K une extension finie. Alors L/K est normale si et seulement si, pour toute extension F de L et tout K-isomorphisme σ de L dans F, on a $\sigma(L) = L$.*

Démonstration. La condition est nécessaire pour que l'extension L/K soit normale : cela résulte du lemme 1.14 et du théorème 1.15.

Inversement, si cette condition est vérifiée, soit $\alpha \in L$, soit N une extension normale de K contenant L et soit $\beta \in N$ un conjugué de α sur K. Les corps $K(\alpha)$ et $K(\beta)$ sont K-isomorphes, donc (proposition 1.16) il existe un K-automorphisme de N qui envoie α sur β. Soit σ la restriction de cet automorphisme à L. On a $\sigma(\alpha) = \beta$, $\sigma(L) = L$ et $\alpha \in L$. Donc $\beta \in L$.

□

1.6 Extensions séparables

Soient K un corps, $f \in K[X]$ un polynôme non constant et α une racine de f dans K. Alors $f(X)$ est divisible par $X - \alpha$ dans $K[X]$: il existe $q \in K[X]$ tel que $f(X) = (X - \alpha)q(X)$. On dit que α est *racine simple* de f si $q(\alpha) \neq 0$; autrement on dit que α est *racine multiple* de f. Ainsi pour $f \in K[X]$ et $\alpha \in K$, les conditions suivantes sont équivalentes :
(i) α est racine multiple de f
(ii) $f(X)$ est divisible par $(X - \alpha)^2$
(iii) $f(\alpha) = f'(\alpha) = 0$.

On a noté f' la dérivée du polynôme f :

$$\text{pour} \quad f(X) = \sum_{i=0}^{n} a_i X^i, \quad \text{on a} \quad f'(X) = \sum_{i=1}^{n} i a_i X^{i-1}.$$

Pour un polynôme $f \in K[X]$ de degré ≥ 1 les conditions suivantes sont équivalentes :
(i) Les facteurs irréductibles de f dans l'anneau factoriel $K[X]$ apparaissent tous avec la multiplicité 1
(ii) Si g est un polynôme non constant, alors $f(X)$ n'est pas divisible par g^2
(iii) $\text{pgcd}(f, f') = 1$.

Si un polynôme n'a pas de racines multiples dans un corps de décomposition, alors dans une extension quelconque de K il n'a pas des racines multiples.

Quand K est un corps et $f \in K[X]$ un polynôme irréductible, on dit que f est *séparable* si les racines de f dans un corps de décomposition sont toutes simples. Un polynôme de $K[X]$ est dit *séparable* si tous ses facteurs irréductibles le sont. Sinon il est dit *inséparable*.

Soit L/K une extension algébrique. Un élément α de L est dit *séparable* sur K si son polynôme irréductible sur K est séparable sur K. L'extension L/K est dite *séparable* si elle est algébrique et si tout élément de L est séparable sur K. Un élément algébrique ou une extension algébrique est dite *inséparable* si elle n'est pas séparable.

Lemme 1.18. *Soient K un corps et $f \in K[X]$ un polynôme irréductible. Alors les conditions suivantes sont équivalentes :*
(i) f est séparable sur K
(ii) $f' \neq 0$.

Un corps K est *parfait* si toutes ses extensions algébriques sont séparables, c'est-à-dire si tout polynôme de $K[X]$ est séparable. Il résulte du lemme 1.18 que tout corps de caractéristique nulle est parfait.

Démonstration du lemme 1.18. Si $f' = 0$ alors toute racine de f dans un corps de décomposition est multiple, donc f n'est pas séparable.

Réciproquement si f n'est pas séparable choisissons une racine multiple α de f dans un corps de décomposition de f sur K. Alors f est le polynôme irréductible de α sur K. Comme $f'(\alpha) = 0$ le polynôme f' est multiple de f et, comme il est de degré inférieur à celui de f, il est nul.

□

On en déduit que dans un corps de caractéristique nulle tout polynôme est séparable. En caractéristique finie p, un polynôme irréductible

$$f(X) = \sum_{i=0}^{n} a_i X^i,$$

est inséparable si et seulement si $ia_i = 0$ pour tout $i = 0, \ldots, n$, donc si et seulement si $a_i = 0$ pour tout i premier à p. Cela s'écrit encore : il existe $g \in K[X]$ tel que $f(X) = g(X^p)$.

Exemple. Sur $K = \mathbf{F}_p(T)$ le polynôme $X^p - T \in K[X]$ est irréductible et inséparable.

Théorème 1.19. *Soient $k \subset K \subset N$ trois corps. On suppose l'extension N/k finie et normale et l'extension K/k séparable. On pose $d = [K : k]$. Alors il existe d k-isomorphismes de K dans N.*

La démonstration se fait par récurrence grâce au lemme suivant, où on utilise la notation que voici : quand k est un corps et E, F deux extensions de K, $H(k; E, F)$ désigne l'ensemble des k isomorphismes de E dans F.

Lemme 1.20. *Soient $k \subset L \subset K \subset N$ quatre corps, avec N/k finie normale. Il existe une bijection entre l'ensemble $H(k, K, N)$ et le produit cartésien $H(k, L, N) \times H(L, K, N)$.*

Démonstration du lemme 1.20. Pour chaque $\sigma \in H(k, L, N)$ choisissons un prolongement de σ en un automorphisme $\overline{\sigma}$ de N (proposition 1.16). La bijection recherchée est obtenue en associant à $\varphi \in H(k, K, N)$ le couple (σ, ψ), où $\sigma \in H(k, L, N)$ est la restriction de φ à L et $\psi = \overline{\sigma}^{-1} \circ \varphi \in H(L, K, N)$.

□

Démonstration du Théorème 1.19. Si l'extension K/k est monogène on écrit $K = k(x)$ avec $x \in K$; il y a d conjugués $x_1, \ldots, x_d$ de x dans N et les d isomorphismes cherchés sont déterminés respectivement par $x \to x_i$.

Dans le cas général soit $x \in K \setminus k$ et soit $L = k(x)$. L'extension N/L est normale et l'extension K/L séparable. Il suffit alors d'appliquer l'hypothèse de récurrence en utilisant les lemmes 1.1 et 1.20.

□

Une première application du théorème 1.19 est le *théorème de l'élément primitif* :

Corollaire 1.21. *Soit K/k une extension finie séparable. Alors cette extension est monogène : il existe $\alpha \in K$ tel que $K = k(\alpha)$.*

Démonstration. Nous verrons au § 2 que si k est un corps fini, alors toute extension finie de k est séparable sur k et monogène.

Supposons k infini. Soit $d = [K : k]$. Soit N une extension finie normale de k contenant K et soient $\sigma_1, \ldots, \sigma_d$ les k-isomorphismes de K dans N.

Comme le corps k est infini, si un k espace vectoriel V contient des sous-espaces $V_1, \ldots, V_m$ et est contenu dans leur réunion, alors il est égal à l'un au moins des V_i (on utilise le fait que k a au moins m éléments et on procède par récurrence sur m). On en déduit qu'il existe un élément α de K dont les images $\sigma_1(\alpha), \ldots, \sigma_d(\alpha)$ sont deux-à-deux distinctes. Le polynôme irréductible de α sur k a d racines distinctes dans N, donc est de degré d sur k, ce qui permet de conclure $K = k(\alpha)$.

□

Notons que la réciproque n'est pas vraie : l'extension inséparable $K(\sqrt{T})$ du corps $K = \mathbf{F}_2(T)$ est monogène.

Exercice. Soit K le corps $\mathbf{F}_2(T_1, T_2)$ des fractions rationnelles en deux indéterminées T_1 et T_2 sur le corps à 2 éléments et soit L le corps de décomposition du polynôme $(X^2 - T_1)(X^2 - T_2)$ sur K. Montrer que l'extension L/K n'est pas monogène.

1.7 Polynômes cyclotomiques

Soit n un entier positif. Une racine n-ième de l'unité dans un corps K est un élément de $K^\times$ qui satisfait $x^n = 1$. Une racine primitive n-ième de l'unité dans K est un élément de $K^\times$ d'ordre n : il satisfait, pour k dans $\mathbf{Z}$, $x^k = 1$ si et seulement si n divise k.

Exercice. Soient K un corps, G un sous-groupe fini de $K^\times$, n l'ordre de G. Soit ℓ le plus grand ordre d'un élément de G. Vérifier $x^\ell = 1$ pour tout $x \in G$. En déduire $\ell = n$, montrer que G est cyclique, que G est l'ensemble des racines n-ièmes de l'unité dans K et que

$$X^n - 1 = \prod_{x \in G} (X - x)$$

dans $K[X]$.

L'application $\mathbf{C} \to \mathbf{C}^\times$ qui envoie z sur $e^{2i\pi z/n}$ est un homomorphisme du groupe additif $\mathbf{C}$ dans le groupe multiplicatif $\mathbf{C}^\times$ qui est périodique de période n. Donc il se factorise en un homomorphisme du groupe $\mathbf{C}/n\mathbf{Z}$ dans $\mathbf{C}^\times$: on le note encore $z \mapsto e^{2i\pi z/n}$.

Le groupe multiplicatif $(\mathbf{Z}/n\mathbf{Z})^\times$ de l'anneau $\mathbf{Z}/n\mathbf{Z}$ est formé des classes des entiers premiers avec n. Son ordre est donc le nombre, noté $\varphi(n)$, d'entiers k dans l'intervalle $1 \leq k \leq n$ vérifiant $\mathrm{pgcd}(n,k) = 1$. L'application $\varphi : \mathbf{N} \to \mathbf{Z}$ ainsi définie est appelée *indicatrice d'Euler*.

Les nombres complexes

$$e^{2i\pi k/n}, \qquad k \in (\mathbf{Z}/n\mathbf{Z})^\times$$

sont les $\varphi(n)$ racines primitives de l'unité dans $\mathbf{C}$.

On définit un polynôme $\Phi_n(X) \in \mathbf{C}[X]$ par

$$\Phi_n(X) = \prod_{k \in (\mathbf{Z}/n\mathbf{Z})^\times} (X - e^{2i\pi k/n}).$$

Ce polynôme est unitaire, de degré $\varphi(n)$. La partition de l'ensemble des racines de l'unité suivant leur ordre montre que l'on a, pour tout $n \geq 1$,

$$X^n - 1 = \prod_{d|n} \Phi_d(X). \tag{1.22}$$

Les premiers polynômes cyclotomiques sont

$$\Phi_1(X) = X - 1, \quad \Phi_2(X) = X + 1, \quad \Phi_3(X) = X^2 + X + 1, \quad \Phi_4(X) = X^2 + 1,$$

$$\Phi_5(X) = X^5 + X^4 + X^3 + X^2 + X + 1, \quad \Phi_6(X) = X^2 - X + 1.$$

Théorème 1.23. *Pour tout entier positif n, le polynôme $\Phi_n(X)$ a ses coefficients dans $\mathbf{Z}$. De plus $\Phi_n(X)$ est irréductible dans $\mathbf{Z}[X]$.*

Avant de démontrer le théorème 1.23 nous allons rappeler quelques propriétés de l'anneau $\mathbf{Z}[X]$. Le pgcd des coefficients d'un polynôme $f \in \mathbf{Z}[X]$ est appelé *contenu* de f et noté $c(f)$. Un polynôme de $\mathbf{Z}[X]$ est dit *primitif* si son contenu est 1. Tout polynôme non nul $f \in \mathbf{Z}[X]$ s'écrit de manière unique $f = c(f)g$ avec $g \in \mathbf{Z}[X]$ primitif. Plus généralement pour tout $f \in \mathbf{Q}[X]$ non nul il existe un unique nombre rationnel positif c tel que le polynôme cf soit dans $\mathbf{Z}[X]$ et primitif.

Lemme 1.24 (Lemme de Gauss). *Pour f et g dans $\mathbf{Z}[X]$ non nuls,*

$$c(fg) = c(f)c(g).$$

Démonstration. Il suffit de montrer que le produit de deux polynômes primitifs est primitif. Plus précisément, soit p un nombre premier, f et g deux polynômes de $\mathbf{Z}[X]$ dont le contenu n'est pas divisible par p. On va montrer que le contenu du produit fg n'est pas divisible par p.

Considérons le morphisme surjectif d'anneaux

$$\Psi_p : \mathbf{Z}[X] \to \mathbf{F}_p[X] \tag{1.25}$$

qui envoie X sur X et $\mathbf{Z}$ sur $\mathbf{F}_p$ par réduction modulo p des coefficients. Le noyau de Ψ_p est formé des polynômes dont le contenu est divisible par p. Donc $\Psi_p(f) \neq 0$ et $\Psi_p(g) \neq 0$. Comme p est premier, l'anneau $\mathbf{F}_p[X]$ est intègre, donc $\Psi_p(fg) = \Psi_p(f)\Psi_p(g) \neq 0$, ce qui montre que fg n'appartient pas au noyau de Ψ_p.

□

L'anneau $\mathbf{Z}$ est *euclidien*, donc *factoriel* et, quand A est un anneau factoriel, l'anneau $A[X]$ des polynômes en une indéterminée à coefficients dans A est aussi factoriel. Par conséquent $\mathbf{Z}[X]$ est un anneau factoriel. Les éléments inversibles de $\mathbf{Z}[X]$ sont $\{+1, -1\}$. Les éléments irréductibles de $\mathbf{Z}[X]$ sont
– les nombres premiers $\{2, 3, 5, 7, 11, \ldots\}$,
– les polynômes irréductibles de $\mathbf{Q}[X]$ qui sont à coefficients dans $\mathbf{Z}$ et ont un contenu égal à 1
– et bien entendu le produit par -1 d'un de ces éléments.

Le lemme de Gauss 1.24 montre que, si f et g sont deux polynômes unitaires de $\mathbf{Q}[X]$ tels que $fg \in \mathbf{Z}[X]$, alors f et g sont dans $\mathbf{Z}[X]$. En particulier les facteurs irréductibles d'un polynôme unitaire de $\mathbf{Z}[X]$ sont des polynômes unitaires de $\mathbf{Z}[X]$.

La démonstration que nous allons donner du théorème 1.23 utilisera le lemme suivant, sur lequel nous reviendrons au § 2 :

Lemme 1.26. *Si p est un nombre premier et $A \in \mathbf{F}_p[X]$ un polynôme, alors $A(X^p) = A(X)^p$.*

Démonstration du théorème 1.23. La démonstration du fait que $\Phi_n(X) \in \mathbf{Z}[X]$ repose sur la division euclidienne dans $\mathbf{Z}[X]$: quand A et B sont deux éléments de $\mathbf{Z}[X]$ avec B *unitaire*, pour tout $A \in B[X]$ il existe un couple unique (Q, R) formé de deux polynômes de $\mathbf{Z}[X]$ tels que $A = BQ + R$ et soit $R = 0$, soit $\deg R < \deg B$.

On démontre alors le fait que $\Phi_n(X) \in \mathbf{Z}[X]$ par récurrence sur n. C'est vrai pour $n = 1$ car $\Phi_1(X) = X - 1$. Supposons $\Phi_m(X) \in \mathbf{Z}[X]$ pour tout entier $m < n$. L'hypothèse de récurrence implique que le polynôme

$$h(X) = \prod_{\substack{d|n \\ d \neq n}} \Phi_d(X)$$

est unitaire et à coefficients dans $\mathbf{Z}$. On divise le polynôme $X^n - 1$ par h dans $\mathbf{Z}[X]$: désignons par $Q \in \mathbf{Z}[X]$ le quotient et par $R \in \mathbf{Z}[X]$ le reste :

$$X^n - 1 = h(X)Q(X) + R(X).$$

On a aussi $X^n - 1 = h(X)\Phi_n(X)$ dans $\mathbf{C}[X]$ par (1.22). Par unicité de la division euclidienne dans $\mathbf{C}[X]$ il en résulte $Q = \Phi_n$ et $R = 0$, donc $\Phi_n \in \mathbf{Z}[X]$.

Montrons que le polynôme Φ_n est irréductible dans $\mathbf{Z}[X]$. Comme il est unitaire, son contenu est 1. Il s'agit donc de vérifier qu'il est irréductible dans $\mathbf{Q}[X]$.

Soit $f \in \mathbf{Q}[X]$ un facteur unitaire irréductible de Φ_n et soit $g \in \mathbf{Q}[X]$ le quotient : on a donc $\Phi_n = fg$. Le but est de montrer $g = 1$.

Soit $\zeta \in \mathbf{C}$ une racine de f (donc ζ est une racine primitive n-ième de l'unité) et soit p un nombre premier ne divisant pas n. On commence par vérifier que $f(\zeta^p) = 0$.

Comme ζ^p est aussi une racine primitive n-ième de l'unité, c'est une racine de Φ_n, donc si $f(\zeta^p) \neq 0$ on a $g(\zeta^p) = 0$. Comme f est le polynôme irréductible de ζ, il en résulte que $f(X)$ divise $g(X^p)$.

Considérons le morphisme d'anneaux Ψ_p de $\mathbf{Z}[X]$ sur $\mathbf{F}_p[X]$ déjà introduit en (1.25). dans la démonstration du lemme 1.24. Notons F et G les images dans $\mathbf{F}_p[X]$ de f et g respectivement. L'image de $\Phi_n(X)$ est FG et c'est un diviseur de $X^n - 1$ dans $\mathbf{F}_p[X]$. Le lemme 1.26 montre que l'image de $g(X^p)$ est $G(X^p) = G(X)^p$ car $G(X) \in \mathbf{F}_p[X]$. De plus $F(X)$ divise $G(X)^p$ dans $\mathbf{F}_p[X]$. Le polynôme $F(X)$ est unitaire de même degré que f, il admet un diviseur irréductible $k(X)$ dans $\mathbf{F}_p[X]$. Alors $k(X)$ divise $F(X)$ et $G(X)^p$, donc il divise $G(X)$ et son carré divise $F(X)G(X)$. Mais

comme p ne divise pas n, le polynôme $X^n - 1$ n'est divisible par aucun carré de polynôme non constant dans $\mathbf{F}_p[X]$. On en conclut $f(\zeta^p) = 0$.

Par conséquent dès que f s'annule en ζ il s'annule en ζ^p quand p est un nombre premier ne divisant pas n. On en déduit (par récurrence sur le nombre de facteurs de m) qu'il s'annule en chaque ζ^m quand m est premier avec n ; mais dans le groupe cyclique formé par les racines n-ièmes de l'unité, l'ensemble des ζ^m avec $\mathrm{pgcd}(m, n) = 1$ est l'ensemble des générateurs de ce groupe, donc l'ensemble des racines de Φ_n. D'où $g = 1$.

□

Quand K est un corps de caractéristique finie p et quand n est un multiple de p, le polynôme $X^n - 1$ est une puissance p-ième d'un polynôme de $K[X]$: plus précisément, si $n = p^a m$ avec m non divisible par p, alors

$$X^n - 1 = (X^m - 1)^{p^a}.$$

Ainsi, quand on veut étudier le polynôme $X^n - 1$, on est ramené à étudier $X^m - 1$ avec m non multiple de p. Cela justifie l'hypothèse qui va apparaître.

Comme le polynôme Φ_n est à coefficients dans $\mathbf{Z}$ pour tout corps K on peut considérer $\Phi_n(X)$ comme un élément de $K[X]$: en caractéristique nulle, c'est parce que K contient $\mathbf{Q}$, en caractéristique finie p on considère l'image de Φ_n par le morphisme Ψ_p introduit en (1.25) : on note encore Φ_n cette image.

Proposition 1.27. *Soient K un corps et n un entier positif. On suppose que K est soit de caractéristique nulle, soit de caractéristique p premier ne divisant pas n. Alors le polynôme $\Phi_n(X)$ est séparable sur K et ses racines dans K sont exactement les racines primitives de l'unité qui appartiennent à K.*

Démonstration. La dérivée du polynôme $X^n - 1$ est n. Dans K on a $n \neq 0$, donc $X^n - 1$ est séparable sur K et comme $\Phi_n(X)$ est un facteur de $X^n - 1$ il est aussi séparable sur K. Les racines dans K de $X^n - 1$ sont exactement les racines n-ièmes de l'unité contenues dans K. Dire qu'une racine n-ième de l'unité est primitive signifie qu'elle n'est pas racine d'un polynôme Φ_d avec $d|n$, $d \neq n$. D'après (1.22) cela signifie donc qu'elle est racine de Φ_n.

□

Soit n un entier positif. On définit le corps cyclotomique de niveau n sur $\mathbf{Q}$ par

$$R_n = \mathbf{Q}\big(\{e^{2i\pi k/n} \ ; \ k \in (\mathbf{Z}/n\mathbf{Z})^\times\}\big) \subset \mathbf{C}.$$

C'est le corps de décomposition de Φ_n sur $\mathbf{Q}$ et c'est aussi le corps de rupture de Φ_n sur $\mathbf{Q}$. Si $\zeta \in \mathbf{C}$ est une racine primitive de l'unité, alors $\{1, \zeta, \ldots, \zeta^{\varphi(n)-1}\}$ est une base de R_n comme espace vectoriel sur $\mathbf{Q}$.

Proposition 1.28. *Le groupe des automorphismes du corps R_n est naturellement isomorphe au groupe mulltiplicatif $(\mathbf{Z}/n\mathbf{Z})^\times$.*

Démonstration. Soit ζ_n une racine primitive n-ième de l'unité. Pour $\varphi \in \mathrm{Aut}(R_n)$, on définit $\theta(\varphi) \in (\mathbf{Z}/n\mathbf{Z})^\times$ par

$$\varphi(\zeta_n) = \zeta_n^{\theta(\varphi)}.$$

Alors l'application θ est un isomorphisme du groupe de $\mathrm{Aut}(R_n/\mathbf{Q})$ sur $(\mathbf{Z}/n\mathbf{Z})^\times$.

□

Exemple. Le sous corps de R_n fixé par le sous-groupe $\theta^{-1}(\{1,-1\})$ de $G(R_n/\mathbf{Q})$ est le sous-corps réel maximal de R_n :

$$R_n^+ = \mathbf{Q}(\zeta_n + \zeta_n^{-1}) = \mathbf{Q}\big(\cos(2\pi/n)\big) = R_n \cap \mathbf{R}$$

avec $[R_n : R_n^+] = 2$.

1.8 Théorie de Galois

Une extension algébrique L/K est dite *galoisienne* si elle est normale et séparable. C'est équivalent à dire que pour tout $\alpha \in L$ le nombre de conjugués de α dans L est le degré $[K(\alpha) : K]$ de α sur K.

Soit L/K une extension. On note $\mathrm{Aut}(L/K)$ le groupe des K-automorphismes de L.

Lemme 1.29. *Quand L/K est une extension finie, le groupe $\mathrm{Aut}(L/K)$ est fini d'ordre $\leq [L : K]$.*

Démonstration. On écrit $L = K(\alpha_1, \ldots, \alpha_m)$. Un K-automorphisme σ de L est entièrement déterminé par $\big(\sigma(\alpha_1), \ldots, \sigma(\alpha_m)\big) \in L^m$. Pour $1 \leq i \leq m$ soit d_i le degré de α_i sur $K(\alpha_1, \ldots, \alpha_{i-1})$. Ainsi $[L : K] = d_1 \cdots d_m$. Quand σ décrit $\mathrm{Aut}(L/K)$, il y a au plus d_1 valeurs possibles $\sigma(\alpha_1) \in L$ (à savoir les conjugués sur K de α_1 dans L) et quand on impose les valeurs de $\sigma(\alpha_1), \ldots, \sigma(\alpha_{i-1})$, il y a au plus d_i valeurs possibles $\sigma(\alpha_i) \in L$ (les conjugués dans L de α_i sur le corps $K\big(\sigma(\alpha_1), \ldots, \sigma(\alpha_{i-1})\big)$). □

Théorème 1.30. *Soit L/K une extension finie. Alors l'extension L/K est galoisienne si et seulement si le groupe $\mathrm{Aut}(L/K)$ est d'ordre égal à $[L : K]$.*

Démonstration. Si l'extension L/K est galoisienne finie, le théorème 1.19 (dans lequel on prend $N = K$) montre que le groupe $\mathrm{Aut}(L/K)$ a $[L : K]$ éléments.

Inversement, si $\mathrm{Aut}(L/K)$ a $[L : K]$ éléments, soit $\alpha_1 \in L$; on peut écrire (comme dans la démonstration du lemme 1.29) $L = K(\alpha_1, \ldots, \alpha_m)$ avec des éléments $\alpha_2, \ldots, \alpha_m$ dans L. L'égalité $|\mathrm{Aut}(L/K)| = d_1 \cdots d_m$ montre en particulier que α_1 a d_1 conjugués sur K dans L, avec $d_1 = [K(\alpha_1) : K]$. Donc l'extension L/K est galoisienne.

□

Soit L/K une extension algébrique et soit $G = \mathrm{Aut}(L/K)$. Pour chaque extension M de K contenue dans L le groupe $\mathrm{Aut}(L/M)$ est un sous-groupe de G. Inversement pour chaque sous-groupe H de G, le sous-ensemble

$$L^H = \{x \in L \,;\, \sigma(x) = x \text{ pour tout } \ \sigma \in H\}$$

de L est un sous-corps de L contenant K, appelé *sous-corps de L fixé par H*.

Des définitions on déduit immédiatement :

Lemme 1.31. *Soit L/K une extension algébrique et soit $G = \mathrm{Aut}(L/K)$. Les deux applications*

$$M \mapsto \mathrm{Aut}(L/M) \quad \textit{et} \quad H \mapsto L^H$$

sont décroissantes :

Si H et H' sont des sous-groupes de G avec $H \subset H'$, alors $L^{H'} \subset L^H$.

Si M et M' sont deux extensions de K contenues dans L avec $M \subset M'$, alors $\mathrm{Aut}(L/M') \subset \mathrm{Aut}(L/M)$.

Quand L/K est une extension galoisienne, le groupe $\mathrm{Aut}(L/K)$ est appelé *groupe de Galois de L sur K* et noté $\mathrm{Gal}(L/K)$.

Théorème 1.32.
1. *Soient L/k une extension, G un sous-groupe de $\mathrm{Aut}(L/k)$ et K le corps L^G.*
   a) *Si G est fini, alors L/K est une extension galoisienne finie de groupe de Galois G.*
   b) *Si l'extension L/k est algébrique, alors L/K est une extension galoisienne.*
2. *Soit L/K une extension galoisienne de groupe de Galois $G = \mathrm{Aut}(L/K)$. Alors $L^G = K$.*

Démonstration. 1. a) Soit $\alpha \in L$. Soit m le nombre d'éléments de l'ensemble $E = \{\sigma(\alpha)\ ;\ \sigma \in G\}$. Notons $E = \{\alpha_1, \ldots, \alpha_m\}$. Le groupe G opère sur E par $(\sigma, \alpha_i) \mapsto \sigma(\alpha_i)$, ce qui signifie que l'application qui à $\sigma \in G$ associe $\alpha_i \mapsto \sigma(\alpha_i)$ est un homomorphisme de G dans le groupe symétrique $\mathfrak{S}_E$.

Le polynôme $P(X) = \prod_{i=1}^m (X - \alpha_i)$ vérifie $\sigma(P) = P$. Par définition de K cela signifie $P \in K[X]$. Comme $P(\alpha) = 0$ α est algébrique sur K. Soit f le polynôme irréductible de α sur K. Comme $P \in K[X]$ s'annule en α, f divise P dans $K[X]$. Mais f s'annule en chaque conjugué de α sur K, donc en chaque élément de E et par conséquent P divise f, donc finalement $P = f$. Cela montre que E a autant d'éléments que le degré de α sur K, donc E est l'ensemble de tous les conjugués de α sur K et l'extension L/K est galoisienne. Nous venons de voir que tout élément de L est de degré $\leq |G|$ sur K ; d'après le corollaire 1.21 toute extension finie de K contenue dans L a un degré $\leq |G|$; donc L est une extension finie de K et $[L : K] \leq |G|$. Mais on a $[L : K] = \mathrm{Aut}(L/K)$; de plus G est un sous-groupe de $\mathrm{Aut}(L/K)$. Par conséquent $G = \mathrm{Aut}(L/K)$.
1. b) Soit $\alpha \in L$. L'ensemble $E = \{\sigma(\alpha)\ ;\ \sigma \in G\}$ est constitué de conjugués de α sur k, donc est fini. Comme ci-dessus le polynôme irréductible de α sur K est $\prod_{\beta \in E}^m (X - \beta)$. On vérifie ainsi que le nombre de conjugués de α sur K est égal à $[K(\alpha) : K]$. Donc l'extension L/K est galoisienne.
2. Soit d le degré de α sur K. D'après ce que nous venons de voir il existe des éléments $\sigma_1, \ldots, \sigma_d$ dans $\mathrm{Aut}(L/K)$ tels que le polynôme irréductible de α sur K s'écrive $\prod_{j=1}^d \big(X - \sigma_j(\alpha)\big)$. Alors $\alpha \in L^{\mathrm{Aut}(L/K)}$ équivaut à $d = 1$, donc à $\alpha \in K$.

□

Du théorème 1.32 (parties 1.b) et 2.) on déduit qu'une extension algébrique L/K est galoisienne si et seulement si $L^{\mathrm{Aut}(L/K)} = K$.

Voici le théorème principal de la théorie de Galois pour les extensions finies ; il affirme que, pour une extension galoisienne finie, la correspondance que nous venons d'introduire entre les extensions intermédiaires et les sous-groupes du groupe de Galois est bijective.

Théorème 1.33 (Théorème de Galois). *Soit L/K une extension galoisienne finie de groupe de Galois $G = \mathrm{Gal}(L/K)$.*

1. *Si M est une extension de K contenue dans L et si on note $H = \mathrm{Aut}(L/M)$, alors L/M est une extension galoisienne de groupe de Galois H et on a*

$$[L : M] = |H| \quad \textit{et} \quad M = L^H.$$

2. *Si H est un sous-groupe de G et $M = L^H$ le sous-corps de L fixé par H, alors L/M est une extension galoisienne et on a*

$$[L : M] = |H| \quad \textit{et} \quad H = \mathrm{Gal}(L/M).$$

3. *Si M est une extension de K contenue dans L et si on note H le sous-groupe* $\mathrm{Gal}(L/M)$ *de G, alors l'extension M/K est galoisienne si et seulement si H est normal dans G. Dans ce cas le groupe de Galois de M/K est isomorphe au quotient G/H.*

Démonstration. 1. L'extension L/M est séparable et normale, donc galoisienne et son groupe de Galois est $H = \mathrm{Aut}(L/M)$. On a $M \subset L^H \subset L$ et l'extension L/L^H est galoisienne finie de groupe de Galois H par le théorème 1.32. Donc $[L : M] = |H|$ et $M = L^H$.

2. Comme $M = L^H$ est un corps intermédiaire $K \subset M \subset L$, l'extension L/M est galoisienne de groupe de Galois $\mathrm{Aut}(L/M)$. Le théorème 1.32 montre que l'extension L/L^H est galoisienne finie de groupe de Galois H. Comme $M = L^H$ on en déduit $H = \mathrm{Aut}(L/M)$ et $[L : M] = |H|$.

3. Supposons l'extension M/K galoisienne. Soient $\sigma \in H$ et $\tau \in G$. Il s'agit de vérifier $\tau^{-1} \circ \sigma \circ \tau \in H$. Pour cela on prend $x \in M$; l'extension M/K étant galoisienne, on a $\tau(x) \in M$, donc $\sigma \circ \tau(x) = \tau(x)$ et ainsi $\tau^{-1} \circ \sigma \circ \tau(x) = x$. Cela montre que le sous-groupe H de G est normal.

Inversement si H est normal dans G soit $x \in M$ et soit $\tau \in G$. Il s'agit de vérifier $\tau(x) \in M$, c'est-à-dire $\sigma \circ \tau(x) = \tau(x)$ pour tout $\sigma \in H$. En effet comme $\sigma \in H$ et que H est normal dans G on a $\tau^{-1} \circ \sigma \circ \tau \in H$, donc $\tau^{-1} \circ \sigma \circ \tau(x) = x$.

On suppose encore que H est normal dans G, c'est-à-dire que l'extension M/K est galoisienne ; la restriction de σ à M est alors un K-automorphisme de M. L'application qui envoie un élément $\sigma \in \mathrm{Aut}(L/K)$ sur sa restriction M définit un homomorphisme de G dans $\mathrm{Aut}(M/K)$ de noyau H. Son image est donc isomorphe au quotient G/H. Comme

$$|G| = [L : K] = [L : M][M : K] = |H|[M : K],$$

il en résulte que cet homomorphisme est surjectif : son image est $\mathrm{Aut}(M/K)$.

□

Une extension galoisienne est dite *abélienne, cyclique, résoluble,...* si son groupe de Galois l'est.

Université P. et M. Curie (Paris VI),
Deuxième semestre 2006/2007

Michel Waldschmidt
date de mise à jour: 24/04/2007

Master de sciences et technologies 1ère année -
Spécialité : Mathématiques Fondamentales

Mention : Mathématiques et applications
MO11 : Théorie des nombres (12 ECTS)

Première partie: Théorie des Corps

Fascicule 3 : Chapitre 1 (fin), section 1.9 (9 pages) [2]

1.9 Théorie de Galois : quelques exemples

1.9.1 Constructions à la règle et au compas

Les trois questions classiques posées par les géomètres grecs sur les constructions à la règle et au compas sont les suivantes : peut-on construire, en utilisant uniquement ces deux instruments,
• (*Duplication du cube*) un cube ayant un volume double d'un cube donné ?
• (*Trisection d'un angle*) un angle égal au tiers d'un angle donné ?
• (*Quadrature du cercle*) un carré ayant une aire égale à celle d'un disque donné ?

Ces questions reviennent à construire respectivement la racine cubique d'un nombre donné, le cosinus du tiers d'un angle dont le cosinus est donné, le nombre π.

En termes algébriques on considère le plan cartésien $\mathbf{R}^2$ avec l'unité de longueur donnée par la distance entre $(0,0)$ et $(0,1)$ et à partir de ces deux points on itère les constructions suivantes, dont la réunion produit l'ensemble des *points constructibles* :
– On peut construire la droite qui passe par deux points donnés.
– On peut construire un cercle de rayon donné et de centre préalablement construit.
– À chaque étape on peut ajouter à l'ensemble déjà construit l'intersection de deux droites, de deux cercles, d'une droite et d'un cercle, chacune de ces lignes ayant été précédemment construites.

Un nombre réel est dit *constructible* si le point $(x,0)$ est constructible à la règle et au compas à partir de $(0,0)$ et $(0,1)$.

Des constructions géométriques classiques montrent que les nombres constructibles forment un sous-corps de $\mathbf{R}$ et que si x est constructible, alors $\sqrt{x}$ l'est aussi. Les images suivantes sont extraites de [1] § 13.3.

[2] Ce texte est téléchargeable à partir de la page http ://www.math.jussieu.fr/∼miw/enseignement.html

It is an elementary fact from geometry that if two lengths a and b are given one may construct using straightedge and compass the lengths $a \pm b$, ab and a/b (the first two are clear and the latter two are given by the construction of parallel lines (Figure 1)).

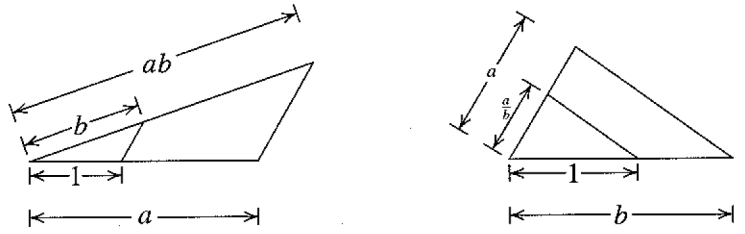

Fig. 1

It is also an elementary geometry construction to construct $\sqrt{a}$ if a is given: construct the circle with diameter $1 + a$ and erect the perpendicular to the diameter as indicated in Figure 2. Then $\sqrt{a}$ is the length of this perpendicular.

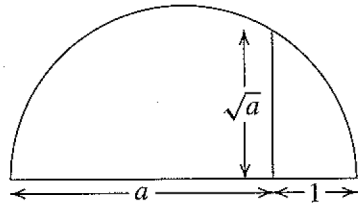

Fig. 2

L'énoncé suivant est facile à démontrer (voir par exemple [1] § 13.3).

Proposition 1.34. *Soit x un nombre réel. Les assertions suivantes sont équivalentes :*
- *x est constructible.*
- *x est algébrique sur $\mathbf{Q}$ et son corps de décomposition sur $\mathbf{Q}$ a pour degré une puissance de 2.*
- *x appartient à un corps de nombres galoisien sur $\mathbf{Q}$ de degré une puissance de 2.*

Comme $\sqrt[3]{2}$ est de degré 3 sur $\mathbf{Q}$, on en déduit l'impossibilité de la duplication du cube.

Il existe des angles dont on peut construire le tiers à la règle et au compas (par exemple π), mais il en existe aussi pour lesquels une telle construction est impossible. Un exemple est $\pi/3$. On a $\cos(\pi/3) = -1/2$ et la formule

$$\cos\theta = 4\cos^3(\theta/3) - 3\cos(\theta/3)$$

montre que le nombre $\beta = 2\cos(\pi/9) = 1,87938\ldots$ est racine du polynôme $X^3 - 3X + 1$. Ce polynôme est irréductible sur $\mathbf{Q}$. Donc β est de degré 3 sur $\mathbf{Q}$, par conséquent il n'est pas constructible.

Pour la quadrature du cercle, l'impossibilité vient de la transcendance du nombre π que nous ne démontrons pas ici (une démonstration est donnée dans l'Annexe A du livre de Lang *Algèbre* [4]).

Un nombre complexe est dit *exprimable par radicaux* s'il existe un corps de nombres K le contenant, une tour de corps

$$\mathbf{Q} = K_0 \subset K_1 \subset \cdots \subset K_{s-1} \subset K_s = K,$$

et, pour $1 \leq i \leq s$, un entier $n_i \geq 1$ et un élément $\alpha_i \in K_i$ tels que $K_i = K_{i-1}(\alpha_i)$ avec $\alpha_i^{n_i} \in K_{i-1}$.

On pose $a_i = \alpha_i^{n_i}$ et on écrit $\alpha_i = \sqrt[n_i]{a_i}$ (avec un léger abus de notation : il y a plusieurs racines n_i-ièmes de α_i, mais le corps engendré ne dépend pas de ce choix lorsque les racines n_i-ièmes appartiennent au corps de base, ce qui est une hypothèse licite ici) et donc $K_i = K_{i-1}(\sqrt[n_i]{a_i})$.

Soit K un corps de caractéristique nulle. On définit le *groupe de Galois d'un polynôme séparable* $f \in K[X]$ comme le groupe de Galois d'un corps de décomposition de f sur K.

Un polynôme est *résoluble par radicaux* si toutes ses racines sont exprimables par radicaux.

D'autre part un groupe fini G est *résoluble* s'il existe une suite de sous-groupes

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_{s-1} \subset G_s$$

dans laquelle chaque G_i est un sous-groupe normal de G_{i+1} avec un quotient G_{i+1}/G_i cyclique $(0 \leq i \leq s-1)$.

Le théorème de Galois 1.33 permet de démontrer l'énoncé suivant (voir par exemple [1] § 14.7 Th. 39).

Théorème 1.35. *Un polynôme f est résoluble par radicaux si et seulement si son groupe de Galois est résoluble.*

Soit n un entier ≥ 5. Il est connu que le groupe $\mathfrak{S}_n$ n'est pas résoluble et qu'il existe des corps de nombres galoisiens sur $\mathbf{Q}$ de groupe de Galois $\mathfrak{S}_n$. Un tel corps est le corps de décomposition d'un polynôme qui n'est donc pas résoluble par radicaux.

Par exemple le polynôme $X^5 - 6X + 3$ a pour groupe de Galois sur $\mathbf{Q}$ le groupe symétrique $\mathfrak{S}_5$ d'ordre $5! = 120$, il n'est donc pas résoluble par radicaux.

L'outil essentiel pour la démonstration du théorème 1.35 est un théorème dû à Kummer dont nous donnons seulement l'énoncé :

Théorème 1.36. *Soient L/K une extension et n un entier positif qui n'est pas divisible par la caractéristique de K. On suppose que K contient les racines n-ièmes de l'unité. Alors l'extension est cyclique si et seulement s'il existe $\alpha \in L$ tel que $L = K(\alpha)$ et $\alpha^n \in K$.*

1.9.2 Corps cyclotomiques

Soit n un entier positif. Le corps cyclotomique E_n d'indice n est le corps de décomposition sur $\mathbf{Q}$ du polynôme $X^n - 1$. C'est aussi le corps de rupture du polynôme cyclotomique Φ_n sur $\mathbf{Q}$. Notons ζ_n une racine primitive n-ième de l'unité, de sorte que $E_n = \mathbf{Q}(\zeta_n)$.

Nous avons vu (Proposition 1.28) que E_n est une extension galoisienne de $\mathbf{Q}$ de groupe de Galois $(\mathbf{Z}/n\mathbf{Z})^\times$.

Supposons n premier et notons $n = p$, $E_p = E$, $\zeta_p = \zeta$. Le groupe des éléments inversibles du corps $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ est cyclique, donc l'extension $E/\mathbf{Q}$ est cyclique de groupe de Galois $G \simeq (\mathbf{Z}/p\mathbf{Z})^\times$ d'ordre $p-1$. Si k est un entier premier à p, notons σ_k l'automorphisme de E déterminé par $\sigma_k(\zeta) = \zeta^k$.

Lemme 1.37. *L'ordre de σ_k dans G est égal à l'ordre de la classe de k modulo p.*

Démonstration. Pour $h \geq 1$ on a $\zeta^h = 1$ si et seulement si p divise h. Donc pour $n \geq 1$ on a $\zeta^n = \zeta$ si et seulement si $n \equiv 1 \pmod{p}$. D'autre part $\sigma_k^m(\zeta) = \zeta^{k^m}$. Donc l'ordre de σ_k dans G est le plus petit entier m tel que $k^m \equiv 1 \pmod{p}$, c'est l'ordre de la classe de k dans $(\mathbf{Z}/p\mathbf{Z})^\times$. □

Une base sur $\mathbf{Q}$ de E est $\{1, \zeta, \zeta^2, \ldots, \zeta^{p-2}\}$ puisque ζ est de degré $p-1$ sur $\mathbf{Q}$, racine du polynôme

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

On préfère d'utiliser comme base $\{\zeta, \zeta^2, \ldots, \zeta^{p-2}, \zeta^{p-1}\}$ car ce sont précisément les racines primitives p-ièmes de l'unité, qui sont donc permutés par les σ_k.

Soit H un sous-groupe de G. Posons

$$\alpha_H = \sum_{\sigma \in H} \sigma(\zeta).$$

On vérifie facilement que $\mathbf{Q}(\alpha_H)$ est le sous-corps E^H de E fixé par H.

Par exemple pour $p = 7$ le groupe G est cyclique d'ordre 6, il est engendré par σ_3 :

$$G = \{1,\ \sigma_3,\ \sigma_3^2 = \sigma_2,\ \sigma_3^3 = \sigma_6,\ \sigma_3^4 = \sigma_4,\ \sigma_3^5 = \sigma_5\},$$

ce qui correspond au fait que $(\mathbf{Z}/7\mathbf{Z})^\times$ est engendré par 3 (on dit que 3 est une *racine primitive modulo* 7) :

$$(\mathbf{Z}/7\mathbf{Z})^\times = \{1,\ 3,\ 3^2 \equiv 2,\ 3^3 \equiv 6,\ 3^4 \equiv 4,\ 3^5 \equiv 5\}.$$

Le groupe G a quatre sous-groupes, deux triviaux $\{1\}$ et G d'ordres 1 et 6 respectivement, et deux non triviaux $\{1, \sigma_6\}$ et $\{1, \sigma_2, \sigma_4\}$. Le seul élément d'ordre 2 dans G est σ_6 qui est la restriction à E de la conjugaison complexe, puisque $\sigma_6(\zeta) = \zeta^{-1} = \overline{\zeta}$. Le sous corps fixé par la conjugaison complexe est le sous-corps réel maximal M de E, il est engendré sur $\mathbf{Q}$ par $\alpha = \zeta + \overline{\zeta}$, comme nous l'avons déjà vu au § **??** comme exemple d'application de la proposition 1.28. Le corps $M = \mathbf{Q}(\alpha)$ est cubique cyclique sur $\mathbf{Q}$, le groupe de Galois est engendré par la restriction de σ_2 à M : les conjuqués de α sur $\mathbf{Q}$ sont

$$\alpha_1 = \alpha, \quad \alpha_2 = \sigma_2(\alpha) = \zeta^2 + \zeta^5 = \zeta^2 + \overline{\zeta}^2, \quad \alpha_3 = \sigma_2^2(\alpha) = \zeta^4 + \zeta^3 = \zeta^3 + \overline{\zeta}^3.$$

On trouve le polynôme irréductible de α sur $\mathbf{Q}$ en calculant (facilement) $\alpha_1 + \alpha_2 + \alpha_3 = -1$, $\alpha_1\alpha_2\alpha_3 = 1$ et (un peu moins facilement) $\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 = -2$. Le polynôme cherché est donc $X^3 + X^2 - 2X - 1$.

Il reste un dernier sous-corps N de E dont nous n'avons pas encore parlé, c'est le sous-corps fixé par le sous-groupe d'ordre 3 (et d'indice 2) de G. Donc N est l'unique sous-corps quadratique de E, engendré sur $\mathbf{Q}$ par

$$\beta = \zeta + \sigma_2(\zeta) + \sigma_4(\zeta) = \zeta + \zeta^2 + \zeta^4.$$

Le conjugué de β est

$$\beta^* = \tau(\beta) = \sigma_3(\beta) = \zeta^3 + \zeta^6 + \zeta^5.$$

On vérifie facilement $\beta + \beta^* = -1$, $\beta\beta^* = 2$, donc β est racine du polynôme quadratique $X^2 + X + 2$ dont le discriminant est -7. Ainsi l'unique sous-corps quadratique de L est $\mathbf{Q}(\sqrt{-7})$.

De façon générale, il résulte de la proposition 1.44 ci-dessous que *l'unique sous-corps quadratique de* $\mathbf{Q}(\zeta_p)$ *pour* p *premier est le corps* $\mathbf{Q}(\sqrt{\epsilon p})$, *où* $\epsilon = 1$ *si* $p \equiv 1 \pmod{4}$ *et* $\epsilon = -1$ *si* $p \equiv 3 \pmod{4}$ (voir aussi [1] § 14.5).

Soit $n = p_1^{a_1} \cdots p_k^{a_k}$ la décomposition en facteurs premiers d'un entier $n \geq 2$. La décomposition du groupe multiplicatif $(\mathbf{Z}/n\mathbf{Z})^\times$ par le théorème chinois :

$$(\mathbf{Z}/n\mathbf{Z})^\times \simeq (\mathbf{Z}/p_1^{a_1}\mathbf{Z})^\times \times \cdots \times (\mathbf{Z}/p_k^{a_k}\mathbf{Z})^\times$$

permet de déduire du théorème 1.28 l'énoncé suivant :

Corollaire 1.38. *Soit $n = p_1^{a_1} \cdots p_k^{a_k}$ un entier ≥ 2 décomposé en facteurs premiers. Notons E_n le corps cyclotomique $\mathbf{Q}(\zeta_n)$ d'indice n et F_i le corps cyclotomique $E_{p_i^{a_i}} = \mathbf{Q}(\zeta_{p_i^{a_i}})$ d'indice $p_i^{a_i}$. Alors*

$$\mathrm{Gal}(E_n/\mathbf{Q}) \simeq \mathrm{Gal}(F_1/\mathbf{Q}) \times \cdots \times \mathrm{Gal}(F_k/\mathbf{Q}).$$

On en déduit qu'un polygone régulier à n côtés peut être construit à la règle et au compas si et seulement si $\varphi(n)$ est une puissance de 2.

Pour un nombre premier p, dire que $\varphi(p) = p-1$ est une puissance de 2 revient à dire que p est de la forme $2^m + 1$. Il est facile de voir que dans ce cas l'exposant m est lui même une puissance de 2 : quand k est impair, l'identité $x^k + 1 = (x+1)(x^{k-1} - x^{k-2} + \cdots + x^2 - x + 1$ montre que $x^k + 1$ est divisible par $x + 1$.

On appelle *nombre premier de Fermat* tout nombre premier de la forme $F_s = 2^{2^s} + 1$ avec s entier ≥ 0. Les nombres

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65\,537$$

sont des nombres premiers de Fermat. On ignore s'il y en a d'autres (on s'attend à ce que leur nombre soit fini mais on ne le sait pas). Que $F_5 = 2^{2^5} + 1$ ne soit pas un nombre premier a été découvert par Euler. On peut le vérifier ainsi.

Lemme 1.39. *Le nombre $F_5 = 2^{32} + 1$ est divisible par* 641.

Démonstration. (D'après [3], § 2.5). On écrit

$$641 = 625 + 16 = 5^4 + 2^4 \quad \text{et} \quad 641 = 5 \cdot 128 + 1 = 5 \cdot 2^7 + 1.$$

L'identité $x^4 - 1 = (x+1)(x-1)(x^2+1)$ montre que $x^4 - 1$ est divisible par $x+1$, donc $5^4 \cdot 2^{28} - 1$ est divisible par 641. Mais 641 divise aussi $5^4 \cdot 2^{28} + 2^{32}$, donc il divise la différence $2^{32} + 1$. □

Le résultat que fournit le théorème de Galois 1.33 est le suivant :

Proposition 1.40. *Soit n un entier ≥ 3. Un polygone régulier peut être construit à la règle et au compas si et seulement si n est de la forme $2^k p_1 \cdots p_r$ où k est un entier ≥ 0 et $p_1, \ldots, p_r$ des nombres premiers de Fermat deux-à-deux distincts.*

On trouvera dans [1] § 14.5 d'autres informations sur ce thème, notamment une construction géométrique du polygone régulier à 17 côtés due à J.H. Conway (voir aussi [2]).

1.9.3 Résolution par radicaux

Soit $f \in K[X]$ un polynôme séparable de degré n à coefficient dans un corps K. Le groupe de Galois de f sur K a été défini (§ 1.9.1) comme le groupe de Galois $G = \mathrm{Gal}(L/K)$ du corps de décomposition L de f sur K. Ce groupe de Galois agit sur l'ensemble E des racines de f par permutation, donc s'injecte dans le groupe symétrique $\mathfrak{S}_n$.

Si f est produit de polynômes irréductibles $f = f_1 \cdots f_k$ dans $K[X]$ et si n_i désigne le degré de f_i, alors le groupe de Galois s'injecte dans le produit $\mathfrak{S}_{n_1} \times \cdots \times \mathfrak{S}_{n_k}$.

Si f est irréductible sur K, alors G agit sur E de façon *transitive* : pour tout α et β dans E il existe $\sigma \in G$ tel que $\sigma(\alpha) = \beta$.

Nous allons donner un sens précis à l'affirmation suivante :

• *Le groupe de Galois d'un polynôme "générique" de degré n est le groupe symétrique $\mathfrak{S}_n$.*

On désigne par L le corps $\mathbf{Q}(x_1, \ldots, x_n)$ des fractions rationnelles en n indéterminées sur $\mathbf{Q}$ (on peut remplacer le corps de base $\mathbf{Q}$ par un corps de caractéristique nulle, mais cela en fait n'ajoute rien). On définit les *fonctions symétriques élémentaires* $s_1, \ldots, s_n \in \mathbf{Q}[x_1, \ldots, x_n]$ par la relation

$$(X - x_1)(X - x_2) \cdots (X - x_n) = X^n - s_1 X^{n-1} + s_2 X^{n-2} - \cdots + (-1)^n s_n.$$

On a par exemple

$$s_1 = x_1 + \cdots + x_n, \quad s_n = x_1 \cdots x_n$$

et

$$s_2 = x_1x_2 + x_1x_3 + \cdots + x_1x_n + x_2x_3 + \cdots + x_2x_n + \cdots + x_{n-1}x_n.$$

Plus généralement, pour $1 \leq k \leq n$, la k-ième fonction symétrique élémentaire en n variables est

$$s_k = \sum_{i_1 < i_2 < \cdots < i_k} x_{i_1} x_{i_2} \cdots x_{i_k}.$$

Le *polynôme général de degré n* est le polynôme $f(X) = (X - x_1)(X - x_2) \cdots (X - x_n)$. On note encore K le corps $\mathbf{Q}(s_1, \ldots, s_n)$, qui est un sous-corps de L. Le polynôme f a ses coefficients dans K et son corps de décomposition sur K est L. Comme f est de degré n le groupe de Galois de L sur K est (isomorphe à) un sous-groupe de $\mathfrak{S}_n$. En particulier on a $[L : K] \leq n!$.

Toute permutation de $\{1, \ldots, n\}$ induit un automorphisme de L qui laisse invariant chacun des s_k $(1 \leq k \leq n)$. Donc K est contenu dans le sous-corps $L^{\mathfrak{S}_n}$ de L fixé par $\mathfrak{S}_n$. Par le théorème de Galois 1.33, l'extension $L/L^{\mathfrak{S}_n}$ est de degré $n!$ On en déduit $K = L^{\mathfrak{S}_n}$. Il en résulte que L est une extension de K de degré $n!$ et de groupe de Galois $\mathfrak{S}_n$.

Une fonction rationnelle $F(x_1, \ldots, x_n) \in L$ est appelée *symétrique* si elle est invariante sous l'action de $\mathfrak{S}_n$. Nous avons ainsi démontré :

Proposition 1.41. *Une fraction rationnelle $F(x_1, \ldots, x_n) \in \mathbf{Q}(x_1, \ldots, x_n)$ est symétrique si et seulement s'il existe une fraction rationnelle G en n indéterminées telle que*

$$F(x_1, \ldots, x_n) = G(s_1, \ldots, s_n).$$

La fraction rationnelle G est unique. Si F est un polynôme, alors G est aussi un polynôme : un algorithme pour calculer G est donné dans l'exercice 37 du § 14.6 de [1]. L'idée consiste à considérer le monome $Ax_1^{a_1} \cdots x_n^{a_n}$ de F qui est dominant pour l'ordre lexicographique et à soustraire $As_1^{a_1 - a_2} s_2^{a_2 - a_3} \cdots s_n^{a_n}$.

Pour revenir à notre affirmation sur les polynômes "génériques", on part d'un polynôme unitaire f de degré n dont les coefficients sont des indéterminées ; on l'écrit

$$f(X) = X^n - s_1 X^{n-1} + s_2 X^{n-2} - \cdots + (-1)^n s_n. \tag{1.42}$$

On désigne par K le corps des fractions rationnelles $\mathbf{Q}(s_1, \ldots, s_n)$ en n indéterminées sur $\mathbf{Q}$, par L un corps de décomposition de f sur K et par $x_1, \ldots, x_n$ les racines de f dans L. Ainsi $L = K(x_1, \ldots, x_n)$. Vérifions que les x_i sont *algébriquement indépendants sur* $\mathbf{Q}$, c'est-à-dire que si $p \in \mathbf{Q}[X_1, \ldots, X_n]$ est un polynôme non nul, alors $p(x_1, \ldots, x_n) \neq 0$. Sinon le produit

$$P(X_1, \ldots, X_n) = \prod_{\sigma \in \mathfrak{S}_n} p(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$$

serait un polynôme non nul symétrique qui s'annule en $(x_1, \ldots, x_n)$, ce qui fournirait une relation de dépendance algébrique non triviale entre $s_1, \ldots, s_n$. On en déduit :

Théorème 1.43. *Si $s_1, \ldots, s_n$ sont des indéterminées sur $\mathbf{Q}$, le polynôme générique (1.42) est séparable et a pour groupe de Galois $\mathfrak{S}_n$ sur le corps $\mathbf{Q}(s_1, \ldots, s_n)$.*

Un exemple de polynôme symétrique est donné par le *discriminant*.

Définition. Soient L un corps et $x_1, \ldots, x_n$ des éléments de L. On définit le *discriminant* de $(x_1, \ldots, x_n)$ par

$$D = \prod_{1 \leq i < j \leq n} (x_i - x_j)^2 = (-1)^{n(n-1)/2} \prod_{1 \leq i \neq j \leq n} (x_i - x_j).$$

Le *discriminant générique* est celui pour lequel $x_1, \ldots, x_n$ sont des indéterminées et $L = \mathbf{Q}(x_1, \ldots, x_n)$. C'est un polynôme symétrique, donc d'après la proposition 1.41 il s'exprime comme un polynôme en les fonctions symétriques élémentaires $s_1, \ldots, s_n$. Une des deux racines carrées de D est

$$\sqrt{D} = \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

Le corps quadratique engendré par $\sqrt{D}$ sur $\mathbf{Q}$ est le sous-corps fixé par le groupe alterné $\mathfrak{A}_n$ de $\mathfrak{S}_n$.

On définit aussi le discriminant d'un polynôme unitaire $f \in K[X]$ en considérant un corps de décomposition L de f sur K : dans $L[X]$ ce polynôme se factorise complètement

$$f(X) = (X - \alpha_1) \cdots (X - \alpha_n)$$

et le discriminant de f est défini comme le discriminant de $(\alpha_1, \ldots, \alpha_n)$. D'après ce qui précède il appartient à K.

Le groupe de Galois G d'un polynôme irréductible f de degré n sur $\mathbf{Q}$ est un sous-groupe de $\mathfrak{S}_n$; on obtient un tel isomorphisme en numérotant les racines de f dans L et en considérant G comme un groupe de permutation de ces racines. Alors G est un sous-groupe de $\mathfrak{A}_n$ si et seulement si le discriminant D de f est un carré dans $\mathbf{Q}$.

Le discriminant d'un polynôme quadratique $X^2 + aX + b$ est $a^2 - 4b$, celui d'un polynôme cubique $X^3 + pX + q$ est $-4p^3 - 27q^2$. Un polynôme irréductible de degré 3 a pour groupe de Galois sur $\mathbf{Q}$ le groupe cyclique d'ordre 3 (qui n'est autre que le groupe alterné $\mathfrak{A}_3$) si le discriminant est

un carré dans $\mathbf{Q}$, c'est le groupe symétrique $\mathfrak{S}_3$ (groupe non commutatif d'ordre 6) sinon. Cela permet de distinguer les polynômes cubiques dont un corps de rupture est galoisien des autres.

Voici une méthode pour calculer un discriminant. Soit L un corps, soient $x_1, \ldots, x_n$ des éléments de L et soit D leur discriminant. Considérons le polynôme

$$P(X) = \prod_{i=1}^{n} (X - x_i).$$

Sa dérivée est

$$P('X) = \sum_{i=1}^{n} \prod_{\substack{1 \leq j \leq n \\ j \neq i}} (X - x_j).$$

Ainsi pour $1 \leq i \leq n$ on a

$$P'(\alpha_i) = \prod_{\substack{1 \leq j \leq n \\ j \neq i}} (x_i - x_j).$$

Par conséquent

$$\prod_{i=1}^{n} P'(\alpha_i) = (-1)^{n(n-1)/2} D.$$

Comme exemple nous utilisons cet argument pour calculer le discriminant des polynômes cyclotomiques d'indice un nombre premier ([2] Chap. 10, § 10.5, Exemple 10.12).

Proposition 1.44. *Soit p un nombre premier impair. Le discriminant du polynôme cyclotomique Φ_p d'indice p est*

$$(-1)^{(p-1)/2} p^{p-2}.$$

Démonstration. On utilise ce qui précède avec $P = \Phi_p$, $n = p - 1$ et $x_i = \zeta^i$ $(1 \leq i \leq p-1)$. On a

$$P(X) = \frac{X^p - 1}{X - 1} \quad \text{et} \quad P'(X) = \frac{pX^{p-1}}{X - 1} - \frac{X^p - 1}{(X-1)^2}.$$

Par conséquent pour $1 \leq i \leq p - 1$

$$P'(\zeta^i) = \frac{p\zeta^{i(p-1)}}{\zeta^i - 1}.$$

Le produit des racines de P est le terme constant $P(0)$ (le degré $p - 1$ est pair)

$$\prod_{i=1}^{p-1} \zeta^i = 1.$$

Le polynôme minimal des nombres $\zeta^i - 1$ $(1 \leq i \leq p-1)$ est $P(X+1)$ dont le terme constant est p :

$$\prod_{i=1}^{p-1} (\zeta^i - 1) = p.$$

On trouve ainsi

$$\prod_{i=1}^{p-1} P'(\zeta^i) = p^{p-2}.$$

□

1.9.4 Compléments

Nous avons vu que le corps cyclotomique $\mathbf{Q}(\zeta_p)$ contenait un unique sous-corps quadratique. Il n'est pas difficile de développer l'argument pour déduire qu'inversement, tout corps quadratique sur $\mathbf{Q}$ est contenu dans un corps cyclotomique. Un résultat beaucoup plus général est le *théorème de Kronecker-Weber : toute extension abélienne de* $\mathbf{Q}$ *est contenue dans une extension cyclotomique.*

Un des problèmes ouverts les plus important du sujet est le *problème inverse de Galois* : *Est-il vrai que tout groupe fini est un groupe de Galois sur* $\mathbf{Q}$ *?* C'est facile pour un groupe abélien, c'est connu pour beaucoup de groupes (en particulier pour $\mathfrak{S}_n$ et $\mathfrak{A}_n$), mais pas encore pour tous.

Références

[1] D.S. Dummit & R.M. Foote – *Abstract Algebra*, Prentice Hall 1991, 1999.

[2] D. Duverney – *Théorie des Nombres, cours et exercices corrigés*, Dunod, 2è cycle, 1998.

[3] G. H. ; Hardy & E. M. Wright – *An introduction to the theory of numbers*. Fifth edition. Oxford University Press, 1979.

[4] S. Lang – *Algèbre*, Dunod, 2004.

Université P. et M. Curie (Paris VI),
Deuxième semestre 2006/2007

Michel Waldschmidt
date de mise à jour: 24/04/2007

Master de sciences et technologies 1ère année -
Spécialité : Mathématiques Fondamentales

Mention : Mathématiques et applications
MO11 : Théorie des nombres (12 ECTS)

Deuxième partie : Corps finis

Fascicule 4 : Chapitre 2, sections 2.1 à 2.5 (8 pages) [3]

2 Corps finis

2.1 Structure des corps finis

Soit K un corps fini ayant q éléments. La caractéristique de K est alors un nombre premier p, le sous-corps premier est (isomorphe à) $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ et K est une extension finie de $\mathbf{F}_p$. Si on pose $s = [\mathbf{F}_p : \mathbf{F}]$, alors $q = p^s$.

Le groupe multiplicatif de K est d'ordre $q-1$, tout élément de K vérifie $x^q = x$ et par conséquent K est l'ensemble des racines du polynôme $X^q - X$:

$$X^q - X = \prod_{x \in K} (X - x),$$

tandis que $K^\times$ est l'ensemble des racines du polynôme $X^{q-1} - 1$:

$$X^{q-1} - 1 = \prod_{x \in K^\times} (X - x).$$

Soit K un corps de caractéristique finie p. Pour x et y dans K on a $(x+y)^p = x^p + y^p$. Il en résulte que l'application

$$\begin{array}{rccc} F : & K & \to & K \\ & x & \mapsto & x^p \end{array}$$

est un automorphisme du corps K ; on l'appelle le *Frobenius* de K. Si ℓ est un entier ≥ 0, on désigne par F^ℓ l'automorphisme composé

$$F^0 = I, \quad F^\ell = F^{\ell-1} \circ F \qquad (\ell \geq 1),$$

de sorte que $F^\ell(x) = x^{p^\ell}$ pour $x \in K$. Si K est fini avec p^s éléments alors $F^s = I$.

Tout sous-groupe fini du groupe multiplicatif d'un corps est cyclique. En particulier si K est fini avec $q = p^s$ éléments alors le groupe multiplicatif $K^\times$ de K est cyclique d'ordre $q-1$. Si α un générateur de $K^\times$ on a $F^\ell(\alpha) \neq 1$ pour $1 \leq \ell < s$ donc F est d'ordre s dans le groupe des

[3] Ce texte est téléchargeable à partir de la page http ://www.math.jussieu.fr/∼miw/enseignement.html

automorphismes de K. Il en résulte que l'extension $K/\mathbf{F}_p$ est galoisienne, de groupe de Galois le groupe cyclique d'ordre s engendré par F. On en déduit aussi que si K est un corps fini, tout polynôme de $K[X]$ est séparable : *tout corps fini est parfait.*

En passant nous pouvons compléter la démonstration du corollaire 1.21 :

Proposition 2.1. *Si k est un corps fini et K une extension finie de k, alors l'extension K/k est monogène.*

Démonstration de la proposition 2.1. Soit $q = p^s$ le nombre d'éléments de K ; le groupe multiplicatif $K^\times$ est cyclique : soit α un générateur de ce groupe. Alors

$$K = \{0, 1, \alpha, \alpha^2, \dots, \alpha^{q-2}\} = \mathbf{F}_p(\alpha),$$

et à plus forte raison $K = k(\alpha)$.

□

2.2 Construction des corps finis et théorie de Galois

Théorème 2.2. *Soient p un nombre premier et s un entier positif. On pose $q = p^s$. Il existe un corps ayant q éléments. Deux corps ayant q éléments sont isomorphes. Si Ω est un corps algébriquement clos de caractéristique p, alors Ω contient un unique sous-corps fini ayant q éléments,*

Démonstration. Soit K un corps de décomposition sur $\mathbf{F}_p$ du polynôme $X^q - X$. Alors K est l'ensemble des racines de ce polynôme et donc a q éléments.

Inversement, si K est un corps avec q éléments, alors K est l'ensemble des racines du polynôme $X^q - X$.

Par conséquent si Ω est un corps algébriquement clos de caractéristique p, alors le seul sous-corps de Ω ayant q éléments est l'ensemble des racines du polynôme $X^q - X$.

□

Notons $\overline{\mathbf{F}}_p$ une clôture algébrique de $\mathbf{F}_p$. Pour chaque entier $s \geq 1$ il existe un unique sous-corps fini de $\overline{\mathbf{F}}_p$ ayant p^s éléments : c'est l'ensemble des racines du polynôme $X^{p^s} - X$. On le note $\mathbf{F}_{p^s}$. Pour n et m entiers positifs, on a l'équivalence

$$\mathbf{F}_{p^n} \subset \mathbf{F}_{p^m} \iff n \text{ divise } m; \tag{2.3}$$

si ces conditions sont vérifiées, alors l'extension $\mathbf{F}_{p^m}/\mathbf{F}_{p^n}$ est cyclique, de groupe de Galois le groupe cyclique d'ordre m/n engendré par F^n.

Exercice. Soient K un corps, m et n deux entiers ≥ 1, a et b deux entiers ≥ 2. Vérifier que les conditions suivantes sont équivalentes.
(i) n divise m
(ii) Dans $K[X]$ le polynôme $X^n - 1$ divise $X^m - 1$
(iii) $a^n - 1$ divise $a^m - 1$.
(ii') Dans $K[X]$ le polynôme $X^{a^n} - X$ divise $X^{a^m} - X$
(iii') $b^{a^n} - b$ divise $b^{a^m} - b$.

`Indication.` *Si r est le reste de la division de m par n, alors $a^r - 1$ est le reste de la division de $a^m - 1$ par $a^n - 1$.*

Lemme 2.4. *Soient K un corps de caractéristique p et f un élément de $K[X]$. Alors $f \in \mathbf{F}_p[X]$ si et seulement si $f(X)^p = f(X^p)$.*

Démonstration. Nous avons vu au § 2.1 que, pour a dans K, on a $a^p = a$ si et seulement si $a \in \mathbf{F}_p$. Comme K est de caractéristique p, si on écrit

$$f(X) = a_0 + a_1 X + \cdots + a_n X^n,$$

on a

$$f(X)^p = a_0^p + a_1^p X^p + \cdots + a_n^p X^{np}.$$

Par conséquent $f(X)^p = f(X^p)$ si et seulement si $a_i^p = a_i$ pour tout $i = 0, 1, \ldots, n$.

□

Proposition 2.5. *Soient K un corps de caractéristique finie p, α un élément non nul de K algébrique sur $\mathbf{F}_p$. Il existe des entiers $s \geq 1$ tels que $\alpha^{p^s} = \alpha$. Notons r le plus petit. Alors le corps $\mathbf{F}_p(\alpha)$ a p^r éléments et le polynôme irréductible de α sur $\mathbf{F}_p$ est*

$$\prod_{i=0}^{r-1} (X - \alpha^{p^i}). \tag{2.6}$$

Démonstration. L'extension $\mathbf{F}_p(\alpha)/\mathbf{F}_p$ est finie, donc le corps $\mathbf{F}_p(\alpha)$ est fini : soit p^s son nombre d'éléments. Soit m l'ordre de α dans le groupe multiplicatif $\mathbf{F}_p(\alpha)^\times$. Comme ce groupe est d'ordre $p^s - 1$, on a $p^s \equiv 1 \pmod{m}$. Donc $\alpha^{p^s - 1} = 1$ et $\alpha^{p^s} = \alpha$.

Soit f le polynôme irréductible de α sur $\mathbf{F}_p$. On a $f(X^p) = f(X)^p$ car $f \in \mathbf{F}_p[X]$, donc l'ensemble des racines de f est stable sous le Frobenius $F : x \mapsto x^p$.

Il en résulte que f est multiple du polynôme g défini par (2.6). Mais ce polynôme g appartient à $\mathbf{F}_p[X]$ car $g(X^p) = g(X)^p$. Par conséquent $g = f$. Ainsi f est de degré r, donc $[\mathbf{F}_p(\alpha) : \mathbf{F}_p] = r$, par conséquent $\mathbf{F}_p(\alpha)$ a p^r éléments. On en déduit aussi $r = s$.

□

Proposition 2.7. *Soient p un nombre premier et r un entier positif. Le polynôme $X^{p^r} - X$ est le produit de tous les polynômes unitaires irréductibles de $\mathbf{F}_p[X]$ dont le degré divise r.*

Démonstration. Soit $f \in \mathbf{F}_p[X]$ un polynôme irréductible de degré d. Notons $K = \mathbf{F}_p[X]/(f)$ son corps de rupture sur K : c'est une extension de degré d de K, il a donc p^d éléments, la classe α de X vérifie $\alpha^{p^d} = \alpha$, donc le polynôme $X^{p^d} - X$ est multiple de f.

Si d divise r, alors le polynôme $X^{p^r} - X$ est multiple de $X^{p^d} - X$, donc multiple de f. Ceci montre que $X^{p^r} - X$ est multiple de tous les polynômes irréductibles de degré divisant r. Comme sa dérivée est -1, il n'a pas de facteur multiple.

Réciproquement si le polynôme $X^{p^r} - X$ est multiple de f, on a $\alpha^{p^r} = \alpha$ dans K, l'ensemble des $\alpha \in K$ qui vérifient $\alpha^{p^r} = \alpha$ est K lui-même et tout générateur γ du groupe multiplicatif $K^\times$, qui est d'ordre $p^d - 1$, satisfait $\gamma^{p^r - 1} = 1$. Il en résulte que $p^d - 1$ divise $p^r - 1$, donc d divise r.

□

2.3 Décomposition des polynômes cyclotomiques en facteurs irréductibles

Théorème 2.8. *Soient $\mathbf{F}_q$ un corps fini à q éléments et n un entier premier avec q. On désigne par d l'ordre de q modulo n. Alors tous les facteurs irréductibles du polynôme Φ_n dans $\mathbf{F}_q[X]$ sont de degré d.*

Démonstration. Soient p la caractéristique de K, $\overline{\mathbf{F}}_p$ une clôture algébrique de $\mathbf{F}_q$, P un facteur irréductible de Φ_n dans $\mathbf{F}_q[X]$, s son degré et $\mathbf{F}_{q^s}$ le sous-corps de $\overline{\mathbf{F}}_p$ ayant q^s éléments. Le corps $\mathbf{F}_{q^s}$ est donc un corps de rupture de P sur $\mathbf{F}_q$. Soit ζ une racine de P dans K. Comme ζ est racine de P et que P est facteur de Φ_n on a $\Phi_n(\zeta) = 0$, donc ζ est une racine primitive n-ième de l'unité.

D'un côté le fait que ζ soit dans $\mathbf{F}_{q^s}^\times$ implique $\zeta^{q^s-1} = 1$. Il en résulte que n divise $q^s - 1$, donc $q^s \equiv 1 \pmod{n}$ et par conséquent d divise s.

D'un autre côté comme $q^d \equiv 1 \pmod{n}$ et que $\zeta^n = 1$ on a $\zeta^{q^d} = \zeta$, donc ζ appartient au sous-corps $\mathbf{F}_{q^d}$ à q^d éléments de $\overline{\mathbf{F}}_p$. Comme $\mathbf{F}_{q^s} = \mathbf{F}_q(\zeta)$ on a $\mathbf{F}_{q^s} \subset \mathbf{F}_{q^d}$, donc (2.3) s divise d. □

Pour $d = 1$ cela signifie que si $\mathbf{F}_q$ un corps fini à q éléments et n un entier premier avec q, le polynôme cyclotomique Φ_n est complètement décomposé dans $\mathbf{F}_q$ si et seulement si $q \equiv 1 \pmod{n}$. On le voit directement puisque $\mathbf{F}_q^\times$ est cyclique d'ordre $q - 1$.

L'autre cas extrême est $d = \varphi(n)$:

Corollaire 2.9. *Soient $\mathbf{F}_q$ un corps fini et n un entier premier avec q. Le polynôme Φ_n est irréductible sur $\mathbf{F}_q$ si et seulement si la classe de q modulo n est un générateur de $(\mathbf{Z}/n\mathbf{Z})^\times$.*

Bien entendu cela ne peut arriver que si le groupe $((\mathbf{Z}/n\mathbf{Z})^\times$ est cyclique.

Voici un troisième exemple d'application du théorème 2.8 :

Corollaire 2.10. *Soient $\mathbf{F}_q$ un corps fini et m un entier positif. Le polynôme Φ_{q^m-1} se décompose en produit de polynômes irréductibles sur $\mathbf{F}_q$ qui sont tous de degré m.*

2.4 Loi de réciprocité quadratique

Soit p un nombre premier. Un élément α du corps $\mathbf{F}_p$ est appelé *résidu quadratique* si l'équation $X^2 - \alpha$ a une racine dans $\mathbf{F}_p$, on dit qu'il est *non résidu quadratique* sinon, c'est-à-dire si ce polynôme $X^2 - \alpha$ est irréductible sur $\mathbf{F}_p$. On dit qu'un entier $a \in \mathbf{Z}$ est *résidu quadratique modulo p* si sa classe $\alpha \in \mathbf{Z}/p\mathbf{Z}$ modulo p l'est, *non résidu modulo p* dans le cas contraire. En notant α la classe de a modulo p on définit le *symbole de Legendre* par

$$\left(\frac{\alpha}{p}\right) = \left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } \alpha = 0 \\ 1 & \text{si } \alpha \text{ est résidu quadratique} \\ -1 & \text{si } \alpha \text{ est non résidu quadratique.} \end{cases}$$

Supposons p impair. L'application $x \mapsto x^2$ est un endomorphisme du groupe $\mathbf{F}_p^\times$, de noyau $\{-1, +1\}$. L'image de cette application a donc $(p-1)/2$ éléments, ce qui veut dire qu'il y a $(p-1)/2$ éléments qui sont des résidus quadratiques non nuls dans $\mathbf{F}_p$ et il y en a autant qui ne sont pas résidus quadratiques. On en déduit

$$\sum_{\alpha \in \mathbf{F}_p} \left(\frac{\alpha}{p}\right) = 0. \tag{2.11}$$

Si $\zeta \in \mathbf{F}_p$ est une *racine primitive modulo* p (c'est-à-dire un générateur de $\mathbf{F}_p^\times$, ou encore une racine primitive $p-1$-ième de l'unité), alors les résidus quadratiques moduio p sont les éléments ζ^k de $\mathbf{F}_p^\times$ avec $0 \leq k \leq p-3$ et k pair, tandis que les non résidus quadratiques sont les ζ^k avec $1 \leq k \leq p-2$ et k impair. En particulier

$$\left(\frac{\zeta}{p}\right) = -1$$

et (*théorème de Wilson*)

$$(p-1)! \equiv \prod_{k=1}^{p-1} \zeta^k \equiv \zeta^{p(p-1)/2} \equiv \zeta^{(p-1)/2} \equiv \left(\frac{\zeta}{p}\right) \equiv -1 \pmod{p}.$$

Les résidus quadratiques dans $\mathbf{F}_p^\times$ sont les racines du polynôme $X^{(p-1)/2} - 1$. Par conséquent pour $\alpha \in \mathbf{F}_p$ on a

$$\left(\frac{\alpha}{p}\right) = \alpha^{(p-1)/2}. \tag{2.12}$$

Par exemple

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{si } p \equiv 1 \pmod 4 \\ -1 & \text{si } p \equiv -1 \pmod 4. \end{cases}$$

Lemme 2.13. *Pour α et β dans $\mathbf{F}_p$ on a*

$$\left(\frac{\alpha\beta}{p}\right) = \left(\frac{\alpha}{p}\right)\left(\frac{\beta}{p}\right).$$

De plus

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \textit{si } p \equiv \pm 1 \pmod 8 \\ -1 & \textit{si } p \equiv \pm 3 \pmod 8. \end{cases}$$

Démonstration. La relation (2.12) montre que l'application

$$\alpha \longmapsto \left(\frac{\alpha}{p}\right)$$

est un homomorphisme du groupe multiplicatif $\mathbf{F}_p^\times$ sur le groupe à deux éléments $\{-1, +1\}$. Le noyau est d'ailleurs constitué des résidus quadratiques dans $\mathbf{F}_p^\times$.

Pour savoir si 2 est résidu quadratique modulo p, on doit déterminer si le polynôme $X^2 - 2$ est réductible ou non dans $\mathbf{F}_p[X]$. Soit $\overline{\mathbf{F}}_p$ une clôture algébrique de $\mathbf{F}_p$ et soit $\mathbf{F}_{p^2}$ le sous-corps de $\mathbf{F}_p$ ayant p^2 éléments. Comme $p^2 - 1$ est multiple de 8 il existe une racine primitive 8-ième de l'unité $\alpha \in \mathbf{F}_{p^2}$. Posons $\beta = \alpha + \alpha^{-1}$. On a $\alpha^4 = -1$ et $\alpha^2 = -\alpha^{-2}$, donc

$$\beta^2 = (\alpha + \alpha^{-1})^2 = \alpha^2 + \alpha^{-2} + 2 = 2.$$

Il s'agit maintenant de savoir si β est ou non dans $\mathbf{F}_p^\times$, c'est-à dire si β^p est égal à β ou à $-\beta$.

Si $p \equiv \pm 1 \mod 8$, alors $\{\alpha^p, \alpha^{-p}\} = \{\alpha, \alpha^{-1}\}$, donc $\beta^p = \beta$ et $\beta \in \mathbf{F}_p$, ce qui donne

$$\left(\frac{2}{p}\right) = 1.$$

Si $p \equiv \pm 3 \mod 8$, alors $\{\alpha^p, \alpha^{-p}\} = \{-\alpha, -\alpha^{-1}\}$, donc $\beta^p = -\beta$ et $\beta \notin \mathbf{F}_p$, d'où on conclut

$$\left(\frac{2}{p}\right) = -1.$$

□

Voici l'énoncé de la loi de réciprocité quadratique :

Théorème 2.14. *Soient p et ℓ des nombres premiers impairs distincts. Alors*

$$\left(\frac{\ell}{p}\right)\left(\frac{p}{\ell}\right) = (-1)^{\frac{p-1}{2}\frac{\ell-1}{2}}. \tag{2.15}$$

Il existe un grand nombre de démonstrations de cet énoncé, les premières ayant été données par C.F. Gauss. En voici une qui repose sur l'utilisation des *sommes de Gauss* qui sont définies de la façon suivante : soit K un corps contenant une racine primitive p-ième de l'unité ζ (c'est-à-dire un élément d'ordre p dans $K^\times$). On pose

$$S = \sum_{a=0}^{p-1} \left(\frac{a}{p}\right) \zeta^a.$$

Démonstration du théorème 2.14. Comme ζ^a ne dépend que de la classe de a modulo p et que le symbole de Legendre $\left(\frac{a}{p}\right)$ est nul pour $a = 0$, on peut écrire

$$S = \sum_{\alpha \in \mathbf{F}_p^\times} \left(\frac{\alpha}{p}\right) \zeta^\alpha.$$

Soit $\alpha \in \mathbf{F}_p^\times$. L'application $\beta \mapsto \alpha\beta$ est une bijection du groupe $\mathbf{F}_p^\times$ sur lui même, donc

$$S = \sum_{\beta \in \mathbf{F}_p^\times} \left(\frac{\alpha\beta}{p}\right) \zeta^{\alpha\beta}.$$

Comme

$$\left(\frac{\alpha}{p}\right)\left(\frac{\alpha\beta}{p}\right) = \left(\frac{\alpha^2\beta}{p}\right) = \left(\frac{\beta}{p}\right)$$

on obtient

$$S^2 = \sum_{a=0}^{p-1} \left(\frac{a}{p}\right) \zeta^a \sum_{\beta \in \mathbf{F}_p^\times} \left(\frac{\alpha\beta}{p}\right) \zeta^{\alpha\beta} = \sum_{\beta \in \mathbf{F}_p^\times} \left(\frac{\beta}{p}\right) \sum_{\alpha \in \mathbf{F}_p^\times} \zeta^{\alpha(1+\beta)}.$$

La somme des racines du polynôme $X^p - 1$ est nulle, donc

$$\sum_{\gamma \in \mathbf{F}_p} \zeta^\gamma = 0 \qquad \text{et} \qquad \sum_{\gamma \in \mathbf{F}_p^\times} \zeta^\gamma = -1.$$

En utilisant (2.11) on en déduit

$$\sum_{\alpha \in \mathbf{F}_p^\times} \zeta^{\alpha(1+\beta)} = \begin{cases} p-1 & \text{si } \beta = -1 \\ -1 & \text{si } \beta \neq -1. \end{cases}$$

Ainsi

$$S^2 = (p-1)\left(\frac{-1}{p}\right) - \sum_{\substack{\beta \in \mathbf{F}_p^\times \\ \beta \neq -1}} \left(\frac{\beta}{p}\right) = p\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} p.$$

Choisissons maintenant pour K une clôture algébrique $\overline{\mathbf{F}}_\ell$ de $\mathbf{F}_\ell$. On a dans $\overline{\mathbf{F}}_\ell$

$$S^\ell = \sum_{\alpha \in \mathbf{F}_p^\times} \left(\frac{\alpha}{p}\right) \zeta^{\ell\alpha} = \left(\frac{\ell}{p}\right) \sum_{\alpha \in \mathbf{F}_p^\times} \left(\frac{\ell\alpha}{p}\right) \zeta^{\ell\alpha} = \left(\frac{\ell}{p}\right) S,$$

donc

$$S^{\ell-1} = \left(\frac{\ell}{p}\right).$$

Alors

$$\left(\frac{\ell}{p}\right) = S^{\ell-1} = (S^2)^{(\ell-1)/2} = (-1)^{\frac{p-1}{2}\frac{\ell-1}{2}} p^{(\ell-1)/2} = (-1)^{\frac{p-1}{2}\frac{\ell-1}{2}} \left(\frac{p}{\ell}\right).$$

Ceci démontre la relation (2.15).

□

2.5 Factorisation dans $\mathbf{F}_p[X]$

Soit $f \in \mathbf{Z}[X]$ un polynôme unitaire. Une des méthodes efficaces pour factoriser f en produit de polynômes irréductibles consiste à étudier sa réduction modulo p pour différentes valeurs de p premier. Si, pour un nombre premier p, la réduction modulo p de f est irréductible dans $\mathbf{F}_p[X]$, alors f lui-même est irréductible.

Un critère d'irréductibilité pour un polynôme de $\mathbf{F}_p[X]$ est donné par la proposition suivante :

Proposition 2.16. *Soient p un nombre premier, $A \in \mathbf{F}_p[X]$ un polynôme unitaire non nul et $m \geq 1$ un entier positif. Les deux conditions suivantes sont équivalentes.*
(i) A est produit de polynômes unitaires irréductibles sur $\mathbf{F}_p$ deux-à-deux distincts de degré m.
(ii) $A(X)$ divise $X^{p^m} - X$ et pour tout diviseur premier ℓ de m,

$$\operatorname{pgcd}\big(X^{p^{m/\ell}} - X, A(X)\big) = 1.$$

Démonstration. La proposition 2.7 montre qu'un polynôme unitaire dans $\mathbf{F}_p[X]$ divise $X^{p^m} - X$ si et seulement s'il est produit de facteurs irréductibles unitaires deux-à-deux distincts de degrés divisant m. La condition *(ii)* revient à dire qu'aucun de ces facteurs n'a un degré divisant strictement m.

□

Le critère de Berlekamp permet non seulement de décider si un polynôme de $\mathbf{F}_p[X]$ est irréductible, mais aussi de disposer d'un algorithme pour le factoriser.

Proposition 2.17. *Soient p un nombre premier et $A \in \mathbf{F}_p[X]$ un polynôme unitaire sans facteurs carrés. On écrit sa décomposition en facteurs irréductibles dans $\mathbf{F}_p[X]$:*

$$A = A_1 \cdots A_r$$

où les polynômes A_i sont unitaires et irréductibles dans $\mathbf{F}_p[X]$, deux-à-deux distincts. Soit $Q \in \mathbf{F}_p[X]$. Alors les deux conditions suivantes sont équivalentes :
(i)

$$Q(X)^p \equiv Q(X) \pmod{A(X)}.$$

(ii) Pour tout $i = 1, \ldots, r$, il existe $\alpha_i \in \mathbf{F}_p$ tel que

$$Q(X) \equiv \alpha_i \pmod{A_i(X)}.$$

De plus il existe p^r polynômes satisfaisant ces conditions qui sont soit le polynôme nul, soit de degré $< \deg A$.

Démonstration. Pour $1 \leq i \leq r$ le quotient K_i de $\mathbf{F}_p[X]$ par l'idéal principal (A_i) est un corps et l'anneau quotient $\mathbf{F}_p[X]/(A)$ est isomorphe au produit $K_1 \times \cdots \times K_r$ (ces deux anneaux ont p^d éléments, d désignant le degré de A). Un tel isomorphisme Ψ est

$$P \pmod{A} \longmapsto \big(P \pmod{A_i}\big)_{1 \leq i \leq r}.$$

Dans chaque K_i le polynôme $X^p - X$ a p racines, à savoir les p éléments du sous-corps premier $\mathbf{F}_p$. Donc l'équation

$$(x_1^p, \ldots, x_r^p) = (x_1, \ldots, x_r)$$

a p^r solutions dans $K_1 \times \cdots \times K_r$. Ces solutions sont les images par Ψ des classes modulo A des polynômes $Q \in \mathbf{F}_p[X]$ satisfaisant $Q^p \equiv Q \pmod{A}$.

□

Exercice. Sous les hypothèses de la proposition 2.17, on désigne par R l'anneau quotient $\mathbf{F}_p[X]/A(X)\mathbf{F}_p[X]$, par $S : R \to R$ l'endomorphisme $Q \mapsto Q^p$ du $\mathbf{F}_p$-espace vectoriel R et on pose $N = \ker(S - I)$. Quelle est la dimension du $\mathbf{F}_p$-espace vectoriel N ?

On suppose $r \geq 2$. Soit $Q \in N$. Vérifier

$$A = \prod_{\alpha \in \mathbf{F}_p} \operatorname{pgcd}(A, Q - \alpha).$$

Montrer que si Q n'est pas dans $\mathbf{F}_p$, alors il existe $\alpha \in \mathbf{F}_p$ tel que $\operatorname{pgcd}(A, Q - \alpha)$ soit différent de 1 et de A.

Références

[1] M. Demazure – *Cours d'algèbre. Primalité. Divisibilité. Codes*, Nouvelle Bibliothèque Mathématique Cassini, Paris, 1997.

Université P. et M. Curie (Paris VI),
Deuxième semestre 2006/2007

Michel Waldschmidt
date de mise à jour: 24/04/2007

Master de sciences et technologies 1ère année - Mention : Mathématiques et applications
Spécialité : Mathématiques Fondamentales MO11 : Théorie des nombres (12 ECTS)

Troisième partie : Arithmétique des Corps de Nombres

Fascicule 5 : sections 3.1, 3.2 et 3.3 (10 pages)

3 Corps de Nombres

3.1 Norme, trace, discriminant

Rappelons que tous les anneaux considérés sont commutatifs et unitaires. Les éléments inversibles (on dit encore *les unités*) d'un anneau A forment un groupe multiplicatif noté $A^\times$.

Soient A un anneau, M un A-module libre de type fini et u un endomorphisme de M. On note $\mathrm{Tr}(u)$, $\mathrm{N}(u)$ et $P_u(X)$ la trace, la norme et le polynôme caractéristique de u respectivement. Dans une base $(e_1, \ldots, e_n)$ de M sur A, si $\mathsf{A} = \big(a_{ij}\big)_{1\le i,j\le n}$ désigne la matrice attachée à u, on a

$$\mathrm{Tr}(u) = \sum_{i=1}^{n} a_{ii} \quad \text{et} \quad \mathrm{N}(u) = \det(\mathsf{A}).$$

D'autre part en désignant par I l'endomorphisme identité de M on a

$$P_u(X) = \det(XI - u) = X^n - \mathrm{Tr}(u)X^{n-1} + \cdots + (-1)^n \mathrm{N}(u).$$

Quand u_1 et u_2 sont des endomorphismes de M on a

$$\mathrm{Tr}(u_1 + u_2) = \mathrm{Tr}(u_1) + \mathrm{Tr}(u_2) \quad \text{et} \quad \mathrm{N}(u_1 \circ u_2) = \mathrm{N}(u_1)\mathrm{N}(u_2).$$

Supposons de plus que M est un anneau - on le notera B. Soit donc B un anneau contenant A qui est un A-module libre de rang fini. Pour $x \in B$ l'application

$$[x] : \begin{array}{ccc} B & \longrightarrow & B \\ y & \longmapsto & xy \end{array}$$

est un endomorphisme du A-module B et l'application $x \mapsto [x]$ est un homomorphisme d'anneaux de B dans l'anneau des endomorphismes de B.
La norme, la trace et le polynôme caractéristique de $[x]$ sont appelés *norme*, *trace* et *polynôme caractéristique* de x de B sur A et notés respectivement

$$\mathrm{N}_{B/A}(x), \quad \mathrm{Tr}_{B/A}(x) \quad \text{et} \quad P_{B/A}(x; X).$$

On a donc, pour x et y dans B,

$$\mathrm{N}_{B/A}(xy) = \mathrm{N}_{B/A}(x)\mathrm{N}_{B/A}(y) \tag{3.1}$$

et

$$\mathrm{Tr}_{B/A}(x+y) = \mathrm{Tr}_{B/A}(x) + \mathrm{Tr}_{B/A}(y).$$

Soit L/K une extension finie de corps et soit $m = [L : K]$ son degré. La norme de L sur K définit un homomorphisme du groupe multiplicatif $L^\times$ de L dans le groupe multiplicatif $K^\times$ de K et la trace un homomorphisme du groupe additif L dans le groupe additif K.

Lemme 3.2. *Soit L/K une extension séparable de degré n. Soit N une extension finie de L, normale sur K et soient $\sigma_1, \dots, \sigma_n$ les différents K-isomorphismes de L dans N. Alors pour $\alpha \in L$ on a*

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha), \quad \mathrm{N}_{L/K}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$$

et

$$P_{L/K}(\alpha; X) = \prod_{i=1}^{n} \big(X - \sigma_i(\alpha)\big).$$

Démonstration. Soit d le degré de α sur K et

$$P(X) = X^d + a_1 X^{d-1} + \cdots + a_d \in K[X]$$

son polynôme irréductible sur K. Supposons dans un premier temps que α est un élément primitif de l'extension L/K, c'est-à-dire que $L = K(\alpha)$ ou encore que $d = n$. Quand on prend $\{1, \alpha, \dots, \alpha^{d-1}\}$ comme base de L sur K, la matrice associée à l'endomorphisme $[\alpha]$ est

$$M_\alpha = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_d \\ 1 & 0 & \cdots & 0 & -a_{d-1} \\ 0 & 1 & \cdots & 0 & -a_{d-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_1 \end{pmatrix}.$$

Par conséquent le polynôme caractéristique de $[\alpha]$ est le polynôme irréductible de α sur K. Le fait qu'il s'écrive

$$\prod_{i=1}^{d} \big(X - \sigma_i(\alpha)\big)$$

provient du Théorème 1.19.

Dans le cas général on note $d = [K(\alpha) : K]$ et $m = [L : K(\alpha)]$, de sorte que $n = md$ et on prend une base $(e_1, \dots, e_m)$ de L sur $K(\alpha)$. Dans la base $\{e_i \alpha^j \, ; 1 \le i \le m, \ 0 \le j < d\}$ de L sur K la matrice de $[\alpha]$ s'écrit comme un bloc diagonal $\mathrm{diag}\big(M_\alpha, \dots, M_\alpha\big)$. Donc

$$P_{L/K}(\alpha; X) = P(X)^m,$$

$$\mathrm{Tr}_{L/K}(\alpha) = m\mathrm{Tr}_{K(\alpha)/K}(\alpha), \qquad \mathrm{N}_{L/K}(\alpha) = \big(\mathrm{N}_{K(\alpha)/K}(\alpha)\big)^m.$$

Enfin la suite $(\sigma_1(\alpha), \dots, \sigma_n(\alpha))$ est formée des d conjugués de α sur K, chacun étant répété m fois. □

Lemme 3.3. *Soit L/K une extension finie séparable. L'application*

$$\begin{array}{ccc} L \times L & \to & K \\ (x,y) & \mapsto & \mathrm{Tr}_{L/K}(xy) \end{array}$$

est une forme bilinéaire symétrique non dégénérée sur L.

Il en résulte que l'application qui à $x \in L$ associe $y \mapsto \mathrm{Tr}_{L/K}(xy)$ est un isomorphisme du K-espace vectoriel L sur son dual $\mathrm{Hom}_K(L,K)$.

Démonstration du lemme 3.3. Que ce soit une forme bilinéaire symétrique est clair. Dire qu'elle est non dégénérée signifie que si $x \in L$ est tel que $\mathrm{Tr}_{L/K}(xy) = 0$ pour tout $y \in L$, alors $x = 0$. Cela résulte du lemme 3.4 suivant. □

Lemme 3.4 (Lemme de Dedekind sur l'indépendance linéaire des caractères). *Soient G un groupe, k un corps, $\sigma_1, \ldots, \sigma_n$ des homomorphisms deux-à-deux distincts de G dans le groupe multiplicatif $k^\times$. Alors $\sigma_1, \ldots, \sigma_n$ sont linéairement indépendants sur k dans l'espace vectoriel k^G.*

Démonstration. On démontre le résultat par récurrence sur n. Pour $n = 1$ il est trivial. Supposons $n \geq 2$. Soient $a_1, \ldots, a_n$ des éléments de k tels que

$$\sum_{i=1}^{n} a_i \sigma_i(x) = 0 \quad \text{pour tout } x \in G.$$

Alors pour tout $x \in G$ et tout $y \in G$ on a

$$\sum_{i=1}^{n} a_i \sigma_i(x) \sigma_i(y) = 0.$$

Comme $\sigma_n \neq \sigma_1$ il existe $y \in G$ tel que $\sigma_n(y) \neq \sigma_1(y)$. En utilisant la relation

$$\sum_{i=2}^{n} a_i \big(\sigma_i(y) - \sigma_1(y)\big) \sigma_i(x) = 0$$

avec l'hypothèse de récurrence, on en déduit $a_n = 0$, puis $a_1 = \ldots = a_n = 0$. □

Remarque. Sous l'hypothèse supplémentaire que la caractéristique de K est soit nulle, soit première avec $[L : K]$, le fait que la forme bilinéaire $(x,y) \mapsto \mathrm{Tr}_{L/K}(xy)$ soit non dégénérée se déduit aussi de la relation

$$\mathrm{Tr}_{L/K}(\alpha^n) + a_1 \mathrm{Tr}_{L/K}(\alpha^{n-1}) + \cdots + a_{n-1} \mathrm{Tr}_{L/K}(\alpha) + a_n [L : K] = 0$$

quand le polynôme irréductible de α sur K est $X^n + a_1 X^{n-1} + \cdots + a_{n-1} X + a_n \in K[X]$: comme $a_n \neq 0$, l'un des nombres $\mathrm{Tr}_{L/K}(\alpha^i)$, $(1 \leq i \leq n)$ n'est pas nul.

Définition. Soient $A \subset B$ deux anneaux. On suppose que B est un A-module libre de rang n. On définit une application $D_{B/A} : B^n \to A$ appelée *discriminant de B sur A* par

$$D_{B/A}(x_1, \ldots, x_n) = \det\big(\mathrm{Tr}_{B/A}(x_i x_j)\big)_{1 \leq i,j \leq n}.$$

Lemme 3.5. *Soient* $\mathsf{A} = \big(a_{ij}\big)_{1\leq i,j\leq n}$ *une matrice* $n \times n$ *à coefficients dans* A*. On pose*

$$y_j = \sum_{i=1}^{n} a_{ij}x_i, \quad (1 \leq j \leq n).$$

Alors

$$D_{B/A}(y_1, \ldots, y_n) = (\det \mathsf{A})^2 D_{B/A}(x_1, \ldots, x_n)$$

Démonstration. Cela résulte du fait que l'application $(x, y) \mapsto \mathrm{Tr}_{B/A}(xy)$ est bilinéaire. □

Donc si $x_1, \ldots, x_n$ sont linéairement dépendants sur A, alors $D_{B/A}(x_1, \ldots, x_n)$ est un diviseur de zéro dans A. En particulier si A est intègre alors $D_{B/A}(x_1, \ldots, x_n) = 0$ chaque fois que $x_1, \ldots, x_n$ sont liés sur A.

Si $\{x_1, \ldots, x_n\}$ et $\{y_1, \ldots, y_n\}$ sont deux bases de B comme A-module, alors la matrice de passage A est inversible, donc $\det \mathsf{A}$ est une unité de A. En particulier l'idéal de A engendré par le discriminant $D_{B/A}(x_1, \ldots, x_n)$ d'une base ne dépend pas de la base $\{x_1, \ldots, x_n\}$: on le note $\mathcal{D}_{B/A}$ et on l'appelle *idéal discriminant de* B *sur* A.

Si $A = \mathbf{Z}$ le déterminant $\det \mathsf{A}$ d'une matrice de passage entre deux bases de B sur $\mathbf{Z}$ est ± 1, donc son carré est $+1$ et le discriminant $D_{B/\mathbf{Z}}(x_1, \ldots, x_n)$ d'une base de B sur $\mathbf{Z}$ ne dépend pas de la base $\{x_1, \ldots, x_n\}$. C'est le *discriminant absolu* de B, que l'on note $\mathcal{D}_B$.

Lemme 3.6. *Soient* $A \subset B$ *deux anneaux ; on suppose que* B *est un* A*-module libre de rang* n *et que l'idéal* $\mathcal{D}_{B/A}$ *contient un élément qui n'est pas diviseur de* 0 *dans* A*. Soit* $(x_1, \ldots, x_n) \in B^n$*. Alors* $D_{B/A}(x_1, \ldots, x_n)$ *engendre l'idéal* $\mathcal{D}_{B/A}$ *si et seulement si* $\{x_1, \ldots, x_n\}$ *est une base de* B *comme* A*-module.*

Démonstration. Soit $\{e_1, \ldots, e_n\}$ une base de B sur A. On écrit $x_i = \sum_{j=1}^{n} a_{ij}e_j$ $(1 \leq i \leq n)$ et on note $d_x = D_{B/A}(x_1, \ldots, x_n)$, $d_e = D_{B/A}(e_1, \ldots, e_n)$ et $a = \det(a_{ij})$. D'après le lemme 3.5 on a $d_x = a^2 d_e$. Par hypothèse d_x et d_e engendrent le même idéal $\mathcal{D}_{B/A}$. Donc $d_x = ud_e$ avec $u \in A^\times$. Alors $(a^2 - u)d_e = 0$. Comme l'idéal principal $\mathcal{D}_{B/A}$ contient un élément qui n'est pas diviseur de zéro, aucun de ses générateurs n'est un diviseur de zéro, donc a^2 est inversible. Il en résulte que a est aussi une unité de A, donc la matrice (a_{ij}) est inversible, son inverse étant une matrice à coefficients dans A et par conséquent $\{x_1, \ldots, x_n\}$ est une base de B sur A.

□

Proposition 3.7. *Soit* L/K *une extension séparable de degré* n*, soit* N *une extension finie de* L*, normale sur* K *et soient* $\sigma_1, \ldots, \sigma_n$ *les différents* K*-isomorphismes de* L *dans* N*. Alors*

$$D_{L/K}(x_1, \ldots, x_n) = \Big(\det\big(\sigma_h(x_j)\big)_{1\leq h,j\leq n}\Big)^2.$$

De plus, si $(x_1, \ldots, x_n)$ *est une base de* L *sur* K*, alors*

$$D_{L/K}(x_1, \ldots, x_n) \neq 0.$$

Démonstration. On utilise le lemme 3.2 :

$$\mathrm{Tr}_{L/K}(x_i x_j) = \sum_{h=1}^{n} \sigma_h(x_i)\sigma_h(x_j).$$

Donc

$$D_{L/K}(x_1,\dots,x_n) = \det\big(\mathrm{Tr}_{L/K}(x_i x_j)\big) = \det\big(\sigma_h(x_i)\big)\det\big(\sigma_h(x_j)\big) = \big(\det(\sigma_h(x_j))\big)^2.$$

Pour compléter la démonstration il reste à voir que la matrice $\big(\sigma_h(x_j)\big)$ est régulière. Si $b_1,\dots,b_n$ sont des éléments de N tels que $b_1\sigma_1(x_j)+\cdots+b_n\sigma_n(x_j)=0$ pour $1\le j\le n$, alors $b_1\sigma_1(x)+\cdots+b_n\sigma_n(x)=0$ pour tout $x\in B$ et d'après le lemme 3.4 il en résulte $b_1=\cdots=b_n=0$. □

Soit P un polynôme non nul à coefficients dans un corps K et soit E une extension de K dans laquelle P est complètement décomposé :

$$P(X) = a_0\prod_{i=1}^{n}(X-x_i),$$

où n est le degré de P, a_0 son coefficient directeur et $x_i\in E$. On définit le *discriminant de P* par

$$D(P) = a_0^{n(n-1)}\prod_{1\le i<j\le n}(x_i-x_j)^2 = (-1)^{n(n-1)/2}a_0^{n(n-1)}\prod_{\substack{1\le i,j\le n,\\ i\ne j}}(x_i-x_j).$$

De la définition on déduit $D(P)=0$ si et seulement si P a au moins une racine multiple. La théorie de Galois §1.8 montre que $D(P)$ est un élément de K. De la proposition 3.7, on déduit que si $P\in K[X]$ est un polynôme unitaire irréductible de degré n et si $L=K(\alpha)$ est un corps de rupture de P sur K, avec $P(\alpha)=0$, alors

$$D(P) = D_{L/K}(1,\alpha,\dots,\alpha^{n-1}).$$

Exercice. Vérifier que le discriminant du polynôme aX^2+bX+c est b^2-4ac et que celui de X^3+pX+q est $-4p^3-27q^2$.

3.2 Entiers algébriques

Proposition 3.8. *Soient A un anneau intègre, K un corps contenant A et $\alpha\in K$. Les propriétés suivantes sont équivalentes :*
(i) α est racine d'un polynôme unitaire à coefficients dans A.
(ii) Le sous-anneau $A[\alpha]$ de K engendré par α sur A est un A-module de type fini.
(iii) $A[\alpha]$ est contenu dans un sous-anneau de K qui est de type fini comme A-module.

`Exemple :` Le sous-anneau de $\mathbf{C}$ engendré par $1/2$:

$$\mathbf{Z}[1/2] = \big\{a/2^n\ ;\ a\in\mathbf{Z},\ n\in\mathbf{Z}_{\ge 0}\big\}$$

n'est pas un $\mathbf{Z}$-module de type fini, alors que $\mathbf{Z}[i]=\mathbf{Z}+\mathbf{Z}i$ et $\mathbf{Z}[\sqrt{2}]=\mathbf{Z}+\mathbf{Z}\sqrt{2}$ sont des $\mathbf{Z}$-modules de type fini.

Démonstration. Supposons la propriété *(i)* vérifiée ; soit

$$X^n+a_1X^{n-1}+\cdots+a_{n-1}X+a_n\in A[X]$$

un polynôme unitaire à coefficients dans A ayant α comme racine. De la relation

$$\alpha^n = -a_1\alpha^{n-1} - \cdots - a_{n-1}\alpha - a_n$$

on déduit par récurrence sur m

$$\alpha^m \in A + A\alpha + \cdots + A\alpha^{n-1} \quad \text{pour tout } m \geq 1,$$

donc $A[\alpha] = A + A\alpha + \cdots + A\alpha^{n-1}$ et par conséquent l'anneau $A[\alpha]$ est un A-module de type fini.

L'implication *(ii)*⇒*(iii)* est triviale.

Supposons la propriété *(iii)* vérifiée. Soit B un sous anneau de K contenant $A[\alpha]$. On suppose que B est un A-module de type fini et on écrit $B = Ax_1 + \cdots + Ax_m$. Pour $1 \leq i \leq m$ le fait que αx_i appartienne à B entraîne qu'il existe des éléments a_{ij} de A $(1 \leq j \leq m)$ tels que

$$\alpha x_i = \sum_{j=1}^{m} a_{ij} x_j.$$

Posons $M = \left(a_{ij}\right)_{1 \leq i,j \leq m}$ et soit I la matrice identité $m \times m$. La matrice $\alpha I - M$ est associée à un endomorphisme de K^m dont le noyau contient $(x_1, \ldots, x_m)$. Soit $P \in A[X]$ le déterminant de la matrice $XI - M$. Alors P est un polynôme unitaire qui admet α comme racine. D'où *(i)*.

□

Définition. On dit que $\alpha \in K$ est *entier sur* A s'il vérifie les propriétés équivalentes de la proposition 3.8.

Par exemple si A est un corps, un élément de K est entier sur A si et seulement s'il est algébrique sur A.

Corollaire 3.9. *L'ensemble des éléments de K entiers sur A est un sous-anneau de K.*

Démonstration. Si α et β sont des éléments de K entiers sur A, alors l'anneau $A[\alpha, \beta]$ est un sous-A-module de type fini de K (un système générateur fini est formé d'éléments $\alpha^i\beta^j$), donc tous ses éléments sont entiers sur A.

□

Définition. L'ensemble des éléments de K qui sont entiers sur A est appelé la *fermeture intégrale de A dans K*.

De la proposition 3.8 on déduit que la relation d'intégralité est transitive :

Corollaire 3.10. *Soient K un corps, A un sous-anneau de K, A_0 la fermeture intégrale de A dans K et B un sous-anneau de A_0 contenant A. Alors la fermeture intégrale de B dans K est A_0.*

Définition. La *clôture intégrale* d'un anneau est la fermeture intégrale de cet anneau dans son corps des fractions.

La clôture intégrale de A est un anneau qui contient A et qui est contenu dans la fermeture intégrale de A dans K, pour tout corps K contenant A.

Définition. Un anneau est dit *intégralement clos* s'il est égal à sa clôture intégrale.

Un anneau factoriel est intégralement clos : en effet, si A est un anneau factoriel de corps des fractions K et si $\alpha \in K$ est racine d'un polynôme unitaire à coefficients dans A :

$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0,$$

on écrit $\alpha = p/q$ avec p et q dans A sans facteurs irréductibles communs et de la relation

$$p^n + a_1 p^{n-1} q + \cdots + a_n q^n = 0$$

on déduit que q divise p, donc que q est inversible et $\alpha \in A$.

En particulier un anneau principal est intégralement clos. On en déduit par exemple qu'un nombre rationnel qui est entier sur $\mathbf{Z}$ est dans $\mathbf{Z}$.

L'anneau $\mathbf{Z}[2i] = \mathbf{Z} + 2i\mathbf{Z}$ n'est pas intégralement clos, puisque son corps des fractions $\mathbf{Q}(i)$ contient i, qui est racine du polynôme $X^2 + 1$, donc est entier sur $\mathbf{Z}[2i]$, mais n'appartient pas à $\mathbf{Z}[2i]$.

Définition. On appelle *nombre algébrique* tout nombre complexe qui est algébrique sur $\mathbf{Q}$ et *entier algébrique* tout nombre complexe qui est entier sur $\mathbf{Z}$.

Si α est un nombre algébrique, dont le polynôme irréductible sur $\mathbf{Q}$ est

$$X^n + a_1 X^{n-1} + \cdots + a_n \in \mathbf{Q}[X],$$

l'unique polynôme irréductible de $\mathbf{Z}[X]$ qui s'annule au point α et dont le coefficient directeur soit positif est

$$dX^n + da_1 X^{n-1} + \cdots + da_n \in \mathbf{Z}[X], \tag{3.11}$$

où d est le plus petit commun multiple des dénominateurs des nombres $a_1, \ldots, a_n$. Nous appellerons ce polynôme (3.11) le *polynôme minimal de α sur $\mathbf{Z}$*.

Si α est un entier algébrique, alors les valeurs propres de $[\alpha]$ sont des entiers algébriques, donc le polynôme caractéristique de α sur $\mathbf{Z}$ est à coefficients dans $\mathbf{Z}$; en particulier $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$ et $\mathrm{Tr}_{K/\mathbf{Q}}(\alpha)$ sont dans $\mathbf{Z}$.

Le lemme de Gauss 1.24 montre que pour un nombre algébrique α les conditions suivantes sont équivalentes :
(i) α est entier (sur $\mathbf{Z}$)
(ii) Le polynôme minimal de α sur $\mathbf{Z}$ est unitaire.
(iii) Le polynôme irréductible de α sur $\mathbf{Q}$ a ses coefficients dans $\mathbf{Z}$.
(iv) Le polynôme minimal de α sur $\mathbf{Z}$ coïncide avec son polynôme irréductible sur $\mathbf{Q}$.

Quand on parle du polynôme irréductible ou du polynôme minimal d'un nombre algébrique, on omet souvent de préciser "sur $\mathbf{Q}$" et "sur $\mathbf{Z}$" respectivement.

Le corollaire 3.9 montre que les entiers algébriques forment un sous-anneau de $\mathbf{C}$, dont le corps des fractions est le corps $\overline{\mathbf{Q}}$ des nombres algébriques. Si α est un nombre algébrique, l'ensemble des entiers $d \in \mathbf{Z}$ tels que $d\alpha$ soit entier algébrique est un idéal non nul de $\mathbf{Z}$: il contient le coefficient directeur du polynôme minimal de α sur $\mathbf{Z}$.

On appelle *corps de nombres* une extension finie de $\mathbf{Q}$. D'après le théorème de l'élément primitif 1.21, un corps de nombres est un sous-corps de $\mathbf{C}$ de la forme $\mathbf{Q}(\alpha)$ avec α nombre algébrique. Le *degré* d'un corps de nombres est son degré sur $\mathbf{Q}$. Un *corps quadratique* est une extension de $\mathbf{Q}$ de

degré 2, un *corps cubique* une extension de $\mathbf{Q}$ de degré 3, un corps *biquadratique* une extension de degré 4...

L'*anneau des entiers* d'un corps de nombres K est l'intersection de K avec l'anneau des entiers algébriques. On le notera $\mathbf{Z}_K$. Le corps des fractions de $\mathbf{Z}_K$ est K.

Les éléments inversibles (*unités*) de l'anneau $\mathbf{Z}_K$ forment un groupe multiplicatif $\mathbf{Z}_K^\times$; ce sont les éléments de $\mathbf{Z}_K$ de norme ± 1.

Quand K est un corps de nombres, on utilise des expressions comme "unités de K", "idéaux de K", "discriminant de K" pour parler des unités, des idéaux ou du discriminant de l'anneau des entiers de K.

Définition. Soit α un nombre algébrique. On appelle *norme absolue* de α (resp. *trace absolue* de α) la norme (resp. la trace) $\mathrm{N}_{\mathbf{Q}(\alpha)/\mathbf{Q}}(\alpha)$ (resp. $\mathrm{Tr}_{\mathbf{Q}(\alpha)/\mathbf{Q}}(\alpha)$). On les note respectivement $\mathrm{N}(\alpha)$ et $\mathrm{Tr}(\alpha)$.

Du lemme 3.2 on déduit que si α est un nombre algébrique dont le polynôme irréductible sur $\mathbf{Q}$ est

$$P(X) = X^d + a_1 X^{d-1} + \cdots + a_d \in \mathbf{Q}[X],$$

alors

$$\mathrm{N}(\alpha) = (-1)^d a_d \quad \text{et} \quad \mathrm{Tr}(\alpha) = -a_1.$$

Plus généralement, si K est un corps de nombres de degré n sur $\mathbf{Q}$, α un élément de K, d le degré de α sur $\mathbf{Q}$ et $\alpha_1, \ldots, \alpha_d$ les conjugués de α dans $\mathbf{C}$, alors

$$\mathrm{N}_{K/\mathbf{Q}}(\alpha) = (\alpha_1 \cdots \alpha_d)^{n/d} \quad \text{et} \quad \mathrm{Tr}_{K/\mathbf{Q}}(\alpha) = \frac{n}{d}(\alpha_1 + \cdots + \alpha_d).$$

Soit k un corps quadratique. Il existe un entier $d \in \mathbf{Z}$ sans facteur carré tel que $k = \mathbf{Q}(\sqrt{d})$. Soit α un élément de k, alors α est racine du polynôme $X^2 - X\mathrm{Tr}_{k/\mathbf{Q}}(\alpha) + \mathrm{N}_{k/\mathbf{Q}}(\alpha)$, donc α est entier si et seulement si $\mathrm{Tr}_{k/\mathbf{Q}}(\alpha)$ et $\mathrm{N}_{k/\mathbf{Q}}(\alpha)$ sont dans $\mathbf{Z}$.

Soit $\alpha = x + y\sqrt{d} \in k$, avec x et y dans $\mathbf{Q}$. On a $\mathrm{Tr}_{k/\mathbf{Q}}(\alpha) = 2x$ et $\mathrm{N}_{k/\mathbf{Q}}(\alpha) = x^2 - dy^2$. Si α est entier, alors les nombres $a = 2x$ et $b = x^2 - dy^2$ sont dans $\mathbf{Z}$. Comme d n'est pas divisible par 4, le nombre $c = 2y$ est aussi dans $\mathbf{Z}$. Alors de la relation $a^2 - dc^2 = 4b$ on déduit que soit a et c sont pairs, soit a et c sont impairs et dans ce dernier cas $d \equiv 1 \pmod 4$. Par conséquent l'anneau $\mathbf{Z}_k$ des entiers de k est

$$\mathbf{Z}_k = \begin{cases} \mathbf{Z} + \mathbf{Z}\sqrt{d} & \text{si } d \equiv 2 \text{ ou } 3 \pmod 4 \\ \mathbf{Z} + \mathbf{Z}\dfrac{1+\sqrt{d}}{2} & \text{si } d \equiv 1 \pmod 4. \end{cases}$$

Ainsi $\mathbf{Z}_k = \mathbf{Z} + \mathbf{Z}\alpha$ où α est une des deux racines du polynôme $X^2 - d$ si $d \equiv 2$ ou $3 \pmod 4$, et l'une des deux racines du polynôme $X^2 - X - (d-1)/2$ si $d \equiv 1 \pmod 4$.

Le discriminant D_k de k est le discriminant $D_{\mathbf{Z}_k}$ de l'anneau des entiers de k :

$$D_k = \begin{cases} \det \begin{vmatrix} 2 & 0 \\ 0 & 2d \end{vmatrix} = 4d & \text{si } d \equiv 2 \text{ ou } 3 \pmod 4 \\ \det \begin{vmatrix} 2 & 1 \\ 1 & (1+d)/2 \end{vmatrix} = d & \text{si } d \equiv 1 \pmod 4. \end{cases}$$

Ainsi le discriminant est toujours congru à 0 ou 1 modulo 4 et le corps quadratique s'écrit aussi $k = \mathbf{Q}(\sqrt{D_k})$.

Le groupe des racines de l'unités d'un corps de nombres quadratique k est $\{1, i, -1, -i\}$ si k a pour discriminant -4 — c'est-à-dire $k = \mathbf{Q}(i)$—, c'est $\{1, \varrho, \varrho^2, -1, -\varrho, -\varrho^2\}$ si k a pour discriminant -3, où ϱ est une racine primitive cubique de l'unité — c'est-à-dire pour $k = \mathbf{Q}(\sqrt{-3})$— , enfin les seules racines de l'unité dans $\mathbf{Z}_k$ sont $\{\pm 1\}$ sinon.

Quand d est négatif, il est facile de vérifier que le groupe des unités du corps $k = \mathbf{Q}(\sqrt{d})$ est fini : il est composé des racines de l'unité. Nous verrons plus tard que pour $d > 0$ le groupe $\mathbf{Z}_k^\times$ des unités de $\mathbf{Z}_k$ est un $\mathbf{Z}$-module de rang 1.

Proposition 3.12. *Soit K un corps de nombres de degré n. Alors l'anneau des entiers $\mathbf{Z}_K$ de K est un $\mathbf{Z}$-module libre de rang n.*

Démonstration. La conclusion signifie qu'il existe n éléments $e_1, \dots, e_n$ de $\mathbf{Z}_K$, linéairement indépendants sur $\mathbf{Q}$, tels que

$$\mathbf{Z}_K = \mathbf{Z}e_1 + \cdots + \mathbf{Z}e_n.$$

Soit $f_1, \dots, f_n$ une base de K sur $\mathbf{Q}$ formée d'éléments de $\mathbf{Z}_K$ (partant d'une base quelconque il suffit de multiplier par un dénominateur pour obtenir une telle base).

La forme bilinéaire $(x, y) \mapsto \mathrm{Tr}_{K/\mathbf{Q}}(xy)$ étant non dégénérée (lemme 3.2), il existe une base $f_1^*, \dots, f_n^*$ de K sur $\mathbf{Q}$ telle que $\mathrm{Tr}_{K/\mathbf{Q}}(f_i f_j^*) = \delta_{ij}$ (symbole de Kronecker). Soit $a \in \mathbf{Z}$, $a > 0$ tel que af_j^* soit entier algébrique pour $1 \leq j \leq d$.

Pour $x \in K$ on écrit

$$x = x_1 f_1 + \cdots + x_d f_d$$

avec $x_1, \dots, x_d$ dans $\mathbf{Q}$ et on a $\mathrm{Tr}_{K/\mathbf{Q}}(xf_j^*) = x_j$. Maintenant si $x \in \mathbf{Z}_K$ on a $xaf_j^* \in \mathbf{Z}_K$, donc $\mathrm{Tr}_{K/\mathbf{Q}}(xaf_j^*) = ax_j \in \mathbf{Z}$. On en déduit

$$\mathbf{Z}f_1 + \cdots + \mathbf{Z}f_d \subset \mathbf{Z}_K \subset \frac{1}{a}(\mathbf{Z}f_1 + \cdots + \mathbf{Z}f_d).$$

Pour conclure on utilise alors les résultats du §3.3 suivant sur la structure des modules sur un anneau principal (proposition 3.14).

□

3.3 Structure des modules sur les anneaux principaux

Commençons par quelques rappels sur les modules. Soit A un anneau, soit M un A-module et soient N_1 et N_2 deux sous-A-modules de M. On dit que M est somme directe de N_1 et N_2, et on écrit $M = N_1 \oplus N_2$, si l'application $(x_1, x_2) \mapsto x_1 + x_2$ est un isomorphisme de A-modules de $N_1 \times N_2$ sur M. Cela revient à dire que l'on a $M = N_1 + N_2$ et $N_1 \cap N_2 = \{0\}$.

Si $\mathfrak{A}_1$ et $\mathfrak{A}_2$ sont deux idéaux d'un anneau A tels que $\mathfrak{A}_1 + \mathfrak{A}_2 = A$, alors $\mathfrak{A}_1 \cap \mathfrak{A}_2 = \mathfrak{A}_1\mathfrak{A}_2$ et $A/\mathfrak{A}_1\mathfrak{A}_2$ est isomorphe à $A/\mathfrak{A}_1 \times A/\mathfrak{A}_2$.

Proposition 3.13. *Soient A un anneau et M un A-module. Les propriétés suivantes sont équivalentes :*
(i) Toute famille non vide de sous-modules de M admet un élément maximal.
(ii) Toute suite croissante de sous-modules de M est stationnaire à partir d'un certain rang.
(iii) Tout sous-module de M est de type fini.

Démonstration. Voir [S] § 1.4. □

Définition. Quand les conditions de la proposition 3.13 sont satisfaites on dit que M est un *A-module noethérien.* Un anneau est dit *noethérien* s'il est noethérien comme A-module, c'est-à-dire si tout suite croissante d'idéaux

$$\mathfrak{A}_1 \subset \mathfrak{A}_2 \subset \cdots$$

est stationnaire.

De la condition (iii) de la la proposition 3.13 il résulte qu'un anneau principal est noethérien.

Quand A est un anneau intègre et M un A-module, on définit le *rang de M* comme le nombre maximal ($\leq \infty$) d'éléments de M linéairement indépendants sur A. Si K est le corps des fractions de A, et si M est un A-module libre, il possède une base, et on peut plonger M dans un K-espace vectoriel V. Le rang de M est donc le nombre d'éléments d'une base de M comme A-module, et plus généralement le rang d'un sous-module N de M est la dimension du K-espace vectoriel engendré par N dans V.

Proposition 3.14. (Modules sur les anneaux principaux.) *Soit A un anneau principal, soit M un A-module libre de rang m et soit N un sous-A-module de M. Alors N est libre de rang $n \leq m$. De plus il existe une base $\{e_1, \ldots, e_m\}$ de M comme A-module et des éléments $a_1, \ldots, a_n$ de A tels que $\{a_1 e_1, \ldots, a_n e_n\}$ soit une base de N sur A et que a_i divise a_{i+1} dans A pour $1 \leq i < n$.*

Les idéaux $a_1 A \supset a_2 A \supset \cdots \supset a_n A$ de A sont appelés *facteurs invariants* du sous-A-module N de M : ils ne dépendent pas de la base $(a_1, \ldots, e_n)$ de M vérifiant les conditions de la proposition 3.14.

Démonstration. Voir [S] § 1.5. □

[S] P. Samuel, *Théorie algébrique des nombres*, Hermann, Collection Méthodes, 1967.

Université P. et M. Curie (Paris VI),
Deuxième semestre 2006/2007

Michel Waldschmidt
date de mise à jour: 24/04/2007

Master de sciences et technologies 1ère année -
Spécialité : Mathématiques Fondamentales

Mention : Mathématiques et applications
MO11 : Théorie des nombres (12 ECTS)

Troisième partie : Arithmétique des Corps de Nombres

Fascicule 6 : section 3.4 (12 pages)

3.4 Unités d'un corps de nombres

3.4.1 Énoncé du théorème de Dirichlet

Une *unité algébrique* est un élément inversible de l'anneau des entiers algébriques.

Lemme 3.15. *Pour un entier algébrique α d'un corps de nombres k, les conditions suivantes sont équivalentes*
(i) α est une unité algébrique.
(ii) $\mathrm{N}(\alpha) = \pm 1$.
(iii) $\mathrm{N}_{k/\mathbf{Q}}(\alpha) = \pm 1$.

Démonstration. .
L'équivalence entre (ii) et (iii) est banale, puisque $\mathrm{N}(\alpha) = \mathrm{N}_{\mathbf{Q}(\alpha)/\mathbf{Q}}(\alpha)$ et que

$$\mathrm{N}_{k/\mathbf{Q}}(\alpha) = \big(\mathrm{N}(\alpha)\big)^{[k:\mathbf{Q}(\alpha)]}.$$

Si α est une unité algébrique, d'inverse β, et si k est un corps de nombres contenant α, alors on a d'une part $\mathrm{N}_{k/\mathbf{Q}}(\alpha) \in \mathbf{Z}$ et $\mathrm{N}_{k/\mathbf{Q}}(\beta) \in \mathbf{Z}$ car α et β sont entiers algébriques, et d'autre part $\mathrm{N}_{k/\mathbf{Q}}(\alpha)\mathrm{N}_{k/\mathbf{Q}}(\beta) = \mathrm{N}_{k/\mathbf{Q}}(\alpha\beta) = 1$ car $\alpha\beta = 1$. Donc $\mathrm{N}_{k/\mathbf{Q}}(\alpha)$ est un élément inversible de $\mathbf{Z}$, ce qui montre $(i) \Rightarrow (ii)$.

Enfin si α est un entier algébrique de norme ± 1, son polynôme minimal sur $\mathbf{Z}$ s'écrit

$$X^n + a_1 X^{n-1} + \cdots + a_{n-1} X + a_n \in \mathbf{Z}[X]$$

avec $a_n = \pm 1$, et l'entier algébrique

$$\beta = -a_n(\alpha^{n-1} + a_1\alpha^{n-2} + \cdots + a_{n-1})$$

vérifie $\alpha\beta = a_n^2 = 1$, donc β est l'inverse de α.

□

Notons qu'il existe des *nombres* algébriques de norme ± 1 qui ne sont pas des unités algébriques : un exemple est

$$\frac{-1 + i\sqrt{15}}{4}$$

qui est racine du polynôme $2X^2 + X + 2$.

Soient k un corps de nombres et n son degré. D'après le théorème de l'élément primitif 1.21, il existe $\alpha \in k$ tel que $k = \mathbf{Q}(\alpha)$. On décompose le polynôme irréductible $P \in \mathbf{Q}[X]$ de α dans $\mathbf{R}[X]$: soient r_1 le nombre de facteurs irréductibles de degré 1 et r_2 le nombre de facteurs irréductibles de degré 2. Ainsi $r_1 + 2r_2 = n$. Notons $\alpha_1, \dots, \alpha_{r_1}$ les racines réelles de P :

$$P(X) = \prod_{i=1}^{r_1}(X - \alpha_j) \prod_{j=r_1+1}^{r_1+r_2} (X^2 + b_j X + c_j).$$

Pour $r_1 + 1 \leq j \leq r_1 + r_2$ le polynôme $X^2 + b_j X + c_j$ a deux racines complexes conjuguées, que l'on note α_j et $\alpha_{r_2+j} = \overline{\alpha}_j$. Ainsi la décomposition de P en facteurs irréductibles dans $\mathbf{C}$ est

$$P(X) = \prod_{i=1}^{n}(X - \alpha_j).$$

Il y a n $\mathbf{Q}$-isomorphismes $\sigma_1, \dots, \sigma_n$ de k dans $\mathbf{C}$, qui sont déterminés respectivement par

$$\sigma_j(\alpha) = \alpha_j \quad (1 \leq j \leq n).$$

Pour $1 \leq j \leq r_1$ l'image $\sigma_j(k)$ de k par σ_j est dans $\mathbf{R}$, tandis que σ_{r_1+j} et $\sigma_{r_1+r_2+j}$ sont complexes conjugués pour $1 \leq j \leq r_2$. L'ensemble $\{\sigma_1, \dots, \sigma_{r_1}\}$ des plongements réels et celui $\{\sigma_{r_1+1}, \dots, \sigma_{r_1+2r_2}\}$ des plongements non réels ne dépendent pas du choix de l'élément primitif α. Le *plongement canonique* de k est l'application $\mathbf{Q}$-linéaire injective $\underline{\sigma} : k \to \mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ définie par

$$\underline{\sigma}(x) = \big(\sigma_1(x), \dots, \sigma_{r_1+r_2}(x)\big).$$

Le seul choix qui ne soit pas intrinsèque est celui entre un plongement non réel et son conjugué. On identifie $\mathbf{C}$ à $\mathbf{R}^2$ par $z = \Re(z) + i\Im(z)$ et on note encore $\underline{\sigma}$ l'application $\mathbf{Q}$-linéaire de k dans $\mathbf{R}^n$ qui envoie $x \in k$ sur

$$\Big(\sigma_1(x), \dots, \sigma_{r_1}(x), \Re\big(\sigma_{r_1+1}(x)\big), \Im\big(\sigma_{r_1+1}(x)\big), \dots, \Re\big(\sigma_{r_1+r_2}(x)\big), \Im\big(\sigma_{r_1+r_2}(x)\big)\Big).$$

La structure du groupe des unités $\mathbf{Z}_k^\times$ d'un corps de nombres k est donnée par le *Théorème de Dirichlet* :

Théorème 3.16. *Soient k un corps de nombres, n son degré, r_1 le nombre de plongements réels de k et $2r_2$ le nombre de plongements complexes deux-à-deux conjugués complexes. Alors le groupe des unités $\mathbf{Z}_k^\times$ de k est un groupe de type fini et de rang $r = r_1 + r_2 - 1$.*

Dire que $\mathbf{Z}_k^\times$ est un groupe abélien de type fini et de rang r signifie que d'une part son groupe de torsion, qui est le groupe $k_{\text{tors}}^\times$ des racines de l'unité contenues dans k, est fini, et d'autre part que le quotient $\mathbf{Z}_k/k_{\text{tors}}^\times$ est isomorphe à $\mathbf{Z}^r$: il existe r unités $\epsilon_1, \dots, \epsilon_r$ dans $\mathbf{Z}_k^\times$, qui sont linéairement indépendantes dans $\mathbf{Z}_k^\times$ (on dit *multiplicativement indépendantes* puisque la loi est multiplicative), telles que toute unité de k s'écrive de manière unique

$$\zeta \epsilon_1^{a_1} \cdots \epsilon_r^{a_r}$$

avec ζ racine de l'unité et $a_i \in \mathbf{Z}$ $(1 \leq i \leq r)$. On dit que $(\epsilon_1, \dots, \epsilon_r)$ est un système fondamental d'unités de k si cette propriété est vérifiée, c'est-à-dire si les images de $\epsilon_1, \dots, \epsilon_r$ modulo torsion forment une base du groupe abélien libre $\mathbf{Z}_k^\times/k_{\text{tors}}^\times$.

La démonstration du théorème 3.16 nécessite quelques préliminaires sur les sous-groupes de $\mathbf{R}^n$.

3.4.2 Sous-groupes de $\mathbf{R}^n$

Des exemples de sous-groupes de $\mathbf{R}$ sont d'une part

$$\{0\}, \quad \mathbf{Z} \quad \text{et plus généralement } \mathbf{Z}x \text{ pour } x \in \mathbf{R}$$

et d'autre part

$$\mathbf{Z} + \mathbf{Z}\sqrt{2}, \quad \mathbf{Q} \quad \text{et} \quad \mathbf{R}.$$

Les sous-groupes de la première liste sont discrets dans $\mathbf{R}$: un sous-groupe G de $\mathbf{R}^n$ est *discret* si pour tout compact K de $\mathbf{R}^n$, l'intersection $G \cap K$ est finie. Ceux de la deuxième liste sont denses.

On remarquera que l'adhérence d'un sous-groupe de $\mathbf{R}^n$ est encore un sous-groupe de $\mathbf{R}^n$.

Quand G_1 et G_2 sont deux sous-groupes de $\mathbf{R}^{n_1}$ et $\mathbf{R}^{n_2}$ respectivement, le produit $G_1 \times G_2$ est un sous-groupe de $\mathbf{R}^n$ avec $n = n_1 + n_2$.

Nous allons voir que, dans une certaine mesure, ces remarques permettent de décrire tous les sous-groupes de $\mathbf{R}^n$.

Nous commençons par décrire les sous-groupes discrets de $\mathbf{R}^n$.

Lemme 3.17. *Un sous-groupe G de $\mathbf{R}^n$ est discret dans $\mathbf{R}^n$ si et seulement s'il existe un ouvert U de $\mathbf{R}^n$ contenant 0 tel que $G \cap U$ soit discret.*

Démonstration. Si G est discret on peut prendre $U = \mathbf{R}^n$. Inversement, si G n'est pas discret, il existe un élément $z \in \mathbf{R}^n$ qui est un point d'accumulation d'éléments de G : pour tout $\epsilon > 0$ il existe $x \in G$ tel que $0 < |z - x| < \epsilon$ et il existe $y \in G$ tel que $0 < |z - y| < |z - x|$. Alors $0 < |x - y| < 2\epsilon$, ce qui montre que 0 est point d'accumulation de G.

□

Exercice. 1. Montrer qu'un sous-groupe non discret de $\mathbf{R}$ est partout dense.
2. En déduire la liste des sous-groupes fermés de $\mathbf{R}$.
3. Soit G un sous-groupe de type fini de $\mathbf{R}$. Donner une condition nécessaire et suffisante sur son rang pour que G soit dense dans $\mathbf{R}$.
4. Soit $\theta \in \mathbf{R}$. Donner une condition nécessaire et suffisante sur θ pour que le sous-groupe $\mathbf{Z} + \mathbf{Z}\theta$ soit dense dans $\mathbf{R}$.

Proposition 3.18. *Soit G un sous-groupe discret de $\mathbf{R}^n$. Il existe un entier t dans l'intervalle $0 \leq t \leq n$ et des éléments $e_1, \ldots, e_t$ de G, linéairement indépendants sur $\mathbf{R}$, tels que $G = \mathbf{Z}e_1 + \cdots + \mathbf{Z}e_t$.*

En particulier $e_1, \ldots, e_t$ sont linéairement indépendants sur $\mathbf{Z}$, donc G est libre de rang t. Le nombre t est la dimension du $\mathbf{R}$-sous–espace vectoriel de $\mathbf{R}^n$ engendré par G. La proposition 3.18 montre que dans un sous-groupe discret de $\mathbf{R}^n$, des éléments linéairement indépendants sur $\mathbf{Z}$ sont automatiquement linéairement indépendants sur $\mathbf{R}$.

Définition. Un sous-groupe discret de $\mathbf{R}^n$ de rang maximal n est appelé *réseau* (en anglais *lattice*) de $\mathbf{R}^n$.

Démonstration de la proposition 3.18. Soit $f_1, \ldots, f_t$ une partie de G libre sur $\mathbf{R}$ maximale. C'est une base du sous-espace vectoriel V de $\mathbf{R}^n$ engendré par G. De plus $G' = \mathbf{Z}f_1 + \cdots + \mathbf{Z}f_t$ est un sous-groupe de G. Montrons que G' est d'indice fini dans G.

Soit K un compact de $\mathbf{R}^n$ contenant

$$\{u_1 f_1 + \cdots + u_t f_t \ ; \ 0 \leq u_i < 1 \ (1 \leq i \leq t)\}.$$

Soit $x \in G$. Alors $x \in V$, donc on peut écrire $x = x_1 f_1 + \cdots + x_t f_t$ avec $x_i \in \mathbf{R}$. Soit $m_i = [x_i]$ la partie entière de x_i :

$$m_i \in \mathbf{Z}, \quad 0 \leq x_i - m_i < 1 \qquad (1 \leq i \leq n).$$

Posons $x' = m_1 f_1 + \cdots + m_t f_t$. Alors $x' \in G'$ et $x - x' \in G \cap K$. Comme G est discret, $G \cap K$ est fini. Donc le groupe quotient G/G' est fini et G' est d'indice fini dans G.

Soit s l'ordre de G/G' et soit $f_i' = f_i/s$ $(1 \leq i \leq t)$. On a

$$G' = \mathbf{Z}f_1 + \cdots + \mathbf{Z}f_t \subset G \subset \mathbf{Z}f_1' + \cdots + \mathbf{Z}f_t',$$

ce qui permet de conclure grâce à la proposition 3.14.

□

Théorème 3.19 (Structure des sous-groupes de $\mathbf{R}^n$). *Soit G un sous-groupe additif de $\mathbf{R}^n$. Il existe un plus grand sous-espace vectoriel V de $\mathbf{R}^n$ sur $\mathbf{R}$ contenu dans l'adhérence de G. Soient d la dimension de V et $d+t$ la dimension de l'espace vectoriel engendré par G sur $\mathbf{R}$. Posons enfin $G' = G \cap V$. Alors il existe un sous-groupe discret G'' de G, discret de rang t, tel que G soit la somme directe de G' et G''.*

Démonstration. Pour $\varrho > 0$ notons

$$B(0, \varrho) = \{x \in \mathbf{R}^n \ ; \ \|x\| \leq \varrho\}$$

la boule euclidienne de rayon ϱ et soit V_ϱ le $\mathbf{R}$-espace vectoriel engendré par $G \cap B(0, \varrho)$ dans $\mathbf{R}^n$. Posons

$$V = \bigcap_{\varrho > 0} V_\varrho.$$

L'application $\varrho \mapsto \dim V_\varrho$ est croissante à valeurs entières ≥ 0, donc il existe $\varrho_0 > 0$ tel que $V = V_\varrho$ pour $0 < \varrho \leq \varrho_0$.

Montrons que $G' = G \cap V$ est dense dans V. Soit $\epsilon > 0$ et soit $x \in V$. Posons $\varrho = \min\{\epsilon/d, \ \varrho_0\}$ et soit $\{e_1, \ldots, e_d\}$ une base de V sur $\mathbf{R}$ avec $e_i \in G \cap B(0, \varrho)$. On écrit $x = x_1 e_1 + \cdots + x_d e_d$, on pose $m_i = [x_i]$ $(1 \leq i \leq d)$ et $y = m_1 e_1 + \cdots + m_d e_d$. Alors $y \in G'$ vérifie $\|x - y\| \leq \epsilon$.

Soit maintenant W le sous-espace de $\mathbf{R}^n$ engendré par G. Comme il contient V sa dimension est $d + t$ avec $t \geq 0$. Soit V' un supplémentaire de V dans W et soit $p : W \to V'$ la projection de noyau V.

Montrons que $p(G)$ est un sous-groupe discret de V'. Sinon il existerait $z \in p(G)$ tel que $0 < \|z\| < \epsilon$ avec $\epsilon = \varrho_0/2$. Soit $w \in G$ tel que $z = p(w)$; on a $u = w - z \in V$. Comme G' est dense dans V il existe $w' \in G'$ tel que $\|u - w'\| < \epsilon$. Alors $\|w - w'\| < \varrho_0$ et $p(w - w') = z \neq 0$, ce qui signifie que $w - w' \in G$ vérifie $w - w' \notin V$ et contredit le fait que $V = V_{\varrho_0}$.

Alors $p(G)$ est un sous-groupe discret de V' de rang t, donc un réseau de V'. On en prend une base $p(y_1), \ldots, p(y_t)$ et on pose $G'' = \mathbf{Z}y_1 + \cdots + \mathbf{Z}y_t$. Ainsi $G = G' \oplus G''$.

Enfin comme G'' est discret, V est le plus grand sous-espace vectoriel de $\mathbf{R}^n$ contenu dans l'adhérence de G.

□

Le théorème 3.19 permet de préciser la structure des sous-groupes fermés de $\mathbf{R}^n$:

Corollaire 3.20. *Soit G un sous-groupe fermé de $\mathbf{R}^n$. Il existe un plus grand sous-espace vectoriel V contenu dans G ; si W est un sous-espace vectoriel de $\mathbf{R}^n$ supplémentaire de V, alors $W \cap G$ est un sous-groupe discret de $\mathbf{R}^n$, et G est somme directe de V et de $W \cap G$.*

Exercice. Soit $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbf{R}^n$. On considère le sous-groupe

$$G = \mathbf{Z}^n + \mathbf{Z}\mathbf{x} = \{(a_1 + a_0 x_1, \ldots, a_n + a_0 x_n) \ ; \ (a_0, \ldots, a_n) \in \mathbf{Z}^{n+1}\}$$

de $\mathbf{R}^n$.
1. Montrer que G est discret dans $\mathbf{R}^n$ si et seulement si $\mathbf{x} \in \mathbf{Q}^n$.
2. En déduire que les conditions suivantes sont équivalentes.
(i) 0 est un point d'accumulation de G
(ii) Pour tout $\epsilon > 0$ il existe des entiers $p_1, \ldots, p_n$, q, avec $q > 0$, tels que

$$0 < \max_{1 \leq i \leq n} |q x_i - p_i| < \epsilon.$$

(iii) L'un au moins des n nombres $x_1, \ldots, x_n$ est irrationnel.
3. Montrer que G est dense dans $\mathbf{R}^n$ si et seulement si les nombres $1, x_1, \ldots, x_n$ sont linéairement indépendants sur $\mathbf{Q}$.
En déduire que pour tout $(\xi_1, \xi_2) \in \mathbf{R}^2$ et pour tout $\epsilon > 0$ il existe des entiers rationnels p_1, p_2 et q avec

$$|\xi_1 - p_1 - q\sqrt{2}| \leq \epsilon \quad \text{et} \quad |\xi_2 - p_1 - q\sqrt{3}| \leq \epsilon.$$

Exercice. On appelle *caractère* de $\mathbf{R}^n$ tout homomorphisme continu de $\mathbf{R}^n$ dans $\mathbf{R}/\mathbf{Z}$ (ou dans le groupe multiplicatif $\mathbf{U}$ des nombres complexes de module 1, cela revient au même).
1. Vérifier que tout homomorphisme continu du groupe additif $\mathbf{R}$ dans lui-même est une application $\mathbf{R}$-linéaire, c'est-à-dire de la forme $x \mapsto \lambda x$, pour un $\lambda \in \mathbf{R}$. En déduire d'abord que tout homomorphisme continu du groupe additif $\mathbf{R}$ dans le groupe multiplicatif $\mathbf{R}^\times$ est de la forme $x \mapsto e^{\lambda x}$, ensuite que tout homomorphisme continu du groupe additif $\mathbf{R}$ dans le groupe multiplicatif $\mathbf{U}$ est de la forme $x \mapsto e^{i\lambda x}$. En déduire que tout homomorphisme continu $\chi : \mathbf{R} \to \mathbf{R}/\mathbf{Z}$ se factorise en $\chi = s \circ h$:

$$\begin{array}{ccc} \mathbf{R} & \xrightarrow{\ h\ } & \mathbf{R} \\ & \chi \searrow & \downarrow s \\ & & \mathbf{R}/\mathbf{Z} \end{array}$$

où $s : \mathbf{R} \to \mathbf{R}/\mathbf{Z}$ est la surjection canonique et $h : \mathbf{R} \to \mathbf{R}$ est une application linéaire.
2. Quand u est un élément de $\mathbf{R}^n$, l'application ψ_u de $\mathbf{R}^n$ dans $\mathbf{U}$ donnée par $x \mapsto e^{2i\pi u \cdot x}$ (où $u \cdot x$ est le produit scalaire standard dans $\mathbf{R}^n$) est un caractère de $\mathbf{R}^n$. Vérifier qu'on les obtient tous ainsi. Le noyau de ψ_u est $\{x \in \mathbf{R}^n ; \ u \cdot x \in \mathbf{Z}\}$.
3. En déduire que l'application de $\mathrm{Hom}_{\mathbf{R}}(\mathbf{R}^n, \mathbf{R})$ dans le groupe des caractères de $\mathbf{R}^n$ qui, à une forme linéaire φ, associe $\chi_\varphi : x \mapsto e^{2i\pi\varphi(x)}$, est un isomorphisme de groupes. Le noyau de χ_φ est $\varphi^{-1}(\mathbf{Z})$.
4. Soit G un sous-groupe de type fini de $\mathbf{R}^n$. Montrer que les conditions suivantes sont équivalentes.
(i) G est dense dans $\mathbf{R}^n$.
(ii) Pour tout sous-espace vectoriel V de $\mathbf{R}^n$ distinct de $\mathbf{R}^n$, on a

$$\mathrm{rang}_{\mathbf{Z}}(G/G \cap V) > \dim_{\mathbf{R}}(\mathbf{R}^n/V).$$

(iii) Pour tout hyperplan H de $\mathbf{R}^n$, on a $\mathrm{rang}_{\mathbf{Z}}(G/G\cap H)\geq 2$.
(iv) Pour toute forme linéaire non nulle $\varphi : \mathbf{R}^n \longrightarrow \mathbf{R}$ on a $\varphi(G)\not\subset \mathbf{Z}$.
(v) Pour tout caractère non trivial χ de $\mathbf{R}^n$, on a $\chi(G)\neq\{1\}$.
(vi) Choisissons des générateurs $g_1,\dots,g_\ell$ de G sur $\mathbf{Z}$ et écrivons les coordonnées des g_j dans la base canonique de $\mathbf{R}^n$:

$$g_j=(g_{1j},\dots,g_{nj}),\qquad (1\leq j\leq \ell);$$

pour tout $(s_1,\dots,s_\ell)$ dans $\mathbf{Z}^\ell$ distinct de $(0,\dots,0)$, la matrice

$$\begin{pmatrix} g_{11} & \cdots & g_{1\ell}\\ \vdots & \ddots & \vdots\\ g_{n1} & \cdots & g_{n\ell}\\ s_1 & \cdots & s_\ell\end{pmatrix}$$

est de rang $n+1$.
Montrer aussi que dans le cas $\ell=n+1$, la condition (vi) est équivalente à la suivante :
(vii) Les $n+1$ nombres réels

$$\Delta_h=\det\Big(g_{ij}\Big)_{\substack{1\leq i\leq n\\ 1\leq j\leq n+1,\ j\neq h}},\qquad (1\leq h\leq n+1)$$

sont linéairement indépendants sur $\mathbf{Q}$.

Voici une caractérisation des réseaux parmi les sous-groupes discrets d'un sous-espace vectoriel de $\mathbf{R}^n$.

Lemme 3.21. *Soient V un sous-espace vectoriel de $\mathbf{R}^n$ et soit G un sous-groupe discret de $\mathbf{R}^n$ contenu dans V. Pour que G engendre V sur $\mathbf{R}$, il faut et il suffit qu'il existe un ensemble borné B de V tel que*

$$V=\bigcup_{g\in G}(B+g).$$

Démonstration. Si G contient une base $\{e_1,\dots,e_n\}$ de V sur $\mathbf{R}$, alors

$$B=\{x_1e_1+\cdots+x_ne_n\ ;\ 0\leq x_i<1\ (1\leq i\leq n)\}$$

convient.

Inversement, si G est contenu dans un sous-espace vectoriel V' de V avec $V'\neq V$, et si $p : V\to W$ est la projection de V sur un supplémentaire W de V' dans V, alors pour toute partie B de V on a

$$p\left(\bigcup_{g\in G}(B+g)\right)=p(B).$$

Comme $W=p(V)$ est de dimension ≥ 1, si B est borné, alors $p(B)\neq p(V)$, donc

$$\bigcup_{g\in G}(B+g)\neq V.$$

□

Soit G un réseau de $\mathbf{R}^n$. Pour chaque base $\mathbf{e} = \{e_1, \ldots, e_n\}$ de G le parallélogramme

$$P_{\mathbf{e}} = \{x_1 e_1 + \cdots + x_n e_n \ ; \ 0 \leq x_i < 1 \ (1 \leq i \leq n)\}$$

est un *domaine fondamental* pour G, c'est-à-dire un système complet de représentants des classes modulo G. En écrivant

$$\mathbf{R}^n = \bigcup_{g \in G} (P_{\mathbf{e}} + g) \tag{3.22}$$

on obtient une partition de $\mathbf{R}^n$.

Le passage d'une base de G à une autre se fait avec une matrice de déterminant ± 1, donc la mesure de Lebesgue $\mu(P_{\mathbf{e}})$ de $P_{\mathbf{e}}$ ne dépend pas de $\mathbf{e}$: ce nombre est appelé *le volume* du réseau G et noté $v(G)$.

Voici un exemple des résultats obtenus par Minkowski au XIXème siècle comme application de sa *géométrie des nombres.*

Théorème 3.23 (*Minkowski*)**.** *Soient G un réseau de $\mathbf{R}^n$ et B un sous-ensemble mesurable de $\mathbf{R}^n$. On suppose $\mu(B) > v(G)$. Alors il existe x et y distincts dans B tels que $x - y \in G$.*

Démonstration. Grâce à (3.22) on peut écrire B comme réunion disjointe des $B \cap (P_{\mathbf{e}} + g)$ avec g parcourant G. Alors

$$\mu(B) = \sum_{g \in G} \mu\left(B \cap (P_{\mathbf{e}} + g)\right).$$

Comme la mesure de Lebesque est invariante par translation on a

$$\mu\left(B \cap (P_{\mathbf{e}} + g)\right) = \mu\left((-g + B) \cap P_{\mathbf{e}}\right).$$

Les ensembles $(-g + B) \cap P_{\mathbf{e}}$ sont tous contenus dans $P_{\mathbf{e}}$ et la somme de leurs mesures est $\mu(B) > \mu(P_{\mathbf{e}})$. Donc ils ne sont pas deux-à-deux disjoints (c'est une des versions du *principe des tiroirs de Dirichlet*). Il existe $g \neq g'$ dans G tels que

$$(-g + B) \cap (-g' + B) \neq \emptyset.$$

Soient x et y dans B tels que $-g + x = -g' + y$. Alors $x - y = g - g' \in G \setminus \{0\}$.

□

Corollaire 3.24. *Soit G un réseau de $\mathbf{R}^n$ et soit B un sous-ensemble mesurable de $\mathbf{R}^n$, convexe et symétrique par rapport à l'origine, tel que $\mu(B) > 2^n v(G)$. Alors $B \cap G \neq \{0\}$.*

Démonstration. On applique le théorème 3.23 à l'ensemble

$$B' = \frac{1}{2} B = \{x \in \mathbf{R}^n \ ; \ 2x \in B\}.$$

On a $\mu(B') = 2^{-n} \mu(B) > v(G)$, donc il existe $x \neq y$ dans B' tels que $x - y \in G$. Alors $2x$ et $2y$ sont dans B, et comme B est symétrique $-2y \in B$. Enfin B est convexe, donc $(2x - 2y)/2 = x - y \in G \cap B$.

□

Remarque. Avec les notations du corollaire 3.24, si on suppose que B est une partie compacte de $\mathbf{R}^n$, alors l'inégalité large $\mu(B) \geq 2^n v(G)$ suffit pour obtenir la conclusion. On le voit par exemple en appliquant le corollaire 3.24 à $(1 + \epsilon)B$ avec $\epsilon \to 0$.

3.4.3 Plongements d'un corps de nombres

Nous utiliserons plusieurs fois la remarque suivante : la somme des modules des coefficients d'un polynôme

$$(X-\alpha_1)\cdots(X-\alpha_n)\in\mathbf{C}[X]$$

est majorée par

$$(1+|\alpha_1|)\cdots(1+|\alpha_n|). \tag{3.25}$$

Proposition 3.26. *L'image de l'anneau des entiers $\mathbf{Z}_k$ de k par le plongement canonique $\underline{\sigma}$ est un réseau de $\mathbf{R}^n$.*

Démonstration. Si K est un compact de $\mathbf{R}^n$, il existe un nombre réel $C>0$ tel que tout $(x_1,\dots,x_n)\in K$ vérifie $|x_i|\leq C$ $(1\leq i\leq n)$. Si $x\in k$ est tel que $\underline{\sigma}(x)\in K$, alors $|\sigma_i(x)|\leq C\sqrt{2}$ pour tout $i=1,\dots,n$. De (3.25) on déduit que pour $x\in\mathbf{Z}_k\cap\underline{\sigma}^{-1}(K)$ la somme des modules des coefficients du polynôme minimal de x est majorée par $(1+C\sqrt{2})^n$, donc les polynômes unitaires irréductibles de $\mathbf{Z}[X]$ dont ces x sont racines sont en nombre fini. Ainsi $\underline{\sigma}(\mathbf{Z}_k)\cap K$ est fini, et par conséquent $\underline{\sigma}(\mathbf{Z}_k)$ est un sous-groupe discret de $\mathbf{R}^n$. Comme $\underline{\sigma}$ est un homomorphisme injectif de $\mathbf{Z}$-modules et que $\mathbf{Z}_k$ est de rang n, son image $\underline{\sigma}(\mathbf{Z}_k)$ est un sous-groupe de rang n de $\mathbf{R}^n$.

□

Le calcul du volume de ce réseau se déduit de la proposition suivante :

Proposition 3.27. *Soit M un sous-$\mathbf{Z}$-module libre de k de rang n et soit $x_1,\dots,x_n$ une base de M sur $\mathbf{Z}$. Alors $\underline{\sigma}(M)$ est un réseau de $\mathbf{R}^n$ de volume*

$$v\big(\underline{\sigma}(M)\big)=2^{-r_2}\big|\det\big(\sigma_i(x_j)\big)\big|.$$

Démonstration. Soit d un entier positif tel que $dx_i\in\mathbf{Z}_k$ pour $1\leq i\leq n$. Alors $dM\subset\mathbf{Z}_k$. Donc $\underline{\sigma}(dM)$ est un sous-groupe d'indice fini de $\underline{\sigma}(\mathbf{Z}_k)$, et il résulte de la proposition 3.26 que $\underline{\sigma}(dM)$ et $\underline{\sigma}(M)$ sont des réseaux de $\mathbf{R}^n$.

Le volume de $\underline{\sigma}(M)$ est la valeur absolue du déterminant de la matrice $n\times n$ dont la $i$ème colonne est

$$\Big(\sigma_1(x_i),\dots,\sigma_{r_1}(x_i),\Re\big(\sigma_{r_1+1}(x_i)\big),\Im\big(\sigma_{r_1+1}(x_i)\big),\dots,\Re\big(\sigma_{r_1+r_2}(x_i)\big),\Im\big(\sigma_{r_1+r_2}(x_i)\big)\Big).$$

Par combinaison linéaire des lignes, la valeur absolue de ce déterminant est égale au module du déterminant de la matrice dont la $i$ème colonne est

$$\Big(\sigma_1(x_i),\dots,\sigma_{r_1}(x_i),\sigma_{r_1+1}(x_i),(1/2)\overline{\sigma}_{r_1+1}(x_i),\dots,\sigma_{r_1+r_2}(x_i),(1/2)\overline{\sigma}_{r_1+r_2}(x_i)\Big).$$

□

On en déduit immédiatement :

Corollaire 3.28. *Le volume du réseau $\underline{\sigma}(\mathbf{Z}_k)$ de $\mathbf{R}^n$ est*

$$2^{-r_2}|D_k|^{1/2}$$

où D_k est le discriminant de k.

Le plongement canonique d'un corps de nombres est utile pour étudier la structure additive de l'anneau des entiers. Pour étudier la structure multiplicative on introduit le *plongement logarithmique* λ de k : c'est l'application de $k^\times$ dans $\mathbf{R}^{r_1+r_2}$ qui envoie $x \in k^\times$ sur

$$\lambda(x) = \Big(\log|\sigma_1(x)|, \dots, \log|\sigma_{r_1}(x)|, 2\log|\sigma_{r_1+1}(x)|, \dots, 2\log|\sigma_{r_1+r_2}(x)|\Big).$$

Comme

$$\mathrm{N}_{k/\mathbf{Q}}(x) = \prod_{i=1}^{n} \sigma_i(x),$$

si $s : \mathbf{R}^{r_1+r_2} \to \mathbf{R}$ est l'application $s(t_1, \dots, t_{r_1+r_2}) = t_1 + \cdots + t_{r_1+r_2}$, alors pour $x \in k^\times$ on a $s \circ \lambda(x) = \log|\mathrm{N}_{k/\mathbf{Q}}(x)|$.

En particulier un élément x de $k^\times$ vérifie $|\mathrm{N}_{k/\mathbf{Q}}(x)| = 1$, si et seulement si $\lambda(x)$ appartient à l'hyperplan $H = \ker s$ de $\mathbf{R}^{r_1+r_2}$ d'équation $t_1 + \cdots + t_{r_1+r_2} = 0$.

Grâce au lemme 3.15 on en déduit :

Lemme 3.29. *Soit $x \in \mathbf{Z}_k$, $x \neq 0$. Les trois propriétés suivantes sont équivalentes :*
(i) $x \in \mathbf{Z}_k^\times$
(ii) $\mathrm{N}_{k/\mathbf{Q}}(x) = \pm 1$
(iii) $\lambda(x) \in H$.

Le résultat suivant, dû à Kronecker, nous permettra de déterminer le noyau de la restriction de λ à $\mathbf{Z}_k \setminus \{0\}$:

Lemme 3.30. *Si un entier algébrique non nul α a tous ses conjugués complexes de modules ≤ 1, alors α est une racine de l'unité.*

Démonstration. L'hypothèse sur α et la majoration (3.25) impliquent que la somme des modules des coefficients des polynômes minimaux des nombres α^m, $m \in \mathbf{Z}$, $m \geq 0$, est bornée par $2^{[\mathbf{Q}(\alpha):\mathbf{Q}]}$, indépendamment de m, donc ces nombres α^m forment un ensemble fini : il existe $m \neq m'$ tel que $\alpha^m = \alpha^{m'}$, d'où le lemme 3.30.

□

On déduit du lemme 3.30

$$\mathbf{Z}_k \cap \ker \lambda = k^\times_{\mathrm{tors}}.$$

Comme la fonction d'Euler $\varphi(n)$ tend vers l'infini avec n, le groupe de torsion d'un corps de nombres est fini (donc cyclique).

3.4.4 Théorème de Dirichlet

Le théorème 3.16 de Dirichlet, qui donne la structure du groupe des unités d'un corps de nombres, est une conséquence de l'énoncé plus précis suivant :

Théorème 3.31. *L'image $\lambda(\mathbf{Z}_k)$ de l'anneau des entiers de k par le plongement logarithmique est un réseau de l'hyperplan H.*

La démonstration du théorème 3.31 va utiliser plusieurs lemmes auxiliaires.

Lemme 3.32. *Pour tout compact K de $\mathbf{R}^{r_1+r_2}$ l'ensemble de $\alpha \in \mathbf{Z}_k^\times$ tels que $\lambda(\alpha) \in K$ est fini.*

Démonstration. La majoration (3.25) montre que si K est un compact de $\mathbf{R}^{r_1+r_2}$ les polynômes unitaires irréductibles de $\mathbf{Z}[X]$ dont les éléments de $\lambda^{-1}(K) \cap \mathbf{Z}_k$ sont racines sont en nombre fini. □

Il résulte du lemme 3.32 que $\mathbf{Z}_k^\times$ est un groupe de type fini, produit direct du groupe fini $k_{\text{tors}}^\times$ par un groupe libre de type fini et de rang $r \leq r_1 + r_2 - 1$:

$$\mathbf{Z}_k^\times \simeq k_{\text{tors}}^\times \times \mathbf{Z}^r.$$

Pour compléter la démonstration des théorèmes 3.31 et 3.16 il reste à vérifier que $r = r_1 + r_2 - 1$, c'est-à-dire que $\mathbf{Z}_k^\times$ contient $r_1 + r_2 - 1$ éléments multiplicativement indépendants, ce qui revient encore à dire que $\lambda(\mathbf{Z}_k^\times)$ engendre l'hyperplan H sur $\mathbf{R}$. Pour cela on part d'un élément z de H et on veut montrer qu'il existe un élément de $\lambda(\mathbf{Z}_k^\times)$ à distance bornée de z (pour pouvoir utiliser le lemme 3.21). On construit déjà un élément α de $\mathbf{Z}_k$ tel que $\lambda(\alpha)$ ne soit pas trop loin de z, on majore la valeur absolue de la norme de α en utilisant le fait que $\lambda(\alpha)$ est proche de H, et cela suffit pour approcher $\lambda(\alpha)$, donc z, par un élément de $\lambda(\mathbf{Z}_k^\times)$, grâce au lemme 3.33 que voici.

Lemme 3.33. *Soit $\kappa > 0$. Il existe un sous-ensemble fini Γ de $\mathbf{Z}_k$ tel que tout entier $\alpha \in \mathbf{Z}_k$ vérifiant $|\mathrm{N}_{k/\mathbf{Q}}(\alpha)| \leq \kappa$, puisse s'écrire $\alpha = \epsilon\gamma$ avec $\gamma \in \Gamma$ et $\epsilon \in \mathbf{Z}_k^\times$.*

Démonstration. Le seul élément de $\mathbf{Z}_k$ de norme 0 est 0. Donc si $\kappa < 1$ le résultat est vrai avec $\Gamma = \{0\}$.

Soit m un entier non nul dans l'intervalle $-\kappa \leq m \leq \kappa$. L'anneau $\mathbf{Z}_k/m\mathbf{Z}_k$ est fini ; il n'y a donc qu'un nombre fini d'idéaux de $\mathbf{Z}_k$ qui contiennent $m\mathbf{Z}_k$. Si $\alpha \in \mathbf{Z}_k$ vérifie $\mathrm{N}_{k/\mathbf{Q}}(\alpha) = m$, alors $m \in \alpha\mathbf{Z}_k$.

Ceci montre qu'il n'y a qu'un nombre fini d'idéaux principaux de $\mathbf{Z}_k$ ayant un générateur dont la norme a une valeur absolue $\leq \kappa$. Pour chacun d'eux on choisit un générateur γ et on prend pour Γ l'ensemble de ces γ (sans oublier 0). □

Lemme 3.34. *Il existe une constante $\kappa > 0$ ayant la propriété suivante : si $\lambda_1, \dots \lambda_n$ sont des nombres réels positifs vérifiant $\lambda_1 \cdots \lambda_n = \kappa$ et $\lambda_{r_1+r_2+j} = \lambda_{r_1+j}$ pour $1 \leq j \leq r_2$, alors il existe $\alpha \in \mathbf{Z}_k$ tel que*

$$0 < |\sigma_i(\alpha)| \leq \lambda_i \quad \textit{pour} \quad 1 \leq i \leq n.$$

Démonstration. Soit K le compact de $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ défini par

$$|z_i| \leq \lambda_i \quad \text{pour} \quad 1 \leq i \leq r_1 + r_2.$$

Son volume est

$$\prod_{i=1}^{r_1}(2\lambda_i) \prod_{j=r_1+1}^{r_1+r_2} \pi\lambda_j^2 = 2^{r_1}\pi^{r_2}\kappa.$$

On prend $\kappa > (2/\pi)^{r_2}|D_k|^{1/2}$ de telle sorte que ce volume soit $> 2^{r_1+r_2}|D_k|^{1/2}$. Comme le volume de $\underline{\sigma}(\mathbf{Z}_k)$ est $2^{-r_2}|D_k|^{1/2}$ (lemme 3.28), on a $\mu(K) > 2^n v(\underline{\sigma}(\mathbf{Z}_k))$ et il ne reste plus qu'à appliquer le théorème de Minkowski 3.24.

□

Remarque. Sous les hypothèses du lemme 3.34, l'élément α qui est donné par la conclusion satisfait $1 \leq |\mathrm{N}_{k/\mathbf{Q}}(\alpha)| \leq \kappa$.

Démonstration du théorème 3.31. Soit $(t_1, \dots, t_{r_1+r_2}) \in H$. Posons $n_j = 1$ pour $1 \leq j \leq r_1$, $n_j = 2$ pour $r_1 < j \leq r_1 + r_2$,

$$\lambda_j = \kappa^{1/n} e^{t_j/n_j} \quad (1 \leq j \leq r_1 + r_2)$$

et $\lambda_{r_1+r_2+j} = \lambda_{r_1+j}$ pour $1 \leq j \leq r_2$, où κ est la constante dont l'existence est affirmée dans l'énoncé du lemme 3.34. Alors $\lambda_1 \cdots \lambda_n = \kappa$, donc il existe $\alpha \in \mathbf{Z}_k$ tel que

$$0 < |\sigma_j(\alpha)| \leq \lambda_j \quad \text{pour} \quad 1 \leq j \leq n$$

et $1 \leq |\mathrm{N}_{k/\mathbf{Q}}(\alpha)| \leq \kappa$. Comme $t_1 + \cdots +, t_{r_1+r_2} = 0$ on en déduit, pour $1 \leq j \leq r_1 + r_2$,

$$|\sigma_j(\alpha)| = |\mathrm{N}_{k/\mathbf{Q}}(\alpha)| \prod_{\substack{1 \leq i \leq n \\ i \neq j}} |\sigma_i(\alpha)|^{-1} \geq \kappa^{-(n-1)/n} e^{t_j/n_j}.$$

Cela montre qu'il existe une constante κ' telle que, pour tout $(t_1, \dots, , t_{r_1+r_2}) \in H$, il existe $\alpha \in \mathbf{Z}_k$ vérifiant $|\mathrm{N}_{k/\mathbf{Q}}(\alpha)| \leq \kappa$ et

$$\max_{1 \leq j \leq, r_1+r_2} \big| t_j - n_j \log |\sigma_j(\alpha)| \big| \leq \kappa'.$$

On utilise le lemme 3.33 : soit Γ un sous-ensemble fini de $\mathbf{Z}_k$ tel que tout élément $\alpha \in \mathbf{Z}_k$ satisfaisant $|\mathrm{N}_{k/\mathbf{Q}}(\alpha)| \leq \kappa$ s'écrive $\epsilon\gamma$ avec $\epsilon \in \mathbf{Z}_k^\times$ et $\gamma \in \Gamma$. Alors pour tout $t \in H$ il existe $\gamma \in \Gamma$ et $\epsilon \in \mathbf{Z}_k^\times$ tels que

$$\|t - \lambda(\gamma) - \lambda(\epsilon)\| \leq \kappa',$$

ce qui montre que si B désigne la boule de $\mathbf{R}^{r_1+r_2}$ de centre 0 et de rayon

$$R = \kappa' + \max_{\gamma \in \Gamma} \|\lambda(\gamma)\|,$$

on a

$$H \subset \bigcup_{\epsilon \in \mathbf{Z}_k^\times} \big(B + \lambda(\epsilon)\big).$$

Le lemme 3.21 permet de conclure que $\lambda(\mathbf{Z}_k^\times)$ est un réseau de H.

□

Définition. *Un système fondamental d'unités d'un corps de nombres k* est un ensemble de $r = r_1 + r_2 - 1$ unités $\epsilon_1, \dots, \epsilon_r$ dans $\mathbf{Z}_k^\times$ dont les images modulo $k_{\mathrm{tors}}^\times$ forment une base du groupe $\mathbf{Z}_k^\times / k_{\mathrm{tors}}^\times$.

Cela signifie que toute unité ϵ de k peut s'écrire de manière unique

$$\zeta \epsilon_1^{a_1} \cdots \epsilon_r^{a_r}$$

avec ζ racine de l'unité et $a_j \in \mathbf{Z}$.

Soit $\eta_1, \dots, \eta_r$ un ensemble de r unités de k. On définit le *régulateur* $R(\eta_1, \dots, \eta_r)$ de ce système d'unités comme le module du déterminant d'un mineur $r \times r$ de la matrice $(r+1) \times r$ dont les colonnes sont

$$\lambda(\eta_j), \qquad (1 \leq j \leq r).$$

Le fait que la norme de η_j soit ± 1 montre que tous ces mineurs ont le même module. Un système de r unités est indépendant (dans le $\mathbf{Z}$-module $\mathbf{Z}_k^\times$) si et seulement si son régulateur n'est pas nul.

Lemme 3.35. *Soit $\epsilon_1, \dots, \epsilon_r$ un système fondamental d'unités de k et soit $\eta_1, \dots, \eta_r$ un système indépendant de r unités de k. Alors le quotient*

$$R(\eta_1, \dots, \eta_r)/R(\epsilon_1, \dots, \epsilon_r)$$

est égal à l'indice du sous-groupe de $\mathbf{Z}_k^\times/k_{\text{tors}}^\times$ engendré par les classes de $\eta_1, \dots, \eta_r$.

Démonstration. Soit E le sous-groupe de $\mathbf{Z}_k^\times$ engendré par $\eta_1, \dots, \eta_r$. D'après la proposition 3.14 qui donne la structure des modules sur les anneaux principaux, il existe une base $x_1, \dots, x_r$ de $\mathbf{Z}_k^\times/k_{\text{tors}}^\times$ et des entiers positifs $a_1, \dots, a_r$ tels que $a_1x_1, \dots, a_rx_r$ soit une base de $E/k_{\text{tors}}^\times$. Alors l'indice de $E/k_{\text{tors}}^\times$ dans $\mathbf{Z}_k^\times/k_{\text{tors}}^\times$ est $a_1 \cdots a_r$, et le quotient des régulateurs aussi. □

En particulier le régulateur d'un système fondamental d'unités de k est le minimum parmi les régulateurs des systèmes indépendants de r unités de k, il ne dépend donc pas du système fondamental choisi : on l'appelle le *régulateur de k* et on le note R_k. Si $r = 0$ (c'est-à-dire $k = \mathbf{Q}$ ou si k est un corps quadratique imaginaire) on pose $R_k = 1$.

3.5 Idéaux d'un corps de nombres

3.5.1 Idéaux entiers

Soient K un corps de nombres, $\mathbf{Z}_K$ son anneau d'entiers, $\mathfrak{a}$ un idéal non nul de $\mathbf{Z}_K$, $\alpha \neq 0$ un élément de $\mathfrak{a}$. Alors $\mathbf{Z}_K\alpha \subset \mathfrak{a}$. Des propositions 3.12 et 3.14 on déduit que $\mathfrak{a}$ est un $\mathbf{Z}$-module libre de rang $n = [K : \mathbf{Q}]$. Par conséquent il existe une base $\{e_1, \dots, e_n\}$ de $\mathbf{Z}_K$ comme $\mathbf{Z}$-module et des entiers positifs $a_1, \dots, a_n$ tels que $\{a_1e_1, \dots, a_ne_n\}$ soit une base de $\mathfrak{a}$ sur $\mathbf{Z}$ et que a_i divise a_{i+1} dans $\mathbf{Z}$ pour $1 \leq i < n$. On en déduit que le quotient $\mathbf{Z}_K/\mathfrak{a}$ est fini avec $a_1 \cdots a_n$ éléments. Le nombre d'éléments de $\mathbf{Z}_K/\mathfrak{a}$ est appelé *norme de* $\mathfrak{a}$ et noté $\mathrm{N}(\mathfrak{a})$.

Le lemme suivant montre que la norme d'un idéal principal est égale à la valeur absolue de la norme d'un générateur.

Lemme 3.36. *Soit K un corps de nombres et soit $\alpha \in \mathbf{Z}_K$. Alors*

$$\mathrm{N}(\alpha\mathbf{Z}_K) = |\mathrm{N}_{K/\mathbf{Q}}(\alpha)|.$$

Démonstration. Soit $\alpha \in \mathbf{Z}_K$. On utilise la proposition 3.14 : il existe une base $\{e_1, \dots, e_n\}$ de $\mathbf{Z}_K$ et des entiers $a_1, \dots, a_n$ tels que $\{a_1e_1, \dots, a_ne_n\}$ soit une base de l'idéal $\alpha\mathbf{Z}_K$. Soit u l'endomorphisme du $\mathbf{Z}$-module $\mathbf{Z}_K$ qui envoie e_i sur a_ie_i. Son image est $\alpha\mathbf{Z}_K$ et sa matrice dans la base $\{e_1, \dots, e_n\}$ est la matrice diagonale $\mathrm{diag}(a_1, \dots, a_n)$, donc son déterminant est $a_1 \cdots a_n = \mathrm{N}(\alpha\mathbf{Z}_K)$. Comme $\{\alpha e_1, \dots, \alpha e_n\}$ est aussi une base de $\alpha\mathbf{Z}_K$, il existe un automorphisme v du $\mathbf{Z}$-module $\alpha\mathbf{Z}_K$ tel que $v(a_ie_i) = \alpha e_i$. Alors $\det v = \pm 1$; comme $v \circ u$ est la restriction de $[\alpha]$ à $\mathbf{Z}_K$, le déterminant de u est aussi égal à $\pm\mathrm{N}_{K/\mathbf{Q}}(\alpha)$. □

Soient K un corps de nombres, $n = [K : \mathbf{Q}]$ son degré et $\underline{\sigma} : k \to \mathbf{R}^n$ son plongement canonique.

Lemme 3.37. *Soit $\mathfrak{a}$ un idéal non nul de $\mathbf{Z}_K$. Alors $\underline{\sigma}(\mathfrak{a})$ est un réseau de $\mathbf{R}^n$ de volume $2^{-r_2}|D_K|^{1/2}\mathrm{N}(\mathfrak{a})$.*

Démonstration. En effet $\mathfrak{a}$ est un sous-groupe d'indice fini $\mathrm{N}(\mathfrak{a})$ de $\mathbf{Z}_K$, donc $\underline{\sigma}(\mathfrak{a})$ est un sous-groupe d'indice fini $\mathrm{N}(\mathfrak{a})$ de $\underline{\sigma}(\mathbf{Z}_K)$.

□

Il en résulte que le discriminant de $\mathfrak{a}$ est $|D_K|\mathrm{N}(\mathfrak{a})^2$.

Le théorème de Minkowski (corollaire 3.24) joint à un petit calcul de volume (voir le livre de Samuel, § 4.2) donne l'énoncé suivant, dont nous déduirons plusieurs conséquences ultérieurement (§ 3.6.5). Quand r_1 et r_2 sont deux entiers ≥ 0 avec $n = r_1 + 2r_2 \geq 1$ on définit la *constante de Minkowski* $M(r_1, r_2)$ par

$$M(r_1, r_2) = \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n}.$$

On écrit encore $M(K)$ au lieu de $M(r_1, r_2)$ quand K est un corps de nombres de degré n ayant r_1 plongements réels et $2r_2$ plongements imaginaires deux-à-deux conjugués.

Théorème 3.38. *Soient K un corps de nombres et $\mathfrak{a}$ un idéal non nul de $\mathbf{Z}_K$. Il existe $\alpha \in \mathfrak{a}$ tel que*

$$1 \leq |N_{K/\mathbf{Q}}(\alpha)| \leq M(K)|D_K|^{1/2}\mathrm{N}(\mathfrak{a}).$$

3.5.2 Idéaux premiers

Soient K un corps de nombres, $\mathbf{Z}_K$ son anneau d'entiers, $\mathfrak{p}$ un idéal premier de $\mathbf{Z}_K$.

L'injection de $\mathbf{Z}$ dans $\mathbf{Z}_K$ induit une injection de $\mathbf{Z}/\mathfrak{p} \cap \mathbf{Z}$ dans l'anneau $\mathbf{Z}_K/\mathfrak{p}$ qui est intègre, donc $\mathbf{Z}/\mathfrak{p} \cap \mathbf{Z}$ est intègre et l'idéal $\mathfrak{p} \cap \mathbf{Z}$ de $\mathbf{Z}$ est premier.

Rappelons le résultat élémentaire suivant :

Lemme 3.39. *Un anneau fini intègre est un corps.*

Démonstration. Si A est un anneau fini intègre, pour $x \in A \setminus \{0\}$ l'application $y \mapsto xy$ est une injection de A dans A, donc une bijection. □

Si $\mathfrak{p}$ est un idéal premier non nul de $\mathbf{Z}_K$ alors le quotient $k = \mathbf{Z}_K/\mathfrak{p}$ est un anneau fini intègre, donc un corps. Le corps fini $k = \mathbf{Z}_K/\mathfrak{p}$ est appelé *corps résiduel de* $\mathfrak{p}$. Dans ce cas $\mathbf{Z}/\mathfrak{p} \cap \mathbf{Z}$ est un sous-corps de k, donc $\mathfrak{p} \cap \mathbf{Z} \neq \{0\}$. Soit p le générateur positif de $\mathbf{Z} \cap \mathfrak{p}$. La caractéristique du corps résiduel k (on dit encore la *caractéristique résiduelle de* $\mathfrak{p}$) est p. La norme de $\mathfrak{p}$ est donc p^f où $f = [k : \mathbf{F}_p]$ est le *degré du corps résiduel*.

Si $\alpha \in \mathfrak{p}$ a pour polynôme minimal $X^m + a_1X^{m-1} + \cdots + a_m$ (avec $m = [\mathbf{Q}(\alpha) : \mathbf{Q}]$) alors a_m appartient $\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$, donc $N(\alpha) = (-1)^m a_m$ est divisible par p.

Lemme 3.40. *Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux non nuls de $\mathbf{Z}_K$. Si $\mathfrak{a} = \mathfrak{a}\mathfrak{b}$, alors $\mathfrak{b} = \mathbf{Z}_K$.*

Démonstration. Soit $\alpha_1, \ldots, \alpha_n$ une base de l'idéal $\mathfrak{a}$ comme $\mathbf{Z}$-module. Comme $\alpha_i \in \mathfrak{a}\mathfrak{b}$ pour $1 \leq i \leq n$, on peut écrire

$$\alpha_i = \sum_{j=1}^{n} \beta_{ij}\alpha_j \quad \text{pour} \quad 1 \leq i \leq n,$$

avec des coefficients β_{ij} dans $\mathfrak{b}$. Alors la matrice $\left(\beta_{ij}\right)_{1 \leq i,j \leq n} - I$ a un déterminant nul, d'où on déduit en développant $1 \in \mathfrak{b}$.

□

Lemme 3.41. *Soit $\mathfrak{a}$ un idéal non nul de $\mathbf{Z}_K$ et soit $\mathfrak{p}$ un idéal premier non nul de $\mathbf{Z}_K$. On désigne par k le corps résiduel $\mathbf{Z}_K/\mathfrak{p}$. Alors $\mathfrak{a}/\mathfrak{p}\mathfrak{a}$ est un k-espace vectoriel de dimension ≥ 1.*

Démonstration. La structure de $\mathbf{Z}_K$-module du quotient $\mathfrak{a}/\mathfrak{p}\mathfrak{a}$ est donnée par un homomorphisme de $\mathbf{Z}_K$-modules

$$\begin{array}{ccc} \mathbf{Z}_K & \to & \mathrm{Hom}_{\mathbf{Z}_K}(\mathfrak{a}/\mathfrak{p}\mathfrak{a}, \mathfrak{a}/\mathfrak{p}\mathfrak{a}) \\ a & \mapsto & (x \mapsto ax) \end{array}$$

dont le noyau contient $\mathfrak{p}$. On en déduit un homomorphisme de $\mathbf{Z}_K$-modules de $\mathbf{Z}_K/\mathfrak{p}$ dans $\mathrm{Hom}_{\mathbf{Z}_K}(\mathfrak{a}/\mathfrak{p}\mathfrak{a}, \mathfrak{a}/\mathfrak{p}\mathfrak{a})$ qui confère à $\mathfrak{a}/\mathfrak{p}\mathfrak{a}$ une structure de k-espace vectoriel. Le lemme 3.65 implique $\mathfrak{a} \neq \mathfrak{p}\mathfrak{a}$, donc la dimension de ce k-espace vectoriel est ≥ 1. □

Soit $\mathfrak{p}$ un idéal premier non nul de $\mathbf{Z}_K$. En utilisant au choix le lemme 3.65 ou bien le lemme 3.66, on obtient $\mathfrak{p}^m \neq \mathfrak{p}^{m+1}$ pour tout $m \geq 0$. La suite

$$\mathbf{Z}_K \supset \mathfrak{p} \supset \mathfrak{p}^2 \cdots \supset \mathfrak{p}^m \supset \cdots$$

est donc strictement décroissante. D'après le lemme 3.66 le quotient $\mathfrak{p}^m/\mathfrak{p}^{m+1}$ est isomorphe comme $\mathbf{Z}_K$-module à $\mathbf{Z}_K/\mathfrak{p}$; il en résulte que la norme de $\mathfrak{p}^m$ est $\mathrm{N}(\mathfrak{p})^m$, qui tend vers $+\infty$ avec m, donc l'intersection de tous les $\mathfrak{p}^m$ est $\{0\}$.

Soit $\mathfrak{a}$ un idéal non nul de $\mathbf{Z}_K$. L'ensemble des entiers $t \geq 0$ tels que $\mathfrak{a} \subset \mathfrak{p}^t$ est non vide (il contient 0) et fini. On désigne par $v_\mathfrak{p}(\mathfrak{a})$ le plus grand de ces entiers :

$$\mathfrak{a} \subset \mathfrak{p}^t \quad \text{pour} \quad 0 \leq t \leq v_\mathfrak{p}(\mathfrak{a}) \quad \text{et} \quad \mathfrak{a} \not\subset \mathfrak{p}^t \quad \text{pour} \quad t = v_\mathfrak{p}(\mathfrak{a}) + 1.$$

On a $v_\mathfrak{p}(\mathfrak{a}) > 0$ si et seulement si $\mathfrak{a} \subset \mathfrak{p}$. On a aussi $v_\mathfrak{p}(\mathfrak{a}\mathfrak{p}) = v_\mathfrak{p}(\mathfrak{a}) + 1$, donc $v_\mathfrak{p}(\mathfrak{p}^m) = m$ pour $m \geq 0$. Enfin $v_\mathfrak{p}(\mathfrak{p}') = 0$ si $\mathfrak{p}$ et $\mathfrak{p}'$ sont deux idéaux premiers distincts.

Théorème 3.42. *Soit $\mathfrak{a}$ un idéal non nul de $\mathbf{Z}_K$. L'ensemble des idéaux premiers $\mathfrak{p}$ de $\mathbf{Z}_K$ qui contiennent $\mathfrak{a}$ est fini et on a*

$$\mathfrak{a} = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})},$$

où le produit est étendu à l'ensemble des idéaux premiers non nuls de $\mathbf{Z}_K$.

De plus une telle décomposition est unique : si on a

$$\mathfrak{a} = \prod_\mathfrak{p} \mathfrak{p}^{a_\mathfrak{p}},$$

où les $a_\mathfrak{p}$ sont des entiers rationnels ≥ 0 tous nuls sauf un nombre fini, alors $a_\mathfrak{p} = v_\mathfrak{p}(\mathfrak{a})$ pour tout $\mathfrak{p}$.

Remarque. Le théorème 3.67 montre que, sous les hypothèses du lemme 3.66, $\mathfrak{a}/\mathfrak{a}\mathfrak{p}$ est de dimension 1 comme espace vectoriel sur $\mathbf{Z}_K/\mathfrak{p}$ car il n'y a pas d'idéal entre $\mathfrak{a}\mathfrak{p}$ et $\mathfrak{a}$.

La démonstration du théorème 3.67 nécessite des préliminaires. Commençons par quelques lemmes sur les idéaux d'un anneau (unitaire commutatif).

Lemme 3.43. *Soit $\mathfrak{a}_1, \ldots, \mathfrak{a}_m$ des idéaux d'un anneau A et soit $\mathfrak{p}$ un idéal premier de A contenant le produit $\mathfrak{a}_1 \cdots \mathfrak{a}_m$. Alors $\mathfrak{p}$ contient l'un au moins des $\mathfrak{a}_i$.*

Démonstration. Supposons que $\mathfrak{p}$ ne contienne aucun des $\mathfrak{a}_i$. Pour $1 \leq i \leq n$ il existe $\alpha_i \in \mathfrak{a}_i$ tel que $\alpha_i \notin \mathfrak{p}$. Alors $\alpha_1 \cdots \alpha_n$ n'appartient pas à $\mathfrak{p}$, donc $\mathfrak{p}$ ne contient pas $\mathfrak{a}_1 \cdots \mathfrak{a}_m$.

□

Lemme 3.44. *On suppose A noethérien. Soit $\mathfrak{a}$ un idéal non nul de A. Il existe des idéaux premiers non nuls $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ de A dont le produit $\mathfrak{p}_1 \cdots \mathfrak{p}_m$ est contenu dans $\mathfrak{a}$.*

Démonstration. Soit E l'ensemble des idéaux non nuls de A qui ne satisfont pas la conclusion. Si cet ensemble n'était pas vide, comme A est noethérien, il admettrait un élément maximal $\mathfrak{a}$. Alors $\mathfrak{a}$ n'est pas premier, donc il existe α_1 et α_2 dans $A \setminus \mathfrak{a}$ tels que $\alpha_1\alpha_2 \in \mathfrak{a}$. Posons $\mathfrak{a}_i = \mathfrak{a} + A\alpha_i$. Alors $\mathfrak{a}_1$ et $\mathfrak{a}_2$ sont des idéaux contenant strictement $\mathfrak{a}$, donc ils n'appartiennent pas à E : chacun d'eux contient un produit d'idéaux premiers non nuls

$$\mathfrak{a}_1 \supset \mathfrak{p}_1 \cdots \mathfrak{p}_m, \qquad \mathfrak{a}_2 \supset \mathfrak{p}_{m+1} \cdots \mathfrak{p}_n$$

et $\mathfrak{a}$ contient $\mathfrak{a}_1\mathfrak{a}_2$, d'où la contradiction. □

Lemme 3.45. *Soit $\mathfrak{p}$ un idéal premier non nul de $\mathbf{Z}_K$. Il existe $x \in K \setminus \mathbf{Z}_K$ tel que $x\mathfrak{p} \subset \mathbf{Z}_K$.*

Démonstration. Soit $\alpha \in \mathfrak{p} \setminus \{0\}$. D'après le lemme 3.44 l'idéal $\mathbf{Z}_K\alpha$ contient un produit d'idéaux premiers non nuls. On considère un tel produit

$$\mathbf{Z}_K\alpha \supset \mathfrak{p}_1 \cdots \mathfrak{p}_m$$

avec m minimal. Comme $\mathbf{Z}_K\alpha \subset \mathfrak{p}$ le lemme 3.43 entraîne que $\mathfrak{p}$ contient l'un des $\mathfrak{p}_i$ - quitte à changer la numérotation on peut supposer que c'est $\mathfrak{p}_1$. Comme $\mathfrak{p}_1$ est maximal on a $\mathfrak{p} = \mathfrak{p}_1$. Soit $\mathfrak{b} = \mathfrak{p}_2 \cdots \mathfrak{p}_m$. On a $\mathbf{Z}_K\alpha \supset \mathfrak{p}\mathfrak{b}$, et le choix de m minimal donne $\mathbf{Z}_K\alpha \not\supset \mathfrak{b}$. Soit $\beta \in \mathfrak{b}$ tel que $\beta \notin \mathbf{Z}_K\alpha$. Alors $x = \beta/\alpha \in K \setminus \mathbf{Z}_K$ vérifie $x\mathfrak{p} \subset \mathbf{Z}_K$.

□

3.5.3 Idéaux fractionnaires

Soient A un anneau intègre, K son corps des fractions. Un sous-A-module $\mathfrak{a}$ non nul de K est un idéal fractionnaire de K par rapport à A s'il vérifie les propriétés équivalentes suivantes :
(i) Il existe $\alpha \in A$, $\alpha \neq 0$ tel que $\alpha\mathfrak{a} \subset A$.
(ii) Il existe $\beta \in K$, $\beta \neq 0$ tel que $\beta\mathfrak{a} \subset A$.

L'équivalence vient du fait que si $\beta\mathfrak{a} \subset A$ avec $\beta \in K^\times$, alors on peut écrire $\beta = \alpha/\gamma$ avec α et γ dans $A \setminus \{0\}$, d'où $\alpha\mathfrak{a} \subset A$.

On dira aussi que $\mathfrak{a}$ est un idéal fractionnaire de A.

Lemme 3.46. *Si $\mathfrak{a}_1$ et $\mathfrak{a}_2$ sont des idéaux fractionnaires de A, alors*

$$\mathfrak{a}_1 + \mathfrak{a}_2, \quad \mathfrak{a}_1 \cap \mathfrak{a}_2, \quad \mathfrak{a}_1\mathfrak{a}_2$$

et

$$(\mathfrak{a}_1 : \mathfrak{a}_2) := \{x \in K \ ; \ x\mathfrak{a}_2 \subset \mathfrak{a}_1\}$$

sont des idéaux fractionnaires de A.

Démonstration. Si α_1 et α_2 sont des éléments non nuls de $A \setminus \{0\}$ tels que $\mathfrak{a}_i \subset \alpha_i^{-1}A$ pour $i = 1$ et $i = 2$, alors $\mathfrak{a}_1 + \mathfrak{a}_2$, $\mathfrak{a}_1 \cap \mathfrak{a}_2$ et $\mathfrak{a}_1\mathfrak{a}_2$ sont des sous-A-modules non nuls de K contenus dans $(\alpha_1\alpha_2)^{-1}A$.

Si a_1 est un élément non nul de $\mathfrak{a}_1$ et α_2 un élément non nul de A tel que $\mathfrak{a}_2 \subset \alpha_2^{-1}A$, alors $a_1\alpha_2$ est un élément non nul de $(\mathfrak{a}_1 : \mathfrak{a}_2)$:

$$a_1\alpha_2\mathfrak{a}_2 \subset a_1A \subset \mathfrak{a}_1.$$

Si α_1 est un élément non nul de A tel que $\mathfrak{a}_1 \subset \alpha_1^{-1}A$ et si a_2 est un élément non nul de $\mathfrak{a}_2$, alors pour tout $x \in (\mathfrak{a}_1 : \mathfrak{a}_2)$ on a

$$\alpha_1 a_2 x \in \alpha_1 x\mathfrak{a}_2 \subset \alpha_1\mathfrak{a}_1 \subset A,$$

donc $\alpha_1 a_2(\mathfrak{a}_1 : \mathfrak{a}_2) \subset A$.

□

On déduit du lemme 3.68 que si $\mathfrak{a}$ est un idéal fractionnaire de A, alors

$$(A : \mathfrak{a}) = \{x \in K \ ; \ x\mathfrak{a} \subset A\} \quad \text{et} \quad (\mathfrak{a} : \mathfrak{a}) = \{x \in K \ ; \ x\mathfrak{a} \subset \mathfrak{a}\}$$

sont des idéaux fractionnaires de A.

Tout sous-A-module de type fini de K non nul est un idéal fractionnaire.

Réciproquement, quand A est un anneau noethérien, tout idéal fractionnaire de A est de type fini : pour $\alpha \in A \setminus \{0\}$ les A-modules $\mathfrak{a}$ et $\alpha\mathfrak{a}$ sont isomorphes. Donc, quand A est noethérien, un idéal fractionnaire n'est autre qu'un sous-A-module non nul de type fini de K. Si $\mathfrak{a}$ admet $\{a_i\}$ comme partie génératrice et si $\mathfrak{b}$ est engendré par $\{b_j\}$, alors $\mathfrak{a} + \mathfrak{b}$ est engendré par $\{a_i\} \cup \{b_j\}$ et $\mathfrak{a}\mathfrak{b}$ par $\{a_ib_j\}$.

Lemme 3.47. *Soit $\mathfrak{a}$ un idéal non nul de $\mathbf{Z}_K$ et soit $x \in K$ tel que $x\mathfrak{a} \subset \mathfrak{a}$. Alors $x \in \mathbf{Z}_K$.*

Démonstration. L'hypothèse $x\mathfrak{a} \subset \mathfrak{a}$ entraîne, par récurrence sur n, $x^n\mathfrak{a} \subset \mathfrak{a}$ pour tout $n \geq 0$. Soit $\alpha \in \mathfrak{a} \setminus \{0\}$. On a $\alpha x^n \in \mathbf{Z}_K$ pour tout $n \geq 0$, donc $\mathbf{Z}_K[x]$ est un idéal fractionnaire de $\mathbf{Z}_K$:

$$\alpha\mathbf{Z}_K[x] \subset \mathbf{Z}_K.$$

Comme $\mathbf{Z}_K$ est noethérien, $\mathbf{Z}_K[x]$ est un $\mathbf{Z}_K$-module de type fini. Comme c'est aussi un anneau contenant x, on déduit de la proposition 3.8 que x est entier sur $\mathbf{Z}_K$, donc $x \in \mathbf{Z}_K$. □

Le lemme 3.47 montre que sous les hypothèses du lemme 3.45, l'élément x donné dans la conclusion satisfait $x\mathfrak{p} \not\subset \mathfrak{p}$.

Quand K est un corps de nombres, un *idéal entier* de K est un idéal de $\mathbf{Z}_K$, c'est-à-dire un idéal fractionnaire de $\mathbf{Z}_K$ contenu dans $\mathbf{Z}_K$.

Proposition 3.48. *Soit $\mathfrak{p}$ un idéal premier non nul de $\mathbf{Z}_K$. Soit*

$$\mathfrak{p}' = \{x \in K \ ; \ x\mathfrak{p} \subset \mathbf{Z}_K\}.$$

Alors $\mathfrak{p}'$ est un idéal fractionnaire de $\mathbf{Z}_K$ qui contient $\mathbf{Z}_K$ et $\mathfrak{p}\mathfrak{p}' = \mathbf{Z}_K$.

Démonstration. Que $\mathfrak{p}' = (\mathbf{Z}_K : \mathfrak{p})$ soit un idéal fractionnaire résulte du lemme 3.68, comme nous l'avons vu. Il contient évidemment $\mathbf{Z}_K$ puisque $\mathfrak{p}$ est un idéal de $\mathbf{Z}_K$; donc $\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}'$. Le lemme 3.45 entraîne $\mathfrak{p}' \neq \mathbf{Z}_K$ et le lemme 3.47 livre $\mathfrak{p}'\mathfrak{p} \neq \mathfrak{p}$. Comme $\mathfrak{p} \subset \mathfrak{p}'\mathfrak{p} \subset \mathbf{Z}_K$ et que $\mathfrak{p}$ est un idéal maximal de $\mathbf{Z}_K$, il en résulte que l'on a $\mathfrak{p}\mathfrak{p}' = \mathbf{Z}_K$.

□

Le lemme 3.69 signifie que les idéaux premiers non nuls sont inversibles dans le monoïde des idéaux fractionnaires de $\mathbf{Z}_K$. L'inverse $\mathfrak{p}'$ de $\mathfrak{p}$ est aussi noté $\mathfrak{p}^{-1}$:

$$\mathfrak{p}^{-1} = \{x \in K \ ; \ x\mathfrak{p} \subset \mathbf{Z}_K\}.$$

Démonstration du théorème 3.67.
a) Montrons que tout idéal entier non nul de $\mathbf{Z}_K$ admet une décomposition

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{a_\mathfrak{p}}, \tag{3.49}$$

avec des entiers $a_\mathfrak{p} \geq 0$, où l'ensemble $\{\mathfrak{p} \ ; \ a_\mathfrak{p} \neq 0\}$ est un ensemble fini. Pour cela soit E l'ensemble des idéaux non nuls de $\mathbf{Z}_K$ qui n'admettent pas une telle décomposition et soit $\mathfrak{a}$ un élément maximal de E. Comme l'idéal $\mathbf{Z}_K$ n'est pas dans E (il est égal au produit vide d'idéaux premiers), on a $\mathfrak{a} \neq \mathbf{Z}_K$, donc il existe un idéal premier $\mathfrak{p}$ de $\mathbf{Z}_K$ qui contient $\mathfrak{a}$. On utilise la proposition 3.69.

Comme $\mathfrak{a} \subset \mathfrak{p}$, on a $\mathfrak{a}\mathfrak{p}^{-1} \subset \mathfrak{p}\mathfrak{p}^{-1} = \mathbf{Z}_K$. Ceci montre que $\mathfrak{a}\mathfrak{p}^{-1}$ est un idéal de $\mathbf{Z}_K$.

Comme $\mathfrak{p}^{-1} \supset \mathbf{Z}_K$, on a $\mathfrak{a}\mathfrak{p}^{-1} \supset \mathfrak{a}$.

Comme $\mathfrak{a} = \mathfrak{a}\mathfrak{p}^{-1}\mathfrak{p}$ est dans E, $\mathfrak{a}\mathfrak{p}^{-1}$ aussi. Comme $\mathfrak{a}$ est un élément maximal de E on a donc $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$.

Soit $x \in \mathfrak{p}^{-1}$; on a $x\mathfrak{a} \subset \mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$, donc (lemme 3.47) $x \in \mathbf{Z}_K$. Cela contredit le lemme 3.45. Donc E est vide.
b) Montrons que la décomposition (3.49) est unique : si un idéal est produit de deux façons distinctes d'idéaux premiers,

$$\prod_{\mathfrak{p}} \mathfrak{p}^{a_\mathfrak{p}} = \prod_{\mathfrak{p}} \mathfrak{p}^{b_\mathfrak{p}},$$

en ne conservant que les exposants non nuls et en simplifiant les termes communs on trouve

$$\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_m^{a_m} = \mathfrak{q}_1^{b_1} \cdots \mathfrak{p}_\ell^{b_\ell}$$

avec des idéaux $\mathfrak{p}_i$ $(1 \leq i \leq m)$ et $\mathfrak{q}_j$ $(1 \leq j \leq \ell)$ deux-à-deux distincts et des exposants a_i, b_j tous > 0. Alors $\mathfrak{p}_1$ contient le produit d'idéaux premiers $\mathfrak{q}_1^{b_1} \cdots \mathfrak{p}_\ell^{b_\ell}$, donc il contient l'un d'eux, disons $\mathfrak{q}_1$, et comme $\mathfrak{q}_1$ est maximal on a $\mathfrak{p}_1 = \mathfrak{q}_1$. C'est une contradiction.
c) Il reste à vérifier que dans la décomposition (3.49) on a $a_\mathfrak{p} = v_\mathfrak{p}(\mathfrak{a})$ pour tout $\mathfrak{p}$ idéal premier non nul de $\mathbf{Z}_K$.

Il est clair que si $a_\mathfrak{p} \geq m$ alors

$$\mathfrak{p}^m \supset \mathfrak{p}^{a_\mathfrak{p}} \supset \mathfrak{a}.$$

Inversement si $\mathfrak{p}^m \supset \mathfrak{a}$ alors $a_\mathfrak{p} \geq m$: cela se voit grâce au lemme 3.43 en multipliant les deux côtés de cette inclusion par $\mathfrak{p}^{-a_\mathfrak{p}}$.

Ainsi $\mathfrak{a} \not\subset \mathfrak{p}^{a_\mathfrak{p}+1}$, donc $a_\mathfrak{p} = v_\mathfrak{p}(\mathfrak{a})$.

□

Remarque. *La démonstration du lemme 3.66 n'est pas complète. Le fait qu'il n'y ait pas d'idéal de* $\mathbf{Z}_K$ *entre* $\mathfrak{pa}$ *et* $\mathfrak{a}$ *demande à être justifiée. On peut le faire de la façon suivante : la démonstration qui précède du théorème 3.67 établit, sans utiliser le lemme 3.66, l'existence et l'unicité de la décomposition d'un idéal non nul* $\mathfrak{a}$ *en produit d'idéaux premiers. On a vérifié que pour chaque idéal premier non nul* $\mathfrak{p}$*, on a*

$$\mathfrak{p}^a\mathfrak{p} \subset \mathfrak{a} \quad et \quad \mathfrak{p}^a\mathfrak{p}^{+1} \not\subset \mathfrak{a}.$$

Cela justifie la définition de $v_\mathfrak{p}(\mathfrak{a})$ *et démontre* $a_\mathfrak{p} = v_\mathfrak{p}(\mathfrak{a})$.

Pour établir le lemme 3.66, on pose $m = v_\mathfrak{p}(\mathfrak{a})$*. On a* $v_\mathfrak{p}(\mathfrak{ap}) = m + 1$*, donc* $\mathfrak{ap} \neq \mathfrak{a}$*. Le théorème 3.67 montre qu'il n'y a pas d'idéal entre* $\mathfrak{ap}$ *et* $\mathfrak{a}$*. Donc* $\mathfrak{a}/\mathfrak{ap}$ *est de dimension* 1 *comme espace vectoriel sur* $\mathbf{Z}_K/\mathfrak{p}$*.*

Petit aperçu historique

L'invention de la notion d'idéal provient des recherches au XIXème siècle sur le *dernier théorème de Fermat* : il s'agissait de démontrer qu'il n'y a pas d'entiers positifs $n \geq 3$, x, y et z satisfaisant $x^n + y^n = z^n$. En supposant n impair et en utilisant l'identité

$$x^n + y^n = (x + y)(x + \zeta y) \cdots (x + \zeta^{n-1} y), \quad \zeta = \zeta_n = e^{2i\pi/n}$$

Kummer a démontré en 1844 que l'énoncé de Fermat est vrai pour un exposant premier $n = p$ pour lequel l'anneau des entiers du corps $\mathbf{Q}(\zeta_p)$ est factoriel ; Dirichlet a alors remarqué que l'existence d'une décomposition en facteurs irréductibles est toujours vraie, mais que l'unicité n'est pas claire. C'est dès 1844 que Kummer a su qu'il n'y avait pas unicité de la décomposition en éléments irréductibles dans l'anneau $\mathbf{Z}[\zeta_{23}]$. Il l'a écrit à Liouville en 1847 (à la suite d'une note de G. Lamé à l'Académie des Sciences le 11 mars 1847), ajoutant qu'il avait trouvé un substitut qui étaient les "nombres idéaux". L'idée est la suivante.

Dans le corps $k = \mathbf{Q}(\sqrt{-5})$ la décomposition en facteurs irréductibles n'est pas unique

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}).$$

Kummer affirme qu'il existe des objets qu'il appelle *nombres idéaux* donnant une décomposition unique

$$(21) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$$

qui explique la décomposition précédente :

$$\mathfrak{p}_1\mathfrak{p}_2 = (3), \quad \mathfrak{p}_3\mathfrak{p}_4 = (7), \qquad \mathfrak{p}_1\mathfrak{p}_3 = (1 + 2\sqrt{-5}), \quad \mathfrak{p}_2\mathfrak{p}_4 = (1 - 2\sqrt{-5}).$$

Dedekind a précisé cette construction de nombres idéaux. Si $\mathfrak{a}$ est un nombre idéal, on veut satisfaire les relations, pour a et b dans $\mathbf{Z}_k$,

$$\text{si } \mathfrak{a}|a \text{ et } \mathfrak{a}|b \text{ alors pour tout } \lambda \in \mathbf{Z}_k \text{ et } \mu \in \mathbf{Z}_k \text{ on a } \mathfrak{a}|\lambda a + \mu b.$$

On veut aussi que $\mathfrak{a}$ soit déterminé par $\{a \in \mathbf{Z}_k \ ; \ \mathfrak{a}|a\}$. L'idée est donc de considérer les sous-ensembles $\mathfrak{a}$ de $\mathbf{Z}_k$ qui vérifient la propriété

$$a \in \mathfrak{a},\ b \in \mathfrak{a}, \lambda \in \mathbf{Z}_k,\ \mu \in \mathbf{Z}_k \ \Rightarrow \lambda a + \mu b \in \mathfrak{a}.$$

Ce sont donc les idéaux de $\mathbf{Z}_k$.

Dans l'exemple précédent on prend

$$\mathfrak{p}_1 = (3, 1 - \sqrt{-5}), \quad \mathfrak{p}_2 = (3, 1 + \sqrt{-5}), \quad \mathfrak{p}_3 = (7, 3 - \sqrt{-5}), \quad \mathfrak{p}_4 = (7, 3 + \sqrt{-5}).$$

Références : [R], [P], Sk].

Soit K un corps de nombres. Le théorème 3.67 montre que la propriété (3.1) de multiplicativité de la norme s'étend aux idéaux de $\mathbf{Z}_K$:

Corollaire 3.50. *Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux de $\mathbf{Z}_K$. Alors*

$$\mathrm{N}(\mathfrak{ab}) = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{b}). \tag{3.51}$$

Démonstration. Grâce au théorème 3.67 il suffit de vérifier la propriété (3.72) quand $\mathfrak{b}$ est un idéal premier. Notons-le $\mathfrak{p}$.

L'homomorphisme canonique

$$\mathbf{Z}_K/\mathfrak{ap} \to \mathbf{Z}_K/\mathfrak{a}$$

est surjectif et a pour noyau $\mathfrak{a}/\mathfrak{ap}$. Le quotient $k = \mathbf{Z}_K/\mathfrak{p}$ est un corps fini (ayant $\mathrm{N}(\mathfrak{p})$ éléments) et $\mathfrak{a}/\mathfrak{ap}$ est un k-espace vectoriel de dimension 1 (car $\mathfrak{p}$ est maximal - cf lemme 3.66 et la remarque qui suit le théorème 3.67), donc est isomorphe à k. Ainsi $\mathfrak{a}/\mathfrak{ap}$ a $\mathrm{N}(\mathfrak{p})$ éléments et par conséquent $\mathbf{Z}_K/\mathfrak{ap}$ en a $\mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{p})$.

□

Exercice. Soient $\mathfrak{a}$ un idéal non nul et $\mathfrak{p}$ un idéal premier non nul de $\mathbf{Z}_K$.
1. Montrer qu'il existe $\alpha \in \mathfrak{a}$ tel que $\alpha \notin \mathfrak{ap}$.
Montrer qu'il existe un idéal $\mathfrak{b}$ de $\mathbf{Z}_K$ tel que $\mathfrak{ab} = \alpha\mathbf{Z}_K$.
Vérifier $\mathfrak{a} = \alpha\mathbf{Z}_K + \mathfrak{ap}$.
2. Soient $a_1, \ldots, a_N$ des représentants des classes de $\mathbf{Z}_K$ modulo $\mathfrak{a}$, avec $N = \mathrm{N}(\mathfrak{a})$, et soient $b_1, \ldots, b_M$ des représentants des classes de $\mathbf{Z}_K$ modulo $\mathfrak{p}$, avec $M = \mathrm{N}(\mathfrak{p})$. Vérifier que $\{a_i + \alpha b_j\}_{\substack{1 \le i \le N \\ 1 \le j \le M}}$ est un système complet de représentants des classes de $\mathbf{Z}_K$ modulo $\mathfrak{ap}$.

Du théorème 3.67 on déduit que les idéaux fractionnaires de $\mathbf{Z}_K$ forment un groupe abélien d'élément neutre $\mathbf{Z}_K = (1)$.

Corollaire 3.52. *Soit $\mathfrak{a}$ un idéal fractionnaire de $\mathbf{Z}_K$. Il existe une décomposition unique*

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{a_\mathfrak{p}},$$

où le produit est étendu à l'ensemble des idéaux premiers non nuls de $\mathbf{Z}_K$ et les $a_\mathfrak{p}$ sont des entiers rationnels tels que $\{\mathfrak{p} \ ; \ a_\mathfrak{p} \neq 0\}$ soit fini.

Démonstration. Soit $\alpha \in \mathbf{Z}_K \setminus \{0\}$ tel que $\alpha\mathfrak{a} \subset \mathbf{Z}_K$. On décompose les idéaux entiers $\alpha\mathbf{Z}_K$ et $\alpha\mathfrak{a}$ en produit d'idéaux premiers, on multiplie par les inverses des idéaux premiers apparaissant dans la décomposition de $\alpha\mathbf{Z}_K$ et on trouve la décomposition annoncée de $\mathfrak{a}$. L'unicité résulte de ce qui précède.

□

On pose encore, avec les notations du corollaire 3.70, $v_{\mathfrak{p}}(\mathfrak{a}) = a_{\mathfrak{p}}$ et

$$\mathrm{N}(\mathfrak{a}) = \prod_{\mathfrak{p}} \mathrm{N}(\mathfrak{p})^{a_{\mathfrak{p}}}.$$

La norme d'un idéal fractionnaire principal de $\mathbf{Z}_K$ est égale à la norme de K sur $\mathbf{Q}$ d'un générateur : pour tout $\alpha \in K^\times$ on a $\mathrm{N}(\alpha\mathbf{Z}_K) = \mathrm{N}_{K/\mathbf{Q}}(\alpha)$.

Du théorème 3.67 on déduit, pour $\mathfrak{p}$ idéal premier de $\mathbf{Z}_K$ et $\mathfrak{a}$, $\mathfrak{b}$ idéaux fractionnaires de $\mathbf{Z}_K$:

$$\begin{array}{rcl} v_{\mathfrak{p}}(\mathfrak{a}\mathfrak{b}) & = & v_{\mathfrak{p}}(\mathfrak{a}) + v_{\mathfrak{p}}(\mathfrak{b}), \\ v_{\mathfrak{p}}(\mathfrak{a}+\mathfrak{b}) & = & \min\{v_{\mathfrak{p}}(\mathfrak{a}), v_{\mathfrak{p}}(\mathfrak{b})\}, \\ v_{\mathfrak{p}}(\mathfrak{a}\cap\mathfrak{b}) & = & \max\{v_{\mathfrak{p}}(\mathfrak{a}), v_{\mathfrak{p}}(\mathfrak{b})\}. \end{array}$$

Soit $\mathfrak{p}$ un idéal premier de $\mathbf{Z}_K$. On définit *l'indice de ramification* $e(\mathfrak{p})$ de $\mathfrak{p}$ par $e(\mathfrak{p}) = v_{\mathfrak{p}}(p\mathbf{Z}_K)$ où p désigne la caractéristique résiduelle de $\mathfrak{p}$. Ainsi $e(\mathfrak{p}) \geq 1$.

Soit p un nombre premier et soit $p\mathbf{Z}_K$ l'idéal principal de $\mathbf{Z}_K$ qu'il engendre. Le théorème 3.67 montre qu'il existe une décomposition, unique à l'ordre près des facteurs,

$$p\mathbf{Z}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}, \tag{3.53}$$

où g est un entier ≥ 1, $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ sont des idéaux premiers de $\mathbf{Z}_K$ deux-à-deux distincts et $e_i \geq 1$ est l'indice de ramification de $\mathfrak{p}_i$ $(1 \leq i \leq g)$.

Les idéaux $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ sont précisément les idéaux premiers $\mathfrak{p}$ de $\mathbf{Z}_K$ tels que $\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$. On dit que ce sont les *idéaux premiers de* $\mathbf{Z}_K$ *au dessus de* p. De la décomposition (3.73) on déduit

$$\mathbf{Z}_K/p\mathbf{Z}_K \simeq \mathbf{Z}_K/\mathfrak{p}_1^{e_1} \cdots \mathbf{Z}_K/\mathfrak{p}_g^{e_g}.$$

En utilisant le corollaire 3.71 on obtient, en notant $n = [K : \mathbf{Q}]$ et en désignant par f_i le degré du corps résiduel de $\mathfrak{p}_i$,

$$p^n = \mathrm{N}_{K/\mathbf{Q}}(p) = \mathrm{N}(\mathfrak{p}_1)^{e_1} \cdots \mathrm{N}(\mathfrak{p}_g)^{e_g} = p^{e_1 f_1 + \cdots + e_g f_g}.$$

Par conséquent

$$e_1 f_1 + \cdots + e_g f_g = n. \tag{3.54}$$

On dit que $\mathfrak{p}_i$ est *ramifié au dessus de* p si l'exposant e_i est ≥ 2. On dit que p est *ramifié dans* K si l'un des exposants e_i est ≥ 2. On dit encore que p est
- *totalement ramifié dans* K si $e_1 = n$: alors $g = 1$ et $f_1 = 1$
- *totalement décomposé dans* K si $g = n$: alors $e_1 = \cdots = e_n = f_1 = \cdots = f_n = 1$
- *inerte dans* K si $f_1 = n$: alors $g = 1$ et $e_1 = 1$; cela revient à dire que $p\mathbf{Z}_K$ est un idéal premier.

Voici ce qui se passe pour les corps quadratiques

Proposition 3.55. *Soit d un entier sans facteur carré et soit p un nombre premier impair. Dans le corps $K = \mathbf{Q}(\sqrt{d})$, p se décompose de la façon suivante :*
(i) Si p divise d, alors p est ramifié dans K :
$p\mathbf{Z}_K = \mathfrak{p}^2$ *avec* $\mathrm{N}(\mathfrak{p}) = p$.
(ii) Si $\left(\frac{d}{p}\right) = 1$, *alors p est décomposé dans K :*
$p\mathbf{Z}_K = \mathfrak{p}_1\mathfrak{p}_2$ *avec* $\mathrm{N}(\mathfrak{p}_1) = \mathrm{N}(\mathfrak{p}_1) = p$.
(iii) Si $\left(\frac{d}{p}\right) = -1$, *alors p est inerte dans K :*
$p\mathbf{Z}_K = \mathfrak{p}$.

Démonstration. Si $d \equiv 2$ ou $3 \pmod 4$, alors $\mathbf{Z}_K = \mathbf{Z}[\sqrt{d}]$. Si $d \equiv 1 \pmod 4$, on a $\mathbf{Z}_K = \mathbf{Z}[(1+\sqrt{d})/2]$, dans ce dernier cas comme p est un nombre premier impair on peut écrire $\mathbf{Z}_K = \mathbf{Z}[\sqrt{d}] + p\mathbf{Z}_K$. Par conséquent on a toujours

$$\mathbf{Z}_K/p\mathbf{Z}_K = \mathbf{Z}[\sqrt{d}]/p\mathbf{Z}[\sqrt{d}] \simeq \mathbf{Z}[X]/(p, X^2-d) \simeq \mathbf{F}_p[X]/(X^2-d).$$

- Le polynôme $X^2 - d$ a une racine double dans $\mathbf{F}_p$ si et seulement si p divise d.
- Il se décompose en deux facteurs linéaires distincts si et seulement si $\left(\frac{d}{p}\right) = 1$.
- Il est irréductible si et seulement si $\left(\frac{d}{p}\right) = -1$. □

Exercice. Soit d un entier sans facteur carré et soit K le corps quadratique $\mathbf{Q}(\sqrt{d})$. Vérifier :
(i) 2 est ramifié dans K si et seulement si $d \equiv 2$ ou $3 \pmod 4$, c'est-à-dire si et seulement si le discriminant de K est pair.
(ii) 2 est décomposé dans K si et seulement si $d \equiv 1 \pmod 8$.
(iii) 2 est inerte dans K si et seulement si $d \equiv 5 \pmod 8$.

3.5.4 Discriminant et ramification

Nous admettrons (provisoirement ?) l'énoncé suivant :

Théorème 3.56. *Soit K un corps de nombres. Les nombres premiers qui se ramifient dans K sont en nombre fini : ce sont les diviseurs premiers du discriminant D_K.*

3.5.5 Classes d'idéaux - théorèmes de finitude

Soit K un corps de nombres. Les idéaux fractionnaires de $\mathbf{Z}_K$ forment un groupe multiplicatif. Les idéaux fractionnaires principaux (c'est-à-dire monogènes) forment un sous-groupe, et le quotient est le *groupe* $\mathrm{Cl}(K)$ *des classes d'idéaux de* K. Dire que deux idéaux fractionnaires $\mathfrak{a}$ et $\mathfrak{b}$ sont *équivalents* signifie qu'il existe $\alpha \in K$, $\alpha \neq 0$, tel que $\mathfrak{a} = \mathfrak{b} \cdot \alpha\mathbf{Z}_K$.

Soit $\mathfrak{a}$ un idéal fractionnaire et soit α un élément non nul de $\mathbf{Z}_K$ tel que $\alpha\mathfrak{a}$ soit un idéal entier. Il résulte de la définition que $\mathfrak{a}$ est équivalent à $\alpha\mathfrak{a}$. Donc toute classe d'équivalence contient un idéal entier.

Rappelons que $M(K)$ désigne la constante de Minkowski du corps K (théorème 3.63).

Proposition 3.57. *Toute classe d'idéaux contient un idéal entier $\mathfrak{a}$ de norme $\mathrm{N}(\mathfrak{a}) \leq M(K)|D_K|^{1/2}$.*

Démonstration. Si $\mathfrak{a}_1$ est un idéal dans la classe considérée, si α est un élément non nul de $\mathbf{Z}_K$ tel que l'idéal $\mathfrak{a}_2 = \alpha\mathfrak{a}_1^{-1}$ soit entier, en appliquant le théorème 3.63 à $\mathfrak{a}_2$ on trouve un élément $\beta \in \mathfrak{a}_2$ vérifiant $|\mathrm{N}_{K:\mathbf{Q}}(\beta)| \leq M(K)|D_K|^{1/2}\mathrm{N}(\mathfrak{a}_2)$. Alors $\mathfrak{a} = \beta\mathfrak{a}_2^{-1}$ est équivalent à $\mathfrak{a}_1$ et vérifie la propriété requise.

□

Théorème 3.58 (Minkowski). *Le groupe $\mathrm{Cl}(K)$ des classes d'idéaux de K est fini.*

Le nombre d'éléments de $\mathrm{Cl}(K)$ est le *nombre de classes* du corps K. On le note $h(K)$. Pour tout idéal fractionnaire $\mathfrak{a}$ l'idéal $\mathfrak{a}^{h(K)}$ est principal.

Par conséquent l'anneau $\mathbf{Z}_K$ est principal si et seulement si $h(K) = 1$.

Démonstration du théorème 3.78. La proposition 3.77 montre qu'il suffit de vérifier qu'il n'y a qu'un nombre fini d'idéaux entiers ayant une norme donnée. Soit donc N un entier non nul (seul l'idéal nul a pour norme 0). Soit $\mathfrak{a}$ un idéal entier de norme N. Alors $\mathfrak{a}$ est d'indice N dans $\mathbf{Z}_K$ (lemme 3.61), donc $\mathfrak{a}$ appartient à l'ensemble fini des idéaux de $\mathbf{Z}_K$ qui contiennent N.

□

Le théorème 3.63 donne une minoration du discriminant d'un corps de nombres : comme la norme de l'idéal $(1) = \mathbf{Z}_K$ vaut 1 on a

$$|D_K| \geq M(K)^{-2}. \tag{3.59}$$

On en déduit $|D_K| > 1$ pour $K \neq \mathbf{Q}$, donc il n'y a pas d'extension de $\mathbf{Q}$ autre que $\mathbf{Q}$ qui ne soit pas ramifiée.

La minoration (3.79) montre aussi que $|D_K|$ tend vers l'infini quand le degré n de K sur $\mathbf{Q}$ tend vers l'infini. Nous allons en déduire :

Corollaire 3.60 (*Hermite*). *Il n'y a qu'un nombre fini de sous-corps de* $\mathbf{C}$ *de discriminant donné.*

Démonstration. Il reste à vérifier qu'il n'y a qu'un nombre fini de corps de nombres de discriminant et de degré bornés.

Soit K un tel corps. Supposons pour commencer qu'il existe un plongement réel, c'est-à-dire $r_1 \geq 1$. Si A_0, A, B sont des nombres positifs, le volume du domaine convexe symétrique

$$|x_1| < A_0, \quad |x_i| < A \quad (2 \leq i \leq r_1), \quad |x_{r_1+i}| < B \quad (1 \leq i \leq r_2)$$

de $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ est $2^{r_1} A_0 A^{r_1-1} (\pi B^2)^{r_2}$. On prend $A = B = 1$ et on choisit A_0 de telle sorte que ce volume soit $> 2^{n-r_2} |D_K|^{1/2} = 2^n v\big(\underline{\sigma}(\mathbf{Z}_K)\big)$ (cf. lemme 3.27). Par exemple $A_0 = 2^{n+1-r_1-r_2} \pi^{-r_2} |D_K|^{1/2}$. Alors le théorème de Minkowski (corollaire 3.24) montre qu'il existe un élément non nul α de $\mathbf{Z}_K$ tel que

$$|\sigma_1(\alpha)| < A_0 \text{ et } |\sigma_i(\alpha)| < 1 \text{ pour } 2 \leq i \leq n \ .$$

Comme α est entier sur $\mathbf{Z}$ et non nul sa norme est un entier de valeur absolue ≥ 1, donc $|\sigma_1(\alpha)| \geq 1 > |\sigma_i(\alpha)|$ pour $2 \leq i \leq n$. D'après le lemme 3.2 le polynôme caractéristique de α sur $\mathbf{Q}$ est la puissance $[K : \mathbf{Q}(\alpha)]$ du polynôme irréductible de α sur $\mathbf{Q}$. Le fait que $\sigma_1(\alpha)$ soit distinct des $\sigma_i(\alpha)$ pour $i \neq 1$ implique donc que α est un générateur de K sur $\mathbf{Q}$. Comme tous ses conjugués sont bornés en termes de n et de $|D_K|$, α appartient à un ensemble fini ne dépendant que de n et de $|D_K|$ (cela résulte de (3.25)).

Supposons maintenant qu'il n'existe pas de plongement de K dans $\mathbf{R}$, autrement dit $r_1 = 0$, $n = 2r_2$. Si A_0, A, B sont des nombres positifs, le volume du domaine convexe symétrique

$$|z_1 - \bar{z}_1| < A_0, \quad |z_1 + \bar{z}_1| < A \quad (2 \leq i \leq r_1), \quad |z_i| < B \quad (2 \leq i \leq r_2)$$

de $\mathbf{C}^{r_2}$ est $A_0 A (\pi B^2)^{r_2-1}$. On prend $A = 2$, $B = 1$ et on choisit A_0 de telle sorte que ce volume soit $> 2^{r_2} |D_K|^{1/2}$, disons $A_0 = 2(\pi/2)^{r_2-1} |D_K|^{1/2}$. Alors il existe $\alpha \in \mathbf{Z}_K \setminus \{0\}$ tel que $|\sigma_i(\alpha)| < 1$ pour $2 \leq i \leq r_2$, $|\Re \sigma_1(\alpha)| < 1$ et $|\Im \sigma_1(\alpha)| < A_0/2$. On a encore $|\sigma_1(\alpha)| = |\overline{\sigma}_1(\alpha)| \geq 1 > |\sigma_i(\alpha)|$ pour $2 \leq i \leq r_2$. De plus $\sigma_1(\alpha)$ n'est pas réel, donc $\sigma_1(\alpha) \neq \sigma_i(\alpha)$ pour $2 \leq i \leq n$. On en déduit de nouveau que α est un générateur de K qui appartient à un ensemble fini ne dépendant que de n et de $|D_K|$ □

3.5.6 Décomposition des idéaux premiers dans une extension

Soient k_1 un corps de nombres, k_2 une extension finie de k_1 de degré n, $\mathfrak{p}$ un idéal de $\mathbf{Z}_{k_1}$; on peut décomposer l'idéal engendré par $\mathfrak{p}$ dans $\mathbf{Z}_{k_2}$ sous la forme

$$\mathbf{Z}_{k_2}\mathfrak{p} = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$$

où $\mathfrak{P}_i$ sont des idéaux premiers deux-à-deux distincts de $\mathbf{Z}_{k_2}$ et $e_1, \ldots, e_g$ des entiers ≥ 1. Alors $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ sont les idéaux premiers de $\mathbf{Z}_{k_2}$ tels que $\mathfrak{P} \cap \mathbf{Z}_{k_1} = \mathfrak{p}$. L'entier e_i est *l'indice de ramification de* $\mathfrak{P}_i$ *sur* $\mathfrak{p}$. Si f_i désigne le *degré résiduel de* $\mathfrak{P}_i$ *sur* $\mathfrak{p}$, c'est-à-dire le degré de l'extension $[\mathbf{Z}_{k_2}/\mathfrak{P}_i : \mathbf{Z}_{k_1}/\mathfrak{p}]$, alors

$$\mathbf{Z}_{k_2}/\mathfrak{p}\mathbf{Z}_{k_2} \simeq \prod_{i=1}^{g} \mathbf{Z}_{k_2}/\mathfrak{P}_i^{e_i}.$$

Montrons que pour $1 \leq i \leq g$ le quotient $\mathbf{Z}_{k_2}/\mathfrak{P}_i^{e_i}$ est un $\mathbf{Z}_{k_1}/\mathfrak{p}$-espace vectoriel de dimension $e_i f_i$. Pour cela on considère la suite de $\mathbf{Z}_{k_1}/\mathfrak{p}$-espaces vectoriels

$$\mathbf{Z}_{k_2}/\mathfrak{P}_i^{e_i} \supset \mathbf{Z}_{k_2}/\mathfrak{P}_i^{e_i-1} \supset \cdots \supset \mathbf{Z}_{k_2}/\mathfrak{P}_i \supset \{0\}.$$

Le quotient de deux termes consécutifs est isomorphe $\mathfrak{P}_i^r/\mathfrak{P}_i^{r+1}$, qui est un $\mathbf{Z}_{k_2}/\mathfrak{P}_i$-espace vectoriel de dimension 1, donc un $\mathbf{Z}_{k_1}/\mathfrak{p}$-espace vectoriel de dimension f_i.

Montrons ensuite que $\mathbf{Z}_{k_2}/\mathfrak{p}\mathbf{Z}_{k_2}$ est un $\mathbf{Z}_{k_1}/\mathfrak{p}$ espace vectoriel de dimension n. Soit $\omega_1, \ldots, \omega_m$ une famille d'éléments de $\mathbf{Z}_{k_2}$ dont les classes $\bar{\omega}_1, \ldots, \bar{\omega}_m$ modulo $\mathfrak{p}\mathbf{Z}_{k_2}$ constituent une base du $\mathbf{Z}_{k_1}/\mathfrak{p}$-espace vectoriel $\mathbf{Z}_{k_2}/\mathfrak{p}\mathbf{Z}_{k_2}$. Il s'agit de vérifier que $\omega_1, \ldots, \omega_m$ est une base de k_2 sur k_1.

On commence par vérifier que $\{\omega_1, \ldots, \omega_m\}$ est une famille libre sur k_1. S'il y a une relation non triviale $a_1\omega_1 + \cdots + a_m\omega_m = 0$ avec des a_i dans $\mathbf{Z}_{k_1}$ non tous nuls, soit $\mathfrak{a}$ l'idéal de $\mathbf{Z}_{k_1}$ engendré par ces coefficients $a_1, \ldots, a_m$ et soit $\alpha \in \mathfrak{a}^{-1} \setminus \mathfrak{a}^{-1}\mathfrak{p}$. Alors $\alpha\mathfrak{a} \not\subset \mathfrak{p}$, donc $\alpha a_1, \ldots, \alpha a_m$ appartiennent à $\mathbf{Z}_{k_1}$ mais ne sont pas tous dans $\mathfrak{p}$, et la relation $\alpha a_1\omega_1 + \cdots + \alpha a_m\omega_m \equiv 0 \pmod{\mathfrak{p}}$ donne une contradiction avec l'hypothèse que $\{\bar{\omega}_1, \ldots, \bar{\omega}_m\}$ est une famille libre sur $\mathbf{Z}_{k_1}/\mathfrak{p}$.

Montrons enfin que la famille $\{\omega_1, \ldots, \omega_m\}$ engendre k_2 comme k_1-espace vectoriel. Soit $M = \mathbf{Z}_{k_1}\omega_1 + \cdots + \mathbf{Z}_{k_1}\omega_m$ et soit $N = \mathbf{Z}_{k_2}/M$. Par hypothèse $\{\bar{\omega}_1, \ldots, \bar{\omega}_m\}$ est une partie génératrice du $\mathbf{Z}_{k_1}/\mathfrak{p}$-espace vectoriel $\mathbf{Z}_{k_2}/\mathfrak{p}\mathbf{Z}_{k_2}$, donc $\mathbf{Z}_{k_2} = M + \mathfrak{p}\mathbf{Z}_{k_2}$. Alors $\mathfrak{p}N = N$. Le *Lemme de Nakayama* (voir 3.82) implique qu'il existe $\alpha \in 1 + \mathfrak{p}$ tel que $\alpha N = 0$. Alors $\alpha\mathbf{Z}_{k_2} \subset M$ et par conséquent $k_2 = k_1\omega_1 + \cdots + k_1\omega_m$. En particulier $m = n$.

De ceci on déduit une généralisation de (3.74) :

$$e_1 f_1 + \cdots + e_g f_g = n.$$

Université P. et M. Curie (Paris VI),
Deuxième semestre 2006/2007

Michel Waldschmidt
date de mise à jour: 24/04/2007

Master de sciences et technologies 1ère année -
Spécialité : Mathématiques Fondamentales

Mention : Mathématiques et applications
MO11 : Théorie des nombres (12 ECTS)

Troisième partie : Arithmétique des Corps de Nombres

Fascicule 7 : section 3.5 (11 pages)

3.6 Idéaux d'un corps de nombres

Petit aperçu historique

L'invention de la notion d'idéal provient des recherches au XIXème siècle sur le *dernier théorème de Fermat* : il s'agissait de démontrer qu'il n'y a pas d'entiers positifs $n \geq 3$, x, y et z satisfaisant $x^n + y^n = z^n$. En supposant n impair et en utilisant l'identité

$$x^n + y^n = (x+y)(x+\zeta y)\cdots(x+\zeta^{n-1}y), \quad \zeta = \zeta_n = e^{2i\pi/n}$$

Kummer a démontré en 1844 que l'énoncé de Fermat est vrai pour un exposant premier $n = p$ pour lequel l'anneau des entiers du corps $\mathbf{Q}(\zeta_p)$ est factoriel ; Dirichlet a alors remarqué que l'existence d'une décomposition en facteurs irréductibles est toujours vraie, mais que l'unicité n'est pas claire. C'est dès 1844 que Kummer a su qu'il n'y avait pas unicité de la décomposition en éléments irréductibles dans l'anneau $\mathbf{Z}[\zeta_{23}]$. Il l'a écrit à Liouville en 1847 (à la suite d'une note de G. Lamé à l'Académie des Sciences le 11 mars 1847), ajoutant qu'il avait trouvé un substitut qui étaient les "nombres idéaux". L'idée est la suivante.

Dans le corps $k = \mathbf{Q}(\sqrt{-5})$ la décomposition en facteurs irréductibles n'est pas unique

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}).$$

Kummer affirme qu'il existe des objets qu'il appelle *nombres idéaux* donnant une décomposition unique

$$(21) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$$

qui explique la décomposition précédente :

$$\mathfrak{p}_1\mathfrak{p}_2 = (3), \quad \mathfrak{p}_3\mathfrak{p}_4 = (7), \qquad \mathfrak{p}_1\mathfrak{p}_3 = (1 + 2\sqrt{-5}), \quad \mathfrak{p}_2\mathfrak{p}_4 = (1 - 2\sqrt{-5}).$$

Dedekind a précisé cette construction de nombres idéaux. Si $\mathfrak{a}$ est un nombre idéal, on veut satisfaire les relations, pour a et b dans $\mathbf{Z}_k$,

$$\text{si } \mathfrak{a}|a \text{ et } \mathfrak{a}|b \text{ alors pour tout } \lambda \in \mathbf{Z}_k \text{ et } \mu \in \mathbf{Z}_k \text{ on a } \mathfrak{a}|\lambda a + \mu b.$$

On veut aussi que $\mathfrak{a}$ soit déterminé par $\{a \in \mathbf{Z}_k \ ; \ \mathfrak{a}|a\}$. L'idée est donc de considérer les sous-ensembles $\mathfrak{a}$ de $\mathbf{Z}_k$ qui vérifient la propriété

$$a \in \mathfrak{a},\ b \in \mathfrak{a}, \lambda \in \mathbf{Z}_k,\ \mu \in \mathbf{Z}_k \ \Rightarrow \lambda a + \mu b \in \mathfrak{a}.$$

Ce sont donc les idéaux de $\mathbf{Z}_k$.

Dans l'exemple précédent on prend

$$\mathfrak{p}_1 = (3, 1 - \sqrt{-5}), \quad \mathfrak{p}_2 = (3, 1 + \sqrt{-5}), \quad \mathfrak{p}_3 = (7, 3 - \sqrt{-5}), \quad \mathfrak{p}_4 = (7, 3 + \sqrt{-5}).$$

`Références : [R], [P], Sk].`

3.6.1 Idéaux entiers

Soient K un corps de nombres, $\mathbf{Z}_K$ son anneau d'entiers.

Lemme 3.61. *Soit $\alpha \in \mathbf{Z}_K$. Alors $\mathbf{Z}_K/\alpha\mathbf{Z}_K$ a $|\mathrm{N}_{K/\mathbf{Q}}(\alpha)|$ éléments.*

Démonstration. On utilise la proposition 3.14 : il existe une base $\{e_1, \dots, e_n\}$ de $\mathbf{Z}_K$ et des entiers $a_1, \dots, a_n$ tels que $\{a_1e_1, \dots, a_ne_n\}$ soit une base de l'idéal $\alpha\mathbf{Z}_K$. Soit u l'endomorphisme du $\mathbf{Z}$-module $\mathbf{Z}_K$ qui envoie e_i sur a_ie_i. Son image est $\alpha\mathbf{Z}_K$ et sa matrice dans la base $\{e_1, \dots, e_n\}$ est la matrice diagonale $\mathrm{diag}(a_1, \dots, a_n)$, dont le déterminant est $a_1 \cdots a_n = \mathrm{N}(\alpha\mathbf{Z}_K)$. Comme $\{\alpha e_1, \dots, \alpha e_n\}$ est aussi une base de $\alpha\mathbf{Z}_K$, il existe un automorphisme v du $\mathbf{Z}$-module $\alpha\mathbf{Z}_K$ tel que $v(a_ie_i) = \alpha e_i$. Alors $\det v = \pm 1$; comme $v \circ u$ est la restriction de $[\alpha]$ à $\mathbf{Z}_K$, le déterminant de u est aussi égal à $\pm\mathrm{N}_{K/\mathbf{Q}}(\alpha)$. □

Soit $\mathfrak{a}$ un idéal non nul de $\mathbf{Z}_K$, $\alpha \neq 0$ un élément de $\mathfrak{a}$. Alors $\mathbf{Z}_K\alpha \subset \mathfrak{a}$. Des propositions 3.12 et 3.14 on déduit que $\mathfrak{a}$ est un $\mathbf{Z}$-module libre de rang $n = [K : \mathbf{Q}]$. Par conséquent il existe une base $\{e_1, \dots, e_n\}$ de $\mathbf{Z}_K$ comme $\mathbf{Z}$-module et des entiers positifs $a_1, \dots, a_n$ tels que $\{a_1e_1, \dots, a_ne_n\}$ soit une base de $\mathfrak{a}$ sur $\mathbf{Z}$ et que a_i divise a_{i+1} dans $\mathbf{Z}$ pour $1 \leq i < n$. On en déduit que le quotient $\mathbf{Z}_K/\mathfrak{a}$ est fini avec $a_1 \cdots a_n$ éléments. Le nombre d'éléments de $\mathbf{Z}_K/\mathfrak{a}$ est appelé *norme de* $\mathfrak{a}$ et noté $\mathrm{N}(\mathfrak{a})$.

Le lemme 3.61 montre que la norme d'un idéal principal est égale à la valeur absolue de la norme de K sur $\mathbf{Q}$ d'un générateur.

Si $\mathfrak{a}$ et $\mathfrak{b}$ sont deux idéaux de $\mathbf{Z}_K$ avec $\mathfrak{a} \subset \mathfrak{b}$, alors les surjections canoniques de $\mathbf{Z}_K$ sur les quotients induisent une surjection de $\mathbf{Z}_K/\mathfrak{a}$ sur $\mathbf{Z}_K/\mathfrak{b}$, donc $\mathrm{N}(\mathfrak{b})$ divise $\mathrm{N}(\mathfrak{a})$.

Soient $n = [K : \mathbf{Q}]$ le degré de K et $\underline{\sigma} : K \to \mathbf{R}^n$ son plongement canonique.

Lemme 3.62. *Soit $\mathfrak{a}$ un idéal non nul de $\mathbf{Z}_K$. Alors $\underline{\sigma}(\mathfrak{a})$ est un réseau de $\mathbf{R}^n$ de volume $2^{-r_2}|D_K|^{1/2}\mathrm{N}(\mathfrak{a})$ et le discriminant de $\mathfrak{a}$ est $D_K\mathrm{N}(\mathfrak{a})^2$. .*

Démonstration. Le corollaire 3.28 donne le résultat quand $\mathfrak{a} = \mathbf{Z}_K$. Dans le cas général, $\mathfrak{a}$ est un sous-groupe d'indice fini $\mathrm{N}(\mathfrak{a})$ de $\mathbf{Z}_K$, donc $\underline{\sigma}(\mathfrak{a})$ est un sous-groupe d'indice fini $\mathrm{N}(\mathfrak{a})$ de $\underline{\sigma}(\mathbf{Z}_K)$. □

Quand r_1 et r_2 sont deux entiers ≥ 0 avec $n = r_1 + 2r_2 \geq 1$ on définit la *constante de Minkowski* $M(r_1, r_2)$ par

$$M(r_1, r_2) = \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n}.$$

On écrit encore $M(K)$ au lieu de $M(r_1, r_2)$ quand K est un corps de nombres de degré n ayant r_1 plongements réels et $2r_2$ plongements imaginaires deux-à-deux conjugués.

Nous déduirons ultérieurement (§ 3.6.5) plusieurs conséquences du lemme suivant.

Théorème 3.63. *Soient K un corps de nombres et $\mathfrak{a}$ un idéal non nul de $\mathbf{Z}_K$. Il existe $\alpha \in \mathfrak{a}$ tel que*

$$1 \leq |N_{K/\mathbf{Q}}(\alpha)| \leq M(K)|D_K|^{1/2}\mathrm{N}(\mathfrak{a}).$$

Démonstration. Nous renvoyons au livre de Samuel (§ 4.2) pour la démonstration. Le principe consiste à écrire les conditions que doit satisfaire un élément de $\mathfrak{a}$ pour que sa norme vérifie la majoration requise : cela définit dans $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ un *domaine symétrique convexe*. Pour assurer, en utilisant le théorème de Minkowski (corollaire 3.24), que ce domaine contient un élément non nul de l'image par le plongement logarithmique de l'idéal $\mathfrak{a}$, il reste à faire un petit calcul de volume. □

3.6.2 Idéaux premiers

Soient K un corps de nombres, $\mathbf{Z}_K$ son anneau d'entiers, $\mathfrak{p}$ un idéal premier non nul de $\mathbf{Z}_K$. Si $\alpha \in \mathfrak{p}$ a pour polynôme minimal $X^m + a_1X^{m-1} + \cdots + a_m$ (avec $m = [\mathbf{Q}(\alpha) : \mathbf{Q}]$) alors a_m appartient $\mathfrak{p} \cap \mathbf{Z}$ donc cette intersection n'est pas résuite à 0.

L'injection de $\mathbf{Z}$ dans $\mathbf{Z}_K$ induit une injection de $\mathbf{Z}/\mathfrak{p} \cap \mathbf{Z}$ dans l'anneau $\mathbf{Z}_K/\mathfrak{p}$ qui est intègre, donc $\mathbf{Z}/\mathfrak{p} \cap \mathbf{Z}$ est intègre et l'idéal $\mathfrak{p} \cap \mathbf{Z}$ de $\mathbf{Z}$ est premier non nul.

Rappelons le résultat élémentaire suivant :

Lemme 3.64. *Un anneau fini intègre est un corps.*

Démonstration. Si A est un anneau fini intègre, pour $x \in A \setminus \{0\}$ l'application $y \mapsto xy$ est une injection de A dans A, donc une bijection. □

Si $\mathfrak{p}$ est un idéal premier non nul de $\mathbf{Z}_K$, le corps fini $k = \mathbf{Z}_K/\mathfrak{p}$ est appelé *corps résiduel de* $\mathfrak{p}$. Dans ce cas $\mathbf{Z}/\mathfrak{p} \cap \mathbf{Z}$ est un sous-corps de k, donc le générateur positif de $\mathbf{Z} \cap \mathfrak{p}$ est un nombre premier p qui est appelé *la caractéristique du corps résiduel* k (on dit encore la *caractéristique résiduelle de* $\mathfrak{p}$). La norme de $\mathfrak{p}$ est donc p^f où $f = [k : \mathbf{F}_p]$ est le *degré du corps résiduel*.

Lemme 3.65. *Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux non nuls de $\mathbf{Z}_K$. Si $\mathfrak{a} = \mathfrak{a}\mathfrak{b}$, alors $\mathfrak{b} = \mathbf{Z}_K$.*

Démonstration. Soit $\alpha_1, \ldots, \alpha_n$ une base de l'idéal $\mathfrak{a}$ comme $\mathbf{Z}$-module. Comme $\alpha_i \in \mathfrak{a}\mathfrak{b}$ pour $1 \leq i \leq n$, on peut écrire

$$\alpha_i = \sum_{j=1}^{n} \beta_{ij}\alpha_j \quad \text{pour} \quad 1 \leq i \leq n,$$

avec des coefficients β_{ij} dans $\mathfrak{b}$. Alors la matrice $\big(\beta_{ij}\big)_{1\leq i,j\leq n} - I$ a un déterminant nul, d'où on déduit en développant $1 \in \mathfrak{b}$.

□

Soient A est un anneau, M un A-module et $\mathfrak{a}$ un idéal de A différent de A. Alors $\mathfrak{a}M$ est un sous-module de M et le quotient $M/\mathfrak{a}M$ est un A-module. Montrons que $M/\mathfrak{a}M$ a une structure naturelle de $A/\mathfrak{a}$-module.

En effet, la structure de A-module du quotient $M/\mathfrak{a}M$ est donnée par un homomorphisme de A-modules

$$\begin{array}{ccc} A & \to & \mathrm{Hom}_A(M/\mathfrak{a}M, M/\mathfrak{a}M) \\ a & \mapsto & (x \mapsto ax) \end{array}$$

dont le noyau contient $\mathfrak{a}$. On en déduit un homomorphisme de A-modules de $A/\mathfrak{a}$ dans $\mathrm{Hom}_A(M/\mathfrak{a}M, M/\mathfrak{a}M)$ qui confère à $M/\mathfrak{a}M$ la structure de $A/\mathfrak{a}$-module annoncée.

En particulier si $\mathfrak{a}$ est un idéal maximal $\mathfrak{p}$ de A alors $M/\mathfrak{p}M$ a une structure naturelle d'espace vectoriel sur le corps $A/\mathfrak{p}$.

On applique ceci avec $A = \mathbf{Z}_K$.

Lemme 3.66. *Soit $\mathfrak{a}$ un idéal non nul de $\mathbf{Z}_K$ et soit $\mathfrak{p}$ un idéal premier non nul de $\mathbf{Z}_K$. On désigne par k le corps résiduel $\mathbf{Z}_K/\mathfrak{p}$. Alors $\mathfrak{a}/\mathfrak{p}\mathfrak{a}$ est un k-espace vectoriel de dimension ≥ 1.*

Démonstration. Le lemme 3.65 implique $\mathfrak{a} \neq \mathfrak{p}\mathfrak{a}$, donc la dimension de ce k-espace vectoriel est ≥ 1. □

En fait il va résulter de ce qui suit que la dimension de cet espace vectoriel est 1.

Soit $\mathfrak{p}$ un idéal premier non nul de $\mathbf{Z}_K$. En utilisant au choix le lemme 3.65 ou bien le lemme 3.66, on obtient $\mathfrak{p}^m \neq \mathfrak{p}^{m+1}$ pour tout $m \geq 0$. La suite

$$\mathbf{Z}_K \supset \mathfrak{p} \supset \mathfrak{p}^2 \cdots \supset \mathfrak{p}^m \supset \cdots$$

est donc strictement décroissante. D'après le lemme 3.66 le quotient $\mathfrak{p}^m/\mathfrak{p}^{m+1}$ est isomorphe comme $\mathbf{Z}_K$-module à $\mathbf{Z}_K/\mathfrak{p}$; il en résulte que la norme de $\mathfrak{p}^m$ est $\mathrm{N}(\mathfrak{p})^m$.

L'intersection de tous les $\mathfrak{p}^m$ est $\{0\}$: en effet, quand $\mathfrak{b}$ est un idéal de $\mathbf{Z}_K$ distinct de $\mathbf{Z}_K$ et α est un élément non nul de $\mathfrak{b}$, le plus grand entier m tel que $\alpha \in \mathfrak{b}^m$ est borné par la condition que $\mathrm{N}(\mathfrak{b})^m$ divise $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$.

Soit $\mathfrak{a}$ un idéal non nul de $\mathbf{Z}_K$. L'ensemble des entiers $t \geq 0$ tels que $\mathfrak{a} \subset \mathfrak{p}^t$ est non vide (il contient 0) et fini. On désigne par $v_\mathfrak{p}(\mathfrak{a})$ le plus grand de ces entiers :

$$\mathfrak{a} \subset \mathfrak{p}^t \quad \text{pour} \quad 0 \leq t \leq v_\mathfrak{p}(\mathfrak{a}) \quad \text{et} \quad \mathfrak{a} \not\subset \mathfrak{p}^t \quad \text{pour} \quad t = v_\mathfrak{p}(\mathfrak{a}) + 1.$$

On a $v_\mathfrak{p}(\mathfrak{a}) > 0$ si et seulement si $\mathfrak{a} \subset \mathfrak{p}$. On a aussi $v_\mathfrak{p}(\mathfrak{a}\mathfrak{p}) = v_\mathfrak{p}(\mathfrak{a}) + 1$, donc $v_\mathfrak{p}(\mathfrak{p}^m) = m$ pour $m \geq 0$. Enfin $v_\mathfrak{p}(\mathfrak{p}') = 0$ si $\mathfrak{p}$ et $\mathfrak{p}'$ sont deux idéaux premiers distincts.

Théorème 3.67. *Soit $\mathfrak{a}$ un idéal non nul de $\mathbf{Z}_K$. L'ensemble des idéaux premiers $\mathfrak{p}$ de $\mathbf{Z}_K$ qui contiennent $\mathfrak{a}$ est fini et on a*

$$\mathfrak{a} = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})},$$

où le produit est étendu à l'ensemble des idéaux premiers non nuls de $\mathbf{Z}_K$.

De plus une telle décomposition est unique : si on a

$$\mathfrak{a} = \prod_\mathfrak{p} \mathfrak{p}^{a_\mathfrak{p}},$$

où les $a_\mathfrak{p}$ sont des entiers rationnels ≥ 0 tous nuls sauf un nombre fini, alors $a_\mathfrak{p} = v_\mathfrak{p}(\mathfrak{a})$ pour tout $\mathfrak{p}$.

Remarque. Le théorème 3.67 montre que, sous les hypothèses du lemme 3.66, $\mathfrak{a}/\mathfrak{a}\mathfrak{p}$ est de dimension 1 comme espace vectoriel sur $\mathbf{Z}_K/\mathfrak{p}$ car il n'y a pas d'idéal entre $\mathfrak{a}\mathfrak{p}$ et $\mathfrak{a}$.

Pour une démonstration du théorème 3.67, voir par exemple le livre de Samuel.

3.6.3 Idéaux fractionnaires

Soient A un anneau intègre, K son corps des fractions. Un sous-A-module $\mathfrak{a}$ **non nul** de K est un *idéal fractionnaire de K par rapport à A* s'il vérifie les propriétés équivalentes suivantes :
(i) Il existe $\alpha \in A$, $\alpha \neq 0$ tel que $\alpha\mathfrak{a} \subset A$.
(ii) Il existe $\beta \in K$, $\beta \neq 0$ tel que $\beta\mathfrak{a} \subset A$.

L'équivalence vient du fait que si $\beta\mathfrak{a} \subset A$ avec $\beta \in K^\times$, alors on peut écrire $\beta = \alpha/\gamma$ avec α et γ dans $A \setminus \{0\}$, d'où $\alpha\mathfrak{a} \subset A$.

On dira aussi que $\mathfrak{a}$ est un *idéal fractionnaire de A*.

Lemme 3.68. *Si $\mathfrak{a}_1$ et $\mathfrak{a}_2$ sont des idéaux fractionnaires de A, alors*

$$\mathfrak{a}_1 + \mathfrak{a}_2, \quad \mathfrak{a}_1 \cap \mathfrak{a}_2, \quad \mathfrak{a}_1\mathfrak{a}_2$$

et

$$(\mathfrak{a}_1 : \mathfrak{a}_2) := \{x \in K \ ; \ x\mathfrak{a}_2 \subset \mathfrak{a}_1\}$$

sont des idéaux fractionnaires de A.

Démonstration. Si α_1 et α_2 sont des éléments non nuls de $A \setminus \{0\}$ tels que $\mathfrak{a}_i \subset \alpha_i^{-1}A$ pour $i = 1$ et $i = 2$, alors $\mathfrak{a}_1 + \mathfrak{a}_2$, $\mathfrak{a}_1 \cap \mathfrak{a}_2$ et $\mathfrak{a}_1\mathfrak{a}_2$ sont des sous-A-modules non nuls de K contenus dans $(\alpha_1\alpha_2)^{-1}A$.

Si α_1 est un élément non nul de A tel que $\mathfrak{a}_1 \subset \alpha_1^{-1}A$ et si a_2 est un élément non nul de $\mathfrak{a}_2$, alors pour tout $x \in (\mathfrak{a}_1 : \mathfrak{a}_2)$ on a

$$\alpha_1 a_2 x \in \alpha_1 x\mathfrak{a}_2 \subset \alpha_1\mathfrak{a}_1 \subset A,$$

donc $\alpha_1 a_2(\mathfrak{a}_1 : \mathfrak{a}_2) \subset A$.

Il reste à vérifier que le A-module $(\mathfrak{a}_1 : \mathfrak{a}_2)$ n'est pas nul. Si a_1 est un élément non nul de $\mathfrak{a}_1$ et α_2 un élément non nul de A tel que $\mathfrak{a}_2 \subset \alpha_2^{-1}A$, alors $a_1\alpha_2$ est un élément non nul de $(\mathfrak{a}_1 : \mathfrak{a}_2)$:

$$a_1\alpha_2\mathfrak{a}_2 \subset a_1 A \subset \mathfrak{a}_1.$$

□

On déduit du lemme 3.68 que si $\mathfrak{a}$ est un idéal fractionnaire de A, alors

$$(A : \mathfrak{a}) = \{x \in K \ ; \ x\mathfrak{a} \subset A\} \quad \text{et} \quad (\mathfrak{a} : \mathfrak{a}) = \{x \in K \ ; \ x\mathfrak{a} \subset \mathfrak{a}\}$$

sont des idéaux fractionnaires de A.

Tout sous-A-module de type fini de K non nul est un idéal fractionnaire.

Réciproquement, quand A est un anneau noethérien, tout idéal fractionnaire de A est de type fini : pour $\alpha \in A \setminus \{0\}$ les A-modules $\mathfrak{a}$ et $\alpha\mathfrak{a}$ sont isomorphes. Donc, quand A est noethérien, un idéal fractionnaire n'est autre qu'un sous-A-module non nul de type fini de K. Si $\mathfrak{a}$ admet $\{a_i\}$ comme partie génératrice et si $\mathfrak{b}$ est engendré par $\{b_j\}$, alors $\mathfrak{a} + \mathfrak{b}$ est engendré par $\{a_i\} \cup \{b_j\}$ et $\mathfrak{a}\mathfrak{b}$ par $\{a_i b_j\}$.

Quand K est un corps de nombres, un *idéal entier* de K est un idéal de $\mathbf{Z}_K$, c'est-à-dire un idéal fractionnaire de $\mathbf{Z}_K$ contenu dans $\mathbf{Z}_K$.

Proposition 3.69. *Soit $\mathfrak{p}$ un idéal premier non nul de $\mathbf{Z}_K$. Soit*

$$\mathfrak{p}' = \{x \in K \ ; \ x\mathfrak{p} \subset \mathbf{Z}_K\}.$$

Alors $\mathfrak{p}'$ est un idéal fractionnaire de $\mathbf{Z}_K$ qui contient $\mathbf{Z}_K$ et $\mathfrak{p}\mathfrak{p}' = \mathbf{Z}_K$.

Du théorème 3.67 on déduit que les idéaux fractionnaires de $\mathbf{Z}_K$ forment un groupe abélien d'élément neutre $\mathbf{Z}_K = (1)$.

Théorème 3.70. *Soit $\mathfrak{a}$ un idéal fractionnaire de $\mathbf{Z}_K$. Il existe une décomposition unique*

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{a_\mathfrak{p}},$$

où le produit est étendu à l'ensemble des idéaux premiers non nuls de $\mathbf{Z}_K$ et les $a_\mathfrak{p}$ sont des entiers rationnels tels que $\{\mathfrak{p} \ ; \ a_\mathfrak{p} \neq 0\}$ soit fini.

Démonstration. Soit $\alpha \in \mathbf{Z}_K \setminus \{0\}$ tel que $\alpha\mathfrak{a} \subset \mathbf{Z}_K$. On décompose les idéaux entiers $\alpha\mathbf{Z}_K$ et $\alpha\mathfrak{a}$ en produit d'idéaux premiers, on multiplie par les inverses des idéaux premiers apparaissant dans la décomposition de $\alpha\mathbf{Z}_K$ et on trouve la décomposition annoncée de $\mathfrak{a}$. L'unicité résulte de ce qui précède.

□

Soit K un corps de nombres. Le théorème 3.67 montre que la propriété (3.1) de multiplicativité de la norme s'étend aux idéaux de $\mathbf{Z}_K$:

Corollaire 3.71. *Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux de $\mathbf{Z}_K$. Alors*

$$\mathrm{N}(\mathfrak{a}\mathfrak{b}) = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{b}). \tag{3.72}$$

Démonstration. Grâce au théorème 3.67 il suffit de vérifier la propriété (3.72) quand $\mathfrak{b}$ est un idéal premier. Notons-le $\mathfrak{p}$.

L'homomorphisme canonique

$$\mathbf{Z}_K/\mathfrak{a}\mathfrak{p} \to \mathbf{Z}_K/\mathfrak{a}$$

est surjectif et a pour noyau $\mathfrak{a}/\mathfrak{a}\mathfrak{p}$. Le quotient $k = \mathbf{Z}_K/\mathfrak{p}$ est un corps fini (ayant $\mathrm{N}(\mathfrak{p})$ éléments) et $\mathfrak{a}/\mathfrak{a}\mathfrak{p}$ est un k-espace vectoriel de dimension 1 (car $\mathfrak{p}$ est maximal - cf lemme 3.66 et la remarque qui suit le théorème 3.67), donc est isomorphe à k. Ainsi $\mathfrak{a}/\mathfrak{a}\mathfrak{p}$ a $\mathrm{N}(\mathfrak{p})$ éléments et par conséquent $\mathbf{Z}_K/\mathfrak{a}\mathfrak{p}$ en a $\mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{p})$.

□

Grâce au corollaire 3.71 on peut étendre la définition de la norme aux idéaux fractionnaires. Avec les notations du corollaire 3.70, on pose $v_\mathfrak{p}(\mathfrak{a}) = a_\mathfrak{p}$ et

$$\mathrm{N}(\mathfrak{a}) = \prod_{\mathfrak{p}} \mathrm{N}(\mathfrak{p})^{a_\mathfrak{p}}.$$

La norme d'un idéal fractionnaire principal de $\mathbf{Z}_K$ est égale à la valeur absolue de la norme de K sur $\mathbf{Q}$ d'un générateur : pour tout $\alpha \in K^\times$ on a $\mathrm{N}(\alpha\mathbf{Z}_K) = |\mathrm{N}_{K/\mathbf{Q}}(\alpha)|$.

Le lemme 3.69 signifie que les idéaux premiers non nuls sont inversibles dans le monoïde des idéaux fractionnaires de $\mathbf{Z}_K$. L'inverse $\mathfrak{p}'$ de $\mathfrak{p}$ est aussi noté $\mathfrak{p}^{-1}$:

$$\mathfrak{p}^{-1} = \{x \in K \ ; \ x\mathfrak{p} \subset \mathbf{Z}_K\}.$$

Exercice. Soient $\mathfrak{a}$ un idéal non nul et $\mathfrak{p}$ un idéal premier non nul de $\mathbf{Z}_K$.
1. Montrer qu'il existe $\alpha \in \mathfrak{a}$ tel que $\alpha \notin \mathfrak{ap}$.
Montrer qu'il existe un idéal $\mathfrak{b}$ de $\mathbf{Z}_K$ tel que $\mathfrak{ab} = \alpha\mathbf{Z}_K$.
Vérifier $\mathfrak{a} = \alpha\mathbf{Z}_K + \mathfrak{ap}$.
2. Soient $a_1, \dots, a_N$ des représentants des classes de $\mathbf{Z}_K$ modulo $\mathfrak{a}$, avec $N = \mathrm{N}(\mathfrak{a})$, et soient $b_1, \dots, b_M$ des représentants des classes de $\mathbf{Z}_K$ modulo $\mathfrak{p}$, avec $M = \mathrm{N}(\mathfrak{p})$. Vérifier que

$$\{a_i + \alpha b_j\}_{\substack{1 \le i \le N \\ 1 \le j \le M}}$$

est un système complet de représentants des classes de $\mathbf{Z}_K$ modulo $\mathfrak{ap}$.

Du théorème 3.67 on déduit, pour $\mathfrak{p}$ idéal premier de $\mathbf{Z}_K$ et $\mathfrak{a}$, $\mathfrak{b}$ idéaux fractionnaires de $\mathbf{Z}_K$:

$$\begin{aligned} v_{\mathfrak{p}}(\mathfrak{ab}) &= v_{\mathfrak{p}}(\mathfrak{a}) + v_{\mathfrak{p}}(\mathfrak{b}), \\ v_{\mathfrak{p}}(\mathfrak{a}+\mathfrak{b}) &= \min\{v_{\mathfrak{p}}(\mathfrak{a}), v_{\mathfrak{p}}(\mathfrak{b})\}, \\ v_{\mathfrak{p}}(\mathfrak{a}\cap\mathfrak{b}) &= \max\{v_{\mathfrak{p}}(\mathfrak{a}), v_{\mathfrak{p}}(\mathfrak{b})\}. \end{aligned}$$

Soit $\mathfrak{p}$ un idéal premier de $\mathbf{Z}_K$. On définit *l'indice de ramification* $e(\mathfrak{p})$ de $\mathfrak{p}$ par $e(\mathfrak{p}) = v_{\mathfrak{p}}(p\mathbf{Z}_K)$ où p désigne la caractéristique résiduelle de $\mathfrak{p}$. Ainsi $e(\mathfrak{p}) \ge 1$.

Soit p un nombre premier et soit $p\mathbf{Z}_K$ l'idéal principal de $\mathbf{Z}_K$ qu'il engendre. Le théorème 3.67 montre qu'il existe une décomposition, unique à l'ordre près des facteurs,

$$p\mathbf{Z}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}, \tag{3.73}$$

où g est un entier ≥ 1, $\mathfrak{p}_1, \dots, \mathfrak{p}_g$ sont des idéaux premiers de $\mathbf{Z}_K$ deux-à-deux distincts et $e_i \ge 1$ est l'indice de ramification de $\mathfrak{p}_i$ $(1 \le i \le g)$.

Les idéaux $\mathfrak{p}_1, \dots, \mathfrak{p}_g$ sont précisément les idéaux premiers $\mathfrak{p}$ de $\mathbf{Z}_K$ tels que $\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$. On dit que ce sont les *idéaux premiers de* $\mathbf{Z}_K$ *au dessus de* p. De la décomposition (3.73) on déduit

$$\mathbf{Z}_K/p\mathbf{Z}_K \simeq \mathbf{Z}_K/\mathfrak{p}_1^{e_1} \cdots \mathbf{Z}_K/\mathfrak{p}_g^{e_g}.$$

En notant $n = [K : \mathbf{Q}]$, en désignant par f_i le degré du corps résiduel de $\mathfrak{p}_i$ et en utilisant le corollaire 3.71, on obtient

$$p^n = \mathrm{N}_{K/\mathbf{Q}}(p) = \mathrm{N}(\mathfrak{p}_1)^{e_1} \cdots \mathrm{N}(\mathfrak{p}_g)^{e_g} = p^{e_1 f_1 + \cdots + e_g f_g}.$$

Par conséquent

$$e_1 f_1 + \cdots + e_g f_g = n. \tag{3.74}$$

On dit que $\mathfrak{p}_i$ est *ramifié au dessus de* p si l'exposant e_i est ≥ 2. On dit que p est *ramifié dans* K si l'un des exposants e_i est ≥ 2. On dit encore que p est
- *totalement ramifié dans* K si $e_1 = n$: alors $g = 1$ et $f_1 = 1$
- *totalement décomposé dans* K si $g = n$: alors $e_1 = \cdots = e_n = f_1 = \cdots = f_n = 1$
- *inerte dans* K si $f_1 = n$: alors $g = 1$ et $e_1 = 1$; cela revient à dire que $p\mathbf{Z}_K$ est un idéal premier.

Voici ce qui se passe pour les corps quadratiques

Proposition 3.75. *Soit d un entier sans facteur carré et soit p un nombre premier impair. Dans le corps $K = \mathbf{Q}(\sqrt{d})$, p se décompose de la façon suivante :*
(i) Si p divise d, alors p est ramifié dans K :

$p\mathbf{Z}_K = \mathfrak{p}^2$ *avec* $\mathrm{N}(\mathfrak{p}) = p$.

(ii) Si $\left(\frac{d}{p}\right) = 1$*, alors* p *est décomposé dans* K *:*

$p\mathbf{Z}_K = \mathfrak{p}_1\mathfrak{p}_2$ *avec* $\mathrm{N}(\mathfrak{p}_1) = \mathrm{N}(\mathfrak{p}_1) = p$.

(iii) Si $\left(\frac{d}{p}\right) = -1$*, alors* p *est inerte dans* K *:*

$p\mathbf{Z}_K = \mathfrak{p}$.

Démonstration. Si $d \equiv 2$ ou $3 \pmod 4$, alors $\mathbf{Z}_K = \mathbf{Z}[\sqrt{d}]$. Si $d \equiv 1 \pmod 4$, on a $\mathbf{Z}_K = \mathbf{Z}[(1+\sqrt{d})/2]$, dans ce dernier cas comme p est un nombre premier impair on peut écrire $\mathbf{Z}_K = \mathbf{Z}[\sqrt{d}] + p\mathbf{Z}_K$. Par conséquent on a toujours

$$\mathbf{Z}_K/p\mathbf{Z}_K = \mathbf{Z}[\sqrt{d}]/p\mathbf{Z}[\sqrt{d}] \simeq \mathbf{Z}[X]/(p, X^2 - d) \simeq \mathbf{F}_p[X]/(X^2 - d).$$

- Le polynôme $X^2 - d$ a une racine double dans $\mathbf{F}_p$ si et seulement si p divise d.
- Il se décompose en deux facteurs linéaires distincts si et seulement si $\left(\frac{d}{p}\right) = 1$.
- Il est irréductible si et seulement si $\left(\frac{d}{p}\right) = -1$. □

Exercice. Soit d un entier sans facteur carré et soit K le corps quadratique $\mathbf{Q}(\sqrt{d})$. Vérifier :
(i) 2 est ramifié dans K si et seulement si $d \equiv 2$ ou $3 \pmod 4$, c'est-à-dire si et seulement si le discriminant de K est pair.
(ii) 2 est décomposé dans K si et seulement si $d \equiv 1 \pmod 8$.
(iii) 2 est inerte dans K si et seulement si $d \equiv 5 \pmod 8$.

3.6.4 Discriminant et ramification

Nous admettrons l'énoncé suivant :

Théorème 3.76. *Soit* K *un corps de nombres. Les nombres premiers qui se ramifient dans* K *sont en nombre fini : ce sont les diviseurs premiers du discriminant* D_K.

3.6.5 Classes d'idéaux - théorèmes de finitude

Soit K un corps de nombres. Les idéaux fractionnaires de $\mathbf{Z}_K$ forment un groupe multiplicatif. Les idéaux fractionnaires principaux (c'est-à-dire monogènes) forment un sous-groupe, et le quotient est le *groupe* $\mathrm{Cl}(K)$ *des classes d'idéaux de* K. Dire que deux idéaux fractionnaires $\mathfrak{a}$ et $\mathfrak{b}$ sont *équivalents* signifie qu'il existe $\alpha \in K$, $\alpha \neq 0$, tel que $\mathfrak{a} = \mathfrak{b} \cdot \alpha\mathbf{Z}_K$.

Soit $\mathfrak{a}$ un idéal fractionnaire et soit α un élément non nul de $\mathbf{Z}_K$ tel que $\alpha\mathfrak{a}$ soit un idéal entier. Il résulte de la définition que $\mathfrak{a}$ est équivalent à $\alpha\mathfrak{a}$. Donc toute classe d'équivalence contient un idéal entier.

Rappelons que $M(K)$ désigne la constante de Minkowski du corps K (théorème 3.63).

Proposition 3.77. *Toute classe d'idéaux contient un idéal entier* $\mathfrak{a}$ *de norme* $\mathrm{N}(\mathfrak{a}) \leq M(K)|D_K|^{1/2}$.

Démonstration. Si $\mathfrak{a}_1$ est un idéal dans la classe considérée, si α est un élément non nul de $\mathbf{Z}_K$ tel que l'idéal $\mathfrak{a}_2 = \alpha\mathfrak{a}_1^{-1}$ soit entier, en appliquant le théorème 3.63 à $\mathfrak{a}_2$ on trouve un élément $\beta \in \mathfrak{a}_2$ vérifiant $|\mathrm{N}_{K:\mathbf{Q}}(\beta)| \leq M(K)|D_K|^{1/2}\mathrm{N}(\mathfrak{a}_2)$. Alors $\mathfrak{a} = \beta\mathfrak{a}_2^{-1}$ est équivalent à $\mathfrak{a}_1$ et vérifie la propriété requise.

□

Théorème 3.78 (Minkowski). *Le groupe* $\mathrm{Cl}(K)$ *des classes d'idéaux de* K *est fini.*

Le nombre d'éléments de $\mathrm{Cl}(K)$ est le *nombre de classes* du corps K. On le note $h(K)$. Pour tout idéal fractionnaire $\mathfrak{a}$ l'idéal $\mathfrak{a}^{h(K)}$ est principal.

Par conséquent l'anneau $\mathbf{Z}_K$ est principal si et seulement si $h(K) = 1$.

Démonstration du théorème 3.78. La proposition 3.77 montre qu'il suffit de vérifier qu'il n'y a qu'un nombre fini d'idéaux entiers ayant une norme donnée. Soit donc N un entier non nul (seul l'idéal nul a pour norme 0). Soit $\mathfrak{a}$ un idéal entier de norme N. Alors $\mathfrak{a}$ est d'indice N dans $\mathbf{Z}_K$ (lemme 3.61), donc $\mathfrak{a}$ appartient à l'ensemble fini des idéaux de $\mathbf{Z}_K$ qui contiennent N.

□

Le théorème 3.63 donne une minoration du discriminant d'un corps de nombres : comme la norme de l'idéal $(1) = \mathbf{Z}_K$ vaut 1 on a

$$|D_K| \geq M(K)^{-2}. \tag{3.79}$$

On en déduit $|D_K| > 1$ pour $K \neq \mathbf{Q}$, donc il n'y a pas d'extension de $\mathbf{Q}$ autre que $\mathbf{Q}$ qui ne soit pas ramifiée.

La minoration (3.79) montre aussi que $|D_K|$ tend vers l'infini quand le degré n de K sur $\mathbf{Q}$ tend vers l'infini. Nous allons en déduire :

Corollaire 3.80 (*Hermite*). *Il n'y a qu'un nombre fini de sous-corps de* $\mathbf{C}$ *de discriminant donné.*

Démonstration. Il reste à vérifier qu'il n'y a qu'un nombre fini de corps de nombres de discriminant et de degré bornés.

Soit K un tel corps. Supposons pour commencer qu'il existe un plongement réel, c'est-à-dire $r_1 \geq 1$. Si A_0, A, B sont des nombres positifs, le volume du domaine convexe symétrique

$$|x_1| < A_0, \quad |x_i| < A \quad (2 \leq i \leq r_1), \quad |x_{r_1+i}| < B \quad (1 \leq i \leq r_2)$$

de $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ est $2^{r_1} A_0 A^{r_1-1} (\pi B^2)^{r_2}$. On prend $A = B = 1$ et on choisit A_0 de telle sorte que ce volume soit $> 2^{n-r_2} |D_K|^{1/2} = 2^n v\big(\underline{\sigma}(\mathbf{Z}_K)\big)$ (cf. Proposition 3.27). Par exemple $A_0 = 2^{n+1-r_1-r_2} \pi^{-r_2} |D_K|^{1/2}$. Alors le théorème de Minkowski (corollaire 3.24) montre qu'il existe un élément non nul α de $\mathbf{Z}_K$ tel que

$$|\sigma_1(\alpha)| < A_0 \text{ et } |\sigma_i(\alpha)| < 1 \text{ pour } 2 \leq i \leq n\ .$$

Comme α est entier sur $\mathbf{Z}$ et non nul sa norme est un entier de valeur absolue ≥ 1, donc $|\sigma_1(\alpha)| \geq 1 > |\sigma_i(\alpha)|$ pour $2 \leq i \leq n$. D'après le lemme 3.2 le polynôme caractéristique de α sur $\mathbf{Q}$ est la puissance $[K : \mathbf{Q}(\alpha)]$ du polynôme irréductible de α sur $\mathbf{Q}$. Le fait que $\sigma_1(\alpha)$ soit distinct des $\sigma_i(\alpha)$ pour $i \neq 1$ implique donc que α est un générateur de K sur $\mathbf{Q}$. Comme tous ses conjugués sont bornés en termes de n et de $|D_K|$, α appartient à un ensemble fini ne dépendant que de n et de $|D_K|$ (cela résulte de (3.25)).

Supposons maintenant qu'il n'existe pas de plongement de K dans $\mathbf{R}$, autrement dit $r_1 = 0$, $n = 2r_2$. Si A_0, A, B sont des nombres positifs, le volume du domaine convexe symétrique

$$|z_1 - \bar{z}_1| < A_0, \quad |z_1 + \bar{z}_1| < A \quad (2 \leq i \leq r_1), \quad |z_i| < B \quad (2 \leq i \leq r_2)$$

de $\mathbf{C}^{r_2}$ est $A_0 A(\pi B^2)^{r_2-1}$. On prend $A=2$, $B=1$ et on choisit A_0 de telle sorte que ce volume soit $> 2^{r_2}|D_K|^{1/2}$, disons $A_0 = 2(\pi/2)^{r_2-1}|D_K|^{1/2}$. Alors il existe $\alpha \in \mathbf{Z}_K \setminus \{0\}$ tel que $|\sigma_i(\alpha)| < 1$ pour $2 \leq i \leq r_2$, $|\Re\sigma_1(\alpha)| < 1$ et $|\Im\sigma_1(\alpha)| < A_0/2$. On a encore $|\sigma_1(\alpha)| = |\overline{\sigma}_1(\alpha)| \geq 1 > |\sigma_i(\alpha)|$ pour $2 \leq i \leq r_2$. De plus $\sigma_1(\alpha)$ n'est pas réel, donc $\sigma_1(\alpha) \neq \sigma_i(\alpha)$ pour $2 \leq i \leq n$. On en déduit de nouveau que α est un générateur de K qui appartient à un ensemble fini ne dépendant que de n et de $|D_K|$ □

3.6.6 Décomposition des idéaux premiers dans une extension

Soient k_1 un corps de nombres, k_2 une extension finie de k_1 de degré n, $\mathfrak{p}$ un idéal de $\mathbf{Z}_{k_1}$; on peut décomposer l'idéal engendré par $\mathfrak{p}$ dans $\mathbf{Z}_{k_2}$ sous la forme

$$\mathbf{Z}_{k_2}\mathfrak{p} = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$$

où $\mathfrak{P}_i$ sont des idéaux premiers deux-à-deux distincts de $\mathbf{Z}_{k_2}$ et $e_1, \ldots, e_g$ des entiers ≥ 1. Alors $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ sont les idéaux premiers de $\mathbf{Z}_{k_2}$ tels que $\mathfrak{P} \cap \mathbf{Z}_{k_1} = \mathfrak{p}$. L'entier e_i est *l'indice de ramification de* $\mathfrak{P}_i$ *sur* $\mathfrak{p}$. Si f_i désigne le *degré résiduel de* $\mathfrak{P}_i$ *sur* $\mathfrak{p}$, c'est-à-dire le degré de l'extension $[\mathbf{Z}_{k_2}/\mathfrak{P}_i : \mathbf{Z}_{k_1}/\mathfrak{p}]$, alors

$$\mathbf{Z}_{k_2}/\mathfrak{p}\mathbf{Z}_{k_2} \simeq \prod_{i=1}^{g} \mathbf{Z}_{k_2}/\mathfrak{P}_i^{e_i}.$$

Montrons que pour $1 \leq i \leq g$ le quotient $\mathbf{Z}_{k_2}/\mathfrak{P}_i^{e_i}$ est un $\mathbf{Z}_{k_1}/\mathfrak{p}$-espace vectoriel de dimension $e_i f_i$. Pour cela on considère la suite de $\mathbf{Z}_{k_1}/\mathfrak{p}$-espaces vectoriels

$$\mathbf{Z}_{k_2}/\mathfrak{P}_i^{e_i} \supset \mathbf{Z}_{k_2}/\mathfrak{P}_i^{e_i-1} \supset \cdots \supset \mathbf{Z}_{k_2}/\mathfrak{P}_i \supset \{0\}.$$

Le quotient de deux termes consécutifs est isomorphe $\mathfrak{P}_i^r/\mathfrak{P}_i^{r+1}$, qui est un $\mathbf{Z}_{k_2}/\mathfrak{P}_i$-espace vectoriel de dimension 1, donc un $\mathbf{Z}_{k_1}/\mathfrak{p}$-espace vectoriel de dimension f_i.

Montrons ensuite que $\mathbf{Z}_{k_2}/\mathfrak{p}\mathbf{Z}_{k_2}$ est un $\mathbf{Z}_{k_1}/\mathfrak{p}$ espace vectoriel de dimension n. Soit $\omega_1, \ldots, \omega_m$ une famille d'éléments de $\mathbf{Z}_{k_2}$ dont les classes $\bar{\omega}_1, \ldots, \bar{\omega}_m$ modulo $\mathfrak{p}\mathbf{Z}_{k_2}$ constituent une base du $\mathbf{Z}_{k_1}/\mathfrak{p}$-espace vectoriel $\mathbf{Z}_{k_2}/\mathfrak{p}\mathbf{Z}_{k_2}$. Il s'agit de vérifier que $\omega_1, \ldots, \omega_m$ est une base de k_2 sur k_1.

On commence par vérifier que $\{\omega_1, \ldots, \omega_m\}$ est une famille libre sur k_1. S'il y a une relation non triviale $a_1\omega_1 + \cdots + a_m\omega_m = 0$ avec des a_i dans $\mathbf{Z}_{k_1}$ non tous nuls, soit $\mathfrak{a}$ l'idéal de $\mathbf{Z}_{k_1}$ engendré par ces coefficients $a_1, \ldots, a_m$ et soit $\alpha \in \mathfrak{a}^{-1} \setminus \mathfrak{a}^{-1}\mathfrak{p}$. Alors $\alpha\mathfrak{a} \not\subset \mathfrak{p}$, donc $\alpha a_1, \ldots, \alpha a_m$ appartiennent à $\mathbf{Z}_{k_1}$ mais ne sont pas tous dans $\mathfrak{p}$, et la relation $\alpha a_1\omega_1 + \cdots + \alpha a_m\omega_m \equiv 0 \pmod{\mathfrak{p}}$ donne une contradiction avec l'hypothèse que $\{\bar{\omega}_1, \ldots, \bar{\omega}_m\}$ est une famille libre sur $\mathbf{Z}_{k_1}/\mathfrak{p}$.

Montrons enfin que la famille $\{\omega_1, \ldots, \omega_m\}$ engendre k_2 comme k_1-espace vectoriel. Soit $M = \mathbf{Z}_{k_1}\omega_1 + \cdots + \mathbf{Z}_{k_1}\omega_m$ et soit $N = \mathbf{Z}_{k_2}/M$. Par hypothèse $\{\bar{\omega}_1, \ldots, \bar{\omega}_m\}$ est une partie génératrice du $\mathbf{Z}_{k_1}/\mathfrak{p}$-espace vectoriel $\mathbf{Z}_{k_2}/\mathfrak{p}\mathbf{Z}_{k_2}$, donc $\mathbf{Z}_{k_2} = M + \mathfrak{p}\mathbf{Z}_{k_2}$. Alors $\mathfrak{p}N = N$. Le *Lemme de Nakayama* (voir 3.82) implique qu'il existe $\alpha \in 1 + \mathfrak{p}$ tel que $\alpha N = 0$. Alors $\alpha\mathbf{Z}_{k_2} \subset M$ et par conséquent $k_2 = k_1\omega_1 + \cdots + k_1\omega_m$. En particulier $m = n$.

De ceci on déduit une généralisation de (3.74) :

$$e_1 f_1 + \cdots + e_g f_g = n. \tag{3.81}$$

Lemme 3.82 (de Nakayama). *Soient A un anneau, $\mathfrak{a}$ un idéal de A et M un A-module de type fini. On suppose $\mathfrak{a}M = M$. Alors il existe un élément $\alpha \in 1 + \mathfrak{a}$ tel que $\alpha M = 0$.*

Démonstration. Soit $m_1, \ldots, m_n$ une famille génératrice du A-module M. Par hypothèse il existe des éléments x_{ij} dans $\mathfrak{a}$ $(1 \leq i, j \leq n)$ tels que

$$m_i = \sum_{j=1}^{n} x_{ij} m_j \quad (1 \leq i \leq n).$$

Soit M la matrice $\left(x_{ij}\right)_{1 \leq i,j \leq n}$ et soit α le déterminant de $I_n - M$. Alors α appartient à $1 + \mathfrak{a}$ et $\alpha M = 0$.

□

Dans le cas particulier où l'extension L/K est galoisienne le groupe de Galois agit transitivement sur les idéaux de L au dessus d'un idéal donné de K et il conserve les indices de ramification et des caractéristiques résiduelles : la formule (3.81) s'écrit alors simplement $efg = n$.

Définition. Un *anneau de Dedekind* est un anneau noethérien, intégralement clos, dans lequel tout idéal fractionnaire est inversible.

Théorème 3.83. *Soient A un anneau de Dedekind de caractéristique nulle, K son corps des fractions, L une extension finie de K. Alors la fermeture intégrale de A dans L est un anneau de Dedekind.*

En particulier ($A = \mathbf{Z}$, $K = \mathbf{Q}$) l'anneau des entiers d'un corps de nombres est un anneau de Dedekind.

Dans un anneau de Dedekind, tout idéal fractionnaire non nul s'écrit de manière unique

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{a_{\mathfrak{p}}},$$

où $\mathfrak{p}$ décrit les idéaux premiers non nuls de A et où les $a_{\mathfrak{p}}$ sont des entiers rationnels tous nuls sauf un nombre fini.

Université P. et M. Curie (Paris VI),
Deuxième semestre 2006/2007

Michel Waldschmidt
date de mise à jour: 24/04/2007

Master de sciences et technologies 1ère année -
Spécialité : Mathématiques Fondamentales

Mention : Mathématiques et applications
MO11 : Théorie des nombres (12 ECTS)

Quatrième partie : Théorie Analytique des Nombres

Fascicule 8 : Chapitre 4, sections 4.1 à 4.3 (15 pages)

4 Théorie analytique des nombres

4.1 La fonction zêta de Riemann et le théorème des nombres premiers

Pour $x > 0$ on désigne par $\pi(x)$ le nombre de nombres premiers inférieurs ou égaux à x :

$$\pi(x) = \sum_{p \le x} 1. \tag{4.1}$$

Ainsi $\pi(10) = 4$, $\pi(100) = 25$, $\pi(1000) = 168$, $\pi(10\,000) = 1229$.

Le théorème des nombres premiers, conjecturé par Gauss en 1792, a été démontré par Hadamard et de la Vallée Poussin en 1896. Il s'énonce :

Théorème 4.2 (Théorème des nombres premiers). *Pour $x \to \infty$ on a*

$$\pi(x) \sim \frac{x}{\log x}.$$

Une approximation de $\pi(x)$ meilleure que $x/\log x$ est donnée par la fonction *logarithme intégral*

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t}.$$

La démonstration de Hadamard et de la Vallée Poussin repose sur l'analyse complexe et la fonction zêta de Riemann. La série $\sum_{n\ge1} n^{-s}$ converge normalement, donc uniformément pour s dans un compact du demi plan $\Re s > 1$. Par conséquent elle définit une fonction analytique dans ce demi-plan qui est la fonction zêta (introduite par Riemann en 1859 dans son unique article de théorie des nombres) :

$$\zeta(s) = \sum_{n\ge1} \frac{1}{n^s}.$$

Les valeurs de cette fonction pour s réel positif avaient déjà été étudiées par Euler en 1736. Il montrait notamment que pour s entier positif pair le quotient $\zeta(s)/\pi^s$ est un nombre rationnel.

Par exemple $\zeta(2) = \pi^2/6$, $\zeta(4) = \pi^4/90$. Euler ne s'est pas contenté d'étudier les valeurs de cette fonction pour s positif, il a aussi considéré le cas des entiers négatifs (où la série diverge), par exemple $\zeta(0) = -1/2$, $\zeta(-1) = -1/12$. Il a établi que ζ s'annule en les entiers négatifs pairs et prend une valeur rationnelle non nulle en les entiers négatifs impairs.

Le *théorème fondamental de l'arithmétique* selon lequel l'anneau $\mathbf{Z}$ est factoriel est intégré dans l'énoncé suivant qui éclaire l'importance du rôle joué par la fonction zêta dans l'étude de la répartition des nombres premiers.

Théorème 4.3 (Produit d'Euler). *Le produit infini $\prod_p (1-p^{-s})$ étendu aux nombres premiers p, est uniformément sur tout compact du demi plan $\Re s > 1$. Il définit une fonction analytique dans ce demi plan qui vérifie*

$$\zeta(s) = \prod_p \frac{1}{1-p^{-s}}\cdot$$

Le fait que la série harmonique $\sum_{n\geq 1} 1/n$ diverge permet d'en déduire que la série $\sum_p 1/p$ est aussi divergente.

Démonstration. En faisant le produit pour les nombres premiers $\leq X$ des séries géométriques

$$\frac{1}{1-p^{-s}} = \sum_{m\geq 0} \frac{1}{p^{ms}}$$

on trouve

$$\prod_{p\leq X} \frac{1}{1-p^{-s}} = \prod_{p\leq X} \sum_{m\geq 0} \frac{1}{p^{ms}} = \sum_{n\in\mathcal{N}(X)} \frac{1}{n^s},$$

où $\mathcal{N}(X)$ est l'ensemble des entiers positifs dont tous les facteurs premiers sont $\leq X$. Alors pour $\Re s = \sigma > 1$ on a

$$\left|\zeta(s) - \prod_{p\leq X} \frac{1}{1-p^{-s}}\right| = \left|\sum_{n\notin\mathcal{N}(X)} \frac{1}{n^s}\right| \leq \sum_{n>X} \left|\frac{1}{n^s}\right| = \sum_{n>X} \frac{1}{n^\sigma}\cdot$$

La définition de la convergence d'un produit infini dont tous les facteurs sont différents de 0 impose que le produit ne soit pas nul. Afin de vérifier $\zeta(s) \neq 0$ pour $\Re s > 1$, on utilise le développement en série de Taylor de la détermination principale du logarithme complexe : pour $|u| < 1$,

$$\log(1-u) = -\sum_{m\geq 1} \frac{u^m}{m}\cdot$$

On remplace u par p^{-s} :

$$\log(1-p^{-s}) = -\sum_{m\geq 1} \frac{p^{-ms}}{m}$$

et on trouve, pour $\Re s > 1$,

$$\zeta(s) = \exp\left(\sum_p \sum_{m\geq 1} \frac{1}{mp^{ms}}\right). \tag{4.4}$$

Donc $\zeta(s) \neq 0$ pour $\Re s > 1$. □

On écrit (4.4) sous la forme

$$\log \zeta(s) = \sum_p \sum_{m \geq 1} \frac{1}{m p^{ms}}.$$

En dérivant, on obtient le développement en série de la dérivée logarithmique de ζ dans ce demi plan.

Corollaire 4.5. *La série*

$$\sum_p \sum_{m \geq 1} \frac{1}{m p^{ms}}$$

définit une fonction analytique dans le demi plan $\Re s > 1$ qui est une détermination analytique du logarithme de $\zeta(s)$ dans ce demi plan. De plus la dérivée logarithmique de $\zeta(s)$ vérifie pour $\Re s > 1$:

$$\frac{\zeta'(s)}{\zeta(s)} = -\sum_p \sum_{m \geq 1} \frac{\log p}{p^{ms}}.$$

Le développement en série de ζ'/ζ peut aussi s'écrire

$$\frac{\zeta'(s)}{\zeta(s)} = -\sum_{n \geq 1} \frac{\Lambda(n)}{n^s}$$

où Λ désigne la *fonction de Mangoldt*

$$\Lambda(n) = \begin{cases} \log p & \text{si } n = p^m \text{ avec } p \text{ premier} \\ 0 & \text{si } n \text{ n'est pas une puissance d'un nombre premier.} \end{cases}$$

Théorème 4.6 (Prolongement analytique de la fonction zêta de Riemann). *La fonction $\zeta(s) - 1/(s-1)$ se prolonge en une fonction analytique dans le demi plan $\Re s > 0$.*

Démonstration. On écrit, pour $n \geq 1$,

$$\frac{1}{n^s} = s \int_n^\infty t^{-s-1} dt.$$

Alors

$$\zeta(s) = s \sum_{n \geq 1} \int_n^\infty t^{-s-1} dt = s \int_1^\infty [t] t^{-s-1} dt$$

car $\sum_{n=1}^t 1 = [t]$. Donc

$$\zeta(s) = s \int_1^\infty t^{-s} dt + s \int_1^\infty ([t] - t) t^{-s-1} dt.$$

Le premier terme vaut

$$s \int_1^\infty t^{-s} dt = \frac{1}{s-1} + 1$$

et la seconde intégrale est convergente dans $\Re s > 0$ où elle définit une fonction holomorphe.

□

Exercice. Vérifier

$$\lim_{s\to 1}\left(\zeta(s)-\frac{1}{s-1}\right)=\gamma$$

où γ est la *constante d'Euler* :

$$\gamma=\lim_{N\to\infty}\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{N}-\log N.$$

Ainsi la fonction zêta de Riemann se prolonge en une fonction méromorphe dans le demi plan $\Re s>0$ avec un pôle simple en $s=1$, de résidu 1. Une des étapes essentielles dans la démonstration du théorème des nombres premiers 4.2 consiste à montrer qu'il existe une constante $A>0$ telle que la fonction ζ, ainsi prolongée, ne s'annule pas dans le rectangle

$$1-\frac{A}{\log|\Im s|}<\Re s<1.$$

En 1903 E. Landau a montré que le théorème 4.2 des nombres premiers peut se déduire d'un énoncé plus faible, qui avait été obtenu dès 1892 par Hadamard :

Théorème 4.7. *La fonction ζ ne s'annule pas sur la droite $\Re s=1$, $s\neq 1$.*

Il en résulte que la fonction

$$\frac{\zeta'(s)}{\zeta(s)}+\frac{1}{s-1},$$

définie pour $\Re s>1$, s'étend en une fonction holomorphe dans un voisinage de la droite $\Re s=1$.

Riemann a démontré en 1859 que la fonction zêta s'étendait en une fonction méromorphe dans tout le plan complexe, avec un unique pôle simple en $s=1$, et que de plus cette fonction ainsi étendue vérifiait une équation fonctionnelle. Pour l'écrire on introduit la fonction Gamma d'Euler

Proposition 4.8. *L'intégrale*

$$\Gamma(s)=\int_0^\infty e^{-t}t^{s-1}dt$$

définit une fonction holomorphe pour $\Re s>0$ qui vérifie l'équation fonctionnelle

$$\Gamma(s+1)=s\Gamma(s).$$

Elle se prolonge en une fonction méromorphe dans $\mathbf{C}$ ayant un pôle simple en tous les entiers ≤ 0.

Démonstration. Il est facile de vérifier que l'intégrale converge et définit une fonction analytique dans le demi plan $\Re s>0$. En intégrant par parties on trouve

$$\Gamma(s)=\left[\frac{1}{s}e^{-s}+t^s\right]_0^\infty-\frac{1}{s}\int_0^\infty e^{-t}t^s dt=\frac{1}{s}\Gamma(s+1).$$

Cette équation fonctionnelle permet de prolonger la fonction par la formule

$$\Gamma(s)=\frac{\Gamma(s+n+1)}{s(s+1)\cdots(s+n)}.$$

Le membre de droite est bien défini pour $\Re s > -n-1$, celui de gauche seulement pour $\Re s > 0$. Pour $\Re s > 0$, les deux membres coïncident. En prenant $s \in \mathbf{C}$ quelconque et en choisissant $n > -\Re s - 1$, on définit $\Gamma(s)$ en prenant comme définition le membre de droite : il ne dépend pas de n et on obtient ainsi une fonction analytique dans $\mathbf{C} \setminus \{0,\ -1,\ -2\ldots\}$ ayant un pôle simple en $s = -n$ pour n entier ≥ 0 ; le résidu est $(-1)^n/n!$ (avec $0! = 1$, comme il se doit). □

Remarque. Comme $\Gamma(1) = 1$ on en déduit $\Gamma(n+1) = n!$.

On définit une fonction entière dans $\mathbf{C}$ par

$$\xi(s) = s(s-1)\pi^{-s/2}\Gamma(s/2)\zeta(s).$$

Le seul pôle de ζ est $s = 1$. De plus ζ s'annule aux entiers pairs strictement négatifs et ne s'annule pas aux entiers négatifs impairs. Les pôles de $\Gamma(s/2)$ sont tous les entiers pairs ≤ 0 et Γ ne s'annule pas en $s = 1$. C'est pourquoi la fonction ξ est entière (analytique dans $\mathbf{C}$). Sa valeur en $s = 0$ et en $s = 1$ est 1, ce qui revient à dire que l'on a $\Gamma(1/2) = \sqrt{\pi}$. En effet, en effectuant le changement de variables $t = x^2$ on trouve

$$\Gamma(1/2) = \int_0^\infty e^{-t}t^{-1/2}dt = 2\int_0^\infty e^{-x^2}dx.$$

Donc

$$\frac{1}{4}\Gamma(1/2)^2 = \int_0^\infty\int_0^\infty e^{-x^2-y^2}dxdy = \int_0^\infty\int_0^{\pi/2} e^{-r^2}rdrd\theta = \left[-\frac{1}{2}e^{-r^2}\right]_0^\infty \frac{\pi}{2} = \frac{\pi}{4}.$$

B. Riemann a aussi démontré :

Théorème 4.9 (Equation fonctionnelle de la fonction zêta de Riemann). *La fonction ξ vérifie*

$$\xi(s) = \xi(1-s).$$

L'axe de symétrie est $\Re s = 1/2$, l'équation fonctionnelle permet de bien connaître la fonction ζ dans le demi plan $\Re s < 0$ grâce au produit infini qui converge dans $\Re s > 1$. Par exemple les seuls zéros de ζ dans ce demi plan $\Re s < 0$ sont les entiers négatifs pairs.

Le domaine $0 < \Re s < 1$ est la *bande critique* et la droite $\Re s = 1/2$ est la *droite critique*. C'est Riemann qui a montré l'importance des zéros non triviaux (c'est-à-dire dans la bande critique) de la fonction zêta pour l'étude des nombres premiers. Après Euler il a montré le lien entre la fonction zêta et la fonction π – cf. (4.1) en établissant la relation

$$\frac{1}{s}\log\zeta(s) = \int_0^s \frac{\pi(x)}{x^{s-1}}\frac{dx}{x}$$

pour $\Re s > 1$. Le *produit de Hadamard*, qui permet d'exprimer une fonction entière comme produit infini étendu à l'ensemble des zéros, s'écrit [4]

$$\zeta(s) = \frac{2^{s-1}\pi^s}{e^{((\gamma/2)+1)s}(s-1)\Gamma(1+(s/2))}\prod_\varrho\left(1-\frac{s}{\varrho}\right)e^{s/\varrho}$$

[4] Le produit infini sur ϱ est la limite, pour T tendant vers l'infini, du produit étendu à l'ensemble fini des ϱ de partie imaginaire $\leq T$.

où ϱ décrit les zéros de ζ dans la bande critique, et il a estimé le nombre de zéros dans un rectangle $[0,1]\times[0,iT]$ de cette bande : pour $t\to\infty$ il vaut

$$\frac{T}{2\pi}\log\frac{T}{2\pi}-\frac{T}{2\pi}+O(\log T).$$

On démontre le théorème 4.9 qui donne l'équation fonctionnelle de la fonction zêta de Riemann en utilisant la *Formule de Poisson* qui relie la série des valeurs aux entiers rationnels d'une fonction intégrable f sur $\mathbf{R}$ à la série des valeurs de sa transformée de Fourier

$$\widehat{f}(y)=\int_{-\infty}^{+\infty}f(x)e^{2i\pi xy}dx.$$

Si la fonction $x\mapsto\sum_{n\in\mathbf{Z}}f(x+n)$ est continue et à variations bornées sur $[0,1]$, alors

$$\sum_{n\in\mathbf{Z}}f(n)=\sum_{m\in\mathbf{Z}}\widehat{f}(m).$$

Cette formule de Poisson permet de montrer que la *série thêta*

$$\theta(u)=\sum_{n\in\mathbf{Z}}e^{-\pi un^2}$$

satisfait l'équation fonctionnelle, pour $u\in\mathbf{R}_+^\times$:

$$\theta(1/u)=\sqrt{u}\theta(u).$$

On montre ensuite que la fonction ξ du théorème 4.9 satisfait, pour $\Re s>1$,

$$\xi(s)=s(s-1)\int_0^\infty\frac{(\theta(u)-1)u^{s/2}}{2u}du.$$

Pour terminer cette section voici l'énoncé d'un des principaux problèmes ouverts en théorie des nombres.

Conjecture 4.10 (Hypothèse de Riemann). *Les zéros complexes de ζ dans la bande critique sont tous sur la droite critique : si $s\in\mathbf{C}$ vérifie $0<\Re s<1$ et $\zeta(s)=0$, alors $\Re s=1/2$.*

On trouvera d'autres informations sur la fonction zêta de Riemann dans le texte de P. Cartier [Ca].

4.2 Le théorème de la progression arithmétique de Dirichlet

A.M. Legendre a conjecturé en 1785 et Lejeune Dirichlet a démontré en 1837 le théorème de la progression arithmétique :

Théorème 4.11 (Dirichlet). *Soient a et b deux entiers positifs premiers entre eux. Alors il existe une infinité de nombres premiers p congrus à a modulo b.*

La démonstration du théorème 4.2 des nombres premiers s'étend aux progressions arithmétiques et permet de préciser cet énoncé. Pour a et b entiers positifs et pour $x>0$, on désigne par $\pi(x;a,b)$ le nombre de nombres premiers p dans l'intervalle $2\leq p\leq x$ qui sont congrus à a modulo b :

Théorème 4.12. *Soient a et b deux entiers positifs premiers entre eux. Pour $x\to\infty$ on a*

$$\pi(x;a,b)\sim\frac{x}{\varphi(b)\log x}.$$

4.2.1 Caractères

Soit A un groupe abélien d'exposant fini et soit m un multiple de l'exposant ; autrement dit tout élément x de A vérifie $mx = 0$. Les homomorphismes de A dans un groupe cyclique d'ordre m forment un groupe, qui ne dépend (à isomorphisme près) ni du groupe cyclique d'ordre m choisi (deux groupes cycliques d'ordre m sont isomorphes), ni du choix de m multiple de l'exposant de A. En effet, si m_0 est l'exposant de A et si C_m est un groupe cyclique d'ordre m multiple de m_0, alors pour tout homomorphisme de A dans C_m l'image de A appartient à l'unique sous-groupe de C_m d'ordre m_0. On définit le *dual de* A par

$$\widehat{A} = \mathrm{Hom}(A, C_m).$$

Par exemple si k est un corps qui contient les racines m-ièmes de l'unité, alors $\widehat{A}$ est isomorphe au *groupe des caractères de* A, qui sont les homomorphismes de A dans le groupe multiplicatif $k^\times$. On prendra le plus souvent pour k le corps des nombres complexes (les caractères de G sont les homomorphismes de G dans le groupe multiplicatif $\mathbf{U}$ des nombres complexes de module 1, comme l'exposant de A est fini son image est dans le groupe de torsion de $\mathbf{U}$, qui est le groupe des racines de l'unité), mais on peut aussi prendre un corps fini $\mathbf{F}_q$, la condition pour que $\mathbf{F}_q$ contienne les racines m-ièmes de l'unité s'écrivant $m|q-1$, c'est-à-dire $q \equiv 1 \pmod{m}$.

Aussi $\widehat{A}$ est isomorphe au groupe des homomorphismes de A dans le groupe $\mathbf{Q}/\mathbf{Z}$. Noter que $\mathbf{Q}/\mathbf{Z}$ est le groupe de torsion de $\mathbf{R}/\mathbf{Z}$, il est isomorphe au groupe de torsion de $\mathbf{U}$, c'est-à-dire le groupe des racines de l'unité dans $\mathbf{C}$.

Si le groupe C_m est noté additivement, l'élément neutre de $\widehat{A}$ est l'application constante $x \mapsto 0$, tandis que s'il est noté multiplicativement, c'est $x \mapsto 1$.

4.2.2 Dual d'un groupe abélien fini

Le dual est défini pour un groupe abélien d'exposant fini. Il est donc bien défini pour un groupe abélien fini.

Proposition 4.13. *Un groupe cyclique est isomorphe à son dual.*

Démonstration. Soit A un groupe cyclique et soit m son ordre. Alors l'exposant de A est m. Le dual de A est donc isomorphe au groupe des endomorphismes de A. Un tel endomorphisme est déterminé par l'image d'un générateur. Soit x un générateur de A et soit ψ l'application identité de A dans A.

Quand on note A additivement, pour $0 \leq k < m$ l'application $k\psi : A \to A$ qui envoie x sur kx est un endomorphisme de A. En notation multiplicative on considère l'application $\psi^k : A \to A$ qui envoie x sur x^k.

On obtient ainsi tous les endomorphismes de A. De plus ψ est d'ordre m dans $\widehat{A}$. Donc ψ est un générateur du groupe $\widehat{A}$ et par conséquent $\widehat{A}$ est cyclique d'ordre m.

□

Noter que cet isomorphisme entre A et $\widehat{A}$ quand A est cyclique dépend du choix d'un générateur : il n'y a pas plus d'isomorphisme canonique entre A et $\widehat{A}$ que de générateur privilégié d'un groupe cyclique. Il existe exactement $\varphi(m)$ isomorphismes entre un groupe cyclique A d'ordre m et son dual $\widehat{A}$.

Soient A et B deux groupes abéliens finis et soit $f : A \to B$ un homomorphisme de groupes. On lui associe un homomorphisme $f\widehat{\ } : \widehat{B} \to \widehat{A}$ défini de la manière suivante : soit m un multiple commun de l'exposant de A et de celui de B. Si $\psi : B \to C_m$ est un homomorphisme de B dans un groupe cyclique C_m d'ordre m, on pose $f\widehat{\ }(\psi) = \psi \circ f$, qui est un homomorphisme de A dans C_m :

$$f\widehat{\ }(\psi) : A \xrightarrow{f} B \xrightarrow{\psi} C_m.$$

Si $f : A_1 \to A_2$ et $g : A_2 \to A_3$ sont deux homomorphismes de groupes, alors $(g \circ f)\widehat{\ } = f\widehat{\ } \circ g\widehat{\ }$: c'est l'homomorphisme $\widehat{A_3} \to \widehat{A_1}$ qui envoie $\psi : A_3 \to C_m$ sur $\psi \circ g \circ f : A_1 \to C_m$.

Théorème 4.14. *Si B et C sont deux groupes abéliens finis et si $A = B \times C$ est leur produit direct, alors $\widehat{A}$ est isomorphe au produit direct $\widehat{B} \times \widehat{C}$.*

Démonstration. Notons A additivement. Soient $f : A \to B$, $g : A \to C$ les projections de $A = B \times C$ sur chacun des deux facteurs et $i : B \to A$, $j : C \to A$ les injections canoniques. Alors

$$\begin{array}{rccc} f\widehat{\ } + g\widehat{\ } : & \widehat{B} \times \widehat{C} & \to & \widehat{A} \\ & (\psi_1, \psi_2) & \mapsto & \psi_1 \circ f + \psi_2 \circ g \end{array}$$

et

$$\begin{array}{rccc} (i\widehat{\ }, j\widehat{\ }) : & \widehat{A} & \to & \widehat{B} \times \widehat{C} \\ & \psi & \mapsto & (\psi \circ i, \psi \circ j) \end{array}$$

sont deux isomorphismes inverses.

□

En combinant la proposition 4.13 et le théorème 4.14 on déduit du théorème de structure des groupes abéliens finis :

Corollaire 4.15. *Un groupe abélien fini est isomorphe à son dual.*

Lemme 4.16. *Soient G un groupe abélien fini d'ordre n, x un élément de G d'ordre r et ζ une racine primitive r-ième de l'unité. Il existe n/r caractères de G tels que $\xi(x) = \zeta$. De plus on a, dans $\mathbf{C}[T]$,*

$$\prod_{\chi \in \widehat{G}} (1 - \chi(x)T) = (1 - T^r)^{n/r}.$$

Pour $r = 1$ le lemme se réduit à dire que $\widehat{G}$ a n éléments qui envoient tous 1 sur 1.

Si G est cyclique d'ordre n et que l'on prend $r = n$, le lemme dit que si x est un générateur de G, alors pour tout caractère χ de G l'image $\chi(x)$ est une racine r-ième de 1, pour toute racine r-ième de 1 il existe un unique χ qui envoie x sur cette racine, et enfin χ est entièrement connu quand on connaît $\chi(x)$.

Démonstration. Comme $x^r = 1$ pour tout $\chi \in \widehat{G}$ on a $\chi(x)^r = 1$ et donc $\chi(x)$ est une racine r-ième de l'unité. L'application $\chi \mapsto \chi(x)$ de $\widehat{G}$ dans le groupe cyclique des racines de l'unité d'ordre divisant r est un homomorphisme dont le noyau est constitué par les caractères triviaux sur le sous-groupe cyclique H de G engendré par x. Le noyau est isomorphe au dual de G/H, il a donc n/r éléments et par conséquent l'image a r éléments.

□

4.2.3 Bidual

Nous avons vu qu'il n'y avait pas d'isomorphisme canonique entre un groupe abélien fini et son dual. En revanche nous allons voir qu'il y a un isomorphisme canonique entre un groupe abélien et son bidual.

Proposition 4.17. *Soit A un groupe abélien fini. Soit m un multiple de l'exposant de A et soit C_m un groupe cyclique d'ordre m. À un élément x de A on associe l'élément $\widetilde{x}$ de $\widehat{\widehat{A}}$ qui envoie $\chi \in \widehat{A}$ sur $\chi(x) \in C_m$. Alors l'application*

$$\begin{array}{ccc} A & \to & \widehat{\widehat{A}} \\ x & \mapsto & \widetilde{x} \end{array}$$

est un isomorphisme de groupes.

La démonstration de la proposition 4.17 repose sur le lemme de séparation suivant, dans lequel nous notons e l'élément neutre de A (donc $e = 0$ en notation additive et $e = 1$ en notation multiplicative).

Lemme 4.18. *Soit A un groupe abélien fini et soit $x \in A \setminus \{e\}$. Alors il existe $\chi \in \widehat{A}$ tel que $\chi(x) \neq 1$.*

Démonstration. Ce lemme est clair quand A est cyclique, le cas général s'en déduit par le théorème de structure des groupes abéliens finis.

□

Démonstration de la proposition 4.17. L'application $x \mapsto \widetilde{x}$ est un homomorphisme de groupes de A dans son bidual, le lemme 4.18 montre qu'elle est injective, et comme A et son bidual ont le même nombre d'éléments (on sait déjà grâce au théorème de structure des groupes abéliens finis que ces deux groupes sont isomorphes) elle est aussi surjective.

□

4.2.4 Orthogonalité des caractères

On désigne par A un groupe abélien fini, par e son élément neutre, par m son exposant, par k un corps contenant les racines m-ièmes de l'unité et par $\widehat{A}$ le groupe des homomorphismes de A dans le groupe multiplicatif de k. Les éléments de $\widehat{A}$ sont les caractères de A. Ce groupe $\widehat{A}$ est une des formes du dual de A, mais ici nous allons utiliser non seulement la structure multiplicative de k mais aussi sa structure additive. Le caractère unité χ_1 de A (encore appelé *caractère principal de A*) est l'application constante

$$\begin{array}{rccc} \chi_1 : & A & \to & k^\times \\ & x & \mapsto & 1. \end{array}$$

Lemme 4.19. *Soit A un groupe abélien fini.*
(i) Soit $\chi \in \widehat{A}$. Alors

$$\sum_{x \in A} \chi(x) = \begin{cases} 0 & si\ \chi \neq \chi_1, \\ |A| & si\ \chi = \chi_1. \end{cases}$$

(ii) Soit $x \in A$. Alors

$$\sum_{\chi \in \widehat{A}} \chi(x) = \begin{cases} 0 & \text{si } x \neq e, \\ |A| & \text{si } x = e. \end{cases}$$

Démonstration. Commençons par démontrer *(i)*. Soit $y \in A$. Notons A additivement *(la rédaction de la démonstration en notation multiplicative est laissée en exercice)*. L'application $y \mapsto x + y$ est une bijection de A sur A, donc

$$\sum_{x \in A} \chi(x + y) = \sum_{x \in A} \chi(x).$$

Par ailleurs $\chi(x + y) = \chi(x)\chi(y)$, donc

$$\sum_{x \in A} \chi(x + y) = \chi(y) \sum_{x \in A} \chi(x).$$

Par conséquent

$$\big(1 - \chi(y)\big) \sum_{x \in A} \chi(x) = 0$$

pour tout $y \in A$. Si $\chi \neq \chi_1$ alors il existe $y \in A$ tel que $\chi(y) \neq 1$, d'où on déduit

$$\sum_{x \in A} \chi(x) = 0.$$

Dans le cas $\chi = \chi_1$ tous les $\chi(x)$, $x \in A$ valent 1 et il y en a $|A|$. Cela complète la démonstration de *(i)*.

Pour la démonstration de *(ii)* on peut soit répéter la démonstration de *(i)* en utilisant le lemme 4.18, soit utiliser le théorème 4.17 : notons $\tilde{x}$ l'élément de $\widehat{\widehat{A}}$ associé à $x \in A$ par l'isomorphisme canonique entre A et son bidual ; on écrit

$$\sum_{\chi \in \widehat{A}} \chi(x) = \sum_{\chi \in \widehat{A}} \tilde{x}(\chi)$$

et on utilise *(i)* avec A remplacé par $\widehat{A}$. □

Exercice. Pour a et x dans A vérifier

$$\frac{1}{|A|} \sum_{\chi \in \widehat{A}} \overline{\chi}(a)\chi(x) = \begin{cases} 1 & \text{si } x = a, \\ 0 & \text{si } x \neq a. \end{cases}$$

Remarque. Le $\mathbf{C}$-espace vectoriel $\mathbf{C}^A$, qui est de dimension $|A|$, est muni d'une structure Hilbertienne grâce au produit scalaire

$$\langle x, y \rangle = \frac{1}{|A|} \sum_{a \in A} x(a)\overline{y(a)}.$$

Un caractère χ de A considéré comme application de A dans $\mathbf{C}^\times$ est un élément de $\mathbf{C}^A$. Comme ses valeurs sont dans le cercle unité $\mathbf{U} = \{z \in \mathbf{C}\ ;\ |z| = 1\}$, le caractère $\overline{\chi}$ obtenu en composant χ avec l'automorphisme de conjugaison complexe de $\mathbf{C}$ est l'inverse χ^{-1} de χ dans le groupe $\widehat{A}$.

Le produit scalaire de deux caractères χ' et χ'' est alors

$$\begin{aligned}\langle \chi', \chi'' \rangle = & \quad \frac{1}{|A|} \sum_{a \in A} \chi'(a)\overline{\chi''(a)} \\ = & \quad \frac{1}{|A|} \sum_{a \in A} \chi'(a)\chi''^{-1}(a) \\ = & \quad \frac{1}{|A|} \sum_{a \in A} \chi' \circ \chi''^{-1}(a) \\ = & \quad \begin{cases} 1 & \text{si } \chi' = \chi'', \\ 0 & \text{si } \chi' \neq \chi''. \end{cases}\end{aligned}$$

La dernière égalité résulte du lemme 4.19. Ainsi ce lemme exprime que les caractères de A forment une base orthonormée de $\mathbf{C}^A$.

On peut comparer ce résultat au suivant : soit $\mathbf{T} = \mathbf{R}/\mathbf{Z}$ le tore de dimension 1 (isomorphe à $\mathbf{U}$ par l'application $z \mapsto e^{2i\pi z}$). Un caractère de $\mathbf{T}$ est un homomorphisme *continu* de $\mathbf{T}$ dans $\mathbf{C}^\times$; les caractères de $\mathbf{T}$ forment un sous-groupe $\widehat{\mathbf{T}}$ de $\mathbf{C}^{\mathbf{T}}$. Pour chaque $n \in \mathbf{Z}$ l'application

$$\begin{array}{rccc} e_n : & \mathbf{T} & \to & \mathbf{C}^\times \\ & t & \mapsto & e^{2i\pi nt} \end{array}$$

est un caractère de $\mathbf{T}$, et on obtient ainsi tous les éléments de $\widehat{\mathbf{T}}$. De plus la famille $(e_n)_{n \in \mathbf{Z}}$ forme une base orthonormale de l'espace de Hilbert $L^2(\mathbf{T})$ des fonctions définies sur $\mathbf{T}$ et de carré intégrable (pour la mesure de Lebesque sur $[0, 1[$) pour le produit scalaire

$$\langle f, g \rangle = \int_0^1 f(t)\overline{g(t)}dt.$$

4.2.5 Caractères de Dirichlet

Soit q un entier ≥ 2. Le groupe multiplicatif $(\mathbf{Z}/q\mathbf{Z})^\times$ des éléments inversibles de l'anneau $\mathbf{Z}/q\mathbf{Z}$ est d'ordre $\varphi(q)$. Un élément du dual de $(\mathbf{Z}/q\mathbf{Z})^\times$ définit une application de l'ensemble des entiers premiers avec q à valeurs dans $\mathbf{C}^\times$ qui vérifie

$$\chi(ab) = \chi(a)\chi(b) \quad \text{pour tout } (a, b) \in \mathbf{Z}^2 \text{ avec } (ab, q) = 1$$

et

$$\chi(a + q) = \chi(a) \qquad \text{pour tout } a \in \mathbf{Z} \text{ avec } (a, q) = 1.$$

On prolonge χ en une application notée encore χ de $\mathbf{Z}$ dans $\mathbf{C}$ par $\chi(a) = 0$ si $(a, q) \neq 1$ et $\chi(0) = 0$.

On appelle *caractère de Dirichlet* (ou encore *caractère modulaire*) les applications $\mathbf{Z} \to \mathbf{C}$ ainsi obtenues. On notera D_q l'ensemble de celles qui proviennent de $(\mathbf{Z}/q\mathbf{Z})^\times$: ce sont les *caractères modulo* q. L'ensemble D_q a donc $\varphi(q)$ éléments. Pour $\chi \in D_q$ on a

$$\chi^{-1}(0) = \{a \in \mathbf{Z}\ ;\ (a, q) \neq 1\}.$$

Le *caractère principal modulo q* est l'application $\chi_1 = \mathbf{Z} \to \mathbf{C}^\times$ définie par

$$\chi_1(n) = \begin{cases} 0 & \text{si } (n,q) \neq 1, \\ 1 & \text{si } (n,q) = 1. \end{cases}$$

Pour $q = 1$ le quotient $\mathbf{Z}/1\mathbf{Z}$ n'est pas un anneau, mais on convient que $(\mathbf{Z}/1\mathbf{Z})^\times = \{1\}$. Avec cette convention $D_1 = \{\chi_1\}$ où

$$\chi_1(n) = \begin{cases} 0 & \text{si } n = 0, \\ 1 & \text{si } n \neq 0. \end{cases}$$

Exemple. Il y a deux caractères modulo 4, le caractère principal χ_1 modulo 4 et le caractère χ_2 défini par

$$\chi_2(n) = \begin{cases} 0 & \text{si } n \text{ est pair}, \\ 1 & \text{si } n \equiv 1 \pmod 4, \\ -1 & \text{si } n \equiv -1 \pmod 4. \end{cases}$$

Il y a quatre caractères modulo 8, le caractère principal χ_1, le caractère χ_2, le caractère χ_3 défini par

$$\chi_3(n) = \begin{cases} 0 & \text{si } n \text{ est pair}, \\ 1 & \text{si } n \equiv \pm 1 \pmod 8, \\ -1 & \text{si } n \equiv \pm 5 \pmod 8 \end{cases}$$

et le caractère $\chi_2\chi_3$.

Si p est un nombre premier impair le groupe $(\mathbf{Z}/p\mathbf{Z})^\times$ est cyclique d'ordre $p-1$, donc le groupe dual aussi. Soit a une racine primitive modulo p (la classe de a modulo p est un générateur de $(\mathbf{Z}/p\mathbf{Z})^\times$). Pour chacune des $p-1$ racines $p-1$-ièmes de l'unité ζ, on définit un caractère ψ_ζ modulo p par

$$\psi_\zeta(n) = \begin{cases} 0 & \text{si } p|n, \\ \zeta^u & \text{si } n \equiv a^u \pmod p. \end{cases}$$

Par exemple le choix $\zeta = -1$ (licite car p est impair) correspond à l'unique caractère de Dirichlet modulo p qui soit d'ordre 2 ; il est associé au symbole de Legendre :

$$\psi_{-1}(n) = \begin{cases} 0 & \text{si } p|n, \\ \left(\dfrac{n}{p}\right) & \text{si } (n,p) = 1. \end{cases}$$

4.2.6 Série L attachée à un caractère

Soit f une application de l'ensemble des nombres premiers dans $\mathbf{C}$. On a (formellement, ou si on préfère en supposant f à support fini, c'est-à-dire $f(p) = 0$ pour p suffisamment grand)

$$\begin{aligned} \sum_{p \equiv a \pmod m} f(p) &= \frac{1}{\varphi(m)} \sum_\chi \sum_p \overline{\chi}(a)\chi(p)f(p) \\ &= \frac{1}{\varphi(m)} \sum_{p \nmid m} f(p) + \frac{1}{\varphi(m)} \sum_{\chi \neq 1} \overline{\chi}(a) \sum_p \chi(p) f(p). \end{aligned}$$

Définition. Soit χ un caractère de Dirichlet modulo m. On définit la série L de Dirichlet attachée à χ par

$$L(\chi, s) = \sum_{n \geq 1} \chi(n) n^{-s}.$$

Par exemple si χ_1 est le caractère principal modulo m on a

$$\chi_1(n) = \begin{cases} 1 & \text{si } \operatorname{pgcd}(m, n) = 1, \\ 0 & \text{si } \operatorname{pgcd}(m, n) > 1 \end{cases}$$

et donc

$$L(\chi_1, s) = \sum_{\substack{n \geq 1 \\ \operatorname{pgcd}(m,n)=1}} n^{-s} = \zeta(s) \prod_{p \mid m} (1 - p^{-s}).$$

Proposition 4.20. *L'abscisse de convergence de la série $L(\chi, s)$ est*

$$\sigma = \begin{cases} 0 & \textit{si } \chi \neq \chi_1, \\ 1 & \textit{pour } \chi = \chi_1. \end{cases}$$

Démonstration. Pour un caractère χ modulo m qui n'est pas le caractère principal on a

$$\sum_{n=r+1}^{r+m} \chi(n) = 0$$

pour tout entier r, donc

$$\left| \sum_{n \leq x} \chi(n) \right| \leq m.$$

□

Théorème 4.21 (Produit d'Euler généralisé). *Soient m un entier positif et χ un caractère de Dirichlet modulo m. Le produit infini*

$$\prod_p (1 - \chi(p) p^{-s}) \tag{4.22}$$

étendu aux nombres premiers p, est uniformément convergent sur tout compact du demi plan $\Re s > 1$. Il définit une fonction analytique $L(\chi, s)$ dans ce demi plan qui vérifie

$$L(\chi, s) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}.$$

Démonstration. On reprend la démonstration du théorème 4.3 qui est le cas particulier du caractère principal modulo 1. En faisant le produit pour les nombres premiers $\leq X$ des séries géométriques

$$\frac{1}{1 - \chi(p) p^{-s}} = \sum_{m \geq 0} \frac{\chi(p)^m}{p^{ms}}$$

on trouve

$$\prod_{p\le X}\frac{\chi(p)}{1-p^{-s}} = \prod_{p\le X}\sum_{m\ge 0}\frac{\chi(p)^m}{p^{ms}} = \sum_{n\in\mathcal{N}(X)}\frac{\chi(n)}{n^s},$$

où $\mathcal{N}(X)$ est encore l'ensemble des entiers positifs dont tous les facteurs premiers sont $\le X$. Alors pour $\Re s = \sigma > 1$ on a

$$\left| L(\chi,s) - \prod_{p\le X}\frac{\chi(p)}{1-p^{-s}}\right| < \sum_{n>X}\frac{1}{n^\sigma}.$$

□

Corollaire 4.23. *Dans le demi plan $\Re s > 1$ la fonction $L(\chi,s)$ ne s'annule pas et une détermination analytique de son logarithme est*

$$\sum_p\sum_{m\ge 1}\frac{\chi(p)^m}{mp^{ms}}.$$

De plus la dérivée logarithmique de $L(\chi,s)$ vérifie pour $\Re s > 1$:

$$\frac{L'(\chi,s)}{L(\chi,s)} = -\sum_p\sum_{m\ge 1}\frac{\chi(p)^m\log p}{p^{ms}} = -\sum_{n\ge 1}\frac{\chi(p)^m\Lambda(n)}{n^s}.$$

Le résultat clé de la démonstration par Dirichlet de son théorème de la progression arithmétique est le pendant du théorème de Hadamard 4.7 :

Théorème 4.24. *Pour tout caractère de Dirichlet χ différent du caractère principal χ_1,*

$$L(\chi,1)\neq 0.$$

Cet énoncé est équivalent au fait que le produit Eulérien (4.22) converge en $s=1$.

4.3 Autres fonctions zêta

Nous avons vu que l'écriture de la fonction zêta de Riemann à la fois comme série de Dirichlet et comme produit d'Euler (Théorème 4.3) était une formulation du théorème fondamental de l'arithmétique. L'existence et l'unicité de la décomposition des idéaux d'un corps de nombres en produit d'idéaux premiers donne lieu à la fonction zêta de Dedekind (voir par exemple [Co] Définition 4.9.11 ; pour le cas particulier de $\mathbf{Z}[i]$, voir aussi [Ca] § 2.6).

Théorème 4.25. *Soit K un corps de nombres. La fonction zêta de Dedekind, définie pour $\Re s > 1$ par la série*

$$\zeta_K(s) = \sum_{\mathfrak{a}} N(\mathfrak{a})^{-s},$$

où la somme est étendue à l'ensemble des idéaux entiers non nuls de $\mathbf{Z}_K$, est égale au produit infini

$$\prod_{\mathfrak{p}}\left(1-N(\mathfrak{p})^{-s}\right)^{-1},$$

où le produit est étendu aux idéaux premiers non nuls de $\mathbf{Z}_K$.

Bien entendu pour $K = \mathbf{Q}$ on retrouve la fonction zêta de Riemann. Dans le cas général cette fonction admet encore un prolongement analytique (en une fonction méromorphe dans $\mathbf{C}$ avec un unique pôle simple en $s = 1$) et une équation fonctionnelle, qui fait intervenir plusieurs quantités, liées au corps de nombres K, que nous avons déjà rencontrées : le degré $n = [K : \mathbf{Q}]$, le nombre de plongements réels r_1 et le nombre de plongements complexes non réels $2r_2$ (avec $r_1 + 2r_2 = n$), le discriminant Δ, le nombre de classes d'idéaux h, le nombre de racines de l'unité w. Elle fait aussi intervenir le *régulateur* R du corps K, qui est le volume du réseau dans un hyperplan de $\mathbf{R}^{r_1+r_2}$ qui est l'image par le plongement logarithmique du groupe des unités.

On introduit la fonction

$$\Lambda(s) = |\Delta|^{s/2} \left(\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\right)^{r_1} \left(\pi^{-(s+1)/2}\Gamma\left(\frac{s+1}{2}\right)\right)^{r_2} \zeta_K(s).$$

Alors l'équation fonctionnelle de la fonction zêta de Dedekind du corps K est $\Lambda(s) = \Lambda(1 - s)$.

De plus la fonction ζ_K a un zéro en $s = 0$ de multiplicité $r = r_1 + r_2 - 1$ (le rang du groupe des unités de K) et

$$\lim_{s\to 0} s^{-r}\zeta_K(s) = -hR/w.$$

Par l'équation fonctionnelle, cela signifie que le résidu en $s = 1$ est

$$\lim_{s\to 1}(s-1)\zeta_K(s) = 2^{r_1}(2\pi)^{r_2}\frac{hR}{w\sqrt{\Delta}}.$$

L'*hypothèse de Riemann généralisée* dit encore que les zéros de ζ_K dans la bande critique sont sur la droite critique.

Les fonctions L associées à un caractère de Dirichlet ont aussi des généralisations : on définit des fonctions L (Artin) attachées à une extension Galoisienne K/k de corps de nombres et à un caractère du groupe de Galois. Dans le cas d'une extension cyclotomique de $\mathbf{Q}$ on retombe sur les fonctions L précédentes.

On introduit aussi des fonctions ζ et L attachées à d'autres objets géométriques, notamment
• les courbes elliptiques (Hasse Weil), ce qui donne lieu à la Conjecture de Birch et Swinnerton-Dyer (voir par exemple [Co] Conjecture 7.3.9),
• les formes modulaires,
• les représentations automorphes (programme de Langlands, théorie du corps de classes non abélien).

Ce ne sont que les premiers exemples : les fonctions zêta et L jouent un rôle important dans de multiples domaines, aussi bien en géométrie diophantienne (fonction zêta de Hasse–Weil attachée à une variété) que dans l'étude des systèmes dynamiques.

Références

[Ca] Pierre Cartier, An introduction to Zeta functions, *From number theory to physics*,Springer-Verlag, Berlin, (1992), Chap. I p. 1–63.

[Co] Henri Cohen, A course in computatioonal algebraic number theory, Graduate Textes in Math. **138** (1993).