Université P. et M. Curie (Paris VI), Michel Waldschmidt
Deuxième semestre 2007/2008 date de mise à jour: 10/06/2008

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

UE : Théorie des nombres 12 ects code UE : MMAT4020 code Scolar : MM020

Objectifs et descriptions

Ce cours vise à donner les bases de l'arithmétique, de la théorie algébrique des nombres et de la théorie analytique des nombres. Il est aussi utile en cryptographie et en théorie des codes.

Prérequis

Des connaissances en algèbre et analyse complexe du niveau licence.

Contenu :

Arithmétique : factorisation, équations diophantiennes, fractions continues, approximation diophantienne, irrationalité et transcendance.

Extensions algébriques, corps de rupture et corps de décomposition, clôture algébrique, extentions normales et séparables, polynômes cyclotomiques.

Corps finis (structure, construction, décomposition des polynômes cyclotomiques, loi de réciprocité quadratique , théorie de Galois).

Corps de nombres, normes, trace, discriminant ; entier algébriques, unités et idéaux d'un corps de nombres, décomposition des idéaux premiers dans une extension.

Théorie analytique des nombres, fonction zéta de Riemann et théorème des nombres premiers, fonctions L de Dirichlet et théorème de la progression de Dirichlet.

Premier fascicule: 07/01/2008 – Introduction [1]

Introduction

0.1 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

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

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

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 $X = {}^t(x_1, \ldots, x_n)$ 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 [4], § 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 ($\sim$1340–$\sim$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 verrons dans ce cours 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).

0.2 Quelques problèmes ouverts en théorie des nombres

Un des attraits de la théorie des nombres réside dans le contraste entre la simplicité de certains énoncés et leur profondeur. En particulier de nombreux problèmes ouverts sont faciles à énoncer. Nous en donnons un échantillon, les exemples ne manquent pas. On pourra consulter notamment [3] et [4] pour en savoir plus.

Conjecture de Pillai - `voir ci-dessus`

La conjecture de Catalan, datant de 1844, a été résolue en 2003 : *les seules puissances parfaites (c'est-à-dire de la forme a^b avec a et b entiers ≥ 2) qui soient consécutives sont $8 = 2^3$ et $9 = 3^2$.* En 1945 S.S. Pillai a posé un problème plus difficile : *étant donné un entier $k \geq 1$, montrer qu'il n'y a qu'un nombre fini d'entiers x, y, m et n, tous ≥ 2, tels que*

$$x^m - y^n = k.$$

Seul le cas $k = 1$ est résolu.

Conjecture de Beal

Considérons l'équation diophantienne

$$x^p + y^q = z^r$$

en entiers x, y, z, p, q, r, tous positifs, avec les conditions supplémentaires que x, y, z sont premiers entre eux et que p, q, r satisfont

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1.$$

On connaît dix solutions :

$$1 + 2^3 = 3^2, \qquad 2^5 + 7^2 = 3^4, \qquad 7^3 + 13^2 = 2^9, \qquad 2^7 + 17^3 = 71^2,$$
$$3^5 + 11^4 = 122^2, \qquad 17^7 + 76271^3 = 21063928^2, \qquad 1414^3 + 2213459^2 = 65^7,$$
$$9262^3 + 15312283^2 = 113^7, \qquad 43^8 + 96222^3 = 30042907^2, \qquad 33^8 + 1549034^2 = 15613^3.$$

On conjecture qu'*il n'y en a pas d'autres* que celles qu'on déduit trivialement de celles-ci par symétries.

Conjecture *abc*

On désigne par $R(n)$ le *radical* ou *partie sans facteurs carrés* d'un entier positif n : si $n = p_1^{a_1} \cdots p_s^{a_s}$ avec des nombres premiers p_i deux-à-deux distincts et des exposants a_i tous ≥ 1, alors $R(n) = p_1 \cdots p_s$. Une forme faible de la conjecture *abc* est qu'il existe une constante absolue ϑ telle que, pour tout triplet (a, b, c) d'entiers positifs premiers entre eux satisfaisant $a + b = c$, on a $c < R(abc)^\vartheta$. Une telle inégalité aurait beaucoup de conséquences. Une forme plus précise énonce que *pour tout $\epsilon > 0$, il existe une constante $\kappa(\epsilon) > 0$ telle que, pour tout triplet (a, b, c) d'entiers positifs premiers entre eux satisfaisant $a + b = c$, on ait*

$$c < \kappa(\epsilon) R(abc)^{1+\epsilon}.$$

Problème de Waring

Soit $k \geq 2$ un entier rationnel. On définit $g(k)$ comme le plus petit des entiers $g \geq 1$ tels que tout entier positif soit somme d'au plus g puissances k-ièmes. Par exemple $g(4) \geq 19$ car pour écrire le nombre 79 comme somme de puissances 4-ièmes (bicarrés) il faut au moins 19 termes (le plus économique est d'ajouter 4 fois 2^4 et 15 fois 1).

Divisons 3^k par 2^k, ce qui veut dire qu'on écrit $3^k = 2^k q + r$ avec $0 < r < 2^k$. Ainsi $q = [(3/2)^k]$ (où $[\cdot]$ désigne la partie entière). Le nombre $I(k) = 2^k + q - 2$ est appelé *constante de Waring idéale*. L'écriture de $2^k q - 1$ comme somme de puissances k-ième nécessite au moins $I(k)$ termes, à savoir $q - 1$ termes 2^k et $2^k - 1$ termes 1, donc $g(k) \geq I(k)$. L'égalité est vérifiée pour de nombreuses valeurs de k (notamment toutes les valeurs de k "suffisamment grandes" ainsi que pour $2 \leq k \leq 4,716 \cdot 10^8$), mais on ne sait pas démontrer qu'elle est vraie pour tout $k \geq 2$.

Nombres parfaits

Un nombre parfait est un entier positif qui est égal à la moitié de la somme de ses diviseurs. Par exemple 6 a pour diviseurs 1, 2, 3, et 6, dont la somme est 12. De même 28 a pour diviseurs 1, 2, 4, 7, 14 et 28, la somme étant 56. Il est assez facile de démontrer qu'un nombre pair est parfait si et seulement s'il s'écrit $2^{p-1}M_p$, avec p premier tel que le nombre de Mersenne $M_p = 2^p - 1$ soit également premier. La principale question ouverte concerne l'*existence de nombre parfaits impairs.* On n'en connaît pas et on serait surpris qu'il en existe !

Nombres premiers de Mersenne et de Fermat

Une autre question ouverte sur les nombres parfaits consiste à savoir s'il y en a une infinité. On soupçonne que la réponse est positive, et plus précisément qu'*il existe une infinité de nombres premiers p tels que le nombre de Mersenne $M_p = 2^p - 1$ soit également premier.* Mais on ne sait pas non plus démontrer qu'*il existe une infinité de p tels que le nombre $M_p = 2^p - 1$ ne soit pas premier.*

Dans le même ordre d'idée il est facile de voir qu'un entier de la forme $2^m + 1$ ne peut être premier que si m est une puissance de 2. Un nombre premier de la forme $F_n = 2^{2^n} + 1$ est appelé nombre premier de Fermat. On ne sait pas s'il y en a une infinité, on soupçonne que non, mais on ne sait même pas démontrer qu'*il y a une infinité de n tels que le nombre $2^{2^n} + 1$ ne soit pas premier.*

Nombres premiers jumeaux

Y a-t-il une infinité de nombres premiers p tels que $p + 2$ soit aussi premier ?

Hypothèse H de Schinzel

Y a-t-il une infinité de nombres premiers de la forme $n^2 + 1$? Plus généralement A. Schinzel a formulé une hypothèse qui répond aux questions analogues que l'on peut se poser sur la représentation d'une infinité de nombre premiers par des polynômes.

Conjecture de Goldbach

Goldbach a conjecturé que *tout entier pair ≥ 6 est somme de deux nombres premiers impairs* et que *tout entier impair ≥ 9 est somme de trois nombres premiers impairs.*

Sur le petit théorème de Fermat

Si p est un nombre premier alors $2^{p-1} \equiv 1 \pmod{p}$. On connaît deux nombres premiers tels que $2^{p-1} \equiv 1(\pmod{p})^2$, ce sont 1 093 et 3 511. On ignore s'il y en a d'autres, on ignore s'il y en a une infinité, mais on ne sait pas non plus démontrer qu'il y a une infinité de p qui ne satisfont pas cette congruence.

Conjecture d'Artin

Y a-t-il une infinité de p premiers tels que la classe de 2 modulo p soit un générateur du groupe cycle $(\mathbf{Z}/p\mathbf{Z})^\times$? Le même problème se pose si on remplace 2 par un nombre entier rationnel qui n'est pas un carré et qui n'est pas -1.

Spectre de Markoff

L'équation $x^2 + y^2 + z^2 = 3xyz$ en nombre entiers positifs possède une infinité de solutions, et il est facile de donner un algorithme qui les fournit toutes. Mais la question suivante est actuellement l'objet de travaux en cours : *si z est un entier ≥ 3 tel qu'il existe x et y avec $x < y < z$ et (x, y, z) solution de l'équation de Markoff, alors le couple (x, y) est unique.*

Problèmes d'irrationalité et de transcendance

On ignore la nature arithmétique (déterminer si le nombre donné est rationnel, ou bien irrationnel algébrique, ou bien transcendant) de la plupart des constantes de l'analyse. Il serait plus rapide de donner la liste de celles pour lesquelles on connaît la réponse. Parmi les principaux défis citons la constante d'Euler, celle de Catalan, la valeur aux points entiers impairs ≥ 5 de la fonction zêta de Riemann, la valeur au point $1/5$ de la fonction Gamma d'Euler. Une des principales conjectures du sujet est due à Schanuel : *si $x_1, \ldots, x_n$ sont des nombres complexes linéairement indépendants sur le corps des nombres rationnels, alors parmi les nombres $x_1, \ldots, x_n, e^{x_1}, \ldots, e^{x_n}$ il y en a au moins n qui sont algébriquement indépendants.*

Problèmes d'approximation diophantienne

On ne connaît aucun exemple explicite de triplet (α, g, c) formé d'un nombre algébrique réel irrationnel $\alpha \in (0,1)$, d'un entier $g \geq 3$ et d'un *chiffre* $c \in \{0, 1, \ldots, g-1\}$ pour lequel on puisse affirmer que le chiffre c intervient une infinité de fois dans le développement en base g de α :

$$\alpha = c_1 g^{-1} + c_2 g^{-2} + \cdots + c_n g^{-n} + \cdots$$

avec $0 \leq c_i \leq g-1$. E. Borel a conjecturé en 1950 que la suite $(c_1, c_2, \ldots)$ de ces chiffres devrait se comporter comme une suite *aléatoire*, au sens où toute suite donnée de chiffres devrait apparaître une infinité de fois.

Dans le même ordre d'idées, on ne sait pas s'il existe un nombre algébrique réel α de degré ≥ 3 pour lequel la suite des *réduites* successives $(a_0, a_1, \ldots, a_n, \ldots)$ dans le développement en fractions continues

$$\alpha = a_0 + \frac{1}{|a_1+} \; \frac{1}{|a_2+} \; \cdots \; \frac{1}{|a_n+} \; \cdots$$

est bornée. Et on ne sait pas non plus s'il en existe un pour lequel cette suite ne soit pas bornée. Le sentiment le plus généralement partagé est que cette suite n'est jamais bornée.

D'autres problèmes de théorie des nombres demandent un peu plus de connaissances pour pouvoir comprendre leurs énoncés. En voici quelques uns.

Hypothèse de Riemann

La fonction

$$\zeta(s) = \sum_{n \geq 1} n^{-s}$$

est bien définie par cette série de Dirichlet dans le demi–plan où la partie réelle $\Re e(s)$ de s est > 1. Elle a été étudiée par Euler pour les valeurs de s entières (Euler ne se limitait pas aux valeurs ≥ 2, il étudiait aussi les valeurs négatives) et par Riemann pour les valeurs complexes. Elle se prolonge en une fonction méromorphe dans le plan complexe, avec un unique pôle au point $s = 1$. Dans le demi–plan $\Re e(s) \leq 0$, cette fonction prolongée s'annule exactement aux entiers négatifs pairs (ce sont les *zéros triviaux*). L'hypothèse de Riemann est que *les zéros de la fonction zêta dans la bande critique $0 < \Re e(s) < 1$ sont tous situés sur la droite critique $\Re e(s) = 1/2$.*

Nombre de classes 1

Existe-t-il une infinité de corps de nombres ayant un nombre de classes 1 *?* Les tables numériques semblent indiquer que cela devrait être vrai même si on se limite aux corps quadratiques réels.

Problème inverse de la théorie de Galois

Peut-on réaliser tout groupe fini comme groupe de Galois sur $\mathbf{Q}$ *d'un corps de nombres (= extension finie de* $\mathbf{Q}$*) ?*

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] G.H. Hardy & E.M. Wright – *An introduction to the theory of numbers*, Oxford University Press, 1938. Fifth Ed. 1979.

[4] W. Narkiewicz – *Classical problems in number theory*, PWN – Polish Scientific Publishers, Warszàwa, 1986.

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

De nombreux documents sont disponibles sur internet. Voir notamment la liste 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 2007/2008

Michel Waldschmidt
date de mise à jour: 10/06/2008

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

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

Deuxième fascicule : 21/01/2008

1 Approximation diophantienne, irrationalité et transcendance

1.1 Nombres : rationnels, irrationnels

Les *nombres* que nous allons étudier sont les nombres complexes. Leur construction se fait en plusieurs étapes : partant des entiers naturels $\mathbf{N} = \{0, 1, 2, 3, \cdots\}$, on construit l'*anneau des entiers rationnels* $\mathbf{Z} = \{0, \pm 1, \pm 2, \ldots\}$ de façon à ce que chaque élément ait un inverse pour l'addition, puis le *corps des nombres rationnels* $\mathbf{Q} = \{a/b\ ;\ a \in \mathbf{Z},\ b \in \mathbf{Z}_{>0}\}$ de telle sorte que chaque élément non nul ait un inverse pour la multiplication. Chaque nombre rationnel a une unique représentation p/q avec $p \in \mathbf{Z}$ et $q \in \mathbf{Z}_{>0}$ sans facteur commun : $\mathrm{pgcd}(p, q) = 1$.

L'étape suivante est la construction des *nombres réels* : alors que les constructions précédentes étaient de nature algébrique, celle de $\mathbf{R}$ fait intervenir la notion topologique de limite : $\mathbf{R}$ *est le complété de* $\mathbf{Q}$ pour la topologie usuelle sur les rationnels. La dernière étape, la construction de $\mathbf{C}$ à partir de $\mathbf{R}$, est de nouveau de nature algébrique : $\mathbf{C}$ *est la clôture algébrique de* $\mathbf{Q}$, tout polynôme non constant admet au moins une racine complexe.

Un *nombre irrationnel* est un nombre qui n'est pas dans $\mathbf{Q}$. L'ensemble de ces nombres ne jouit pas de bonnes propriétés algébriques : la somme de nombres irrationnels peut être rationnelle ou irrationnelle, le produit de deux nombres irrationnels peut être rationnel ou irrationnel. En revanche la somme d'un nombre rationnel et d'un nombre irrationnel est un nombre irrationnel ; le produit d'un nombre rationnel *non nul* et d'un nombre irrationnel est un nombre irrationnel. La racine carrée (et plus généralement la racine k-ième, pour $k \geq 1$) d'un nombre irrationnel est un nombre irrationnel. Mais le carré d'un nombre irrationnel peut être rationnel ou irrationnel.

Le fait que $\mathbf{R}$ contienne strictement $\mathbf{Q}$ est bien connu : il existe des nombres irrationnels. Un des exemples les plus anciens est celui de $\sqrt{2}$. La démonstration la plus connue se fait par l'absurde : si p/q est un nombre rationnel dont le carré est 2 avec $\mathrm{pgcd}(p, q) = 1$, la relation $p^2 = 2q^2$ implique que p est pair, disons $p = 2a$, puis en simplifiant par 2 la relation $2a^2 = q^2$ montre que q est pair, ce qui est une contradiction.

Une démonstration géométrique se fait de la façon suivante : considérons un rectangle dont les côtés sont $1 + \sqrt{2}$ et 1. Comme le grand côté $1 + \sqrt{2}$ est dans l'intervalle $(2, 3)$, on peut décomposer ce premier rectangle en deux carrés de côté 1 plus un petit rectangle dont le grand côté est 1, et le petit côté $\sqrt{2} - 1$. On remarque alors que les proportions de ce second rectangle sont les mêmes que celles du rectangle initial :

$$\frac{1}{\sqrt{2} - 1} = 1 + \sqrt{2}.$$

par conséquent si on répète cette construction à partir du second carré, on obtiendra de nouveau deux carrés de côtés $\sqrt{2}-1$ et un troisième rectangle dont la proportion des longueurs des côtés sera toujours la même. Par conséquent le processus ne s'arrête pas.

En revanche si on part d'un rectangle dont les côtés sont entiers, la construction précédente va produire des rectangles de plus en plus petits dont les côtés sont toujours des entiers, donc le processus s'arrêtera au bout d'un temps fini (il ne reste plus de petit rectangle). Il en est de même pour tout rectangle dont les proportions sont rationnelles : si le rapport du grand côté par le petit côté est a/b avec $b>0$, on prend comme unité de mesure celle qui donne au petit côté la longueur b, et alors les deux côtés ont des longueurs entières.

Cette démonstration fait intervenir le *développement en fraction continue* d'un nombre réel x. On écrit

$$x=[x]+\{x\} \quad \text{avec } [x]\in\mathbf{Z} \text{ et } 0\leq\{x\}<1.$$

Si x n'est pas entier, alors $\{x\}>0$ et le nombre $x_1=1/\{x\}$ est >1. Posons $a_0=[x]$, $a_1=[x_1]$. Par exemple quand x est >0 le nombre a_0 est le nombre maximal de carrés de côtés 1 que l'on peut disposer côte–à–côte dans un rectangle de côtés 1 et x, tandis que a_1 est le nombre maximal de carrés de côtés $\{x\}$ dans le second rectangle qui reste. Par récurrence on définit une suite $(x_n)_{n\geq 1}$ de nombres réels >1 et une suite $(a_n)_{n\geq 1}$ de nombres entiers ≥ 1 (éventuellement finies) de la façon suivante : si x_{n-1} n'est pas entier, on pose $x_n=1/\{x_{n-1}\}$ et $a_n=[x_n]$, ce qui donne

$$x=a_0+\frac{1}{x_1},\quad x_1=a_1+\frac{1}{x_2},\quad \cdots,\quad x_n=a_n+\frac{1}{x_{n+1}}\cdots$$

On peut donc écrire

$$x=a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\{x_2\}}}=a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{\ddots\;\cfrac{}{a_{n-1}+\cfrac{1}{a_n+\{x_n\}}}}}}$$

avec $0\leq\{x_n\}<1$. La construction s'arrête au premier pas si x est entier : on obtient seulement $x=a_0$. Si x n'est pas entier mais si x_n est entier pour un entier $n\geq 1$ alors $a_n=x_n$ et $\{x_n\}=0$. Noter que la condition $x_n>1$ entraîne $a_n\geq 2$. Il est clair que si la construction s'arrête, alors x est rationnel. Inversement, si x est rationnel l'argument géométrique avec les rectangles montre que la construction s'arrêtera au bout d'un nombre fini d'étapes. Un nombre rationnel admet deux représentations sous forme d'une telle fraction, l'une dont le dernier terme a_n est ≥ 2, l'autre avec un terme de plus et $a_{n+1}=1$: en effet on peut écrire un entier $a\geq 2$ sous la forme $(a-1)+(1/1)$.

On montre [2] que tout nombre réel irrationnel x admet une unique représentation sous forme d'une fraction continue infinie

$$x=a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{\ddots\;\cfrac{}{a_{n-1}+\cfrac{1}{a_n+\cfrac{1}{\ddots}}}}}} \tag{1.1}$$

avec des coefficients a_n entiers rationnels satisfaisant $a_n \geq 1$ pour $n \geq 1$, et inversement pour toute suite $(a_n)_{n\geq 0}$ d'entiers rationnels avec $a_n \geq 1$ pour $n \geq 1$, la fraction continue (1.1) définit un nombre réel irrationnel.

Pour simplifier l'écriture on écrit cette fraction continue sous l'une des formes suivante :

$$x = [a_0; a_1, a_1, a_2, \dots, a_n, \dots] \quad \text{ou} \quad x = a_0 + \frac{1}{|a_1+} \; \frac{1}{|a_2+} \; \cdots \; \frac{1}{|a_n+} \; \cdots$$

Un exemple, dû à Euler, est le développement en fraction continue du nombre e :

$$e = [2;\, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \dots] = 2 + \frac{1}{|1+} \; \frac{1}{|2+} \; \frac{1}{|1+} \; \frac{1}{|1+} \; \frac{1}{|4+} \; \frac{1}{|1+} \; \frac{1}{|1+} \; \frac{1}{|6+} \; \frac{1}{|1+} \; \cdots$$

Voici une démonstration de l'irrationalité du nombre e est due à Fourier (cours à l'école Polytechnique, 1815).

Proposition 1.2. *Le nombre*

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots + \frac{1}{n!} + \cdots$$

est irrationnel.

Démonstration. Soit N un entier positif. On tronque la série définissant e. Soit N un entier positif. On a

$$N!\, e - \sum_{n=0}^{N} \frac{N!}{n!} = \sum_{k\geq 1} \frac{N!}{(N+k)!}. \tag{1.3}$$

Le membre de droite de (1.3) est une somme de nombres positifs, donc n'est pas nul. De la minoration du coefficient binomial

$$\frac{(N+k)!}{N!k!} \geq N+1 \quad \text{pour } k \geq 1,$$

on déduit

$$\sum_{k\geq 1} \frac{N!}{(N+k)!} \leq \frac{1}{N+1} \sum_{k\geq 1} \frac{1}{k!} = \frac{e-1}{N+1}.$$

Par conséquent le membre de droite de (1.3) tend vers 0 quand N tend vers l'infini. Dans le membre de gauche, $N!$ et $\sum_{n=0}^{N} N!/n!$ sont des entiers. Il en résulte que $N!e$ n'est jamais un entier, donc e est un nombre irrationnel.

□

Exercice. a) En adaptant cet argument, montrer que le nombre e n'est pas racine d'un polynôme de degré 2 à coefficients rationnels.
`Indication` : un nombre quadratique x est racine d'une équation $ax + b + cx^{-1} = 0$ avec a, b, c entiers rationnels non tous nuls.
Référence : J. Liouville – *Sur l'irrationalité du nombre* $e = 2,718\dots$, J. Math. Pures Appl. (1) **5** (1840), p. 192.
b) Montrer que le nombre $e^{\sqrt{2}}$ est irrationnel.

`Indication` : Montrer plus précisément que $e^{\sqrt{2}} + e^{\sqrt{-2}}$ est irrationnel. On pourra vérifier que les nombres $(2N)!/2^{N-m}(2m)!$ $(0 \leq m \leq N)$ sont entiers.
c) Montrer que e^2 n'est pas racine d'un polynôme de degré 2 à coefficients rationnels.
`Indication` : On pourra montrer que les nombres

$$\frac{N!}{2^{N-n-1}n!}, \quad (0 \leq n \leq N)$$

sont entiers pour une infinité de N.
Référence : J. Liouville – *Addition à la note sur l'irrationalité du nombre e*, J. Math. Pures Appl. (1) **5** (1840), p. 193–194.
d) Montrer que le nombre $e^{\sqrt{3}}$ est irrationnel.
e) Soit $(a_n)_{n\geq 0}$ une suite bornée de nombres entiers. Montrer que les conditions suivantes sont équivalentes :
(i) Il existe $N_0 > 0$ tel que $a_n = 0$ pour tout $n \geq N_0$.
(ii) Le nombre

$$\vartheta_1 = \sum_{n\geq 0} \frac{a_n}{n!}$$

est rationnel
(iii) Le nombre

$$\vartheta_2 = \sum_{n\geq 0} \frac{a_n 2^n}{n!}$$

est rationnel.

1.2 Critère d'irrationalité

La démonstration d'irrationalité de Fourier que nous venons de donner utilise le fait qu'un nombre rationnel ne possède pas de bonne approximation rationnelle autre que lui-même. En effet, si ϑ est rationnel, on l'écrit a/b avec $b > 0$ et alors, pour tout $p/q \in \mathbf{Q}$ distinct de a/b, on a

$$\left|\vartheta - \frac{p}{q}\right| \geq \frac{1}{bq},$$

comme on le voit en utilisant, pour l'entier $aq - bp$, la propriété qui est à la base de tout argument diophantien : *si m est un entier non nul, alors $|m| \geq 1$.*

Inversement, le lemme suivant montre que, si un nombre est irrationnel, alors il admet de bonnes approximations rationnelles.

Lemme 1.4. *Soit ϑ un nombre réel. Les conditions suivantes sont équivalentes.*
(i) *ϑ est irrationnel.*
(ii) *Pour tout $\epsilon > 0$, il existe $p/q \in \mathbf{Q}$ tel que*

$$0 < \left|\vartheta - \frac{p}{q}\right| < \frac{\epsilon}{q}.$$

(iii) *Pour tout nombre réel $Q > 1$, il existe un entier q dans l'intervalle $1 \leq q < Q$ et un entier rationnel p tel que*

$$0 < \left|\vartheta - \frac{p}{q}\right| < \frac{1}{qQ}.$$

(iv) *Il existe une infinité de* $p/q \in \mathbf{Q}$ *tels que*

$$0 < \left|\vartheta - \frac{p}{q}\right| < \frac{1}{q^2}.$$

Démonstration. Les implications (iii)⇒(iv)⇒(ii)⇒(i) du lemme 1.4 sont faciles. Il ne reste qu'à démontrer (i)⇒(iii), qui est un théorème de Dirichlet. Pour l'établir nous allons utiliser le principe des tiroirs.

Soit Q un nombre réel > 1. On pose $N = \lceil Q \rceil$: autrement dit N est l'entier déterminé par $N - 1 < Q \leq N$. Comme $Q > 1$, on a $N \geq 2$.

Soit $\vartheta \in \mathbf{R} \setminus \mathbf{Q}$. On considère le sous-ensemble E de l'intervalle unité $[0, 1]$ constitué des $N + 1$ éléments

$$0,\ \{\vartheta\},\ \{2\vartheta\},\ \{3\vartheta\},\ \ldots, \{(N-1)\vartheta\},\ 1.$$

Comme ϑ est irrationnel, ces $N + 1$ éléments sont deux-à-deux distincts. On découpe l'intervalle $[0, 1]$ en N intervalles

$$I_j = \left[\frac{j}{N}\,,\, \frac{j+1}{N}\right] \quad (0 \leq j \leq N-1).$$

D'après le principe des tiroirs de Dirichlet, un au moins de ces N intervalles, disons I_{j_0}, contient au moins deux éléments de E. À part 0 et 1, les éléments $\{q\vartheta\}$ de E avec $1 \leq q \leq N-1$ sont irrationnels, donc appartiennent à la réunion des intervalles *ouverts* $(j/N,\ (j+1)/N)$ avec $0 \leq j \leq N-1$.

Si $j_0 = N - 1$, alors l'intervalle

$$I_{j_0} = I_{N-1} = \left[1 - \frac{1}{N}\ ;\ 1\right]$$

contient 1 ainsi qu'un autre élément de E de la forme $\{q\vartheta\}$avec $1 \leq q \leq N-1$. On pose $p = [q\vartheta]+1$. Alors on a $1 \leq q \leq N - 1 < Q$ et

$$p - q\vartheta = [q\vartheta] + 1 - [q\vartheta] - \{q\vartheta\} = 1 - \{q\vartheta\}, \quad \text{donc} \quad 0 < p - q\vartheta < \frac{1}{N} \leq \frac{1}{Q}.$$

Sinon on a $0 \leq j_0 \leq N-2$ et I_{j_0} contient deux éléments $\{q_1\vartheta\}$ and $\{q_2\vartheta\}$ avec $0 \leq q_1 < q_2 \leq N-1$. On pose

$$q = q_2 - q_1, \quad p = [q_2\vartheta] - [q_1\vartheta].$$

Ainsi on a $0 < q = q_2 - q_1 \leq N - 1 < Q$ et

$$|q\vartheta - p| = |\{q_2\vartheta\} - \{q_1\vartheta\}| < 1/N \leq 1/Q.$$

□

Exercice. Soient $\vartheta_1, \ldots, \vartheta_m$ des nombres réels. Les propriétés suivantes sont équivalentes.
(i) Un au moins des nombres $\vartheta_1, \ldots, \vartheta_m$ est irrationel.
(ii) Pour tout $\epsilon > 0$, il existe $p_1, \ldots, p_m, q$ dans $\mathbf{Z}$ avec $q > 0$ tel que

$$0 < \max_{1 \leq i \leq m} \left|\vartheta_i - \frac{p_i}{q}\right| < \frac{\epsilon}{q}.$$

(iii) Pour tout entier $Q > 1$, il existe $p_1, \dots, p_m, q$ dans $\mathbf{Z}$ tel que $1 \le q \le Q^m$ et

$$0 < \max_{1 \le i \le m} \left| \vartheta_i - \frac{p_i}{q} \right| \le \frac{1}{qQ}.$$

(iv) L'ensemble des $q \in \mathbf{Z}$, $q > 0$, pour lesquels il existe $p_1, \dots, p_m$ dans $\mathbf{Z}$ satisfaisant

$$0 < \max_{1 \le i \le m} \left| \vartheta_i - \frac{p_i}{q} \right| < \frac{1}{q^{1+1/m}},$$

est infini.

`Indication.` Pour la démonstration de (i)⇒(iii), on pourra utiliser le principe des tiroirs de Dirichlet : considérer les $Q^m + 1$ éléments

$$\xi_q = \big(\{q\vartheta_1\}, \dots, \{q\vartheta_m\}\big) \quad (q = 0, 1, \dots, Q^m)$$

dans le cube unité $[0,1)^m$ de $\mathbf{R}^m$ et découper ce cube unité en Q^m cubes dont les côtés ont pour longueur $1/Q$.

Il y a d'autres démonstrations de (i)⇒(iii). Par exemple on peut utiliser un théorème de Minkowski en géométrie des nombres ; cela permet de démontrer des variantes du lemme 1.4. En particulier en dimension supérieure le principe des tiroirs donne des énoncés moins précis que la géométrie des nombres.

Une autre variante de la démonstration du théorème de Dirichlet (implication (i)⇒(iii) du lemme 1.4) repose sur les suites de Farey : la *suite de Farey d'indice n* est constituée par la suite croissante des nombres rationnels de l'intervalle unité dont le dénominateur est $\le n$. Par exemple la suite de Farey d'indice 6 est

$$0,\ \frac{1}{6},\ \frac{1}{5},\ \frac{1}{4},\ \frac{1}{3},\ \frac{2}{5},\ \frac{1}{2},\ \frac{3}{5},\ \frac{2}{3},\ \frac{3}{4},\ \frac{4}{5},\ \frac{5}{6},\ 1.$$

On peut montrer (cf [5], Ch. I § 2, Th. 2.A) que deux fractions consécutives $p/q < r/s$ d'une suite de Farey satisfont $qr - ps = 1$. Il en résulte que si

$$\frac{p}{q} < \frac{u}{v} < \frac{r}{s}$$

sont trois fractions consécutives d'une suite de Farey, alors

$$\frac{u}{v} = \frac{p+r}{q+s}.$$

Cela résulte des relations $qu - pv = 1$ et $vr - us = 1$.

L'implication (i)⇒(iv) du lemme 1.4 peut être améliorée :

Lemme 1.5 (Hurwitz)**.** *Soit ϑ un nombre réel. Les propriétés suivantes sont équivalentes.*
(i) *ϑ est irrationnel.*
(ii) *Il existe une infinité de $p/q \in \mathbf{Q}$ satisfaisant*

$$0 < \left| \vartheta - \frac{p}{q} \right| < \frac{1}{\sqrt{5}q^2}.$$

Évidemment l'implication (ii)⇒(i) du lemme 1.5 est une forme affaiblie de l'implication (iv)⇒(i) du lemme 1.4. Ce qui est nouveau est la réciproque.

Les démonstrations classiques de l'équivalence entre les assertions (i) et (ii) du lemme 1.5 font intervenir soit les fractions continues, soit les suites de Farey. Même si les fractions continues n'interviennent pas explicitement dans la démonstration qui suit, elles sont sous-jacentes.

Lemme 1.6. *Soit ϑ un nombre réel irrationnel. Il existe une infinité de couples $(p/q, r/s)$ de fractions rationnelles irréductibles telles que*

$$\frac{p}{q} < \vartheta < \frac{r}{s} \quad \text{et} \quad qr - ps = 1.$$

Dans cet énoncé et les deux suivants, il suffit de démontrer les inégalités larges $\leq$ à la place des inégalités strictes $<$ grâce à l'hypothèse que ϑ est irrationnel.

Démonstration. Soit H un entier positif. Parmi les fractions rationnelles irréductibles a/b avec $1 \leq b \leq H$, on en choisit une pour laquelle $|\vartheta - a/b|$ est minimal. Si $a/b < \vartheta$ on appelle p/q cette fraction a/b, tandis que si $a/b > \vartheta$, alors on l'appelle r/s.

Commençons par le cas où $a/b < \vartheta$, donc $a/b = p/q$. Comme $\mathrm{pgcd}(p, q) = 1$, l'algorithme d'Euclide (théorème de Bézout) montre qu'il existe $(r, s) \in \mathbf{Z}^2$ tel que $qr - ps = 1$ avec $1 \leq s < q$ et $|r| < |p|$. De $1 \leq s < q \leq H$, en rappelant le choix de a/b, on déduit

$$\left|\vartheta - \frac{p}{q}\right| \leq \left|\vartheta - \frac{r}{s}\right|$$

donc r/s n'est pas dans l'intervalle $[p/q, \vartheta]$. Mais $qr - ps > 0$, donc $p/q < r/s$, par conséquent $\vartheta < r/s$.

Dans le second cas où $a/b > \vartheta$ et $r/s = a/b$ on résout $qr - ps = 1$ par l'algorithme d'Euclide avec $1 \leq q < s$ et $|p| < r$. On conclut de la même manière.

Il reste à montrer qu'on obtient une infinité de tels couples de rationnels. Une fois qu'on dispose d'un ensemble fini de couples $(p/q, r/s)$, on utilise le fait qu'il existe un nombre rationnel m/n qui est plus proche de ϑ que chacune de ces fractions de l'ensemble fini (c'est la densité de $\mathbf{Q}$ dans $\mathbf{R}$). On reprend l'argument précédent avec un entier $H > n$. Cela permet de construire un couple $(p/q, r/s)$ de nombres rationnels qui est différent des précédents, puisque l'une au moins des nouvelles approximations p/q ou r/s est meilleure que les précédentes. Donc cette construction fournit une infinité de couples. □

Lemme 1.7. *Soit ϑ un nombre réel irrationnel. Soient $(p/q, r/s)$ deux fractions irréductibles telles que*

$$\frac{p}{q} < \vartheta < \frac{r}{s} \quad \text{et} \quad qr - ps = 1.$$

Alors

$$\min\left\{q^2\left(\vartheta - \frac{p}{q}\right)\ ,\ s^2\left(\frac{r}{s} - \vartheta\right)\right\} < \frac{1}{2}.$$

Démonstration. Posons

$$\delta = \min\left\{q^2\left(\vartheta - \frac{p}{q}\right)\ ,\ s^2\left(\frac{r}{s} - \vartheta\right)\right\}.$$

En ajoutant les inégalités

$$\frac{\delta}{q^2} \leq \vartheta - \frac{p}{q} \quad \text{et} \quad \frac{\delta}{s^2} \leq \frac{r}{s} - \vartheta$$

et en utilisant $qr - ps = 1$, on déduit que le nombre $t = s/q$ satisfait

$$t + \frac{1}{t} \leq \frac{1}{\delta}.$$

Comme le minimum de la fonction $t \mapsto t + 1/t$ est 2 et comme $t \neq 1$, on en déduit $\delta < 1/2$.

□

Remarque. La minoration $t + (1/t) \geq 2$ pour tout $t > 0$, qui est stricte pour $t \neq 1$, est équivalente à l'inégalité arithmético-géométrique

$$\sqrt{xy} \leq \frac{x+y}{2},$$

pour x et y nombres réels positifs, avec égalité si et seulement si if $x = y$. La correspondance entre les deux énoncés se fait en posant $t = \sqrt{x/y}$.

Des lemmes 1.6 et 1.7 on déduit que pour tout $\vartheta \in \mathbf{R} \setminus \mathbf{Q}$, il existe une infinité de $p/q \in \mathbf{Q}$ satisfaisant

$$0 < \left|\vartheta - \frac{p}{q}\right| < \frac{1}{2q^2}.$$

Il faut encore un pas de plus pour compléter la démonstration du lemme 1.5.

Lemme 1.8. *Soit ϑ un nombre irrationnel. On suppose que $(p/q, r/s)$ sont deux fractions irréductibles telles que*

$$\frac{p}{q} < \vartheta < \frac{r}{s} \quad \textit{et} \quad qr - ps = 1.$$

On pose $u = p + r$ et $v = q + s$. Alors

$$\min\left\{q^2\left(\vartheta - \frac{p}{q}\right)\ ,\ s^2\left(\frac{r}{s} - \vartheta\right)\ ,\ v^2\left|\vartheta - \frac{u}{v}\right|\right\} < \frac{1}{\sqrt{5}}.$$

Démonstration. Notons déjà que $qu - pv = 1$ et $rv - su = 1$. Donc

$$\frac{p}{q} < \frac{u}{v} < \frac{r}{s}.$$

On répète la démonstration du lemme 1.7 ; on distingue deux cas selon que u/v est supérieur ou inférieur à ϑ. Comme les deux cas se traitent de la même manière, supposons $\vartheta < u/v$. La démonstration du lemme 1.7 montre que

$$\frac{s}{q} + \frac{q}{s} \leq \frac{1}{\delta} \quad \text{et} \quad \frac{v}{q} + \frac{q}{v} \leq \frac{1}{\delta}.$$

Donc chacun des quatre nombres s/q, q/s, v/q, q/v satisfait $t + 1/t \leq 1/\delta$. La fonction $t \mapsto t + 1/t$ est décroissante sur l'intervalle $(0, 1)$ et croissante sur l'intervalle $(1, +\infty)$. Il en résulte que nos quatre nombres sont dans l'intervalle $(1/x, x)$, où x est la racine > 1 de l'équation $x + 1/x = 1/\delta$.

Les deux racines x et $1/x$ du polynôme quadratique $X^2 - (1/\delta)X + 1$ ont pour distance la racine carrée du discriminant $\Delta = (1/\delta)^2 - 4$ de ce polynôme. Comme

$$\frac{v}{q} - \frac{s}{q} = 1,$$

il en résulte que la longueur $\sqrt{\Delta}$ de l'intervalle $(1/x, x)$ est ≥ 1. Par conséquent $\Delta \geq 1$ et $\delta \leq 1/\sqrt{5}$. Ceci termine la démonstration du lemme 1.8. □

Montrons que le lemme 1.5 est optimal. Désignons par $\Phi = 1.6180339887499\ldots$ le nombre d'or, qui est la racine > 1 du polynôme $X^2 - X - 1$. Le discriminant de ce polynôme est 5.

Lemme 1.9. *Pour tout $q \geq 1$ et tout $p \in \mathbf{Z}$,*

$$\left|\Phi - \frac{p}{q}\right| > \frac{1}{\sqrt{5}q^2 + (q/2)}.$$

Démonstration. Il suffit d'établir la minoration quand p est l'entier le plus proche de $q\Phi$. On factorise le polynôme $X^2 - X - 1 = (X - \Phi)(X + \Phi^{-1})$. Ainsi

$$p^2 - pq - q^2 = q^2 \left(\frac{p}{q} - \Phi\right)\left(\frac{p}{q} + \Phi^{-1}\right).$$

Le membre de gauche est un entier rationnel non nul, sa valeur absolue est donc au moins 1. Majorons maintenant la valeur absolue du membre de droite. Comme $p < q\Phi + (1/2)$ et $\Phi + \Phi^{-1} = \sqrt{5}$ on a

$$\frac{p}{q} + \Phi^{-1} \leq \sqrt{5} + \frac{1}{2q}.$$

Donc

$$1 \leq q^2 \left|\frac{p}{q} - \Phi\right| \left(\sqrt{5} + \frac{1}{2q}\right).$$

Le lemme 1.9 en résulte.

□

Pour le nombre d'or on peut exhiber la suite des meilleures approximations rationnelles. Pour cela on considère la suite de Fibonacci $(F_n)_{n\geq 0}$ définie par :

$$F_0 = 0,\ F_1 = 1,\ F_n = F_{n-1} + F_{n-2} \quad (n \geq 2).$$

Lemme 1.10. *On a*

$$\lim_{n\to\infty} F_{n-1}^2 \left|\Phi - \frac{F_n}{F_{n-1}}\right| = \frac{1}{\sqrt{5}}.$$

Démonstration. L'espace vectoriel formé par les suites $(v_n)_{n\geq 0}$ qui satisfont $v_n = v_{n-1} + v_{n-2}$ a pour dimension 2, une base étant donnée par les deux suites $(\Phi^n)_{n\geq 0}$ et $((-\Phi^{-1})^n)_{n\geq 0}$. La formule

$$F_n = \frac{1}{\sqrt{5}}(\Phi^n - (-1)^n \Phi^{-n}),$$

due à A. De Moivre (1730), L. Euler (1765) et J.P.M. Binet (1843) en résulte. Par conséquent F_n est l'entier le plus proche de

$$\frac{1}{\sqrt{5}}\Phi^n,$$

donc la suite $(u_n)_{n\geq 2}$ des quotients consécutifs de nombres de Fibonacci

$$u_n = F_n/F_{n-1}$$

vérifie $\lim_{n\to\infty} u_n = \Phi$.

Par récurrence on vérifie

$$F_n^2 - F_nF_{n-1} - F_{n-1}^2 = (-1)^{n-1}$$

pour $n \geq 1$. Le membre de gauche est $F_{n-1}^2(u_n - \Phi)(u_n + \Phi^{-1})$, comme nous l'avons déjà vu. Donc

$$F_{n-1}^2|\Phi - u_n| = \frac{1}{\Phi^{-1} + u_n},$$

et la limite du membre de droite est $1/(\Phi + \Phi^{-1}) = 1/\sqrt{5}$. Le lemme 1.10 est ainsi démontré. □

Remarque. La suite $u_n = F_n/F_{n-1}$ est aussi définie par

$$u_2 = 2,\ u_n = 1 + \frac{1}{u_{n-1}},\quad (n \geq 3).$$

Donc

$$u_n = 1 + \frac{1}{1 + \dfrac{1}{u_{n-2}}} = 1 + \frac{1}{1 + \dfrac{1}{1 + \dfrac{1}{u_{n-3}}}} = \cdots = 1 + \frac{1\ |}{|1+}\ \frac{1\ |}{|1+}\ \cdots\ + \frac{1\ |}{|1+}\ \frac{1|}{|2}.$$

Partant d'un rectangle de côtés 1 et 2, si on construit par récurrence des rectangles de plus en plus grands en ajoutant au rectangle précédent un carré posé sur le grand côté, la suite des longueurs des côtés de ces carrés est la suite de Fibonacci. C'est la construction inverse de celle qui donne le développement en fraction continue du nombre d'or, consistant à découper un rectangle dont les proportions sont données par le nombre d'or en un carré plus un rectangle plus petit ayant de nouveau le nombre d'or comme proportions.

Exercice. a) Soit $f(X,Y) = aX^2 + bXY + cY^2 \in \mathbf{R}[X,Y]$ un polynôme homogène de degré 2 à coefficients réels de discriminant positif

$$\Delta = b^2 - 4ac > 0.$$

Soit $\epsilon > 0$. Montrer qu'il existe $(x,y) \in \mathbf{Z}^2$ avec $(x,y) \neq (0,0)$ tel que

$$|f(x,y)| \leq \sqrt{\Delta/5} + \epsilon.$$

b) Soit Δ un nombre réel positif. Donner un exemple d'un polynôme homogène f de degré 2 dont le discriminant est Δ tel que

$$\min\bigl\{|f(x,y)|\ ;\ (x,y)\in\mathbf{Z}\times\mathbf{Z},\ (x,y)\neq(0,0)\bigr\}=\sqrt{\Delta/5}.$$

c) Donner un exemple d'un polynôme homogène f de degré 2 de discriminant $\Delta>0$ tel que

$$\min\bigl\{|f(x,y)|\ ;\ (x,y)\in\mathbf{Z}\times\mathbf{Z},\ (x,y)\neq(0,0)\bigr\}=0.$$

Références

[1] J.H. Conway & R.K. Guy – *The book of numbers*, Copernicus Books, Springer Science + Business Media, 2006.

[2] W. M. Schmidt – *Diophantine approximation*, Lecture Notes in Mathematics, vol. 785, Springer-Verlag, Berlin, 1980.

Troisième fascicule : 04/02/2008

1.2 Critère d'irrationalité (suite et fin)

Si α est racine d'un polynôme quadratique $P(X) = aX^2 + bX + c$, alors $P'(\alpha) = 2a\alpha + b$ est une racine carrée du discriminant de P. D'après le lemme 1.9, le lemme de Hurwitz 1.5 est optimal pour toutes les racines de polynômes quadratiques de discriminant 5. En passant, cela montre que 5 est le plus petit discriminant d'un polynôme quadratique irréductible de $\mathbf{Z}[X]$ (évidemment on vérifie de façon élémentaire que si a, b, c sont trois entiers rationnels satisfaisant $a > 0$ et $b^2 - 4ac$ positif sans être un carré parfait dans $\mathbf{Z}$, alors $b^2 - 4ac \geq 5$).

Soit x un nombre réel irrationnel. Désignons par $\gamma(x) \in [\sqrt{5}, +\infty]$ la borne supérieure des nombres réels $\gamma > 0$ tels qu'il existe une infinité de $p/q \in \mathbf{Q}$ satisfaisant

$$\left|x - \frac{p}{q}\right| \leq \frac{1}{\gamma q^2}.$$

La minoration $\gamma \geq \sqrt{5}$ n'est autre que le lemme 1.5 de Hurwitz. Les lemmes 1.5 et 1.9 montrent que $\gamma(\Phi) = \sqrt{5}$.

En écrivant

$$\left|x + 1 - \frac{p}{q}\right| = \left|x - \frac{p+q}{q}\right| \quad \text{et} \quad \left|-x - \frac{p}{q}\right| = \left|x + \frac{p}{q}\right|,$$

on obtient $\gamma(x+1) = \gamma(-x) = \gamma(x)$. On montre aussi que $\gamma(1/x) = \gamma(x)$. Il en résulte que si x et y sont deux nombres réels que l'on déduit l'un de l'autre en itérant ces trois opérations $x \mapsto x+1$, $x \mapsto -x$ et $x \mapsto 1/x$, alors $\gamma(x) = \gamma(y)$. Un résultat classique ([6] Chap. VII § 1.2) est que le groupe multiplicatif engendré par les trois matrices

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

est le groupe des matrices 2×2

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

à coefficients dans $\mathbf{Z}$ de déterminant ± 1. Nous n'allons pas utiliser cet énoncé mais nous démontrons directement :

Lemme 1.11. *Soit $x \in \mathbf{R} \setminus \mathbf{Q}$ et soient a, b, c, d des entiers rationnels satisfaisant $ad - bc = \pm 1$. On pose*

$$y = \frac{ax + b}{cx + d}.$$

Alors $\gamma(x) = \gamma(y)$.

Démonstration. Soit $\epsilon > 0$ et soit $\gamma = \gamma(x) - \epsilon$. Par définition de $\gamma(x)$, existe une infinité de $p/q \in \mathbf{Q}$ tels que

$$\left| x - \frac{p}{q} \right| \leq \frac{1}{\gamma q^2}.$$

Comme c et d ne sont pas tous deux nuls, au plus un d'entre eux satisfait $cp+dq = 0$. On s'intéresse aux autres. Posons

$$r = ap + bq, \quad s = cp + dq.$$

Quitte à changer les signes de a, b, c et d on peut supposer $s > 0$. On écrit

$$y - \frac{r}{s} = \frac{ax+b}{cx+d} - \frac{ap+bq}{cp+dq} = \frac{(ad-bc)(qx-p)}{(cx+d)(cp+dq)} = \pm \frac{qx-p}{(cx+d)(cp+dq)}$$

et

$$\left| y - \frac{r}{s} \right| \leq \frac{1}{\gamma q} \cdot \left| \frac{1}{(cx+d)(cp+dq)} \right| = \frac{1}{\gamma s^2} \cdot \frac{cp+dq}{q|cx+d|}.$$

Pour q suffisamment grand on a

$$|c| \cdot \left| x - \frac{p}{q} \right| \leq \frac{|c|}{\gamma q^2} \leq \epsilon |cx+d|,$$

donc

$$\left| \frac{cp+dq}{q(cx+d)} - 1 \right| \leq \epsilon$$

et

$$\left| y - \frac{r}{s} \right| \leq \frac{1+\epsilon}{\gamma s^2}.$$

Comme il y a une infinité de $r/s \in \mathbf{Q}$ satisfaisant cette inégalité on en déduit

$$\gamma(y) \geq \frac{\gamma}{1+\epsilon} = \frac{\gamma(x) - \epsilon}{1+\epsilon}.$$

Cette inégalité est vraie pour tout $\epsilon > 0$, par conséquent $\gamma(y) \geq \gamma(x)$. Comme

$$x = \frac{-dy+b}{cy-a},$$

en permutant x et y on obtient l'égalité annoncée $\gamma(y) = \gamma(x)$. □

Des lemmes 1.5, 1.9 et 1.11 on déduit que tous les nombres réels x de la forme $(a\Phi+b)/(c\Phi+d)$ avec a, b, c, d dans $\mathbf{Z}$ et $ad-bc = \pm 1$ satisfont $\gamma(x) = \sqrt{5}$. Hurwitz a aussi montré que pour tous les autres nombres réels irrationnels y, on a $\gamma(y) \geq 2\sqrt{2}$. Cette inégalité est optimale, comme on le voit en prenant $y = \sqrt{2}$ (voir l'exercice ci-dessous). Le lemme 1.11 implique alors $\gamma(y) = 2\sqrt{2}$ pour tout y de la forme $(a\sqrt{2}+b)/(c\sqrt{2}+d)$ avec $ad-bc = \pm 1$, et une fois de plus la minoration peut être améliorée pour tous les autres nombres réels irrationnels. Ce processus donne lieu à une suite d'exposants

$$\sqrt{5}, \sqrt{8}, \sqrt{221}/5, \sqrt{1517}/13, \ldots$$

convergeant vers $1/3$, qui est à l'origine de l'équation de Markoff (cf § 0.2 et [1] Chap. 7).

Exercice. On pose $G_0 = 0$, $G_1 = 1$, et par récurrence on définit $G_n = 2G_{n-1} + G_{n-2}$ pour $n \geq 2$.
a) Vérifier, pour tout $n \geq 1$,

$$G_n^2 - 2G_nG_{n-1} - G_{n-1}^2 = (-1)^{n-1}.$$

b) Montrer que la suite $(G_n/G_{n-1})_{n\geq 2}$ converge quand $n \to \infty$. Quelle est la limite ?
c) Montrer qu'il existe une suite $(p_n/q_n)_{n\geq 1}$ de nombre rationnels telle que

$$\lim_{n\to\infty} q_n \left| q_n\sqrt{2} - p_n \right| = \frac{1}{2\sqrt{2}}.$$

d) Montrer que pour tout $\kappa > 2\sqrt{2}$, il n'y a qu'un nombre fini de nombres rationnels $p/q \in \mathbf{Q}$ satisfaisant

$$\left| \sqrt{2} - \frac{p}{q} \right| \leq \frac{1}{\kappa q^2}.$$

1.3 Nombres : algébriques, transcendants

Un nombre complexe qui est racine d'un polynôme non nul à coefficients rationnels est appelé *algébrique*. Ainsi les nombres rationnels (racines d'un polynôme de degré 1) sont algébriques, $\sqrt{2}$ et i, racines des polynômes X^2-2 et X^2+1 sont algébriques irrationnels – on les appelle *quadratiques* car ils sont racines de polynômes de degré 2. Un nombre *cubique* est une racine d'un polynôme de degré 3 ; un exemple est $\sqrt[3]{2}$.

Étant donné un nombre algébrique α, l'ensemble des polynômes à coefficients rationnels qui s'annulent en α forme un idéal premier de $\mathbf{Q}[X]$, cet idéal est principal, chacun de ses générateurs est un polynôme irréductible de $\mathbf{Q}[X]$ dont le degré est le *degré de* α. Il y a un unique générateur unitaire, qui est appelé **le** *polynôme irréductible* de α. Quand on multiplie ce polynôme par le ppcm des dénominateurs de ses coefficients, on obtient le *polynôme minimal* de α, qui est l'unique polynôme irréductible dans l'anneau *factoriel* $\mathbf{Z}[X]$ s'annulant au point α et ayant un coefficient directeur positif. Voir par exemple [5] Chap. 2 § 5 pour les prérequis concernant notamment les anneaux factoriels.

Les nombres algébriques complexes forment un corps. L'exercice suivant en fournit une démonstration.

Exercice. a) Soient x un nombre complexe et n un entier positif. Montrer que les conditions suivantes sont équivalentes.
(i) Le nombre x est racine d'un polynôme non nul de $\mathbf{Q}[X]$ de degré $\leq n$.
(ii) Les nombres $1, x, x^2, \ldots, x^n$ sont linéairement dépendants sur $\mathbf{Q}$.
(iii) Le $\mathbf{Q}$–espace vectoriel engendré par les nombres x^i, $(i \geq 1)$ est de dimension $\leq n$.
b) Montrer que l'inverse $1/x$ d'un nombre algébrique non nul x est un nombre algébrique.
c) Soient x et y deux nombres algébriques. Montrer que le $\mathbf{Q}$–espace vectoriel engendré par x^iy^j, $(i \geq 0,\ j \geq 0)$ est de dimension finie. En déduire que le produit de deux nombres algébriques est un nombre algébrique.
d) Soient x et y deux nombres algébriques. Montrer que le $\mathbf{Q}$–espace vectoriel engendré par x^i+y^j, $(i \geq 0,\ j \geq 0)$ est de dimension finie. En déduire que la somme de deux nombres algébriques est un nombre algébrique.

Un nombre complexe est dit *transcendant* s'il n'est pas algébrique. L'ensemble des nombres transcendants ne jouit pas de bonnes propriétés algébriques : la somme de nombres transcendants

peut être un nombre rationnel, ou algébrique irrationnel, ou encore transcendant. De même pour le produit de deux nombres transcendants. La somme d'un nombre algébrique et d'un nombre transcendant est un nombre transcendant. Le produit d'un nombre algébrique *non nul* et d'un nombre est un nombre transcendant. La racine carrée (et plus généralement la racine k-ième, pour $k \geq 1$) d'un nombre transcendant est un nombre transcendant. Toute puissance entière ≥ 1 d'un nombre transcendant est encore un nombre transcendant.

L'existence de nombres transcendants a été établie en 1844 par J. Liouville. Son idée consiste à établir une propriété satisfaite par tous les nombres algébriques, puis à exhiber des nombres qui ne satisfont pas cette propriété. Ce que montre Liouville est que les nombres algébriques irrationnels sont relativement mal approchés par des nombres rationnels.

Le lemme suivant ([5] p. 6 Lemma 2E) est une des nombreuses variantes de l'inégalité de Liouville. On peut le voir comme un généralisation du lemme 1.10 : au lieu de $X^2 - X - 1$ on prend n'importe quel polynôme irréductible de degré ≥ 2, ce qui revient à remplacer le nombre d'or par n'importe quel nombre algébrique irrationnel.

Lemme 1.12. *Soit α un nombre algébrique racine de degré $d \geq 2$ et soit $P \in \mathbf{Z}[X]$ son polynôme minimal. On pose $c = |P'(\alpha)|$. Soit $\epsilon > 0$. Alors il existe un entier q_0 tel que, pour tout $p/q \in \mathbf{Q}$ avec $q \geq q_0$, on ait*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{(c+\epsilon)q^d}.$$

Démonstration. Soit q un entier suffisamment grand et soit p l'entier le plus proche de $q\alpha$. En particulier on a

$$|q\alpha - p| \leq \frac{1}{2}.$$

On désigne par a_0 le coefficient directeur de P (quitte à remplacer s'il le faut P par $-P$, on supposera $a_0 > 0$) et par $\alpha_1, \ldots, \alpha_d$ ses racines, avec $\alpha_1 = \alpha$. Ainsi

$$P(X) = a_0(X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_d)$$

et

$$q^d P(p/q) = a_0 q^d \prod_{i=1}^{d} \left(\frac{p}{q} - \alpha_i\right). \tag{1.13}$$

On a aussi

$$P'(\alpha) = a_0 \prod_{i=2}^{d} (\alpha - \alpha_i).$$

Le membre de gauche de (1.13) est un entier rationnel car P est de degré d à coefficients entiers. Il n'est pas nul parce que P est irréductible de degré ≥ 2. Pour $i \geq 2$ on a

$$\left|\alpha_i - \frac{p}{q}\right| \leq |\alpha_i - \alpha| + \frac{1}{2q}.$$

On déduit de (1.13)

$$1 \leq q^d a_0 \left|\alpha - \frac{p}{q}\right| \prod_{i=2}^{d} (|\alpha_i - \alpha| + \frac{1}{2q}).$$

Pour q suffisamment grand le membre de droite est majoré par

$$q^d \left|\alpha - \frac{p}{q}\right| (|P'(\alpha)| + \epsilon).$$

□

Le corollaire suivant du lemme 1.12 est le résultat principal de J. Liouville en 1844 : c'est l'outil qui lui a permis, non seulement de montrer l'existence de nombres transcendants, mais aussi d'en exhiber. Ses premiers exemples utilisaient des fractions continues. Ensuite il a utilisé des séries rapidement convergentes comme

$$\vartheta = \sum_{n\geq 0} g^{-n!}$$

pour tout entier $g \geq 2$.

Lemme 1.14. *Pour tout nombre algébrique α, il existe une constante $\kappa > 0$ telle que, pour tout nombre rationnel $p/q \neq \alpha$,*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{\kappa q^d},$$

où d est le degré de α

Démonstration. Quand $d = 1$ ce résultat est vrai en prenant pour κ le dénominateur de α. Supposons maintenant $d \geq 2$. Le lemme 1.12 avec $\epsilon = 1$ montre que l'inégalité est vraie avec $\kappa = c+1$ pour q suffisamment grand, disons $q \geq q_0$. Pour avoir un résultat uniforme (pour tout p/q) il suffit de prendre

$$\kappa = \max\left\{c+1, \max_{1\leq q<q_0} \frac{1}{q^{d-1}|q\alpha - p|}\right\}.$$

□

Exercice. Le lemme 1.14 est trivial si α n'est pas réel. Dire pourquoi.

Exercice. On désigne par $P \in \mathbf{Z}[X]$ le polynôme minimal de α, par a_0 son coefficient directeur et par $\alpha_1, \ldots, \alpha_d$ ses racines, avec $\alpha_1 = \alpha$:

$$P(X) = a_0(X - \alpha_1)(X - \alpha_2)\cdots(X - \alpha_d).$$

a) Démontrer le lemme 1.14 avec

$$\kappa = \max\{1\ ;\ \max_{|t-\alpha|\leq 1} |P'(t)|\}.$$

b) Démontrer le lemme 1.14 avec

$$\kappa = a_0 \prod_{i=2}^{d} (|\alpha_j - \alpha| + 1).$$

`Indication` *Pour les deux parties de l'exercice, on pourra distinguer deux cas selon que $|\alpha - (p/q)|$ est ≥ 1 ou < 1.*

Définition. Un nombre réel ϑ est un *nombre de Liouville* si, pour tout $\kappa > 0$, il existe $p/q \in \mathbf{Q}$ avec $q \geq 2$ tel que

$$0 < \left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q^\kappa}.$$

Le lemme 1.14 implique que les nombres de Liouville sont transcendants [2]. Dans la théorie des systèmes dynamiques, on dit qu'un nombre réel *satisfait une condition Diophantienne* si ce n'est pas un nombre de Liouville : cela signifie qu'il existe une constante $\kappa > 0$ telle que, pour tout $p/q \in \mathbf{Q}$ avec q suffisamment grand,

$$\left|\alpha - \frac{p}{q}\right| > \frac{1}{q^\kappa}.$$

`Exemple.` Soit $g \geq 2$ un entier rationnel et soit $(a_n)_{n\geq 0}$ une suite bornée d'entiers rationnels. On suppose qu'une infinité d'entre eux ne sont pas nuls. Montrons que *le nombre*

$$\vartheta = \sum_{n\geq 0} a_n g^{-n!}$$

est un nombre de Liouville.

Soit $A = \max_{n\geq 0} |a_n|$ et soit $\kappa > 0$ un nombre réel. Prenons pour N un entier suffisamment grand avec $a_{N+1} \neq 0$ et posons

$$q = g^{N!}, \quad p = \sum_{n=0}^{N} a_n g^{N!-n!}.$$

On a $p \in \mathbf{Z}$, $q \in \mathbf{Z}$, $q > 0$ et

$$\vartheta - \frac{p}{q} = \frac{a_{N+1}}{g^{(N+1)!}} + \sum_{k\geq 2} \frac{a_{N+k}}{g^{(N+k)!}}.$$

Pour $k \geq 2$ on utilise l'estimation grossière

$$(N+k)! - (N+1)! \geq N + k$$

qui donne, pour N suffisamment grand,

$$\sum_{k\geq 2} \frac{|a_{N+k}|}{g^{(N+k)!}} \leq \frac{A}{g^{(N+1)!}} \sum_{k\geq 2} \frac{1}{g^{N+k}} < \frac{1}{g^{(N+1)!}} \leq \frac{|a_{N+1}|}{g^{(N+1)!}},$$

donc $\vartheta \neq p/q$ et

$$0 < \left|\vartheta - \frac{p}{q}\right| \leq \frac{2|a_{N+1}|}{g^{(N+1)!}}.$$

On utilise enfin $|a_{N+1}| \leq A$ et $g^{(N+1)!} = q^{N+1}$, d'où

$$0 < \left|\vartheta - \frac{p}{q}\right| \leq \frac{2A}{q^{N+1}}.$$

Il en résulte que ϑ est un nombre de Liouville.

[2] `Exercice : rédiger la démonstration de cette affirmation.`

Après que Liouville ait construit les premiers exemples de nombres transcendants, G. Cantor a donné un autre argument qui montre non seulement qu'il existe des nombres transcendants, mais aussi qu'il y en a *beaucoup*. La première étape consiste à montrer que les nombres algébriques forment un ensemble dénombrable. Pour cela il remarque que pour chaque couple (d, H) d'entiers positifs, il n'y a qu'un nombre fini de polynômes à coefficients entiers de degré $\leq d$ dont tous les coefficients ont une valeur absolue $\leq H$, et chacun de ces polynômes n'a qu'un nombre fini de racines. La réunion de l'ensemble de ces racines, quand d et H varient, est une réunion dénombrable d'ensembles dénombrables, donc est dénombrable, et c'est l'ensemble des nombres algébriques.

Pour obtenir l'existence de nombres transcendants, Cantor introduit son *argument diagonal* : si on numérote les nombres algébriques de l'intervalle $(0, 1)$ et qu'on écrit chacun d'eux avec son développement en base 2 (en prenant soin d'écrire les deux développements pour les quotients d'un entier par une puissance de 2, l'un qui termine par des 0, l'autre qui termine par des 1), disons

$$\begin{array}{rcl} x_1 & = & 0, a_{11}\, a_{12}\, a_{13} \cdots a_{1n} \cdots \\ x_2 & = & 0, a_{21}\, a_{22}\, a_{33} \cdots a_{2n} \cdots \\ x_3 & = & 0, a_{31}\, a_{32}\, a_{33} \cdots a_{3n} \cdots \\ & \vdots & \\ x_m & = & 0, a_{m1}\, a_{m2}\, a_{m3} \cdots a_{mn} \cdots \\ & \vdots & \end{array}$$

et si on pose $b_n = 1 - a_{nn}$, alors le nombre réel

$$y = 0, b_1 b_2 b_3 \cdots b_n \cdots$$

n'est pas dans la liste, puisqu'il diffère de x_n au moins par le n-ième chiffre ; il est donc transcendant.

Cette construction donne aussi la transcendance du nombre

$$z = 0, a_{11} a_{22} a_{33} \cdots a_{nn} \cdots ,$$

puisque $y + z = 1$.

On sait (voir par exemple l'appendice 1 de [5] ou bien le chapitre 12 de [2]) que le nombre e est transcendant (Hermite, 1873), que le nombre π est transcendant (Lindemann, 1882). Plus généralement le théorème de Hermite–Lindemann s'énonce sous les deux formes équivalentes suivantes.

Théorème 1.15 (Hermite–Lindemann)**.** *a) Soit α un nombre algébrique non nul et soit $\log \alpha$ un logarithme non nul de α (c'est-à-dire un nombre complexe tel que $\exp(\log \alpha) = \alpha$). Alors $\log \alpha$ est un nombre transcendant.*
b) Soit β un nombre algébrique non nul. Alors le nombre e^β est transcendant.

En 1934, A.O. Gel'fond et Th. Schneider ont résolu le 7ème des 23 problèmes posés par D. Hilbert en 1900. On peut de nouveau énoncer ce résultat sous deux formes équivalentes.

Théorème 1.16 (Gel'fond–Schneider)**.** *a) Soient α un nombre algébrique non nul, β un nombre algébrique irrationnel et $\log \alpha$ un logarithme non nul de α. Alors le nombre α^β, qui est défini comme $\exp(\beta \log \alpha)$, est transcendant.*
b) Soient α_1 et α_2 deux nombres algébriques non nuls, $\log \alpha$ et $\log \alpha_2$ des logarithmes non nuls de α_1 et α_2 respectivement. On suppose que le quotient $\log \alpha_1 / \log \alpha_2$ est irrationnel. Alors $\log \alpha_1 / \log \alpha_2$ est transcendant.

Le théorème 1.16 contient la transcendance des nombres

$$2^{\sqrt{2}}, \quad 2^i, \quad e^\pi, \quad \frac{\log 3}{\log 2}, \quad \frac{\pi}{\log 2}.$$

Exercice. On considère un nombre complexe non nul a, un nombre complexe irrationnel b, et une détermination non nulle $\log a$ du logarithme de a. Chacun des trois nombres a, b et $a^b = e^{b \log a}$ peut être algébrique ou transcendant, ce qui fait a priori 8 possibilités, mais le théorème de Gel'fond–Schneider montre que l'une de ces possibilités est exclue : les trois nombres en question ne peuvent pas tous être algébriques. Donner un exemple de chacune des 7 autres situations (on pourra utiliser les théorèmes de Hermite–Lindemann et Gel'fond–Schneider).

2 Extensions Algébriques

Quelques rappels

Consulter [5] (Chap. 2), [4] (§ 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 et, sauf mention explicite du contraire, intègres), sur les corps (ils sont toujours supposés commutatifs), sur les *unités* d'un anneau (= 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.

Dans un anneau, l'élément neutre pour la multiplication (noté 1) est différent de l'élément neutre pour l'addition (noté 0). Un anneau a donc au moins deux éléments. L'homomorphisme canonique de $\mathbf{Z}$ dans un anneau A a pour noyau un idéal premier de $\mathbf{Z}$ (car A est supposé intègre), donc de la forme $\{0\}$ ou $p\mathbf{Z}$ avec p premier. Dans le premier cas, l'anneau A est de *caractéristique nulle* et on identifie $\mathbf{Z}$ à un sous-anneau de A, dans le second A est de *caractéristique* p et on identifie le corps fini $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ à un sous-anneau de A.

Une intersection de sous–anneaux est un sous-anneau, ce qui permet de définir le *sous-anneau de A engendré par une partie E de A* : c'est l'intersection de tous les sous-anneaux de A contenant E, qui est le plus petit sous-anneau de A contenant E. Par exemple, quand E est l'ensemble vide, on obtient ainsi le plus petit sous-anneau de A, qui est $\mathbf{Z}$ en caractéristique nulle et $\mathbf{F}_p$ en caractéristique p. Quand B est un sous-anneau de A et E une partie de A, on désigne par $B[E]$ le sous-anneau de A engendré par $B \cup E$. Si E est un ensemble fini $\{x_1, \ldots, x_n\}$, on écrit $B[x_1, \ldots, x_n]$ au lieu de $B[\{x_1, \ldots, x_n\}]$: c'est l'image de l'unique homomorphisme de B–algèbres de l'anneau des polynômes $B[X_1, \ldots, X_n]$ dans A qui envoie X_i sur x_i.

De même une intersection de sous-corps d'un corps K est un sous-corps de K. Si k est un sous-corps de K et E une partie de K, on désigne par $k(E)$ le sous corps de K engendré par $k \cup E$: c'est le corps des fractions de $k[E]$. Ainsi $k(E)$ est l'ensemble des éléments de K 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 $k(\{\alpha\})$.

2.1 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. On a $[L : K] = 1$ si et seulement si $L = K$.

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 2.1. *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*

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

$$\begin{matrix} & F & \\ [F : L] & | & \\ & L & \end{matrix} \quad \begin{matrix} \\ \Big) [F : K] \\ \\ \end{matrix}$$
$$[L : K] \Big(\quad | \quad$$
$$K$$

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 2.1, on a les équivalences

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

et

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

2.2 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. L'anneau $K[X]$ est principal, donc 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. Comme A est intègre, ce polynôme est irréductible dans l'anneau $K[X]$; on dit que f est *le polynôme irréductible* [3] *de α sur K*. L'idéal $\ker \Phi$ est 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 $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$.

[3] Dans certains ouvrages ce que nous appelons polynôme irréductible est appelé *polynôme minimal de α sur K*. Nous garderons l'appellation *polynôme minimal* pour le polynôme irréductible sur $\mathbf{Z}[X]$ d'un nombre algébrique.

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*. Comme nous l'avons vu, quand le corps de base K est celui des rationnels, on dit seulement qu'un nombre est *algébrique* ou *transcendant*, en sous-entendant *sur* $\mathbf{Q}$.

Lemme 2.2. *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 2.1. □

L

|

$K(\alpha)$

|

K

Par exemple quand α est algébrique sur K, pour tout $\beta \in K(\alpha)$ le degré de β sur K divise le degré de α sur K.

Il résulte aussi du lemme 2.2 que si L est une extension finie de K de degré premier p, alors pour tout élément α de L qui n'est pas dans K on a $L = K(\alpha)$.

Lemme 2.3. *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 2.1 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 2.2, elle est aussi algébrique ; le lemme 2.3 montre que, réciproquement, une extension algébrique de type fini est finie.

Lemme 2.4. *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 sur la définition 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 2.1 montre que l'extension $K(a_0, \ldots, a_m, \alpha)/K$ est finie, donc (lemme 2.2) algébrique et ainsi α est algébrique sur K.

□

Lemme 2.5. *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 2.4 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 $\gamma^{-1} \in K[A]$.

□

Exercice. Soient L/K une extension, $\alpha \in L$ un élément algébrique sur K de degré d et soit

$$\gamma = a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1}$$

un élément non nul de $K(\alpha)$ avec $a_i \in K$ $(0 \leq i \leq d-1)$. On note P le polynôme irréductible de α sur K. En utilisant l'algorithme d'Euclide pour calculer un pgcd, dire comment on peut écrire $1/\gamma$ sous la forme

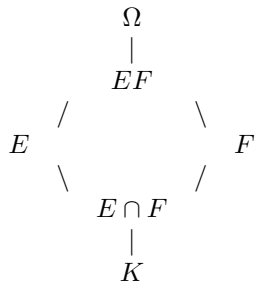
$$\frac{1}{\gamma} = b_0 + b_1\alpha + \cdots + b_{d-1}\alpha^{d-1}$$

avec $b_i \in K$ $(0 \leq i \leq d-1)$.

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 2.6. *Soient Ω/K une extension de corps, E et F deux sous-corps de Ω qui contiennent K. Si l'extension F/K est algébrique, alors l'extension EF/E est aussi algébrique et $EF = E[F]$.*



Démonstration. Soit $\alpha \in F$. Par hypothèse α est algébrique sur K, donc sur E. Le lemme 2.5 avec $A = F$ et $L = EF$ montre que $E[F] = E(F)$ et que l'extension $E(F)/E$ est algébrique. □

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

Exemple. On montre dans le cours d'analyse complexe que le corps $\mathbf{C}(z)$ des fractions rationnelles est algébriquement fermé dans le corps des fonctions méromorphes sur $\mathbf{C}$.

Lemme 2.7. *Soit Ω/K une extension. L'ensemble E des éléments de Ω algébriques sur K est un corps, algébriquement fermé dans Ω.*

Démonstration. Soient α et β deux éléments de E. Les lemmes 2.2 et 2.3 entraînent que l'extension $K(\alpha, \beta)$ est algébrique, donc $\alpha + \beta \in E$ et $\alpha\beta \in E$; de plus $\alpha^{-1} \in E$ si $\alpha \neq 0$.

Soit γ un élément de Ω algébrique sur E. L'extension $E(\gamma)/E$ est finie (lemme 2.3), donc algébrique (lemme 2.2), par conséquent $E(\gamma)$ est une extension algébrique de K (lemme 2.4). Il s'ensuit que γ est algébrique sur K, et par définition de E cela veut dire que γ est dans E.

□

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

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.

Exercice. Montrer que $\overline{\mathbf{Q}}$ est une extension algébrique de $\mathbf{Q}$ qui n'est pas finie.

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 $\mathbf{Q}$ (voir par exemple [4] § 2.3 et appendice du Chap. 2, [5] Chap. V § 2).

Nous admettrons l'existence, pour tout corps K, d'un corps Ω algébriquement clos contenant K (voir par exemple [5] Chap. V § 2 Theorem 2.5).

Théorème 2.8. *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. Il n'y a pas unicité d'un tel isomorphisme : le groupe des automorphismes d'une clôture algébrique de K dont la restriction à K est l'identité est le *groupe de Galois absolu de K*.

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 2.9. *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 $\sigma(\alpha^i) = \beta^i$ $(0 \leq i \leq n-1)$. □

2.3 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 2.10. *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 2.11. *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 2.9.

□

Exercice. Soit L/K une extension finie de degré d et soit $P \in K[X]$ un polynôme irréductible sur K de degré m. On suppose que m et d sont premiers entre eux. Montrer que P est irréductible sur L.

2.4 Corps de décomposition d'un polynôme

Comme nous venons de le voir dans le §2.3, 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 2.12. *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 2.13. *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 2.11 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 2.14. *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] J.H. Conway & R.K. Guy – *The book of numbers*, Copernicus Books, Springer Science + Business Media, 2006.

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

[3] S. Lang – *Algèbre*, Dunod, 2004.

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

[5] W. M. Schmidt – *Diophantine approximation*, Lecture Notes in Mathematics, vol. 785, Springer-Verlag, Berlin, 1980.

[6] J-P. Serre – *Cours d'arithmétique*, Coll. SUP, Presses Universitaires de France, Paris, 1970.

Quatrième fascicule : 18/02/2008

2.5 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 2.15. *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 2.13 il existe un isomorphisme ψ de L sur $L(\beta')$ dont la restriction à $K(\beta)$ est σ. Le lemme 2.14 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.

Proposition 2.16. *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 2.15 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 2.13 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 2.16 permet de donner une caractérisation des extensions normales :

Corollaire 2.17. *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 2.14 et du théorème 2.15.

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 2.16) 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 $\beta \in L$.

□

2.6 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 2.18. *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 2.18 que tout corps de caractéristique nulle est parfait.

Démonstration du lemme 2.18. 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 2.19. *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 2.20. *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 2.20. Pour chaque $\sigma \in H(k, L, N)$ choisissons un prolongement de σ en un automorphisme $\overline{\sigma}$ de N (proposition 2.16). 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 2.19. 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 2.1 et 2.20.

□

Une première application du théorème 2.19 est le *théorème de l'élément primitif* :

Corollaire 2.21. *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 que si k est un corps fini, alors toute extension finie de k est séparable sur k donc 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.

2.7 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 appelé *polynôme cyclotomique d'indice* n, il 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 $n \geq 1$,

$$X^n - 1 = \prod_{d|n} \Phi_d(X). \tag{2.22}$$

Les premiers polynômes cyclotomiques sont

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

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

Exercice. Vérifier $\Phi_p(X) = X^{p-1} + \cdots + X + 1$ si p est premier.
Vérifier $\varphi(2m) = 2\varphi(m)$ si m est pair et $\varphi(2m) = \varphi(m)$ si m est impair.
Vérifier $\Phi_{2m}(X) = \Phi_m(X^2)$ si m est pair et $\Phi_{2m}(X) = (-1)^{\varphi(m)}\Phi_m(-X)$ si m est impair.
En déduire

$$\Phi_8(X) = X^4 + 1, \quad \Phi_{12}(X) = X^4 - X^2 + 1.$$

Théorème 2.23. *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 2.23 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 2.24 (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

$$\Psi_p : \mathbf{Z}[X] \to \mathbf{F}_p[X] \tag{2.25}$$

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 2.24 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 2.23 utilisera le lemme suivant, sur lequel nous reviendrons au § 3 :

Lemme 2.26. *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 2.23. 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 (2.22). 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 (2.25). dans la démonstration du lemme 2.24. 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 2.26 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 $g = 1$.

Remarque. L'irréductibilité des polynômes cyclotomiques résulte aussi du *critère d'Eisenstein* : le polynôme

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

(obtenu à partir de $(X - p - 1)/(X - 1)$ par le changement de variable $Y = X - 1$) est unitaire, tous ses coefficients sauf le coefficient de Y^{p-1} sont divisible par p, et le terme constant n'est pas divisible par p^2.

□

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 (2.25) : on note encore Φ_n cette image.

Proposition 2.27. *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 (2.22) 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 2.28. *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 $[R_n : R_n^+] = 2$.

2.8 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 2.29. *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 2.30. *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 2.19 (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 2.29) $L = K(\alpha_1, \ldots, \alpha_m)$ 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.

□

$$H = \mathrm{Aut}(L/M) \left(\begin{array}{c} L \\ | \\ M = L^H \\ | \\ K \end{array} \right) G$$

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.*

De ces définitions on déduit immédiatement :

$$\left.\begin{array}{c} L \\ | \\ H \left(\begin{array}{c} \\ M = L^H \\ \\ M' = L^{H'} \end{array} \right) H' \\ | \\ K \end{array}\right\} G$$

Lemme 2.31. *Soit L/K une extension algébrique et soit $G = \mathrm{Aut}(L/K)$. Les deux applications*

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

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 2.32.

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.*

$$G \left(\begin{array}{c} L \\ | \\ K = L^G \\ | \\ k \end{array} \right.$$

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 $P(\alpha) = 0$, on en déduit que α est algébrique sur K. Soit f le polynôme irréductible de α sur K. Comme $P \in K[X]$ s'annule en α, il en résulte que 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. Donc L est une extension algébrique de K.

De plus, d"après le corollaire 2.21 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 $[L:K] \geq |\mathrm{Aut}(L/K)|$; 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. Le polynôme irréductible de α sur K est $\prod_{j=1}^{d}\big(X-\sigma_j(\alpha)\big)$ où $\sigma_1,\ldots,\sigma_d$ sont des éléments de $\mathrm{Aut}(L/K)$ et $\sigma_1(\alpha),\ldots,\sigma_d(\alpha)$ sont deux-à-deux distincts. De plus, l'ensemble des $\sigma(\alpha)$ pour σ décrivant $\mathrm{Aut}(L/K)$ est $\{\sigma_1(\alpha),\ldots,\sigma_d(\alpha)\}$. Alors $\alpha \in L^{\mathrm{Aut}(L/K)}$ équivaut à $d=1$, donc à $\alpha \in K$.

□

Du théorème 2.32 (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 2.33 (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*

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

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*

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

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 2.32. 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 2.32 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 $\mathrm{Aut}(M/K)$.

□

Exercice. Soient L/K une extension galoisienne finie de groupe de Galois G, H un sous-groupe de G, $M = L^H$ et $\sigma \in G$. Alors l'extension $L/\sigma(M)$ est galoisienne de groupe de Galois $\sigma H \sigma^{-1}$ et $\sigma(M) = L^{\sigma H \sigma^{-1}}$.

Une extension galoisienne est dite *abélienne, cyclique, résoluble,...* si son groupe de Galois l'est. Rappelons qu'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 $(0 \leq i \leq s-1)$.

2.9 Théorie de Galois : quelques exemples

2.9.1 Corps cyclotomiques

Soient n un entier positif, E_n le corps cyclotomique de niveau n et ζ_n une racine primitive n-ième de l'unité, de sorte que $E_n = \mathbf{Q}(\zeta_n)$.

Nous avons vu (Proposition 2.28) 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 2.34. *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 $m \geq 1$ on a $\zeta^m = \zeta$ si et seulement si $m \equiv 1 \pmod{p}$. D'autre part $\sigma_k^m(\zeta) = \zeta^{k^m}$. Il en résulte que 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 $(\mathbf{Z}/p\mathbf{Z})^\times$. □

Comme ζ est racine du polynôme

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

il est de degré $p-1$ sur $\mathbf{Q}$ et $\{1, \zeta, \zeta^2, \ldots, \zeta^{p-2}\}$ est une base sur $\mathbf{Q}$ de E. 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 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 § 2.7 comme exemple d'application de la proposition 2.28. 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 conjugués 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 $\mathbf{Q}(\sqrt{-7})$.

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 2.28 l'énoncé suivant :

Corollaire 2.35. *Soit $n = p_1^{a_1} \cdots p_k^{a_k}$ un entier ≥ 2 décomposé en facteurs premiers. Notons E_n le corps cyclotomique $\mathbf{Q}(\zeta_n)$ de niveau n et F_i le corps cyclotomique $E_{p_i^{a_i}} = \mathbf{Q}(\zeta_{p_i^{a_i}})$ de niveau $p_i^{a_i}$. Alors*

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

2.9.2 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 [2] § 13.3.

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)).

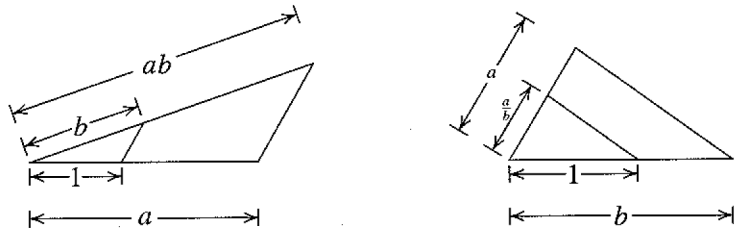


Fig. 1

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.

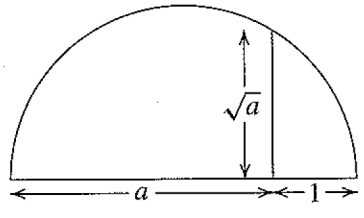


Fig. 2

L'énoncé suivant est facile à démontrer (voir par exemple [2] § 13.3).

Proposition 2.36. *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* [5]).

On déduit du corollaire 2.35 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 2.37. *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 théorème de Galois 2.33 permet de démontrer l'énoncé suivant :

Proposition 2.38. *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 [2] § 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]).

2.9.3 Résolution par radicaux

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.

Le théorème de Galois 2.33 permet de démontrer l'énoncé suivant (voir par exemple [2] § 14.7 Th. 39).

Théorème 2.39. *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 2.39 est un théorème dû à Kummer dont nous donnons seulement l'énoncé :

Théorème 2.40. *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 $\alpha^n \in K$.*

2.9.4 Fonctions symétriques, discriminant

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 (§ 2.9.2) 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 2.33, 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 2.41. *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 [2]. 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 $As_1^{a_1-a_2}s_2^{a_2-a_3} \cdots s_n^{a_n}$.

Ceci montre en passant que $s_1, \ldots, s_n$ sont algébriquement indépendants.

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

$$f(X) = X^n - s_1X^{n-1} + s_2X^{n-2} - \cdots + (-1)^n s_n. \tag{2.42}$$

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 2.43. *Si $s_1, \ldots, s_n$ sont des indéterminées sur $\mathbf{Q}$, le polynôme générique (2.42) 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 $x_1, \dots, x_n$ des éléments de L. On définit le *discriminant* de $(x_1, \dots, x_n)$ 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 $x_1, \dots, x_n$ sont des indéterminées et $L = \mathbf{Q}(x_1, \dots, x_n)$. C'est un polynôme symétrique, donc d'après la proposition 2.41 il s'exprime comme un polynôme en les fonctions symétriques élémentaires $s_1, \dots, s_n$. Une des deux racines carrées de D est

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

L'autre est $-\sqrt{D}$. 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 $(\alpha_1, \dots, \alpha_n)$. 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 $x_1, \dots, x_n$ 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 2.44. *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

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

□

Exercice. Soit p un nombre premier. Vérifier que l'unique sous-corps quadratique de $\mathbf{Q}(\zeta_p)$ 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 [2] § 14.5).

2.9.5 Compléments

Nous avons vu au § 2.9.1 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*. Voir par exemple le Théorème 2.10 de [3].

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.

2.9.6 Exercices

a) *Étude du corps de décomposition de $X^8 - 2$. Référence : [2].*

On désigne par θ la racine réelle du polynôme $X^8 - 2$ et par ζ une racine primitive 8ème de l'unité. Le corps de décomposition du polynôme $X^8 - 2$ est $K = \mathbf{Q}(\theta, \zeta)$. Sous un élément σ du groupe de Galois G de K sur $\mathbf{Q}$ l'image de ζ est une des 4 racines primitives 8èmes de l'unité, à savoir ζ, ζ^3, ζ^5 ou $\zeta^7 = \zeta^{-1} = \overline{\zeta}$. L'image de θ est l'un des 8 conjugués de θ, à savoir $\zeta^j\theta$. À priori cela fait $4 \times 8 = 32$ possibilités pour σ. Mais on a $K = \mathbf{Q}(\theta, i)$, donc K a pour degré 16 sur $\mathbf{Q}$. Donc σ est déterminé par l'image de θ et l'image de i ce qui ne fait plus que 16 possibilités et cela décrit donc tous les éléments de G. Noter que l'existence, pour chaque couple formé d'un conjugué de θ et d'un conjugué de i, d'un éléments du groupe de Galois qui envoie (θ, i) sur ce couple, résulte du dénombrement que nous venons de faire.

Comme $\theta^4 = \sqrt{2} = \zeta + \zeta^7$, les images par un automorphisme de K de θ et ζ doivent vérifier cette relation, ce qui justifie la réduction de 32 à 16.

b) Compositum d'une extension finie et d'une extension Galoisienne

Référence : polycopié online de Robert B. Ash (`www.math.uiuc.edu/~ash/Algebra.html`) Abstract algebra basic graduate year 11/02 Chapter 6 Galois Theory p.6 Theorem 6.2.2)

Dans la correspondance de Galois, si H_1 et H_2 sont deux sous-groupes du groupe de Galois, quel est le corps fixé par $H_1 \cap H_2$? Si K_1 et K_2 sont deux corps intermédiaires, quel est le groupe de Galois associé à $K_1 \cap K_2$?

Soient E/F une extension galoisienne (finie) et K/F une extension finie.
Montrer que EF est une extension galoisienne de K.
Montrer que le groupe de Galois de EK/K est (isomorphe à) un sous-groupe du groupe de Galois de E/F. En déduire que $[EK : K]$ divise $[E : F]$. Donner un exemple qui montre que l'hypothèse E/F galoisienne n'est pas superflue.
Montrer que $[EK : K] = [E : F]$ si et seulement si $E \cap K = F$.
On suppose de plus que l'extension K/F est galoisienne. Montrer que le groupe de Galois $G(EK/E \cap K)$ de EK sur $E \cap K$ est le produit direct de ses deux sous-groupes $G(EK/E)$ et $G(EK/K)$.

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] M. Hindry – *Arithmétique*, Calvage et Mounet, Tableau Noir, Paris, 2008.

[5] S. Lang – *Algèbre*, Dunod, 2004.

Université P. et M. Curie (Paris VI),
Deuxième semestre 2007/2008

Michel Waldschmidt
date de mise à jour: 10/06/2008

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

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

Cinquième fascicule : 10/03/2008

3 Corps finis

3.1 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 $s = [K : \mathbf{F}_p]$, 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 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 2.21 :

Proposition 3.1. *Si k est un corps fini et K une extension finie de k, alors l'extension K/k est monogène.*

Démonstration de la proposition 3.1. 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

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

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

□

3.2 Construction des corps finis et théorie de Galois

Théorème 3.2. *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

$$\mathbf{F}_{p^n} \subset \mathbf{F}_{p^m} \iff n \text{ divise } m; \tag{3.3}$$

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 3.4. *Soient E un corps fini à q éléments, K une extension de E et f un élément de $K[X]$. Alors $f \in E[X]$ si et seulement si $f(X)^q = f(X^q)$.*

Démonstration. Nous avons vu au § 3.1 que, pour a dans K, on a $a^q = a$ si et seulement si $a \in E$. Comme q est une puissance de la caractéristique p de K, si on écrit

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

on a

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

et par récurrence

$$f(X)^q = a_0^q + a_1^q X^q + \cdots + a_n^q X^{nq}$$

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

□

Proposition 3.5. *Soient E un corps fini à q éléments, K une extension de E et α un élément non nul de K algébrique sur E. Il existe des entiers $s \geq 1$ tels que $\alpha^{q^s} = \alpha$. Notons r le plus petit. Alors le corps $E(\alpha)$ a q^r éléments et le polynôme irréductible de α sur E est*

$$\prod_{i=0}^{r-1} (X - \alpha^{q^i}). \tag{3.6}$$

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

Soit f le polynôme irréductible de α sur E. On a $f(X^q) = f(X)^q$ car $f \in E[X]$, donc l'ensemble des racines de f est stable sous l'automorphisme $F : x \mapsto x^q$ (qui est une puissance du Frobenius).

Il en résulte que f est multiple du polynôme g défini par (3.6). Mais ce polynôme g appartient à $E[X]$ car $g(X^q) = g(X)^q$. Par conséquent $g = f$. Ainsi f est de degré r, donc $[E(\alpha) : E] = r$, par conséquent $E(\alpha)$ a q^r éléments. On en déduit aussi $r = s$.

□

Proposition 3.7. *Soient E un corps fini à q éléments et r un entier positif. Le polynôme $X^{q^r} - X$ est le produit de tous les polynômes unitaires irréductibles de $E[X]$ dont le degré divise r.*

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

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

□

3.3 Décomposition des polynômes cyclotomiques en facteurs irréductibles

Théorème 3.8. *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 (3.3) 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 3.9. *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 3.8 :

Corollaire 3.10. *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.*

3.4 Loi de réciprocité quadratique

Soit p un nombre premier. Étudions les extensions quadratiques du corps $\mathbf{F}_p$ à p éléments. Dans une extension algébriquement close de $\mathbf{F}_p$ il y en a une et une seule. Pour l'expliciter on est amené à étudier les polynômes unitaires irréductibles de degré 2 sur $\mathbf{F}_p$. Pour $p = 2$ il y en a un et un seul, $X^2 + X + 1$. Supposons p impair : comme on peut diviser par 2 on écrit $X^2 + aX + b = (X + a/2)^2 + b - a^2/4$. Il reste à déterminer quels sont les carrés dans $\mathbf{F}_p$.

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

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

On a supposé 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

$$\sum_{\alpha\in\mathbf{F}_p}\left(\frac{\alpha}{p}\right)=0. \tag{3.11}$$

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 $0\le k\le p-3$ et k pair, tandis que les non résidus quadratiques sont les ζ^k avec $1\le k\le p-2$ 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

$$\left(\frac{\alpha}{p}\right)=\alpha^{(p-1)/2}. \tag{3.12}$$

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 3.13. *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

$$\left(\frac{2}{p}\right)=(-1)^{(p^2-1)/8}=\begin{cases}1 & \textit{si } p\equiv\pm1 \pmod 8\\ -1 & \textit{si } p\equiv\pm3 \pmod 8.\end{cases}$$

Démonstration. La relation (3.12) 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 $\mathbf{F}_p[X]$.

Dans le corps des nombres complexes, une des racines primitives 8èmes de l'unité est

$$\alpha=e^{2i\pi/8}=\frac{(1+i)\sqrt{2}}{2}.$$

Elle vérifie $\alpha^2 = i$. Le nombre $\beta = \alpha + \alpha^{-1}$ est une racine du polynôme $X^2 - 2$. On vérifie aussi

$$\alpha^n + \alpha^{-n} = \begin{cases} \beta & \text{si } n \equiv 1 \text{ ou } 7 \pmod 8, \\ -\beta & \text{si } n \equiv 3 \text{ ou } 5 \pmod 8. \end{cases}$$

Ces calculs complexes (et faciles) vont motiver ceux que nous allons faire en caractéristique finie p.

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

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

□

Exercice. Vérifier que le polynôme $X^4 + 1$ est irréductible sur $\mathbf{Q}$ mais est réductible sur $\mathbf{F}_p$ pour tout nombre premier p.

Voici l'énoncé de la loi de réciprocité quadratique :

Théorème 3.14. *Soient p et ℓ des nombres premiers impairs distincts. Alors*

$$\left(\frac{\ell}{p}\right)\left(\frac{p}{\ell}\right) = (-1)^{\frac{p-1}{2}\frac{\ell-1}{2}}. \tag{3.15}$$

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 le groupe multiplicatif $K^\times$ [4]. On pose

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

On met donc ensemble un caractère multiplicatif $\mathbf{F}_p^\times \to K^\times$ et un caractère additif $\mathbf{F}_p^\times \to K$ du groupe $\mathbf{F}_p^\times$:

$$a \longmapsto \left(\frac{a}{p}\right) \quad \text{et} \quad a \longmapsto \zeta^a.$$

[4] Par exemple on peut prendre $K = \mathbf{C}$ et $\zeta = e^{2i\pi/p}$. Mais on ne peut pas prendre un corps de caractéristique p bien sûr !

Démonstration du théorème 3.14. Comme ζ^a ne dépend que de la classe de a modulo p, qu'il en est de même du symbole de Legendre $\left(\frac{a}{p}\right)$ et que ce dernier 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

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

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

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

Ainsi

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

En utilisant (3.11) on en déduit

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

Ces calculs sont valables dans tout corps K contenant une racine primitive p-ième de l'unité ζ. Choisissons maintenant pour K une clôture algébrique $\overline{\mathbf{F}}_\ell$ de $\mathbf{F}_\ell$. On a dans $\overline{\mathbf{F}}_\ell$

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

donc

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

Alors, toujours dans $\overline{\mathbf{F}}_\ell$, on a

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

Ceci démontre la relation (3.15).

□

Références

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

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

[3] M. Hindry – *Arithmétique*, Calvage et Mounet, Tableau Noir, Paris, 2008.

Université P. et M. Curie (Paris VI),
Deuxième semestre 2007/2008

Michel Waldschmidt
date de mise à jour: 10/06/2008

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

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

Sixième fascicule : 24/03/2008

4 Corps de Nombres

4.1 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,

$$\mathrm{N}_{B/A}(xy) = \mathrm{N}_{B/A}(x)\mathrm{N}_{B/A}(y) \tag{4.1}$$

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 4.2. *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 2.19.

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 4.3. *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 4.3. 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 4.4 suivant. □

Lemme 4.4 (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 4.5. *Soient* $\mathsf{A} = \left(a_{ij}\right)_{1\leq i,j\leq n}$ *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 $D_{B/A}(x_1, \ldots, x_n) = 0$ (on a supposé A intègre).

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 principal 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 4.6. *Soient* $A \subset B$ *deux anneaux ; on suppose que* B *est un* A*-module libre de rang* n *et que l'idéal* $\mathcal{D}_{B/A}$ *n'est pas l'idéal* $\{0\}$*. 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. Par définition de l'idéal discriminant $\mathcal{D}_{B/A}$, si $\{x_1, \ldots, x_n\}$ est une base de B comme A-module, alors $D_{B/A}(x_1, \ldots, x_n)$ est un générateur de l'idéal $\mathcal{D}_{B/A}$

Inversement supposons que $D_{B/A}(x_1, \ldots, x_n)$ engendre l'idéal $\mathcal{D}_{B/A}$. 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 4.5 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 non nul et que A est intègre, il en résulte que a^2 est inversible, donc 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 4.7. *Soit* L/K *une extension séparable de degré* n*, soit* N *une extension finie de* L*, normale sur* K *,* $x_1, \ldots, x_n$ *des éléments de* L *et soient* $\sigma_1, \ldots, \sigma_n$ *les différents* K*-isomorphismes de* L *dans* N*. Alors*

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

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

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

Démonstration. On utilise le lemme 4.2 :

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

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 4.4 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 $x_i\in E$. Nous avons déjà défini 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 §2.8 montre que $D(P)$ est un élément de K. De la proposition 4.7, 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 $-4p^3-27q^2$.

4.2 Entiers algébriques

Proposition 4.8. *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 $M = \big(a_{ij}\big)_{1\leq i,j\leq m}$ 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 4.8.

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 4.9. *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 4.8 on déduit que la relation d'intégralité est transitive :

Corollaire 4.10. *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.*

Démonstration. Soit B_0 la fermeture intégrale de B dans K. Un élément de A_0 est entier sur A, donc sur B, et par conséquent appartient à B_0. Pour voir l'inclusion dans l'autre sens, on considère un élément x de B_0, il est entier sur B, donc racine d'un polynôme unitaire à coefficients dans B. Soient $b_1, \ldots, b_m$ les coefficients de ce polynôme ; le sous–anneau $A[b_1, \ldots, b_m]$ de B est un A–module de type fini, il en est de même de $A[b_1, \ldots, b_m, x]$, donc par la proposition 4.8 on en déduit que x est entier sur A, ce qui montre $B_0 \subset A_0$. □

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

$$dX^n + da_1 X^{n-1} + \cdots + da_n \in \mathbf{Z}[X], \tag{4.11}$$

où d est le plus petit commun multiple des dénominateurs des nombres $a_1, \ldots, a_n$. Nous appellerons ce polynôme (4.11) 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 2.24 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 4.9 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 2.21, 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 et $\mathbf{Z}_K$ est un anneau intégralement clos (cf. Corollaire 4.10).

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 4.2 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 $d \equiv 2 \text{ ou } 3 \pmod 4$, 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 au § 4.4 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 4.12. *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 $e_1, \ldots, e_n$ de $\mathbf{Z}_K$, linéairement indépendants sur $\mathbf{Q}$, tels que

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

Soit $f_1, \ldots, f_n$ 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 4.2), il existe une base $f_1^*, \ldots, f_n^*$ 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 $x_1, \ldots, x_d$ dans $\mathbf{Q}$ et on a $\mathrm{Tr}_{K/\mathbf{Q}}(x f_j^*) = x_j$. 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 §4.3 suivant sur la structure des modules sur un anneau principal (proposition 4.14).

□

Il résulte de la Proposition 4.12 que tout idéal de $\mathbf{Z}_K$ est un $\mathbf{Z}$–module libre de rang n. Une base de $\mathbf{Z}_K$ comme $\mathbf{Z}$–module est *une base d'entiers de K*, son discriminant ne dépend pas de la base, c'est le *discriminant du corps de nombres K*.

Soient k un corps de nombres et n son degré. D'après le théorème de l'élément primitif 2.21, 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 $\alpha_1, \ldots, \alpha_{r_1}$ 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 $\sigma_1, \ldots, \sigma_n$ 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 $\{\sigma_1, \ldots, \sigma_{r_1}\}$ des plongements réels et celui $\{\sigma_{r_1+1}, \ldots, \sigma_{r_1+2r_2}\}$ 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

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

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

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

Le couple (r_1, r_2) est la *signature* du corps de nombres k. Le degré de k est alors $r_1 + 2r_2$.

Lemme 4.13. *Le signe du discriminant absolu d'un corps de nombres k de signature (r_1, r_2) est $(-1)^{r_2}$.*

Démonstration. . Dans le développement du déterminant de la matrice des $\sigma_i(\alpha_j)$ (cf. proposition 4.7), les nombres réels on des carrés positifs, les nombres imaginaires purs ont des carrés négatifs et il y en a r_2. Voir [C], Prop. 4.8.11. □

Exercice. Soit T un polynôme unitaire irréductible de degré n de $\mathbf{Z}[X]$ et $K = \mathbf{Q}(\theta)$. On désigne par $D(T)$ le discriminant de T et par D_K celui du corps de nombres K.
a) Montrer que le discriminant de $1, \theta, \ldots, \theta^{n-1}$ est $D(T)$.
b) Soit f l'indice de $\mathbf{Z}[\theta]$ dans $\mathbf{Z}_K$. Vérifier $D(T) = D_K f^2$.
`Référence` : [C], § 4.4.

Une famille $(\alpha_1, \ldots, \alpha_n)$ de n éléments dans un corps de nombres de degré n est une base d'entiers de K si et seulement si les deux conditions suivantes sont satisfaites :
(i) Les α_i sont entiers
(ii) Le discriminant $D(\alpha_1, \ldots, \alpha_n)$ est égal au discriminant de K.

Exercice. Montrer que le discriminant d'un corps de nombres est congru à 0 ou 1 modulo 4
`Indication` : en utilisant la proposition 4.7 développer le déterminant de la matrice des $\sigma_i(\alpha_j)$ et regrouper les termes de signature paire et ceux de signature impaire pour écrire le discriminant sous la forme $(P-N)^2 = (P+N)^2 - 4PN$ et vérifier que $P+N$ et PN sont des entiers.
En déduire que si T est un polynôme unitaire irréductible dans $\mathbf{Z}[X]$ de discriminant D qui est soit sans facteur carré et congru à 1 modulo 4, soit de la forme $4d$ avec d sans facteur carré et congru à 1 modulo 4, si θ est une racine de T dans une extension de $\mathbf{Q}$, alors $(1, \theta, \ldots, \theta^{n-1})$ est une base d'entiers de $\mathbf{Q}(\theta)$.

4.3 Structure des modules sur les anneaux principaux

Dans la démonstration de la Proposition 4.12, nous avons utilisé un théorème sur la structure des sous-modules d'un module libre de type fini sur un anneau principal. En voici l'énoncé.

Quand A est un anneau (intègre, rappelons-le) 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 4.14. (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 4.14.

Démonstration. Voir [S] § 1.5. □

`Références :`

[C] H. Cohen. *A course in computational algebraic number theory*, Graduate texts in Math. **138**, Springer Verlag (1993),

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

Université P. et M. Curie (Paris VI),
Deuxième semestre 2007/2008

Michel Waldschmidt
date de mise à jour: 10/06/2008

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

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

Septième fascicule : 26/03/2008

4.4 Unités d'un corps de nombres

Dans cette section nous décrivons la situation sans donner les démonstrations. On pourra consulter la bibliographie, notamment [S].

4.4.1 Énoncé du théorème de Dirichlet

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

Lemme 4.15. *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 $2X^2+X+2$.

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

Théorème 4.16. *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 $\epsilon_1, \ldots, \epsilon_r$ 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 $(\epsilon_1, \ldots, \epsilon_r)$ est un système fondamental d'unités de k si cette propriété est vérifiée, c'est-à-dire si les images de $\epsilon_1, \ldots, \epsilon_r$ modulo torsion forment une base du groupe abélien libre $\mathbf{Z}_k^\times/k_{\text{tors}}^\times$.

La démonstration du théorème de Dirichlet (que nous ne donnerons pas – voir par exemple [S]) repose sur la *géométrie des nombres* de Minkowski.

4.5 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].`

4.5.1 Idéaux entiers

Soient K un corps de nombres, $\mathbf{Z}_K$ son anneau d'entiers.

Lemme 4.17. *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 4.14 : il existe une base $\{e_1, \ldots, e_n\}$ de $\mathbf{Z}_K$ et des entiers $a_1, \ldots, a_n$ tels que $\{a_1e_1, \ldots, a_ne_n\}$ 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 $\{e_1, \ldots, e_n\}$ est la matrice diagonale $\mathrm{diag}(a_1, \ldots, a_n)$, dont le déterminant est $a_1 \cdots a_n = \mathrm{N}(\alpha\mathbf{Z}_K)$. Comme $\{\alpha e_1, \ldots, \alpha e_n\}$ 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 4.12 et 4.14 on déduit que $\mathfrak{a}$ est un $\mathbf{Z}$-module libre de rang $n = [K : \mathbf{Q}]$. Par conséquent il existe une base $\{e_1, \ldots, e_n\}$ de $\mathbf{Z}_K$ comme $\mathbf{Z}$-module et des entiers positifs $a_1, \ldots, a_n$ tels que $\{a_1e_1, \ldots, a_ne_n\}$ 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 4.17 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 4.18. *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 $D_K\mathrm{N}(\mathfrak{a})^2$. .*

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 (§ 4.5.5) plusieurs conséquences du lemme suivant.

Théorème 4.19. *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*

$$1 \leq |N_{K/\mathbf{Q}}(\alpha)| \leq M(K)|D_K|^{1/2}\mathrm{N}(\mathfrak{a}).$$

Nous renvoyons au § 4.2 de [S] pour la démonstration.

4.5.2 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 4.20. *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*.

Rappelons que le produit $\mathfrak{ab}$ de deux idéaux d'un anneau A est par définition l'idéal de A engendré par les produits ab, a parcourant $\mathfrak{a}$ et b parcourant $\mathfrak{b}$. Ainsi

$$\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{a} \subset \mathfrak{a} + \mathfrak{b}.$$

Deux idéaux $\mathfrak{a}$ et $\mathfrak{b}$ de A sont dits *premiers entre eux* si $\mathfrak{a} + \mathfrak{b} = A$. Dans ce cas on a $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$.

Lemme 4.21. *Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux non nuls de $\mathbf{Z}_K$. Si $\mathfrak{a} = \mathfrak{ab}$, 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 $\alpha_i \in \mathfrak{ab}$ 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 $1 \in \mathfrak{b}$.

□

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 4.22. *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 4.21 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 4.21 ou bien le lemme 4.22, 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 4.22 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 4.23. *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 4.23 montre que, sous les hypothèses du lemme 4.22, $\mathfrak{a}/\mathfrak{a}\mathfrak{p}$ 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 4.23, voir par exemple le livre de Samuel.

4.5.3 Idéaux fractionnaires

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 $A/\mathfrak{A}_1 \times A/\mathfrak{A}_2$.

Nous utiliserons la notion d'anneau *noethérien* que voici.

Proposition 4.24. *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 4.24 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 4.24 il résulte qu'un anneau principal est noethérien.

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 4.25. *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 4.25 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 4.26. *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 4.23 on déduit que les idéaux fractionnaires de $\mathbf{Z}_K$ forment un groupe abélien d'élément neutre $\mathbf{Z}_K = (1)$.

Théorème 4.27. *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 4.23 montre que la propriété (4.1) de multiplicativité de la norme s'étend aux idéaux de $\mathbf{Z}_K$:

Corollaire 4.28. *Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux de $\mathbf{Z}_K$. Alors*

$$\mathrm{N}(\mathfrak{ab}) = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{b}). \tag{4.29}$$

Démonstration. Grâce au théorème 4.23 il suffit de vérifier la propriété (4.29) 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 4.22 et la remarque qui suit le théorème 4.23), 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 $\mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{p})$.

□

Remarque. Une autre démonstration, due à H.W. Lenstra, est donnée dans [C], Lemma 4.6.8.

Grâce au corollaire 4.28 on peut étendre la définition de la norme aux idéaux fractionnaires. Avec les notations du corollaire 4.27, 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 4.26 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 $a_1, \ldots, a_N$ 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 4.23 on déduit, pour $\mathfrak{p}$ idéal premier de $\mathbf{Z}_K$ et $\mathfrak{a}$, $\mathfrak{b}$ idéaux fractionnaires de $\mathbf{Z}_K$:

$$\begin{array}{rcl} v_{\mathfrak{p}}(\mathfrak{ab}) & = & v_{\mathfrak{p}}(\mathfrak{a}) + v_{\mathfrak{p}}(\mathfrak{b}), \\ v_{\mathfrak{p}}(\mathfrak{a}+\mathfrak{b}) & = & \min\{v_{\mathfrak{p}}(\mathfrak{a}), v_{\mathfrak{p}}(\mathfrak{b})\}, \\ v_{\mathfrak{p}}(\mathfrak{a}\cap\mathfrak{b}) & = & \max\{v_{\mathfrak{p}}(\mathfrak{a}), v_{\mathfrak{p}}(\mathfrak{b})\}. \end{array}$$

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 4.23 montre qu'il existe une décomposition, unique à l'ordre près des facteurs,

$$p\mathbf{Z}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}, \tag{4.30}$$

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 (4.30) 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 4.28, 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

$$e_1 f_1 + \cdots + e_g f_g = n. \tag{4.31}$$

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 4.32. *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 $d \equiv 5 \pmod 8$.

4.5.4 Discriminant et ramification

Nous admettrons l'énoncé suivant :

Théorème 4.33. *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.*

Exercice. Soit θ un entier algébrique, T le polynôme unitaire irréductible de θ (qui est à coefficients dans $\mathbf{Z}$) et K le corps de nombres $\mathbf{Q}(\theta)$, . On suppose $\mathbf{Z}[\theta] = \mathbf{Z}_K$. Soit p un nombre premier. On décompose le polynôme T en facteurs irréductibles unitaires sur $\mathbf{Z}_p$:

$$T(X) = \prod_{i=1}^{g} T_i(X)^{e_i} \pmod p.$$

Soit $\mathfrak{p}_i$ l'idéal engendré par p et $T_i(\theta)$ dans $\mathbf{Z}_K$. Montrer que la décomposition de l'idéal $p\mathbf{Z}_K$ en produit d'idéaux premiers est

$$p\mathbf{Z}_K = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$$

et que l'indice résiduel f_i est égal au degré de T_i.
`Référence`. Voir [C] Théorème 4.8.13.

4.5.5 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 $\mathfrak{a} = \alpha\mathfrak{b}$.

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 4.19).

Proposition 4.34. *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 4.19 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 4.35 (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 4.35. La proposition 4.34 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 4.17), donc $\mathfrak{a}$ appartient à l'ensemble fini des idéaux de $\mathbf{Z}_K$ qui contiennent N.

□

Le théorème 4.19 donne une minoration du discriminant d'un corps de nombres : comme la norme de l'idéal $(1) = \mathbf{Z}_K$ vaut 1 on a

$$|D_K| \geq M(K)^{-2}. \tag{4.36}$$

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 (4.36) 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 4.37 (*Hermite*)**.** *Il n'y a qu'un nombre fini de sous-corps de* $\mathbf{C}$ *de discriminant donné.*

`Références :`

[A] Y. Amice. *Les nombres p-adiques.* PUF, 1975.

[C] H. Cohen. *A course in computational algebraic number theory*, Graduate texts in Math. **138**, Springer Verlag (1993),

[D] R. Descombes. *Éléments de théorie des nombres.* PUF, 1986.

[H] Y. Hellegouarch. *Invitation aux mathématiques de Fermat-Wiles*, Masson, Enseignement des mathématiques, 1997.

[K] N. Koblitz. *p-adic numbers, p-adic analysis, and Zeta-functions.* Springer Verlag Graduate Texts in Math. **58** 1977.

[L] S. Lang, *Algebra.* Addison Wesley 1993.

[P] A.A. Pantchichkine, Magistère de Mathématiques (ENS Lyon), Algèbre 2, § 3.1.
http ://www-fourier.ujf-grenoble.fr/%7Epanchish/05ensl.pdf

[R] P. Ribenboim, *13 lectures on Fermat's Last Theorem*, Springer Verlag 1979.

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

[Sk] Nils-Peter Skoruppa, *Théorie de Galois et Théorie Algébrique des Nombres*, Notes d'un cours de Maîtrise, UFR de Mathématiques et Informatique, Université de Bordeaux I, 2000.
http ://wotan.algebra.math.uni-siegen.de/∼countnumber/D/

Université P. et M. Curie (Paris VI),
Deuxième semestre 2007/2008

Michel Waldschmidt
date de mise à jour: 10/06/2008

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

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

Huitième fascicule : 07/04/2008

5 Théorie analytique des nombres

Dans cette partie nous nous intéressons à la répartition des nombres premiers. On doit à Euler (1737) la démonstration du fait que la série

$$\sum_p \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \cdots$$

diverge.

Pour $x > 0$ on désigne par $\pi(x)$ le nombre de nombres premiers inférieurs ou égaux à x :

$$\pi(x) = \sum_{p \le x} 1. \tag{5.1}$$

Ainsi $\pi(10) = 4$, $\pi(100) = 25$, $\pi(1000) = 168$, $\pi(10\,000) = 1229$.

Le théorème des nombres premiers, conjecturé par Gauss en 1792, et par Legendre en 1798, a été démontré par Hadamard et de la Vallée Poussin en 1896. Il s'énonce :

Théorème 5.2 (Théorème des nombres premiers)**.** *Pour $x \to \infty$ on a*

$$\pi(x) \sim \frac{x}{\log x}.$$

Une approximation de $\pi(x)$ numériquement meilleure que (mais asymptotiquement équivalente à) $x/\log x$ est donnée par la fonction *logarithme intégral*

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t}.$$

Des estimations plus faibles étaient dues à Tchébychev (1851) :

$$0,921\cdots \frac{x}{\log x} \le \pi(x) \le 0,105\cdots \frac{x}{\log x}$$

pour $x \ge 30$. Nous établirons un tel encadrement (avec des constantes un peu moins précises) par des méthodes élémentaires. Ensuite nous introduirons la fonction zêta de Riemann pour présenter certains des arguments conduisant au théorème des nombres premiers.

Enfin nous étudierons les fonctions arithmétiques et leur produit de convolution.

On trouvera dans [T] des références aux résultats uniformes suivants

$$\prod_{p\le n} p \le 3^n \quad \text{pour tout entier } n \ge 2$$

et

$$\frac{x}{\log x}\left(1+\frac{1}{2\log x}\right) \le \pi(x) \le \frac{x}{\log x}\left(1+\frac{3}{2\log x}\right) \quad \text{pour tout } x \ge 52.$$

5.1 Méthodes élémentaires

On définit des fonctions arithmétiques $\pi(x)$, $\theta(x)$ et $\psi(x)$ (Tchébychev) et Λ (*fonction de von Mangoldt*) par

$$\pi(x) = \sum_{p\le x} 1, \qquad \theta(x) = \sum_{p\le x} \log p, \qquad \Psi(x) = \sum_{p^m \le x} \log p,$$

$$\Lambda(n) = \begin{cases} \log p & \text{si } n = p^m \text{ avec } p \text{ premier} \\ 0 & \text{si } n \text{ n'est pas une puissance d'un nombre premier.} \end{cases}$$

Ainsi

$$\psi(x) = \sum_{n\le x} \Lambda(n) = \sum_{k=1}^{\infty} \theta(x^{1/k}).$$

La somme est finie : les termes sont nuls pour k tel que $2^k > x$.

Lemme 5.3. *On a*

$$\pi(x) \sim \frac{x}{\log x} \iff p_n \sim n\log n.$$

De plus les deux conditions suivantes sont équivalentes :
(i) Il existe deux constantes c_1 et c_2 telles que, pour tout $n \ge 2$,

$$c_1 \frac{x}{\log x} \le \pi(x) \le c_2 \frac{x}{\log x}$$

(ii) Il existe deux constantes c_3 et c_4 telles que, pour tout $n \ge 2$,

$$c_3 n\log n \le p_n \le c_4 n \log n.$$

Démonstration. Les détails de la démonstration (facile) sont laissés en exercice, l'idée est d'utiliser la relation $\pi(p_n) = n$ qui résulte de la définition et permet d'établir

$$\pi(x) \sim \frac{x}{\log x} \iff n \sim \frac{p_n}{\log p_n} \iff p_n \sim n\log n.$$

□

Lemme 5.4. *On a*

$$\pi(x) \sim \frac{x}{\log x} \iff \theta(x) \sim x.$$

De plus les deux conditions suivantes sont équivalentes :
(i) Il existe deux constantes c_1 et c_2 telles que, pour tout $n \geq 2$,

$$c_1 \frac{x}{\log x} \leq \pi(x) \leq c_2 \frac{x}{\log x}$$

(ii) Il existe deux constantes c_5 et c_6 telles que, pour tout $n \geq 2$,

$$c_5 x \leq \theta(x) \leq c_6 x.$$

Démonstration. On a

$$\theta(x) = \sum_{p \leq x} \log p \leq \log x \sum_{p \leq x} 1 = \pi(x) \log x.$$

De l'autre côté pour $2 \leq y \leq x$ on a

$$\pi(x) - \pi(y) = \sum_{y < p \leq x} 1 \leq \frac{1}{\log y} \sum_{y < p \leq x} \log p = \frac{1}{\log y} \big(\theta(x) - \theta(y)\big)$$

donc

$$\pi(x) \leq \frac{\theta(x)}{\log y} + \pi(y) \leq \frac{\theta(x)}{\log y} + y.$$

On prend $y = x/(\log x)^2$:

$$\pi(x) \leq \frac{\theta(x)}{\log x - 2 \log\log x} + \frac{x}{(\log x)^2}. \tag{5.5}$$

Le lemme 5.4 en résulte.

□

Lemme 5.6. *On a l'équivalence entre les deux assertions suivantes,*

$$\psi(x) \sim x \quad \textit{pour } x \to \infty \qquad \Longleftrightarrow \quad \theta(x) \sim x \quad \textit{pour } x \to \infty \quad .$$

De plus les deux conditions suivantes sont équivalentes :
(i) Il existe deux constantes c_7 et c_8 telles que, pour tout $n \geq 2$,

$$c_7 x \leq \psi(x) \leq c_8 x$$

(ii) Il existe deux constantes c_5 et c_6 telles que, pour tout $n \geq 2$,

$$c_5 x \leq \theta(x) \leq c_6 x.$$

Démonstration. L'inégalité $\theta(x) \leq \psi(x)$ est évidente. De l'autre côté

$$\psi(x) = \theta(x) + \theta(\sqrt{x}) + \theta(\sqrt[3]{x}) + \cdots + \theta(\sqrt[N]{x})$$

où N est le plus grand entier tel que $X \geq 2^N$. Comme $\theta(\sqrt[m]{x}) \leq \theta(x)$ pour $m \geq 2$, on en déduit

$$\psi(x) \leq \theta(x) + \theta(\sqrt{x}) \frac{\log x}{\log 2}.$$

Le lemme 5.6 en résulte.

□

Nous allons donner une démonstration élémentaire du résultat suivant.

Proposition 5.7. *On a, pour tout $x \geq 2$,*

$$\theta(x) \leq 2x \log 4.$$

La démonstration utilise le lemme suivant.

Lemme 5.8. *On a, pour $n \geq 2$,*

$$2^n \leq \binom{2n}{n} \leq 4^n.$$

Démonstration. L'inégalité de droite provient du développement de $(1+1)^{2n}$, celle de gauche de la majoration

$$\frac{n+k}{k} \geq 2 \quad \text{pour} \quad 1 \leq k \leq n.$$

□

Démonstration de la proposition 5.7. Chaque nombre premier p dans l'intervalle $n \leq p \leq 2n$ divise

$$\binom{2n}{n} = \frac{2n(2n-1)\cdots(n+1)}{n(n-1)\cdots 1}.$$

Donc

$$4^n \geq \binom{2n}{n} \geq \prod_{n \leq p \leq 2n} p.$$

Par conséquent

$$n \log 4 \geq \theta(2n) - \theta(n).$$

Ainsi

$$\theta(2^m) = \sum_{k=0}^{m-1} \big(\theta(2^{k+1}) - \theta(2^k)\big) \leq \sum_{k=0}^{m-1} 2^k \log 4 = (2^m - 1) \log 4.$$

Pour $x \geq 1$, soit m l'entier tel que $2^m \leq x < 2^{m+1}$; alors

$$\theta(x) \leq \theta(2^{m+1}) \leq 2^{m+1} \log 4 \leq 2x \log 4.$$

□

De la proposition 5.7 jointe à l'inégalité 5.5 on déduit

$$\pi(x) \leq \big(2 \log 4 + o(1)\big)x.$$

Voici maintenant une démonstration élémentaire de l'inégalité dans l'autre sens :

Proposition 5.9. *Il existe une constante $C > 0$ telle que*

$$\pi(x) \geq C \frac{x}{\log x}$$

pour tout $x \geq 2$.

On utilise le lemme bien connu suivant :

Lemme 5.10. *On a*

$$v_p(n!) = \sum_{1 \leq m \leq (\log n)/(\log p)} \left[\frac{n}{p^m} \right].$$

Démonstration. Pour chaque p et chaque $m \geq 1$ on compte le nombre d'entiers dans l'intervalle $1 \leq k \leq n$ divisibles par p^m.

□

Lemme 5.11. *On a*

$$v_p \binom{2n}{n} \leq \frac{\log(2n)}{\log p}.$$

Démonstration. On a, d'après le lemme 5.10,

$$v_p \binom{2n}{n} = v_p(2n)! - 2v_p(n!) = \sum_{m \geq 1} \left[\frac{2n}{p^m} \right] - 2 \left[\frac{n}{p^m} \right].$$

Pour $u \in \mathbf{R}$ on a

$$\begin{cases} [2u] = 2[u], & \{2u\} = 2\{u\} & \text{si } 0 \leq \{u\} < 1/2, \\ [2u] = 2[u] + 1, & \{2u\} = 2\{u\} - 1 & \text{si } 1/2 \leq \{u\} < 1. \end{cases}$$

En particulier $[2u] - 2[u] = 0$ pour $0 \leq u < 1/2$. Les m tels que $2n \leq p^m$ ne contribuent donc pas. Donc on restreint la somme à $p^m < 2n$ et pour $u = n/p^m$ on majore $[2u] - 2[u]$ par 1. Ainsi

$$v_p \binom{2n}{n} \leq \sum_{\substack{m \geq 1 \\ p^m \leq 2n}} 1 = \left[\frac{\log(2n)}{\log p} \right] \leq \frac{\log(2n)}{\log p}.$$

□

Démonstration de la proposition 5.9. Les facteurs premiers du coefficient binomial $\binom{2n}{n}$ sont majorés par $2n$:

$$\binom{2n}{n} = \prod_{p \leq 2n} p^{v_p\left(\binom{2n}{n}\right)}.$$

Du lemme 5.11 on déduit

$$\binom{2n}{n} = \prod_{p \leq 2n} p^{\log(2n)/\log p} \leq (2n)^{\sum_{p \leq 2n} 1} = (2n)^{\pi(2n)},$$

donc (lemme 5.8)

$$n \log 2 \leq \log \binom{2n}{n} \leq \pi(2n) \log(2n).$$

Soit $x \geq 2$ est soit $n \geq 1$ tel que $2n \leq x < 2(n+1)$. On obtient

$$\pi(x) \geq \pi(2n) \geq \frac{n \log 2}{\log(2n)} \geq \left(\frac{x}{2} - 1 \right) \frac{\log 2}{\log x},$$

d'où

$$\pi(x) \geq \left(\frac{1}{2}\log 2 + o(1)\right)\frac{x}{\log x}\cdot$$

□

Voici deux estimations dues à Mertens :

Proposition 5.12. *On a, pour $x \to \infty$,*

$$\sum_{p\leq x}\frac{\log p}{p} = \log x + O(1).$$

De plus il existe une constante $C > 0$ telle que pour $x \to \infty$,

$$\sum_{p\leq x}\frac{1}{p} = \log\log x + C + O(1/\log x).$$

La démonstration repose sur une comparaison entre sommes et intégrales.

Lemme 5.13. *Soit f une fonction C^1 sur un intervalle entier $[M, N]$ avec $M \geq N \geq 1$. Alors*

$$\sum_{n=M+1}^{N} f(n) = \int_M^N f(t)dt + \int_M^N (t - [t])f'(t)dt.$$

Le lemme 5.13 est un corollaire du résultat suivant :

Lemme 5.14 (Lemme d'Abel)**.** *Soit f une fonction C^1 sur un intervalle $[y, x]$ avec $x > y \geq 1$ et soit $(a_n)_{n\geq 1}$ une suite de nombres complexes. On pose*

$$A(x) = \sum_{n\leq x} a_n.$$

Alors

$$\sum_{y<n\leq x} a_n f(n) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)dt.$$

Démonstration du lemme 5.13. On utilise le lemme 5.14 avec $a_n = 1$ pour tout n, donc $A(t) = [t]$, et $y = M$, $x = N$:

$$\sum_{n=M+1}^{N} f(n) = Nf(N) - Mf(M) - \int_M^N [t]f'(t)dt.$$

On utilise ensuite l'égalité

$$Nf(N) - Mf(M) = \int_M^N f(t)dt + \int_M^N tf'(t)dt,$$

qui s'obtient en intégrant par parties.

□

Avant de démontrer ce lemme 5.14 d'Abel nous déduisons du lemme 5.13 quelques conséquences. On définit la *constante d'Euler* par l'intégrale convergente

$$\gamma = 1 - \int_1^\infty (t - [t]) \frac{dt}{t^2}.$$

Corollaire 5.15. *Pour $N \geq 2$ on a*

$$\left| \sum_{n \leq N} \frac{1}{n} - \log N - \gamma \right| \leq \frac{1}{N}.$$

Démonstration. Pour $f(t) = 1/t$ et $M = 1$, en ajoutant $n = 1$ au deuxième membre de la conclusion du lemme 5.13 on trouve

$$\sum_{n=1}^{N} \frac{1}{n} = 1 + \int_1^N \frac{dt}{t} - \int_1^N (t - [t]) \frac{dt}{t^2}.$$

Alors

$$\sum_{n=1}^{N} \frac{1}{n} = \log N + \gamma + \int_N^\infty (t - [t]) \frac{dt}{t^2},$$

et

$$0 < \int_N^\infty (t - [t]) \frac{dt}{t^2} \leq \int_N^\infty \frac{dt}{t^2} = \frac{1}{N}.$$

□

Corollaire 5.16. *Il existe une constante absolue c telle que, pour $x \to \infty$ on ait*

$$\sum_{n \leq x} \log n = x \log x - x + O(\log x) \quad \textit{quand } x \to \infty.$$

La *formule de Stirling* est un peu plus précise :

$$n! \sim n^n e^{-n} \sqrt{2\pi n}.$$

Démonstration du corollaire 5.16. On utilise le lemme 5.13 avec $f(t) = \log t$, $N = [x]$. On a

$$\sum_{2 \leq n \leq x} f(n) = \sum_{1 \leq n \leq x} \log n = \log\big([x]!\big),$$

$$\int_1^N f(t)dt = \int_1^N (\log t)dt = N \log N - N + 1$$

et

$$\int_1^N (t - [t]) f'(t)dt = \int_1^N (t - [t]) \frac{dt}{t} = O(\log N),$$

d'où

$$\log\big([x]!\big) = [x] \log x - x + 1 - \int_1^x \frac{[t] - t}{t} dt = x \log x - x + O(\log x).$$

□

Démonstration du lemme d'Abel 5.14. Pour $n \leq t < n+1$ on a

$$A(t) = A(n) = \sum_{k=0}^{n} a_k.$$

Alors

$$\int_n^{n+1} A(t)f'(t)dt = A(n)\int_n^{n+1} f'(t)dt = A(n)\big(f(n+1) - f(n)\big).$$

Supposons $x = N$ et $y = M$ entiers. On a

$$\begin{aligned}
\int_M^N A(t)f'(t)dt &= \sum_{n=M}^{N-1}\int_n^{n+1} A(t)f'(t)dt = \sum_{n=M}^{N-1} A(n)\big(f(n+1) - f(n)\big) \\
&= \sum_{n=M+1}^{N} A(n-1)f(n) - \sum_{n=M}^{N-1} A(n)f(n) \\
&= -\sum_{n=M+1}^{N} f(n)\big(A(n) - A(n-1)\big) + f(N)A(N) - f(M)A(M) \\
&= -\sum_{n=M+1}^{N} a_n f(n) + f(N)A(N) - f(M)A(M).
\end{aligned}$$

La formule est démontrée quand x et y sont entiers. Quand x n'est pas entier il suffit d'ajouter

$$\int_{[x]}^{x} A(t)f'(t)dt = A\big([x]\big)\big(f(x) - f\big([x]\big)\big)$$

avec $A\big([x]\big) = A(x)$. De même quand y n'est pas entier. □

Démonstration de la proposition 5.12. On écrit

$$\log[x]! = \sum_{p \leq x} v_p([x]!)\log p$$

et (lemme 5.10)

$$v_p[x]! = \sum_{m \geq 1}\left[\frac{x}{p^m}\right].$$

Dans le membre de droite le terme principal est obtenu pour $m = 1$, il est équivalent à x/p, ce qui va nous permettre de vérifier

$$\log[x]! \sim x\sum_{p \leq x}\frac{\log p}{p}.$$

Pour obtenir la première partie de la proposition 5.12, il suffira alors d'utiliser le corollaire 5.16.

On a

$$\log[x]! = \sum_{p\le x}\sum_{m\ge 1}\left[\frac{x}{p^m}\right]\log p,$$
$$= x\sum_{p\le x}\frac{\log p}{p} + \sum_{p\le x}\left(\left[\frac{x}{p}\right]-\frac{x}{p}\right)\log p + \sum_{p\le x}\sum_{m\ge 2}\left[\frac{x}{p^m}\right]\log p.$$

Or

$$-1 \le \left[\frac{x}{p}\right]-\frac{x}{p}\le 0$$

et (proposition 5.7)

$$\sum_{p\le x}\log p = \theta(x) = O(x).$$

Ensuite

$$\sum_{m\ge 2}\left[\frac{x}{p^m}\right] \le x\sum_{m\ge 2}\frac{1}{p^m} = x\cdot\frac{1/p^2}{1-(1/p)} = x\cdot\frac{1}{p(p-1)},$$

donc

$$\sum_{p\le x}\sum_{m\ge 2}\left[\frac{x}{p^m}\right]\log p \le x\sum_{p\le x}\frac{\log p}{p(p-1)} \le x\sum_{n\ge 2}\frac{\log n}{n^2} = O(x).$$

Finalement

$$\sum_{p\le x}\frac{\log p}{p} = \log x + O(1).$$

Pour démontrer la seconde partie de la proposition 5.12, on utilise le lemme 5.14 d'Abel avec $f(t) = 1/\log t$, $y = 2$ et

$$a_n = \begin{cases}(\log p)/p & \text{si } n = p \text{ est premier,}\\ 0 & \text{si } n \text{ est composé.}\end{cases}$$

On a

$$\sum_{1\le n<x} a_n f(n) = \sum_{p\le x}\frac{1}{p},$$

$$A(x) = \sum_{p\le x}\frac{\log p}{p} = \log x + O(1),$$

$$A(x)f(x) = \sum_{p\le x}\frac{\log p}{p}\cdot\frac{1}{\log x} = 1 + O(1/\log x),$$

$$\int_y^x A(t)f'(t)dt = -\int_2^x A(t)\frac{dt}{t(\log t)^2} = -\int_2^x\frac{dt}{t\log t} - \int_2^x\big(A(t)-\log t\big)\frac{dt}{t(\log t)^2},$$

et

$$\int_2^x\frac{dt}{t\log t} = \log\log x - \log\log 2.$$

Donc

$$\sum_{p\leq x}\frac{1}{p}=\log\log x+C+O(1/\log x).$$

□

5.2 La fonction zêta de Riemann

La démonstration par Hadamard et de la Vallée Poussin du théorème 5.2 des nombres premiers repose sur l'analyse complexe et la fonction zêta de Riemann. La série $\sum_{n\geq 1} n^{-s}$ 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) :

$$\zeta(s)=\sum_{n\geq 1}\frac{1}{n^s}\cdot$$

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.

5.2.1 Produit Eulérien de la fonction zêta de Riemann

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 5.17 (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. Soit X un nombre entier suffisamment grand. 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

$$\left|\zeta(s) - \prod_{p\leq X} \frac{1}{1-p^{-s}}\right| = \left|\sum_{n\notin\mathcal{N}(X)} \frac{1}{n^s}\right| \leq \sum_{n>X} \left|\frac{1}{n^s}\right| = \sum_{n>X} \frac{1}{n^\sigma}.$$

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 $|u| < 1$,

$$\log(1-u) = -\sum_{m\geq 1} \frac{u^m}{m}.$$

On remplace u par p^{-s} :

$$\log(1-p^{-s}) = -\sum_{m\geq 1} \frac{p^{-ms}}{m}$$

et on trouve, pour $\Re s > 1$,

$$\zeta(s) = \exp\left(\sum_p \sum_{m\geq 1} \frac{1}{mp^{ms}}\right). \tag{5.18}$$

Donc $\zeta(s) \neq 0$ pour $\Re s > 1$. □

On écrit (5.18) sous la forme [5]

$$\log \zeta(s) = \sum_p \sum_{m\geq 1} \frac{1}{mp^{ms}}.$$

En dérivant, on obtient le développement en série de la dérivée logarithmique de ζ dans ce demi plan.

Corollaire 5.19. *La série*

$$\sum_p \sum_{m\geq 1} \frac{1}{mp^{ms}}$$

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 von Mangoldt (cf. § 5.1).

[5] Quand f et g sont deux fonctions complexes, on écrit $f = \log g$ pour signifier $g = e^f$.

Théorème 5.20 (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* (voir Corollaire 5.15) :

$$\gamma = \lim_{N \to \infty} \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{N} - \log N.$$

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 5.2 des nombres premiers consiste à montrer que la fonction ζ ainsi prolongée ne s'annule pas dans un ouvert contenant le demi plan fermé $\Re s \geq 1$. Plus précisément *il existe une constante* $A > 0$ *telle que la fonction* ζ*, ainsi prolongée, ne s'annule pas dans le domaine*

$$1 - \frac{A}{\log |\Im s|} < \Re s < 1.$$

Nous utiliserons dans la section 5.2.2 l'énoncé suivant :

Théorème 5.21. *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 $\Re s = 1$.

5.2.2 Démonstration du théorème des nombres premiers

Nous avons vu que le théorème 5.2 des nombres premiers était équivalent à $\theta(x) \sim x$ pour $x \to \infty$. Nous allons montrer que cette équivalence résulte de l'énoncé suivant

Proposition 5.22. *L'intégrale*

$$F(0) := \int_1^\infty \big(\theta(t) - t\big)\frac{dt}{t^2}$$

converge.

Démonstration de l'équivalence $\theta(x) \sim x$ comme conséquence de la proposition 5.22. Montrons d'abord, en utilisant la proposition 5.22, que l'on a

$$\limsup_{x\to\infty} \frac{\theta(x)}{x} \leq 1.$$

On raisonne par l'absurde : si cette limite sup est > 1, il existe $\eta > 1$ et il existe une suite x_n tendant vers l'infini tels que $\theta(x_n) > (1+2\eta)x_n$ pour tout n. Comme la fonction θ est croissante , pour $x_n \leq t \leq (1+\eta)x_n$ on a $\theta(t) \geq \theta(x_n) > (1+2\eta)x_n$ et $\theta(t) - t \geq \eta x_n$,

$$\frac{x_n}{t^2} \geq \frac{1}{x_n}\cdot\frac{1}{(1+\eta)^2}, \geq \frac{1}{x_n}\cdot\frac{1}{1+\eta},$$

donc dans cet intervalle

$$\frac{\theta(t)-t}{t^2} \geq \frac{\eta x_n}{t^2} \geq \frac{\eta}{x_n(1+\eta)}.$$

Donc

$$\int_{x_n}^{x_n(1+\eta)} \big(\theta(t)-t\big)\frac{dt}{t^2} \geq x_n \cdot \frac{\eta}{2+\eta}\cdot\frac{\eta}{x_n} = \frac{\eta^2}{2+\eta},$$

donc l'intégrale ne converge pas, contrairement à ce que donne la proposition 5.22.

Le même argument montre que

$$\liminf_{x\to\infty} \frac{\theta(x)}{x} \geq 1.$$

Par conséquent la proposition 5.22 implique $\lim_{n\to\infty} \theta(x)/x = 1$. □

Remarque. Le fait que $\theta(x)$ soit équivalent à x ne suffit pas à démontrer la proposition 5.22. Si on définit un fonction $\epsilon(t)$ par $\theta(t) = t\big(1+\epsilon(t)\big)$, l'équivalence $\theta(x) \sim x$ signifie que $\epsilon(t)$ tend vers 0 quand t tend vers l'infini, mais cela ne suffit pas à assurer que l'intégrale $\int_1^\infty \epsilon(t)dt/t$ converge. Par exemple l'intégrale $\int_1^\infty dt/t\log t$ ne converge pas.

Pour s complexe de partie réelle > 0, posons

$$F(s) = \int_1^\infty \big(\theta(t)-t\big)\frac{dt}{t^{s+1}}.$$

Le changement de variable $t = e^u$ dans l'intégrale définissant F montre que, pour $\Re s > 1$ on a

$$F(s) = \int_0^\infty \big(\theta(e^u) - e^u\big)\frac{e^u du}{e^{u(s+1)}} = \int_0^\infty h(u)e^{-us}du$$

avec $h(u) = \theta(u) - e^u$. Rappelons que $|e^{-us}| = e^{-u\Re s}$. Donc pour $\Re s > 1$ l'intégrale définissant F converge, et F est analytique dans ce demi–plan.

Proposition 5.23. *La fonction F est analytique dans le demi plan ouvert $\Re s > 1$ et se prolonge en une fonction analytique sur un ouvert contenant le demi plan fermé $\Re s \geq 1$.*

L'énoncé suivant (que nous ne démontrerons pas) dû à Ingham (1935) permet de déduire de la proposition 5.23 que l'intégrale converge en $s = 0$, ce qui est la proposition 5.22.

Théorème 5.24 (Ingham)**.** *Soit f une fonction mesurable bornée sur $[1, \infty)$. On suppose que la fonction holomorphe*

$$F(s) = \int_1^\infty \frac{f(t)}{t^s} dt$$

définie pour $\Re s > 1$ admet un prolongement analytique au voisinage du demi–plan fermé $\Re s \geq 1$. Alors

$$\lim_{T \to \infty} \int_1^T \frac{f(t)}{t} dt = F(1).$$

La démonstration de la proposition 5.23 utilisera le lemme auxiliaire suivant.

Lemme 5.25. *La fonction définie pour $\Re s > 1$ par*

$$f(s) = \frac{\zeta'(s)}{\zeta(s)} + \sum_p \frac{\log p}{p^s},$$

se prolonge en une fonction holomorphe dans $\Re s > 1/2$.

Démonstration du lemme 5.25. Comme

$$\frac{\zeta'(s)}{\zeta(s)} = -\sum_p \sum_{m \geq 1} \frac{\log p}{p^{ms}}$$

on a

$$f(s) = -\sum_p \sum_{m \geq 2} \frac{\log p}{p^{ms}}.$$

Pour tout $\sigma_0 > 1/2$ la série à droite converge normalement dans $\Re s \geq \sigma_0$. □

Démonstration de la proposition 5.23. On écrit, pour $\Re s > 1$,

$$F(s) = \sum_{n \geq 1} \int_n^{n+1} \frac{\theta(t)}{t^{s+1}} dt - \int_1^\infty \frac{dt}{t^s}.$$

On a

$$\int_1^\infty \frac{dt}{t^s} = \frac{1}{s-1}$$

et

$$\int_n^{n+1} \frac{\theta(t)}{t^{s+1}} dt = \theta(n) \int_n^{n+1} \frac{dt}{t^{s+1}} = \frac{\theta(n)}{s} \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right),$$

Donc

$$\begin{aligned} F(s) &= \frac{1}{s}\sum_{n\geq 1}\left(\frac{1}{n^s}-\frac{1}{(n+1)^s}\right)\theta(n)-\frac{1}{s-1} \\ &= \frac{1}{s}\sum_{n\geq 1}\frac{1}{n^s}\big(\theta(n)-\theta(n-1)\big)-\frac{1}{s-1} \\ &= \frac{1}{s}\sum_{p}\frac{\log p}{p^s}-\frac{1}{s-1} \\ &= -\frac{1}{s}\cdot\frac{\zeta'(s)}{\zeta(s)}+\frac{f(s)}{s}-\frac{1}{s-1}, \end{aligned}$$

avec la fonction f introduite au lemme 5.25.

La fonction ζ a un pôle simple en $s=1$, donc ζ'/ζ a un pôle simple de résidu -1 en $s=1$, ce qui signifie que

$$\frac{\zeta'(s)}{\zeta(s)}+\frac{1}{s-1}$$

se prolonge en une fonctions holomorphe en $s=1$. On utilise le théorème 5.21 : la fonction ζ ne s'annule pas sur la demi-droite $\Re s=1$. Donc la fonction $\frac{\zeta'(s)}{\zeta(s)}+\frac{1}{s-1}$ se prolonge en une fonction holomorphe dans un voisinage ouvert de $\Re s\geq 1$. On conclut en observant que

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

est analytique dans $\mathbf{C}\setminus\{0\}$.

□

5.2.3 Equation fonctionnelle de la fonction zêta

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 5.26. *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 5.27 (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. (5.1) 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 [6]

$$\zeta(s) = \frac{2^{s-1}\pi^s}{e^{((\gamma/2)+1)s}(s-1)\Gamma(1+(s/2))} \prod_{\varrho} \left(1 - \frac{s}{\varrho}\right) e^{s/\varrho}$$

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 5.27 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*

$$\theta(u) = \sum_{n\in\mathbf{Z}} e^{-\pi u n^2}$$

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 5.27 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 5.28 (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].

[6] 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 $\leq T$.

5.3 Fonctions arithmétiques

5.3.1 Fonctions additives et multiplicatives

Une fonction arithmétique est une application de $\mathbf{N} \setminus \{0\} = \mathbf{N}_{>0}$ dans $\mathbf{C}$. Il revient au même de se donner une suite de nombres complexes $(f(n))_{n\geq 1}$: nous en avons donc déjà rencontré de nombreux exemples.

Une fonction arithmétique $f : \mathbf{N}_{>0} \to \mathbf{C}$ est dite *multiplicative* si $f(1) = 1$ et si, pour tout couple (m, n) d'entiers positifs premiers entre eux, on a

$$f(mn) = f(m)f(n).$$

Si cette relation est vraie pour tout couple (m, n) d'entiers positifs, on dit que la fonction est *complètement multiplicative.*

On dit aussi qu'une fonction arithmétique $g : \mathbf{N}_{>0} \to \mathbf{C}$ est *additive* si elle satisfait

$$g(mn) = g(m) + g(n) \quad \text{quand } \mathrm{pgcd}(m, n) = 1,$$

et qu'elle est *complètement additive* si $g(mn) = g(m) + g(n)$ pour tout couple $(m, n) \in \mathbf{N}_{>0}$.

Une fonction complètement multiplicative n'est autre que la donnée, pour chaque nombre premier p, d'un nombre complexe u_p. La valeur en un entier n de la fonction f complètement multiplicative vérifiant $f(p) = u_p$ est alors donnée par la décomposition en facteurs premiers de n :

$$f(p_1^{\alpha_1} \cdots p_s^{\alpha_s}) = u_{p_1}^{\alpha_1} \cdots u_{p_s}^{\alpha_s},$$

avec $f(1) = 1$.

De même l'unique fonction g complètement additive satisfaisant $g(p) = u_p$ pour p premier est donnée par

$$g(p_1^{\alpha_1} \cdots p_s^{\alpha_s}) = \alpha_1 u_{p_1} + \cdots + \alpha_s u_{p_s}.$$

Une fonction f multiplicative (resp. g additive) est déterminée par ses valeurs aux puissances de nombres premiers : si pour chaque entier de la forme p^m, avec p premier et m entier ≥ 1, on se donne un nombre complexe $v_{p,m}$, l'unique fonction multiplicative f (resp. additive g) prenant au point p^m la valeur $v_{p,m}$ (pour tout couple (p, m)) est définie par

$$f(p_1^{\alpha_1} \cdots p_s^{\alpha_s}) = v_{p_1,\alpha_1} \cdots v_{p_s,\alpha_s} \quad \big(\text{ resp. } \quad g(p_1^{\alpha_1} \cdots p_s^{\alpha_s}) = v_{p_1,\alpha_1} + \cdots + v_{p_s,\alpha_s} \big).$$

Le produit (resp. la somme) de fonctions multiplicatives ou complètement multiplicatives (resp. additives ou complètement additives) l'est encore.

Exemples (Fonctions complètement multiplicatives ou complètement additives)**.** Soient f et g deux fonctions arithmétiques reliées par $f = e^g$. Si g est complètement additive, alors f est complètement multiplicative. La réciproque est vraie si on suppose par exemple que g est à valeurs réelles. Noter que la fonction

$$g : n \longrightarrow v_p(n) \log 2 + 2i\pi$$

n'est pas additive alors que son exponentielle

$$f : n \longrightarrow 2^{v_p(n)}$$

est complètement multiplicative.
La fonction δ définie par

$$\delta(n) = \begin{cases} 1 & \text{si } n = 1, \\ 0 & \text{si } n \geq 2, \end{cases}$$

est complètement multiplicative.
Pour tout nombre complexe s la fonction f définie par $f(n) = n^s$ est complètement multiplicative. Pour $s = 0$ c'est la fonction arithmétique constante égale à 1, que l'on note $\mathbf{1}$, tandis que pour $s = 1$ c'est la fonction identité, que l'on note j. Pour $n \geq 1$ on a

$$\mathbf{1}(n) = 1 \quad \text{et} \quad j(n) = n.$$

Soit p un nombre premier et soit s un nombre complexe. La fonction $n \to p^{v_p(n)s}$ est complètement multiplicative et la fonction $n \to sv_p(n)$ est complètement additive.
La fonction

$$\Omega(n) = \sum_{p^m \| n} m,$$

qui compte le nombre de diviseurs de n avec multiplicités, est complètement additive ; la notation $p^m \| n$ signifie que m est la plus grande puissance de p qui divise n (ainsi $m = v_p(n)$), autrement dit p^m divise n et p^{m+1} ne divise pas n. La fonction Ω est la fonction complètement additive déterminée par

$$\Omega(p) = 1 \quad \text{pour } p \text{ premier.}$$

Si f est une fonction complètement multiplicative à valeurs > 0, pour tout $s \in \mathbf{C}$ la fonction f^s est aussi complètement multiplicative, et la fonction $\log f$ est complètement additive.
Si f est une fonction complètement additive et si s est un nombre complexe, la fonction $n \to sf(n)$ est complètement additive.

Exemples (Fonctions multiplicatives ou additives)**.** Évidemment toute fonction complètement multiplicative (resp. complètement additive) est multiplicative (resp. additive).
Soient f et g deux fonctions arithmétiques reliées par $f = e^g$. Si g est additive, alors f est multiplicative. La réciproque est vraie si on suppose par exemple que g est à valeurs réelles.
La fonction

$$\omega(n) = \sum_{p|n} 1$$

qui compte le nombre de diviseurs premiers de n sans multiplicités est additive. Elles est déterminée par

$$\omega(p^m) = 1 \quad (p \text{ premier}, m \geq 1).$$

Le nombre de diviseurs de n, traditionnellement noté $\tau(n)$,

$$\tau(n) = \sum_{d|n} 1,$$

est une fonction multiplicative, déterminée par

$$\tau(p^m) = m + 1 \quad (p \text{ premier}, m \geq 1).$$

Plus généralement pour $k \in \mathbf{C}$ on définit

$$\sigma_k(n) = \sum_{d|n} d^k.$$

Ainsi $\tau = \sigma_0$. On écrit aussi σ au lieu de σ_1. La fonction σ_k est la fonction multiplicative déterminée par

$$\sigma_k(p^m) = 1 + p^k + \cdots + p^{mk} = \frac{p^{k(m+1)} - 1}{p^k - 1} \quad (p \text{ premier}, m \geq 1).$$

L'indicatrice d'Euler

$$\varphi(n) = \sum_{\substack{1 \leq k \leq n \\ \text{pgcd}(k,n)=1}} 1$$

est la fonction multiplicative déterminée par

$$\varphi(p^m) = p^{m-1}(p-1) \quad (p \text{ premier}, m \geq 1).$$

La *fonction de Möbius* μ, définie par

$$\mu(n) = \begin{cases} (-1)^{\omega(n)} & \text{si } n \text{ est sans facteur carré,} \\ 0 & \text{sinon,} \end{cases}$$

est multiplicative, déterminée par

$$\mu(p^m) = \begin{cases} -1 & \text{si } m = 1, \\ 0 & \text{si } m \geq 2, \end{cases} \quad (p \text{ premier}, m \geq 1).$$

La *fonction de von Mangoldt* Λ (cf. § 5.1) n'est ni additive ni multiplicative.

5.3.2 Séries de Dirichlet formelles

À une fonction arithmétique f on associe une série de Dirichlet formelle

$$D(f;s) = \sum_{n=1}^{\infty} f(n) n^{-s} = f(1) + \frac{f(2)}{2^s} + \frac{f(3)}{3^s} + \cdots + \frac{f(n)}{n^s} + \cdots$$

La somme et le produit de deux séries de Dirichlet est une série de Dirichlet, l'unité étant la série constante $D(\delta;s) = 1$. Par exemple la série de Dirichlet associée à la fonction $\mathbf{1}$ est la série définissant la fonction zêta de Riemann. D'après le corollaire 5.19 la série de Dirichlet associée à la fonction de von Mangoldt Λ est $D(\Lambda;s) = -\zeta'(s)/\zeta(s)$.

On définit une loi multiplicative $\star$ sur l'ensemble des fonctions arithmétiques, le *produit de convolution de Dirichlet*, par la condition

$$D(f \star g; s) = D(f;s)D(g;s).$$

Autrement dit la fonction arithmétique $f \star g$ est définie par

$$f \star g(n) = \sum_{d|n} f(d)g(n/d) = \sum_{dd'=n} f(d)g(d').$$

On obtient ainsi une structure d'anneau unitaire commutatif sur l'ensemble des fonctions arithmétiques qui en fait un anneau, noté $\mathcal{A}$, isomorphe à l'anneau des séries de Dirichlet formelles. L'élément unité est δ.

Exemples. Voici un récapitulatif de quelques relations de convolution avec les relations associées en termes de séries de Dirichlet.

$$D(\mathbf{1};s)=\zeta(s), \qquad D(\delta;s)=1, \qquad D(j^k)=\zeta(s-k) \quad (k\in\mathbf{C}),$$

$$\begin{array}{ll} \mathbf{1}\star\mathbf{1}=\tau, & D(\tau;s)=\zeta(s)^2,\\ \mathbf{1}\star j=\sigma, & D(\sigma;s)=\zeta(s)\zeta(s-1),\\ \mathbf{1}\star j^k=\sigma_k, & D(\sigma_k;s)=\zeta(s)\zeta(s-k), \quad (k\in\mathbf{C})\\ \mathbf{1}\star\mu=\delta, & D(\mu;s)=1/\zeta(s),\\ j\star\mu=\varphi, & D(\varphi;s)=\zeta(s-1)/\zeta(s). \end{array}$$

La relation $\delta=1\star\mu$, qui s'écrit aussi

$$\sum_{d|n}\mu(d)=\begin{cases}1 & \text{si } n=1,\\ 0 & \text{si } n\geq 2,\end{cases}$$

signifie que la fonction de Möbius est l'inverse de la fonction $\mathbf{1}$ pour la convolution :

$$g=f\star\mathbf{1} \iff f=g\star\mu.$$

Autrement dit :

Corollaire 5.29 (Formule d'inversion de Möbius)**.** *Soient f et g deux fonctions arithmétiques. Les deux assertions suivantes sont équivalentes.*
(i) Pour tout entier $n\geq 1$, on a

$$g(n)=\sum_{d|n}f(d).$$

(ii) Pour tout entier $n\geq 1$, on a

$$f(n)=\sum_{d|n}\mu(n/d)g(d).$$

Par exemple la relation

$$\sum_{d|n}\varphi(d)=n \quad \text{ pour tout } n\geq 1$$

s'écrit $\varphi\star\mathbf{1}=j$, elle est équivalente à $\varphi=j\star\mu$ qui s'écrit

$$\varphi(n)=\sum_{d|n}\mu(n/d)d \quad \text{ pour tout } n\geq 1$$

Voici deux variantes de la formule d'inversion de Möbius.

Proposition 5.30 (Variante 1 de la formule d'inversion de Möbius)**.** *Soient F et G deux fonctions définies sur $[1,+\infty)$ à valeurs complexes. Les deux assertions suivantes sont équivalentes.*
(i) Pour tout nombre réel $x \geq 1$ on a

$$G(x) = \sum_{n \leq x} F(x/n).$$

(ii) Pour tout nombre réel $x \geq 1$ on a

$$F(x) = \sum_{n \leq x} \mu(n) G(x/n).$$

Comme exemple, en prenant la fonction constante $F(x) = 1$ pour tout x et $G(x) = [x]$, on en déduit

$$\sum_{n \leq x} \mu(n)[x/n] = 1$$

pour tout $x \geq 1$. D'après E. Landau (1909), des formes équivalentes du théorème 5.2 des nombres premiers sont

$$\lim_{n \to \infty} \sum_{n \leq x} \mu(n)/n = 0 \Longleftrightarrow \sum_{n \leq x} \frac{\Lambda(n)}{n} = \log x - \gamma + o(1) \Longleftrightarrow M(x) = o(x),$$

où γ est la constante d'Euler et M la fonction sommatoire de la fonction de Möbius

$$M(x) = \sum_{n \leq x} \mu(n).$$

(voir par exemple [T]).

Proposition 5.31 (Variante 2 de la formule d'inversion de Möbius)**.** *Soient G un groupe multiplicatif et f, g deux applications de $\mathbf{N}_{>0}$ dans G. Les deux assertions suivantes sont équivalentes.*
(i) Pour tout entier $n \geq 1$, on a

$$g(n) = \prod_{d|n} f(d).$$

(ii) Pour tout entier $n \geq 1$, on a

$$f(n) = \prod_{d|n} g(d)^{\mu(n/d)}.$$

Exemple. Prenons pour G le groupe multiplicatif $K(X)^\times$ où K est un corps. Le n-ième polynôme cyclotomique Φ_n a été défini par récurrence grâce à la formule

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

Par conséquent

$$\Phi_n = \prod_{d|n} (X^n - 1)^{\mu(n/d)}.$$

Un élément $f \in \mathcal{A}$ est inversible si et seulement si $f(1) \neq 0$. En effet la solution g au système d'équations

$$\sum_{d|n} f(n/d)g(d) = \delta(n) \quad (n \geq 1)$$

existe si et seulement si $f(1) \neq 1$; dans ce cas elle est donnée par $g(1) = 1/f(1)$, et par récurrence (une fois qu'on connaît la valeur de g pour les entiers $< n$ qui divisent n)

$$g(n) = -f(1)^{-1} \sum_{\substack{d|n \\ d<n}} f(n/d)g(d) \quad (n > 1).$$

La démonstration du Théorème donne plus généralement (voir par exemple [T], § I.2.4, Th. 4) :

Proposition 5.32. *Un élément f de $\mathcal{A}^\times$ est une fonction multiplicative si et seulement si sa série de Dirichlet formelle $D(f, s)$ est développable en un produit Eulérien*

$$D(f; s) = \prod_p \left(1 + \sum_{m=1}^{\infty} f(p^m)p^{-ms}\right).$$

L'inverse g d'une fonction multiplicative f est déterminée par l'identité formelle

$$\left(1 + \sum_{m=1}^{\infty} g(p^m)p^{-ms}\right) \cdot \left(1 + \sum_{m=1}^{\infty} f(p^m)p^{-ms}\right) = 1.$$

On en déduit que les fonctions multiplicatives constituent un sous-groupe du groupe $\mathcal{A}^\times$ des éléments inversibles de l'anneau $\mathcal{A}$: *le produit de convolution de deux fonctions multiplicatives est une fonction multiplicative.*

Proposition 5.33. *La fonction de von Mangoldt Λ, que nous avons définie au § 5.1) est égale à $\mu \star \log$.*

Démonstration. Posons $L = \mu \star \log$. Pour $n \geq 1$ on a

$$L(n) = \sum_{d|n} \mu(d) \log(n/d) = -\sum_{d|n} \mu(d) \log d + \delta(n) \log n = -\sum_{d|n} \mu(d) \log d = -\mu \log \star \mathbf{1}.$$

Cela permet de vérifier, quand m et n sont des entiers positifs premiers entre eux,

$$L(mn) = \delta(n)L(m) + \delta(m)L(n).$$

Il reste à remarquer que la fonction Λ satisfait la même relation pour en déduire par récurrence qu'elle coïncide avec L. □

Exercice. Vérifier, pour $k \in \mathbf{C}$,

$$D(\sigma_k; s) = \sum_{n \geq 1} \frac{\sigma_k(n)}{n^s} = \zeta(s)\zeta(s-k) = \prod_p \left(1 - (p^k + 1)p^{-s} + p^{k-2s}\right)^{-1}.$$

5.3.3 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

$$\chi(a+q) = \chi(a) \quad \text{pour tout } a \in \mathbf{Z} \text{ avec } (a,q) = 1.$$

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 :

$$\psi_{-1}(n) = \begin{cases} 0 & \text{si } p|n, \\ \left(\dfrac{n}{p}\right) & \text{si } (n,p) = 1. \end{cases}$$

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).

[T] G. Tenenbaum, *Introduction à la théorie analytique et probabiliste des nombres*, Institut Élie Cartan, **13**, Chap. I.2.