Théorie algébrique des nombres

Cours de Master 1 enseigné à l'École Polytechnique 2011 – 2019

Gaëtan Chenevier

gaetan.chenevier@math.cnrs.fr

Préambule

Ce cours est une introduction à la théorie algébrique des nombres que j'ai enseignée aux étudiants de troisième année de l'École Polytechnique entre 2011 et 2019 (niveau "master 1"). Qu'ils soient remerciés ici pour cette aventure enrichissante et pour leurs nombreux retours. Le cours ne nécessite pas de prérequis particulier, hormis des notions sur les structures algébriques de base (groupes, anneaux, corps). Dans le second chapitre, nous supposons aussi connue la mesure de Lebesgue sur $\mathbb{R}^n$: son utilisation est intuitive et aurait pu être évitée de manière artificielle, mais nous n'avons pas jugé bon de le faire pour conserver l'élégance des énoncés. Sur la forme, nous disposions de 9 séances de 4h, réparties en 2h de cours et 2h d'exercices, et traitions un chapitre par séance en laissant de côté parfois certains développements inessentiels à l'enchainement du cours. Comme toujours, disposer de plus de temps aurait été le bienvenu ! Les chapitres 1 à 4 peuvent être étudiés de manière indépendante. Le fil conducteur de ce texte est la question suivante :

QUESTION : Soit d un entier ≥ 1, peut-on caractériser les nombres premiers de la forme $x^2 + dy^2$ avec x, y entiers ?

Par exemple, on sait depuis Fermat que les nombres premiers qui sont la somme de deux carrés sont exactement ceux $\equiv 1 \bmod 4$ (cas $d = 1$). De même, Euler avait conjecturé qu'un nombre premier $\neq 5$ est de la forme $x^2 + 5y^2$ si et seulement s'il est $\equiv 1, 9 \bmod 20$, conjecture prouvée plus tard par Lagrange et Gauss. Nous verrons dans ce cours de nombreuses explications et généralisations de ces phénomènes.

Chapitre 1. Un entier de la forme x^2+dy^2 est un "carré modulo d", c'est pourquoi le premier chapitre est consacré à l'étude des carrés de $\mathbb{Z}/N\mathbb{Z}$. Le cas crucial est celui où N est un nombre premier, qu'il est commode d'étudier en introduisant le *symbole de Legendre*. Le résultat principal du premier chapitre est la démonstration de la *loi de réciprocité quadratique*, l'un des plus fameux (et difficile) théorème de Gauss. La démonstration donnée passe par l'étude des propriétés arithmétiques des *sommes de Gauss*. Nous introduisons à cette occasion la notion d'*entier algébrique*, amenée à jouer un rôle central dans la suite du cours. Une autre démonstration, plus élémentaire et astucieuse, due à Eisenstein, est proposée dans les exercices.

Chapitre 2. Le second chapitre, très différent du premier, a pour but d'introduire la *géométrie des nombres*. Inventée par Minkowski, elle consiste à donner une minoration du nombre des points d'un *réseau* de l'espace euclidien $\mathbb{R}^n$ appartenant à une partie convexe donnée, et ce en fonction de leurs volumes. Appliquées à certains réseaux de nature arithmétique, ces estimations ont des conséquences nombreuses et spectaculaires en théorie des nombres, et notamment à la Question ci-dessus. Cette théorie de Minkowski jouera aussi un rôle crucial au chapitre 6. Enfin, d'un point de vue technique, la théorie des réseaux développée dans cette partie nous permettra

de démontrer quelques résultats de base sur les groupes abéliens de type finis, que nous n'avons pas supposé connus.

Chapitre 3. Dans ce troisième chapitre, particulièrement élémentaire, nous exposons la théorie des *formes quadratiques binaires entières*, i.e. les fonctions $\mathbb{Z}^2 \to \mathbb{Z}$ de la forme $(x, y) \mapsto ax^2 + bxy + cy^2$, suivant Lagrange et Gauss (et notamment les *Disquisitionnes Arithmeticae*). Pour tout entier négatif $D \equiv 0, 1 \bmod 4$, nous étudions l'ensemble $\mathrm{Cl}(D)$ des formes binaires de discriminant D modulo changements de variables directs (notion d'*équivalence propre*). Comme l'a vu Lagrange, la détermination de l'ensemble $\mathrm{Cl}(D)$ est cruciale pour répondre à la Question ci-dessus (cas $D = -4d$). Nous retrouverons les applications arithmétiques du chapitre 2 de manière beaucoup plus simple et mécanique.

Chapitre 4. Nous introduisons l'*arithmétique* des anneaux généraux, et notamment la propriété de factorisation unique des éléments en produits d'éléments irréductibles. La hierarchie

$$\textit{euclidien} \Rightarrow \textit{principal} \Rightarrow \textit{factoriel} \Rightarrow \textit{intégralement clos}$$

est exposée, et étudiée sur la riche famille des anneaux *d'entiers quadratiques imaginaires* A_D, où D est comme ci-dessus (par exemple, $\mathrm{A}_{-4d} = \mathbb{Z}[\sqrt{d}]$). Les A_D euclidiens sont classifiés, et les premiers liens entre l'arithmétique de A_D et l'ensemble $\mathrm{Cl}(D)$ apparaissent. On donne enfin des applications à la résolution de certaines équations diophantiennes.

Chapitre 5. Il s'agit du premier d'une suite de trois chapitres sur la théorie algébrique des nombres proprement dite, dans laquelle nous nous intéressons à l'arithmétique des anneaux engendrés par un ou plusieurs entiers algébriques (généralisant les anneaux A_D). Nous introduisons d'abord la notion de *corps de nombres*, en faisant les rappels nécessaires sur la théorie des corps, et développons divers outils importants pour leur étude (*plongements, trace, norme, discriminant*). Nous introduisons l'*anneau des entiers* $\mathcal{O}_K$ d'un corps de nombres K, et l'étudions sur quelques exemples. En guise d'illustration des techniques développées, nous démontrons en général que le groupe additif de $\mathcal{O}_K$ possède une $\mathbb{Z}$-base finie (Dedekind).

Chapitre 6. On introduit *l'ensemble des classes d'équivalence d'idéaux* d'un anneau intègre A, noté $\mathrm{Cl}(A)$. Il mesure le défaut de principalité de l'anneau A et est muni d'une loi de composition interne associative, commutative, de neutre la classe des idéaux principaux (non nuls) de A. On utilise la théorie de Minkowski pour montrer que si A est engendré par un nombre fini d'entiers algébriques alors $\mathrm{Cl}(A)$ est un ensemble fini : c'est la *finitude du nombre de classes*. Le côté effectif de la théorie de Minkowski permet de déterminer $\mathrm{Cl}(A)$ sur de nombreux exemples, notamment pour les anneaux de la forme A_D.

Chapitre 7. Nous étudions $\mathrm{Cl}(A)$ dans le cas où $A = \mathcal{O}_K$ est l'anneau des entiers d'un corps de nombres K. Nous montrons d'abord que $\mathrm{Cl}(\mathcal{O}_K)$ est un groupe : tout idéal non nul de $\mathcal{O}_K$ est *inversible*. Après des rappels sur la notion d'*idéal premier*, nous montrons ensuite un résultat central du cours : tout idéal non nul de $\mathcal{O}_K$ s'écrit de manière unique comme produit d'idéaux premiers (Kummer, Dedekind). Nous verrons comment cette propriété (très générale) peut rendre des services analogues à la propriété de factorialité (rarement satisfaite), en montrant comment l'appliquer à l'étude des solutions $(x, y) \in \mathbb{Z}$ de l'*equation de Mordell* $y^2 = x^3 + k$. Nous évoquons

enfin les résultats de Kummer sur l'étude des solutions entières de l'équation $x^p + y^p = z^p$.

Chapitre 8. Dans ce chapitre, nous revisitons la théorie des formes binaires sous l'angle des chapitres précédents. Suivant Dedekind, nous montrons que les ensembles finis $\mathrm{Cl}(D)$ et $\mathrm{Cl}(\mathrm{A}_D)$ sont en bijection naturelle. Par exemple, on a $|\mathrm{Cl}(D)| = 1$ si et seulement si A_D est principal (ou factoriel, c'est équivalent à principal pour un anneau comme A_D). En pratique, cela permet de déterminer très efficacement $\mathrm{Cl}(\mathrm{A}_D)$. Lorsque D est un *discriminant fondamental*, A_D est l'anneau des entiers de $\mathbb{Q}(\sqrt{D})$, de sorte que $\mathrm{Cl}(\mathrm{A}_D)$ est un groupe. Cela munit $\mathrm{Cl}(D)$ d'une structure de groupe qui n'est autre que la fameuse loi de *composition des formes* de Gauss. En guise d'application, nous donnons des critères pour que $|\mathrm{Cl}(\mathrm{A}_D)|$ soit impair, et des conséquences frappantes concernant la Question originelle (Gauss). Nous terminons sur la *partition en genres* de $\mathrm{Cl}(D)$.

Chapitre 9. Dans ce dernier chapitre, qui est une ouverture vers la théorie *analytique* des nombres, nous exposons des résultats de Dirichlet, notamment sa fameuse *formule analytique du nombre de classes*. Cette formule donne une nouvelle expression pour le nombre $|\mathrm{Cl}(D)| = |\mathrm{Cl}(\mathrm{A}_D)|$. Par exemple, si ℓ est un nombre premier $\equiv 3 \bmod 8$, et $\ell \neq 3$, on a

$$|\mathrm{Cl}(-\ell)| = \frac{1}{3}(\mathrm{C}_\ell - \mathrm{N}_\ell)$$

où C_ℓ (resp. N_ℓ) est le nombre de carrés (resp. non carrés) modulo ℓ dans l'intervalle $\{1, 2, \ldots, \frac{\ell-1}{2}\}$. Pour démontrer ces formules, il nous faut utiliser presque tous les chapitres du cours, et étudier deux types de *séries de Dirichlet* : d'une part les *fonctions L* de Dirichlet, et d'autre part la *fonction zêta* d'un corps de nombres (deux généralisations de la fonction ζ de Riemann).

Bonne lecture !

Table des matières

Chapitre 1

La loi de réciprocité quadratique

L'objectif principal de ce premier chapitre est de rappeler la théorie des carrés de $\mathbb{Z}/N\mathbb{Z}$ développée par Fermat, Euler, Lagrange, Legendre et Gauss et notamment de démontrer la loi de réciprocité quadratique, le "theorema aureum" de Gauss, qui en est le résulat central. Nous introduirons au passage le symbole de Legendre, outil indispensable autant à l'élégance des énoncés qu'aux calculs pratiques de résidus quadratiques. Gauss a donné six démonstrations de la loi de réciprocité quadratique. Celle que nous présentons est la dernière, basée sur ce que l'on appelle depuis la somme de Gauss. Il sera commode d'introduire l'anneau des entiers algébriques, un outil dont on aurait pu se passer pour ce chapitre mais d'une grande importance pour la suite du cours. Enfin, nous terminerons par un théorème de Gauss sur la structure du groupe $(\mathbb{Z}/N\mathbb{Z})^\times$ des inversibles de l'anneau $\mathbb{Z}/N\mathbb{Z}$.

Les résultats de ce chapitre joueront un rôle essentiel dans la théorie des formes quadratiques binaires, par exemple pour les questions de représentation des entiers sous la forme $x^2 + dy^2$, ainsi que dans l'arithmétique des corps quadratiques.

Références : — C. F. Gauss, *Disquisitiones Arithmeticae*. Un grand classique traduit en français aux éditions Jacques Gabay. On y trouvera dans les chapitres I, II, III et IV les démonstrations (pour la plupart originales) de tous les résultats de ce chapitre, et bien plus encore.

— K. Ireland & M. Rosen, *A classical introduction to modern number theory*, Springer Verlag GTM **84**. Une excellente présentation, dans le language d'aujourd'hui, avec de multiples notes historiques. Notre présentation de la sixième preuve de Gauss est notamment issue du chapitre 6 de ce livre. De nombreuses autres démonstrations de la loi de réciprocité quadratique y sont exposées.

— Nous utiliserons librement le language de base de la théorie des groupes, pour lequel le lecteur pourra se reporter au livre *Algebra* de Serge Lang aux éditions Addison Wesley.

1. Carrés modulo un entier

Définition 1.1. *Soient N un entier ≥ 1 et $a \in \mathbb{Z}$. On dit que a est un carré modulo N, ou encore un résidu quadratique modulo N, s'il existe $b \in \mathbb{Z}$ vérifiant $a \equiv b^2 \bmod N$.*

Cette propriété ne dépend bien sûr que de la classe de a dans $\mathbb{Z}/N\mathbb{Z}$, et il revient au même de demander que cette classe est le carré d'un élément de l'anneau $\mathbb{Z}/N\mathbb{Z}$, c'est-à-dire de la forme x^2 avec $x \in \mathbb{Z}/N\mathbb{Z}$. Par exemple, les carrés modulo 5 sont

(les classes de ...) $0, 1$ et -1, et les non-carrés sont 2 et -2. De même, les carrés modulo 8 sont $0, 1$ et 4.

Il est évident que si a est un carré modulo N, et si M divise N, alors a est un carré modulo M. Nous allons donc commencer par étudier le cas (qui s'avèrera essentiel) où N est un nombre premier. Le cas du nombre premier 2 étant trivial, nous supposerons souvent que p est un nombre premier impair.

PROPOSITION 1.2. *Soient p un nombre premier impair et $\mathrm{C}_p := \{x^2, x \in (\mathbb{Z}/p\mathbb{Z})^\times\}$ l'ensemble des carrés non nuls de $\mathbb{Z}/p\mathbb{Z}$.*

(i) C_p a exactement $\frac{p-1}{2}$ éléments, à savoir les classes modulo p des éléments de la forme i^2 pour $i = 1, 2, \ldots, \frac{p-1}{2}$.

(ii) C_p est un sous-groupe d'indice 2 du groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^\times$: le produit de deux éléments de $(\mathbb{Z}/p\mathbb{Z})^\times$ est un carré si et seulement s'ils sont soit tous deux des carrés, soit tous deux des non-carrés.

DÉMONSTRATION — Soient $x, y \in \mathbb{Z}/p\mathbb{Z}$. On a la suite d'équivalences $x^2 = y^2 \Leftrightarrow (x-y)(x+y) = 0 \Leftrightarrow x = \pm y$, la dernière provenant de ce que l'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps pour p premier. Pour la même raison, on a $x \neq -x$ pour tout $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ car $p > 2$. La première assertion en découle.

Il est évident que C_p est un sous-groupe de $(\mathbb{Z}/p\mathbb{Z})^*$. On a $|(\mathbb{Z}/p\mathbb{Z})^\times|/|\mathrm{C}_p| = 2$ d'après le (i) [1], autrement dit C_p est d'indice 2. D'après Lagrange, C_p a donc exactement deux translatés (ou "classes") dans $(\mathbb{Z}/p\mathbb{Z})^\times$: on a

$$(\mathbb{Z}/p\mathbb{Z})^\times = \mathrm{C}_p \coprod a\mathrm{C}_p$$

où a est n'importe quel élément qui n'est pas dans C_p, c'est-à-dire un non-carré. Ainsi, si x et y ne sont pas des carrés, et donc tous deux dans $a\mathrm{C}_p$, alors xy est dans $a^2\mathrm{C}_p$: c'est donc un carré. De même, si $x \in \mathrm{C}_p$ et $y \notin \mathrm{C}_p$, alors $xy \in a\mathrm{C}_p$: le produit d'un non-carré par un carré est un non-carré. □

Remarquons que dans le groupe multiplicatif $\mathbb{R}^\times$, les carrés coincident avec les positifs, et forment un sous-groupe d'indice 2 : les carrés de $(\mathbb{Z}/p\mathbb{Z})^\times$ conservent cette prorpiété, même s'il n'y a plus de notion de positivité "modulo p".

DÉFINITION 1.3. (Legendre) *Soient p un nombre premier impair et $a \in \mathbb{Z}$. Si a est premier à p, on pose $\left(\frac{a}{p}\right) = 1$ si a est un carré modulo p, $\left(\frac{a}{p}\right) = -1$ sinon. On pose enfin $\left(\frac{a}{p}\right) = 0$ si $a \equiv 0 \bmod p$.*

Ainsi défini, le nombre $\left(\frac{a}{p}\right)$ ne dépend que de la classe de a modulo p de sorte qu'il y a aussi un sens à écrire $\left(\frac{a}{p}\right)$ pour $a \in \mathbb{Z}/p\mathbb{Z}$. La seconde assertion de la proposition 1.2 se reformule alors de la manière suivante :

1. Nous aurions pu également introduire l'application $f : (\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ définie par $f(x) = x^2$. C'est un morphisme de groupes d'image C_p et de noyau $\{\pm 1\}$ d'après l'argument donné au (i). La formule $|\mathrm{Im}(f)| = |(\mathbb{Z}/p\mathbb{Z})^\times|/|\mathrm{Ker}(f)|$ redonne bien sûr l'égalité $|\mathrm{C}_p| = \frac{p-1}{2}$.

COROLLAIRE 1.4. (Multiplicativité du symbole de Legendre) *Pour tous a, b dans $\mathbb{Z}$, on a $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.*

En particulier, il suffit de savoir déterminer les nombres $\left(\frac{a}{p}\right)$ avec $a = -1$, 2 ou a premier impair. Étant donné p, il est en théorie facile de déterminer tous les $a \in \mathbb{Z}$ tels que $\left(\frac{a}{p}\right) = 1$: il suffit d'énumérer les classes modulo p de i^2 pour $i = 1, \ldots, \frac{p-1}{2}$ (Proposition 1.2), qui est en particulier un problème fini. En revanche, un problème nettement plus difficile est de déterminer, étant donné $a \in \mathbb{Z}$, tous les nombres premiers p tels que $\left(\frac{a}{p}\right) = 1$. La table suivante donne quelques exemples.

p	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79
$\left(\frac{2}{p}\right)$	-1	-1	1	-1	-1	1	-1	1	-1	1	-1	1	-1	1	-1	-1	-1	-1	1	1	1
$\left(\frac{3}{p}\right)$	0	-1	-1	1	1	-1	-1	1	-1	-1	1	-1	-1	1	-1	1	1	-1	1	1	-1
$\left(\frac{5}{p}\right)$	-1	0	-1	1	-1	-1	1	-1	1	1	-1	1	-1	-1	-1	1	1	-1	1	-1	1

TABLE 1. $\left(\frac{a}{p}\right)$ pour $p < 80$ et $a = 2, 3, 5$

Cette table peut soit être obtenue par énumération directe, bien que fastidieuse, des carrés modulo tous ces premiers, soit par exemple à l'aide du critère élégant suivant (mais pas très efficace non plus en pratique, il faut bien l'avouer, du moins sans l'aide de l'ordinateur).

PROPOSITION 1.5. (Critère d'Euler) *Soient p premier impair et $a \in \mathbb{Z}$, on a la congruence $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p$.*

DÉMONSTRATION — On peut supposer $a \not\equiv 0 \bmod p$. Nous allons montrer $(p-1)! \equiv -\left(\frac{a}{p}\right) a^{\frac{p-1}{2}} \bmod p$. Du cas $a = 1$ on en déduira $(p-1)! \equiv -1 \bmod p$ (théorème de Wilson) puis le résultat de l'énoncé.

On remarque que l'application $x \mapsto ax^{-1}$ est une involution [2] de $(\mathbb{Z}/p\mathbb{Z})^\times$ qui est sans point fixe, sauf si a est un carré modulo p auquel cas ses deux seuls points fixes sont u et $-u$ où $u^2 = a \bmod p$. Le produit des éléments de $(\mathbb{Z}/p\mathbb{Z})^\times$, qui est congru à $(p-1)!$, vaut donc $a^{\frac{p-1}{2}} \bmod p$ si $\left(\frac{a}{p}\right) = -1$, et $a^{\frac{p-3}{2}} \cdot (-a)$ si $\left(\frac{a}{p}\right) = 1$, ce qui conclut.

Donnons une seconde démonstration. Le petit théorème de Fermat montre que les $\frac{p-1}{2}$ éléments de l'ensemble C_p des carrés de $(\mathbb{Z}/p\mathbb{Z})^\times$ sont des racines du polynôme $P = X^{\frac{p-1}{2}} - 1$ dans $(\mathbb{Z}/p\mathbb{Z})[X]$. Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, C_p est exactement l'ensemble des racines de P. Ainsi, si x n'est pas dans C_p, et si $y = x^{\frac{p-1}{2}}$, alors

2. Une involution d'un ensemble X est une application $f : X \to X$ vérifiant que $f \circ f = \mathrm{id}_X$. Il est équivalent de se donner une action du groupe $\mathbb{Z}/2\mathbb{Z}$ sur l'ensemble X, l'élément non trivial de $\mathbb{Z}/2\mathbb{Z}$ agissant par la bijection f. En particulier, X est réunion disjointe d'orbites de cette action, qui sont soit de cardinal 1 (points fixes), soit de cardinal 2 (et de la forme $\{x, f(x)\}$ avec $f(x) \neq x$).

$y \neq 1$ par ce que l'on vient de dire, et $y^2 = 1$ par le petit théorème de Fermat, donc $y = -1$. □

Par exemple, modulo 23 on a $\left(\frac{5}{23}\right) \equiv 5^{11} \equiv 5.2^5 \equiv 5.9 \equiv -1$. Remarquons que ce critère donne une autre démonstration de la multiplicativité du symbole de Legendre. Surtout, il admet le corollaire immédiat suivant.

COROLLAIRE 1.6. (Fermat, Euler) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. *Autrement dit,* -1 *est un carré modulo le premier impair* p *si, et seulement si, on a* $p \equiv 1 \bmod 4$.

Un examen de la table 1 ci-dessus suggère des propriétés remarquables tout à fait non triviales. On observe notamment dans tous les cas les

$$\left(\frac{2}{p}\right) = 1 \text{ si, et seulement si, } p \equiv \pm 1 \bmod 8,$$

$$\left(\frac{3}{p}\right) = 1 \text{ si, et seulement si, } p \equiv \pm 1 \bmod 12,$$

$$\left(\frac{5}{p}\right) = 1 \text{ si, et seulement si, } p \equiv \pm 1 \bmod 5.$$

Il s'agit en fait de propriétés générales, toutes cas particulier du résultat fondamental suivant, conjecturé indépendamment par Euler, Gauss et Legendre (qui l'a démontré dans certains cas), et démontré en toute généralité par Gauss dans ses *Disquisitiones Arithmeticae*. En vertu de la multiplicativité du symbole de Legendre, cela fournit une recette pour determiner $\left(\frac{a}{p}\right)$ dans tous les cas.

THÉORÈME 1.7. *(Loi de réciprocité quadratique) Soient* p *et* q *des nombres premiers impairs. On a*

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

De plus, on a la "loi supplémentaire" $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

REMARQUE 1.8. (sur l'énoncé ci-dessus) Autrement dit, si $p \equiv 1 \bmod 4$ ou $q \equiv 1 \bmod 4$ on a $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, et dans les autres cas on a $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$. Si l'on pose $p^\star := (-1)^{\frac{p-1}{2}}p$, le corollaire 1.6 permet également d'écrire la loi de réciprocité quadratique sous la forme condensée $\left(\frac{q}{p}\right) = \left(\frac{p^\star}{q}\right)$. La supplémentaire s'écrit aussi : 2 est un carré modulo p si, et seulement si, $p \equiv \pm 1 \bmod 8$.

La démonstration de ce résultat nous occupera dans les paragraphes qui vont suivre. Donnons-en tout d'abord quelques applications. Par exemple, sachant que 691 est premier, est-ce que 41 est un carré modulo 691 ? L'approche naïve est de lister les carrés modulo 691, ce qui est bien fastidieux ; le critère d'Euler (consistant à calculer $41^{345} \bmod 691$) ne poserait pas de problème à un ordinateur, mais est

assez peu commode à la main. En utilisant la loi de réciprocité quadratique, il est essentiellement immédiat de justifier la suite d'égalités ci-dessous :

$$\left(\frac{41}{691}\right) = \left(\frac{691}{41}\right) = \left(\frac{35}{41}\right) = \left(\frac{7}{41}\right)\left(\frac{5}{41}\right) =$$

$$\left(\frac{41}{5}\right)\left(\frac{41}{7}\right) = \left(\frac{1}{5}\right)\left(\frac{6}{7}\right) = 1.(-1) = -1$$

donc 41 n'est pas un carré modulo 691 ! Le seul calcul réellement effectué ici est $691 \equiv 35 \bmod 41$...

Une autre conséquence immédiate de la loi de réciprocité quadratique, loin d'être évidente, est que q étant donné le nombre $\left(\frac{q}{p}\right)$ ne dépend que de $p \bmod 4q$. Donnons quelques exemples, expliquant notamment la table 1 :

COROLLAIRE 1.9. *Soit p un nombre premier impair.*

(i) 3 *est un carré modulo p si, et seulement si, $p \equiv \pm 1 \bmod 12$ ou $p = 3$.*

(ii) 5 *est un carré modulo p si, et seulement si, $p \equiv \pm 1 \bmod 5$ ou $p = 5$.*

(iii) 7 *est un carré modulo p si, et seulement si, $p \equiv \pm 1, \pm 3, \pm 9 \bmod 28$ ou $p = 7$.*

DÉMONSTRATION — On a $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$ car $5 \equiv 1 \bmod 4$. Les carrés modulo 5 étant 0 et ± 1, cela démontre le (ii). De même, on a $\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)$, duquel on déduit le (i). Le (iii) est laissé en exercice au lecteur. □

Terminons par une discussion des carrés de $\mathbb{Z}/N\mathbb{Z}$ où N n'est plus nécessairement un nombre premier. Remarquons tout d'abord que le lemme chinois des restes, rappelé ci-dessous, montre [3] que $a \in \mathbb{Z}$ est un carré modulo l'entier $N = \prod_i p_i^{n_i}$ où les p_i sont premiers distincts si, et seulement si, a est un carré modulo $p_i^{n_i}$ pour tout i.

LEMME 1.10. (Lemme chinois des restes) *Soient N et M des entiers premiers entre eux. L'application*

$$\mathbb{Z}/MN\mathbb{Z} \to \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$$

définie par $a \bmod MN \mapsto (a \bmod M, a \bmod N)$, est un isomorphisme d'anneaux.

DÉMONSTRATION — C'est évidemment un morphisme d'anneaux. La source et le but ayant même cardinal MN il suffit de voir qu'il est injectif, ce qui est immédiat sous l'hypothèse $(M, N) = 1$. □

3. De manière directe, si pour tout i on a $a \equiv b_i^2 \bmod p_i^{n_i}$ pour un certain $b_i \in \mathbb{Z}$, on peut trouver par le lemme chinois un élément $b \in \mathbb{Z}$ avec $b \equiv b_i \bmod p_i^{n_i}$, et on a alors $a \equiv b^2 \bmod p_i^{n_i}$ pour tout i, et donc $a \equiv b^2 \bmod N$.

Il ne reste donc qu'à traiter le cas $N = p^n$ avec p premier et $n > 1$. Soit $a \in \mathbb{Z}$, écrivons $a = p^m a'$ avec $(a', p) = 1$. On peut également supposer $m < n$ sans quoi $a \equiv 0 \bmod p^n$ est évidemment un carré. Dans ce cas, il est facile de vérifier que a est un carré modulo p^n si, et seulement si, m est pair et a' est un carré modulo p^{n-m}. En conclusion, il suffit de déterminer les carrés de $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

LEMME 1.11. *Soit $a \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ avec p premier et $n > 1$.*

(i) Si p est impair, alors a est un carré si et seulement si c'est un carré modulo p.

(ii) Si $p = 2$ et $n > 2$, alors a est un carré si, et seulement si, c'est un carré modulo 8.

On remarquera que si l'entier a est impair, alors a est un carré modulo 8 si, et seulement si, $a \equiv 1 \bmod 8$, ce qui permet de reformuler la condition du (ii) en la simple congruence "$a \equiv 1 \bmod 8$".

DÉMONSTRATION — Montrons par récurrence sur n que si a est un carré modulo p^n, alors a est un carré modulo p^{n+1} ("raisonnement par approximations successives"). Écrivons $a = u^2 + p^n r$ avec $u, r \in \mathbb{Z}$. Si $v \in \mathbb{Z}$ est un entier quelconque, on observe les congruences

$$(u + p^n v)^2 \equiv u^2 + 2uvp^n \equiv a + (2uv - r)p^n \bmod p^{n+1}.$$

Il suffit donc de voir que l'on peut choisir v de sorte que l'on ait $2uv \equiv r \bmod p$. Mais a est premier à p, ainsi donc que u, et aussi $2u$ si l'on suppose de plus $p > 2$. Dans ce cas, tout entier v tel que $v \equiv r(2u)^{-1} \bmod p$ convient. Si $p = 2$ il faut modifier un peu l'argument précédent à cause du facteur 2 qui devient gênant. Supposons donc $a = u^2 + 2^n r$, $u, r \in \mathbb{Z}$. Si $v \in \mathbb{Z}$ on a l'identité

$$(u + 2^{n-1}v)^2 \equiv a + (uv - r)2^n \bmod 2^{n+1}.$$

(Noter $2(n-1) \geq n+1$ car $n \geq 3$). Mais $uv \equiv r \bmod 2$ si $v \equiv r \bmod 2$, car u est impair, ce qui conclut. □

Si l'on met bout-à-bout les observations précédentes, nous avons démontré la proposition suivante.

PROPOSITION 1.12. *Soit $\mathcal{Q} \subset \mathbb{N}$ la réunion de l'ensemble des premiers impairs et de $\{4, 8\}$. Un élément $a \in (\mathbb{Z}/N\mathbb{Z})^\times$ est un carré si, et seulement si, son image dans $(\mathbb{Z}/q\mathbb{Z})^\times$ est un carré pour tout $q \in \mathcal{Q}$ divisant N.*

2. Digression : l'anneau des entiers algébriques

DÉFINITION 1.13. *(Dedekind) Un entier algébrique est un nombre complexe annulé par un polynôme* unitaire *à coefficients entiers. On note $\overline{\mathbb{Z}} \subset \mathbb{C}$ l'ensemble des entiers algébriques.*

En particulier, un entier algébrique est un nombre algébrique. Par exemple, les complexes $\sqrt{N}$ et $e^{2i\pi/N}$ pour $N \in \mathbb{Z}$, les entiers usuels, ou encore tout $x \in \mathbb{C}$ tel que $x^3 = x+1$, sont des entiers algébriques. On peut dire que les entiers algébriques sont aux nombres algébriques ce que les entiers sont aux nombres rationnels. La proposition suivante, classique à sa formulation près, en est un premier indicateur.

PROPOSITION 1.14. *Les entiers algébriques qui sont rationnels sont dans $\mathbb{Z}$. Autrement dit, on a $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$.*

DÉMONSTRATION — C'est le fait bien connu que si le rationnel p/q, avec $(p,q) = 1$, est racine d'un polynôme $P \in \mathbb{Z}[X]$, alors q divise le coefficient dominant de P, comme on le voit en regardant l'égalité $q^n P(p/q) = 0$ avec $n = \deg(P)$. Si P est unitaire, on a donc $q = \pm 1$, puis $p/q \in \mathbb{Z}$. □

PROPOSITION 1.15. *$\overline{\mathbb{Z}}$ est un sous-anneau de $\mathbb{C}$.*

Observons cependant que $\overline{\mathbb{Z}}$ n'est pas un sous-corps de $\mathbb{C}$. En effet, on a $1/N \notin \overline{\mathbb{Z}}$ pour $N \geq 2$ d'après la proposition précédente. Pour démontrer la proposition 1.15, nous aurons besoin du critère d'intégralité suivant. Si $x_1, \ldots, x_r$ sont des nombres complexes, on note $\mathbb{Z}[x_1, \ldots, x_r] \subset \mathbb{C}$ le sous-ensemble des nombres de la forme $P(x_1, \ldots, x_r)$ avec $P \in \mathbb{Z}[X_1, \ldots, X_r]$. C'est le plus petit sous-anneau de $\mathbb{C}$ contenant les x_i.

PROPOSITION 1.16. *(i) Si $x_1, \ldots, x_r \in \overline{\mathbb{Z}}$ alors le groupe additif de $\mathbb{Z}[x_1, \ldots, x_r]$ est engendré par un nombre fini d'éléments.*

(ii) Soit $x \in \mathbb{C}$. Alors x est un entier algébrique si, et seulement si, il existe un sous-groupe (additif) non nul $A \subset \mathbb{C}$ engendré par un nombre fini d'éléments et tel que $xA \subset A$.

DÉMONSTRATION — Montrons le (i). Fixons $1 \leq i \leq r$ et $P_i \in \mathbb{Z}[X]$ unitaire avec $P_i(x_i) = 0$. Posons $n_i = \deg P_i$. On constate que $x_i^{n_i}$ est une combinaison linéaire à coefficients dans $\mathbb{Z}$ des éléments x_i^k avec $k < n_i$. Par récurrence sur $m \geq n_i$, il en va donc de même des x_i^m avec $m \geq n_i$. On en déduit que le groupe $\mathbb{Z}[x_1, \ldots, x_r]$ est engendré par les éléments $\prod_{i=1}^r x_i^{k_i}$ avec $0 \leq k_i < n_i$, qui sont en nombre fini.

Montrons le (ii). Supposons d'abord x entier algébrique. Alors $A := \mathbb{Z}[x]$ convient d'après le (i). Réciproquement, soient $A \subset \mathbb{C}$ comme dans l'énoncé et $e_1, \ldots, e_n$ une famille génératrice de A. Ainsi, tout $a \in A$ s'écrit sous la forme $\sum_{i=1}^n m_i e_i$ (pas nécéssairement de manière unique) avec $m_i \in \mathbb{Z}$ pour tout i. Par hypothèse, on a $xe_j \in A$ pour tout j, et donc il existe des entiers $m_{i,j}$ tels que pour tout i,

$$xe_j = \sum_{i=1}^n m_{i,j} e_i.$$

Cela s'écrit encore $0 = \sum_{i=1}^n (x\delta_{i,j} - m_{i,j}) e_i$ pour tout $j = 1, \ldots, n$: on reconnaît là un système linéaire en les e_i. Par hypothèse les e_j ne sont pas tous nuls, car on a $A \neq 0$ par hypothèse, il s'ensuit que la matrice $(x\delta_{i,j} - m_{i,j})$ est non inversible. La nullité de son déterminant fournit l'équation $P(x) = 0$ où P est le polynôme caractéristique de $(m_{i,j})$: c'est un polynôme unitaire de $\mathbb{Z}[X]$. □

Démonstration — (de la proposition 1.15) Soient x, y des entiers algébriques. D'après la proposition 1.16 (i), le groupe abélien $A = \mathbb{Z}[x, y]$ est finiment engendré. On a clairement $1 \in A$ (donc $A \neq 0$), $xyA \subset A$ et $(x - y)A \subset A$: les éléments xy et $x - y$ sont donc dans $\overline{\mathbb{Z}}$ d'après le (ii) de la proposition 1.16. □

Observons que ces résultats permettent de vérifier que certains nombres algébriques ne sont pas des entiers algébriques. Par exemple $x = \frac{1+\sqrt{3}}{2}$ est un nombre algébrique, satisfaisant $x^2 - x - 1/2 = 0$. Si x était entier algébrique, il en serait de même de $x^2 - x = 1/2$, ce qui n'est pas. Mentionnons tout de même qu'il ne faut pas toujours se fier aux apparences : le nombre $\frac{1+\sqrt{5}}{2}$ est un entier algébrique ! (pourquoi ?)

3. Congruences dans $\overline{\mathbb{Z}}$

L'arithmétique de l'anneau $\overline{\mathbb{Z}}$, c'est-à-dire les questions de divisibilité, est immensément plus complexe que celle de $\mathbb{Z}$, et c'est un des buts de ce cours que d'en éclaircir les traits fondamentaux. Nous nous contenterons ici de dégager quelques faits élémentaires qui seront utiles à la démonstration de la loi réciprocité quadratique, et reportons une discussion plus raisonnable aux chapitres qui suivent.

Tout comme dans les entiers usuels, il y a un sens à considérer des congruences dans l'anneau $\overline{\mathbb{Z}}$. En effet, pour tout $N \in \overline{\mathbb{Z}}$, l'ensemble $N\overline{\mathbb{Z}} = \{Na, a \in \overline{\mathbb{Z}}\}$ est un idéal de $\overline{\mathbb{Z}}$ et il y a donc un sens à considérer l'anneau quotient

$$\overline{\mathbb{Z}}/N\overline{\mathbb{Z}}.$$

Concrètement, deux entiers algébriques $a, b \in \overline{\mathbb{Z}}$ seront dits congrus modulo N, et on écrira $a \equiv b \bmod N\overline{\mathbb{Z}}$, s'il existe $c \in \overline{\mathbb{Z}}$ tel que $a = b + Nc$, ou ce qui revient au même s'ils ont même image dans $\overline{\mathbb{Z}}/N\overline{\mathbb{Z}}$. Les propriétés générales des anneaux quotients se traduisent simplement par le fait que l'on peut additionner, soustraire et multiplier des congruences. Un cas particulier important est celui où $N \in \mathbb{Z}$.

Lemme 1.17. *Soient a, b et N dans $\mathbb{Z}$. Alors $a \equiv b \bmod N\overline{\mathbb{Z}} \Leftrightarrow a \equiv b \bmod N$.*

Démonstration — Il s'agit de voir que si $a = b + Nc$ avec $c \in \overline{\mathbb{Z}}$, alors $c \in \mathbb{Z}$ ou $N = 0$. On exclut ce dernier cas qui est trivial. Mais alors $c = \frac{a-b}{N} \in \mathbb{Q} \cap \overline{\mathbb{Z}}$, et on conclut d'après la proposition 1.14. □

Pour $a, b, N \in \overline{\mathbb{Z}}$ nous noterons par la suite simplement $a \equiv b \bmod N$ pour $a \equiv b \bmod N\overline{\mathbb{Z}}$. Le lemme ci-dessus assure que cette notation n'est pas en conflit avec la notation usuelle quand les deux ont un sens, c'est-à-dire quand $a, b, N \in \mathbb{Z}$.

La structure de l'anneau $\overline{\mathbb{Z}}/N\overline{\mathbb{Z}}$ est en général sensiblement plus compliquée que celle de $\mathbb{Z}/N\mathbb{Z}$ (qu'il contient par le lemme ci-dessus), et ce même quand N est un nombre premier. Par exemple, $\overline{\mathbb{Z}}/N\overline{\mathbb{Z}}$ n'est jamais un corps si $N > 1$! En effet, l'élément $\sqrt{N}$ est dans $\overline{\mathbb{Z}}$, n'est pas $\equiv 0 \bmod N$ (pourquoi ?) et son carré est $\equiv 0 \bmod N$. Une propriété générale fort utile que nous utiliserons est la suivante.

LEMME 1.18. *Soit p un nombre premier. Si $a, b \in \overline{\mathbb{Z}}$ on a*

$$(a+b)^p \equiv a^p + b^p \bmod p.$$

DÉMONSTRATION — Cela découle de la formule du binôme et de ce que p divise $\binom{p}{k}$ pour $k = 1, \ldots, p-1$. □

4. Sommes de Gauss

Soient p un nombre premier impair et $\zeta = e^{2i\pi/p}$.

DÉFINITION 1.19. (Gauss) *La* somme de Gauss *relative à p est le nombre complexe*

$$G = \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{a}{p}\right) \zeta^a.$$

Par exemple, si $p = 3$ alors $G = \zeta - \zeta^2 = i\sqrt{3}$. De même, si $p = 5$ alors $G = \zeta - \zeta^2 - \zeta^3 + \zeta^4 = 2\cos(2\pi/5) - 2\cos(4\pi/5) = \frac{-1+\sqrt{5}}{2} - \frac{-1-\sqrt{5}}{2} = \sqrt{5}$. La proposition suivante montre que c'est un phénomène général.

PROPOSITION 1.20. (Gauss) $G^2 = (-1)^{\frac{p-1}{2}} p$.

DÉMONSTRATION — Par multiplicativité du symbole de Legendre, on a

$$G^2 = \sum_{a,b \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{ab}{p}\right) \zeta^{a+b}.$$

Rappelons-nous $\left(\frac{a^2 t}{p}\right) = \left(\frac{t}{p}\right)$ si $a \in (\mathbb{Z}/p\mathbb{Z})^\times$. Posant $b = at$ on obtient donc

$$G^2 = \sum_{t \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{t}{p}\right) \left(\sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \zeta^{a(1+t)} \right).$$

Si $t = -1$, alors $\sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \zeta^{a(1+t)} = p - 1$. Sinon, $a \mapsto (1+t)a$ est une bijection de $(\mathbb{Z}/p\mathbb{Z})^\times$, et donc on a

$$\sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \zeta^{a(1+t)} = \zeta + \zeta^2 + \cdots + \zeta^{p-1} = -1.$$

Ainsi, $G^2 = \left(\frac{-1}{p}\right)(p-1) - \sum_{t \in (\mathbb{Z}/p\mathbb{Z})^\times \setminus \{-1\}} \left(\frac{t}{p}\right)$. On conclut d'après le lemme 1.21. □

LEMME 1.21. $\sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{a}{p}\right) = 0$.

DÉMONSTRATION — En effet, il y a autant de carrés que de non carrés dans $(\mathbb{Z}/p\mathbb{Z})^\times$ par la proposition 1.2. □

DÉFINITION 1.22. *La somme de Gauss relativement au nombre premier* 2 *est* $G = \zeta + \zeta^{-1}$ *où* $\zeta = e^{2i\pi/8}$.

Comme $\zeta = \frac{1+i}{\sqrt{2}}$, on a simplement $G = \sqrt{2}$, ce qui constitue un analogue de la proposition 1.20.

REMARQUE 1.23. (signe de la somme de Gauss) Gauss a en fait démontré $G = \sqrt{p}$ si $p \equiv 1 \bmod 4$, et $G = i\sqrt{p}$ si $p \equiv 3 \bmod 4$. La preuve est nettement plus délicate : voir par exemple l'exercice 1.14 pour une élégante démonstration due à Dirichlet.

5. Une démonstration de la loi de réciprocité quadratique

Fixons p un nombre premier et q un nombre premier impair différent de p. Soit G la somme de Gauss relative à p. Par définition on a

$$G \in \overline{\mathbb{Z}}.$$

La stratégie de Gauss est grosso-modo la suivante. Observons que G est une racine carré dans $\overline{\mathbb{Z}}$ de $(-1)^{\frac{p-1}{2}}p$ d'après la proposition 1.20. Sa réduction mod $q\overline{\mathbb{Z}}$ est donc naturellement un candidat pour être une racine carré de $(-1)^{\frac{p-1}{2}}p \bmod q$. La question qui se pose est donc de savoir à quelle condition G est congrue modulo $q\overline{\mathbb{Z}}$ à un élément de $\mathbb{Z}$. Une condition nécessaire[4] est que $G^q \equiv G \bmod q$ (petit théorème de Fermat), ce qui pousse à s'intéresser à $G^q \bmod q\overline{\mathbb{Z}}$.

PROPOSITION 1.24. *Soient* G *la somme de Gauss relative au premier* p *et* $q \neq p$ *premier. On a* $G^q \equiv \left(\frac{q}{p}\right) G \bmod q$ *si* $p > 2$, *et* $G^q \equiv (-1)^{\frac{q^2-1}{8}} G \bmod q$ *si* $p = 2$.

DÉMONSTRATION — Supposons d'abord p impair. Alors d'après le lemme 1.18 on a

$$G^q \equiv \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{a}{p}\right)^q \zeta^{aq} \bmod q.$$

Remarquons que pour tout $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ on a

$$\left(\frac{a}{p}\right)^q = \left(\frac{a}{p}\right) = \left(\frac{q}{p}\right)\left(\frac{qa}{p}\right),$$

la première égalité venant de ce que q est impair et la seconde de la multiplicativité du symbole de Legendre. La proposition résulte alors du changement de variables $t = aq$. Si $p = 2$, on conclut de même en remarquant que $\zeta^q + \zeta^{-q} = G$ si $q \equiv \pm 1 \bmod 8$, $-G$ sinon (noter $\zeta^3 = -\zeta^{-1}$). □

4. Nous renvoyons au *cours d'arithmétique* de Serre chapitre I pour une variante de la démonstration de ce paragraphe utilisant la somme de Gauss dans les corps finis, dans laquelle la stratégie ci-dessus est encore plus transparente.

Démontrons enfin la loi de réciprocité quadratique. On calcule pour cela G^q mod q d'une autre façon. Supposons d'abord p impair. D'après la proposition 1.20, on a

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

Le critère d'Euler assure donc

$$G^q \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right) G \bmod q.$$

En comparant avec la proposition précédente on obtient

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right) G \equiv \left(\frac{q}{p}\right) G \bmod q,$$

puis en multipliant par $(-1)^{\frac{p-1}{2}} G$ et par la proposition 1.20 à nouveau

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right) p \equiv \left(\frac{q}{p}\right) p \bmod q,$$

qui est une congruence traditionnelle, de laquelle on déduit la loi de réciprocité quadratique car p est inversible dans $\mathbb{Z}/q\mathbb{Z}$ et $q \neq 2$.

Il ne reste donc qu'à étudier le cas $p = 2$. L'argument ci-dessus, et la relation $G^2 = 2$, montrent cette fois

$$\left(\frac{2}{q}\right) G \equiv (-1)^{\frac{q^2-1}{8}} G \bmod q$$

d'où l'on déduit la loi supplémentaire. □

6. Symbole de Jacobi

Le symbole de Jacobi est une extension formelle du symbole de Legendre dont les propriétés permettent en retour de calculer plus facilement des symboles de Legendre.

Définition 1.25. (Jacobi) *Soient m et n des entiers avec n impair positif. On pose*

$$\left(\frac{m}{n}\right) = \prod_{i=1}^{r} \left(\frac{m}{p_i}\right)$$

où $n = p_1 p_2 \cdots p_r$ est la décomposition de n en facteurs premiers (non nécessairement distincts).

Par convention on pose aussi $\left(\frac{m}{1}\right) = 1$ pour tout $m \in \mathbb{Z}$. Par définition, $\left(\frac{m}{n}\right)$ ne dépend que de m modulo n et coïncide avec le symbole de Legendre si n est premier. On prendra garde que l'égalité $\left(\frac{m}{n}\right) = 1$ n'entraîne pas en général que m est un carré modulo n, par exemple $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)\cdot(-1) = 1$ mais 2 n'est pas un carré modulo 15 car il ne l'est pas modulo 3 (ni modulo 5).

PROPOSITION 1.26. *Soient $m, m', n, n' \in \mathbb{Z}$ avec n, n' impairs positifs. On a*

$$\left(\frac{mm'}{n}\right) = \left(\frac{m}{n}\right)\left(\frac{m'}{n}\right), \quad \left(\frac{m}{nn'}\right) = \left(\frac{m}{n}\right)\left(\frac{m}{n'}\right),$$

$$\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}, \quad \left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}},$$

et si m est impair positif

$$\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)(-1)^{\frac{n-1}{2}\frac{m-1}{2}}.$$

En effet, la première propriété découle de la multiplicativité du symbole de Legendre et la seconde est évidente. Les autres se déduisent immédiatement par multiplicativité des propriétés correspondantes du symbole de Legendre et du lemme suivant, qui est laissé en exercice au lecteur.

LEMME 1.27. *Soient $n, m \in \mathbb{Z}$ des entiers impairs.*

(i) $\frac{n-1}{2} + \frac{m-1}{2} \equiv \frac{nm-1}{2} \bmod 2$.

(ii) Si $n = \prod_i n_i$ *et* $m = \prod_j m_i$, *alors* $\sum_{i,j} \frac{n_i-1}{2}\frac{m_j-1}{2} \equiv \frac{n-1}{2}\frac{m-1}{2} \bmod 2$.

(iii) $n^2 \equiv 1 \bmod 8$.

(iv) $\frac{n^2-1}{8} + \frac{m^2-1}{8} \equiv \frac{n^2m^2-1}{8} \bmod 2$.

Un premier intérêt du symbole de Jacobi est de fournir un algorithme efficace de calcul de $\left(\frac{m}{n}\right)$ pour tout $m \in \mathbb{Z}$ et tout entier n impair positif premier avec m :

(1) On cherche $-\frac{n-1}{2} \leq m' < \frac{n-1}{2}$ tel que $m \equiv m' \bmod n$ (division euclidienne),

(2) On factorise m' sous la forme $\varepsilon 2^q m''$ avec m'' impair positif et $\varepsilon = \pm 1$,

(3) On applique les propriétés du symbole de Jacobi :

$$\left(\frac{m}{n}\right) = \left(\frac{m'}{n}\right) = \varepsilon^{\frac{n-1}{2}}\left(\frac{2}{n}\right)^q (-1)^{\frac{n-1}{2}\frac{m''-1}{2}}\left(\frac{n}{m''}\right).$$

(4) Si $m'' = 1$ c'est terminé, sinon on retourne au (1) en remarquant que l'on a $m'' < n$ et $(n, m'') = 1$.

L'avantage principal d'un point de vue algorithmique est qu'en phase (2) il n'est pas nécessaire de factoriser m' entièrement (problème réputé très couteux, par exemple impossible pour un ordinateur si m a plus de 200 chiffres), mais simplement d'en extraire la plus grande puissance de 2 (ce qui est très rapide). Au final, on se ramène donc essentiellement à effectuer des divisions euclidiennes.

Par exemple, est-ce que 3763 est un carré modulo le nombre premier 20353 ? On calcule alors $20353 \equiv 1538 \bmod 3763$, $1538 = 2 \cdot 769$, $3763 \equiv -82 \bmod 769$, $82 = 2 \cdot 41$, $769 \equiv -10 \bmod 41$, d'où l'on tire :

$$\left(\frac{3763}{20353}\right) = \left(\frac{1538}{3763}\right) = -\left(\frac{769}{3763}\right)$$

$$= -\left(\frac{-82}{769}\right) = -\left(\frac{41}{769}\right) = -\left(\frac{-10}{41}\right) = -\left(\frac{5}{41}\right) = -1.$$

Ce n'est donc pas un carré. Nous n'avons pas eu à factoriser 3763 (qui vaut en fait $53 \cdot 71$). Le symbole de Jacobi est notamment utilisé dans le test de primalité de *Solovay-Strassen* (voir les exercices).

7. Complément : la structure de $(\mathbb{Z}/N\mathbb{Z})^\times$

Terminons ce chapitre par une étude du groupe $(\mathbb{Z}/N\mathbb{Z})^\times$. On rappelle que c'est un groupe de cardinal $\varphi(N)$ (indicatrice d'Euler).

PROPOSITION 1.28. *L'isomorphisme chinois induit un isomorphisme de groupes*

$$(\mathbb{Z}/MN\mathbb{Z})^\times \xrightarrow{\sim} (\mathbb{Z}/M\mathbb{Z})^\times \times (\mathbb{Z}/N\mathbb{Z})^\times.$$

DÉMONSTRATION — Si A et B sont deux anneaux commutatifs unitaires, on vérifie immédiatement l'égalité $(A \times B)^\times = A^\times \times B^\times$. La proposition découle alors du lemme chinois des restes. □

Il suffit donc d'étudier la structure du groupe $(\mathbb{Z}/p^m\mathbb{Z})^\times$ lorsque p est un nombre premier et $m \geq 1$. Il est de cardinal $\varphi(p^m) = (p-1)p^{m-1}$. Commençons par le cas crucial $m = 1$.

THÉORÈME 1.29. (Gauss) *Le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p-1$.*

Rappelons que $\mathbb{Z}/p\mathbb{Z}$ est un corps, en particulier $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}/p\mathbb{Z} - \{0\}$ a $p-1$ éléments. Nous allons en fait démontrer le résultat plus général suivant : si k est un corps (commutatif) et si G est un sous-groupe fini de $k^\times$, alors G est cyclique.

DÉMONSTRATION — Soient k et $G \subset k^\times$ comme ci-dessus. Posons $n = |G|$. Il suffit de démontrer que, si $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ est la décomposition en facteurs premiers de n, alors G possède un élément x_i d'ordre $p_i^{\alpha_i}$ pour tout i. En effet, le lemme ci-dessous assurera alors que l'élément $x_1 x_2 \cdots x_r$ est d'ordre n.

Considérons le polynôme $P = X^n - 1 \in k[X]$. Comme k est un corps, P admet au plus n racines dans k. D'autre part, le théorème de Lagrange assure que les n éléments de G sont racines de P : il est donc scindé à racines distinctes, égales aux éléments de G. Remarquons que si d est un diviseur de n, alors $X^d - 1$ divise $X^n - 1$ dans $k[X]$, le quotient étant $\sum_{i=0}^{n/d-1} X^{id}$. En particulier, $X^d - 1$ est aussi scindé à racines distinctes dans G. Pour tout i, il existe donc au moins une racine x_i de $X^{p_i^{\alpha_i}} - 1$ dans G qui n'est pas racine de $X^{p_i^{\alpha_i - 1}} - 1$. Un tel élément est donc d'ordre $p_i^{\alpha_i}$, ce qui conclut la démonstration. □

LEMME 1.30. *Soient H un groupe commutatif fini, et $x, y \in H$ d'ordres respectifs a et b. Si a et b sont premiers entre eux alors xy est d'ordre ab.*

DÉMONSTRATION — Considérons l'intersection $M = \langle x \rangle \cap \langle y \rangle$. C'est un sous-groupe de $\langle x \rangle$ et de $\langle y \rangle$. D'après Lagrange, $|M|$ divise a et b et donc $M = \{1\}$. Vérifions maintenant que xy est d'ordre ab. Soit $k \in \mathbb{Z}$. Comme $xy = yx$, on a $(xy)^k = x^k y^k$. En particulier, $(xy)^{ab} = 1$. Réciproquement, si $(xy)^k = 1$ alors $x^k = y^{-k} \in M = \{1\}$, et donc $x^k = y^{-k} = 1$. Ainsi, $a|k$ et $b|k$ puis $ab|k$. □

THÉORÈME 1.31. (Gauss)

(i) Si p est premier impair, alors $(\mathbb{Z}/p^m\mathbb{Z})^\times$ est cyclique.

(ii) Si $m \geq 2$ alors $(\mathbb{Z}/2^m\mathbb{Z})^\times \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{m-2}\mathbb{Z})$.

Commençons par établir une congruence utile.

LEMME 1.32. *Soit $k \geq 0$ un entier.*

(i) Si p est un nombre premier impair, alors $(1+p)^{p^k} \equiv 1 + p^{k+1} \bmod p^{k+2}$.

(ii) De plus, on a $(1+4)^{2^k} \equiv 1 + 2^{k+2} \bmod 2^{k+3}$.

DÉMONSTRATION — Commençons par une observation : si p est un nombre premier, et si $k \geq 1$, alors $a \equiv b \bmod p^k$ entraîne $a^p \equiv b^p \bmod p^{k+1}$. En effet, cela découle immédiatement de ce que $\binom{p}{i} \equiv 0 \bmod p$ si $i = 1, \ldots, p-1$. Le (i) et (ii) s'en déduisent par récurrence sur k. Remarquer aussi que le (i) ne s'étend pas au cas $p = 2$ et $k = 1$. □

DÉMONSTRATION — (de la proposition) Le lemme précédent (ii) assure que la classe de 5 est d'ordre 2^{m-2} dans $(\mathbb{Z}/2^m\mathbb{Z})^\times$. Vérifions que le morphisme de groupes

$$\mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/2^{m-2}\mathbb{Z}) \to (\mathbb{Z}/2^m\mathbb{Z})^\times,$$

donné par $(p, q) \mapsto (-1)^p 5^q \bmod 2^m$, est un isomorphisme. Pour des raisons de cardinalité, il suffit de voir qu'il est injectif. Mais si $(-1)^p 5^q \equiv 1 \bmod 2^m$, alors par réduction modulo 4 on obtient $(-1)^p = 1$, puis $5^q \equiv 1 \bmod 2^m$ et donc $q = 0$ car 5 est d'orde 2^{m-2} modulo 2^m, ce qui démontre le (ii).

Supposons maintenant p impair. Le lemme précédent assure que $1+p$ est d'ordre p^{m-1} modulo p^m. Comme $(p-1, p) = 1$, et d'après le lemme 1.30, il suffit pour conclure de trouver un élément d'ordre $p-1$ dans $(\mathbb{Z}/p^m\mathbb{Z})^\times$. D'après Gauss, il existe un entier a dont la classe engendre $(\mathbb{Z}/p\mathbb{Z})^\times$ modulo p. Soit d l'ordre de la classe de a dans $(\mathbb{Z}/p^m\mathbb{Z})^\times$. En réduisant modulo p la relation $a^d \equiv 1 \bmod p^m$ on constate que $p-1$ divise d. On vérifie alors immédiatement que $a^{\frac{d}{p-1}}$ est d'ordre $p-1$ dans $(\mathbb{Z}/p^m\mathbb{Z})^\times$. □

Un entier a dont la classe dans $\mathbb{Z}/N\mathbb{Z}$ engendre $(\mathbb{Z}/N\mathbb{Z})^\times$ est parfois appelé une *racine primitive modulo N*. Par exemple, 2 est une racine primitive modulo 5 mais pas modulo 7. En effet, les puissances successives de 2 modulo 5 sont $\equiv 1, 2, 4, 3$ et parcourent donc tout $(\mathbb{Z}/5\mathbb{Z})^\times$. Par contre, les puissances successives de 2 modulo 7 sont $\equiv 1, 2, 4$ et 2 est seulement d'ordre 3 modulo 7. Le théorème de Gauss assure l'existence de racines primitives modulo tout nombre premier p, mais ne fournit pas pour autant de procédé constructif efficace pour en construire. Mentionnons cette conjecture célèbre due à E. Artin : "tout entier $a \neq -1$ qui n'est pas un carré est une racine primitive modulo p pour une infinité de nombres premiers p".

En guise d'application du théorème de Gauss, voici une généralisation du critère d'Euler.

PROPOSITION 1.33. (Critère d'Euler généralisé) *Soient p un nombre premier impair et n un entier divisant $p-1$. Alors $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ est une puissance $n$ième si, et seulement si, $x^{\frac{p-1}{n}} = 1$.*

Le critère d'Euler s'en déduit : en effet, le petit théorème de Fermat assure que si $(a,p) = 1$, alors $(a^{\frac{p-1}{2}})^2 \equiv 1 \bmod p$ et donc $a^{\frac{p-1}{2}} \equiv \pm 1 \bmod p$ par un argument déjà donné dans la preuve de la proposition 1.2.

DÉMONSTRATION — (du critère d'Euler généralisé) Si $x = y^n$ avec $y \in (\mathbb{Z}/p\mathbb{Z})^\times$, le petit théorème de Fermat entraîne que $x^{\frac{p-1}{n}} = 1$. Réciproquement, supposons que $x^{\frac{p-1}{n}} = 1$. Soit $y \in (\mathbb{Z}/p\mathbb{Z})^\times$ un générateur (qui existe d'après le théorème de Gauss), écrivons $x = y^k$ pour un certain $k \in \mathbb{Z}$. Il vient $y^{k\frac{p-1}{n}} = 1$ et donc $p-1$ (l'ordre de y) divise $k\frac{p-1}{n}$. Ceci entraîne que n divise k, puis que $x = (y^{k/n})^n$ est une puissance $n$ième. □

REMARQUE 1.34. En guise d'autre application, retrouvons que si $a \equiv 1 \bmod 8$ alors a est un carré dans $\mathbb{Z}/2^m\mathbb{Z}$ pour tout entier $m \geq 3$ (Lemme. 1.11). D'après la démonstration du théorème 1.31, a s'écrit $(-1)^p 5^q$ avec $(p,q) \in (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{m-2}\mathbb{Z})$. Comme $a \equiv 1 \bmod 8$, on a $p = 0$ et $q \equiv 0 \bmod 2$, mézalor $a = (5^{q/2})^2$ est un carré. On en déduirait de même aisément le reste du lemme 1.11.

8. Exercices

Dans ces exercices, le nombre p désignera par défaut un nombre premier impair.

EXERCICE 1.1. *Est-ce que 47 est un carré modulo 79 ?*

EXERCICE 1.2. *Soient p et q des nombres premiers impairs. Vérifier que la loi de réciprocité quadratique s'écrit aussi $\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right)$ où $q^* = (-1)^{\frac{q-1}{2}} q$.*

EXERCICE 1.3. *Soient $a, b \in \mathbb{Z}$ et $D := a^2 - 4b$. Montrer que l'image du polynôme $X^2 + aX + b$ dans $(\mathbb{Z}/p\mathbb{Z})[X]$ (resp. $(\mathbb{Z}/2\mathbb{Z})[X]$) est irréductible si, et seulement si, on a $\left(\frac{D}{p}\right) = -1$ (resp. $D \equiv 5 \bmod 8$).*

EXERCICE 1.4. *On se propose de calculer $\left(\frac{-3}{p}\right)$ sans utiliser la loi de réciprocité quadratique.*

(i) Montrer que $(\mathbb{Z}/p\mathbb{Z})^\times$ admet un élément d'ordre 3 si, et seulement si, $p \equiv 1 \bmod 3$.

(ii) Conclure en considérant le polynôme $X^2 + X + 1$ dans $(\mathbb{Z}/p\mathbb{Z})[X]$.

EXERCICE 1.5. *On suppose $p \equiv 1 \bmod 4$. Montrer $(\frac{p-1}{2})!^2 \equiv -1 \bmod p$.*

EXERCICE 1.6. *(i) Montrer qu'au moins l'un des entiers -1, 2 ou -2 est un carré modulo p.*

(ii) En déduire que le polynôme X^4+1 est irréductible dans $\mathbb{Q}[X]$ mais réductible dans $(\mathbb{Z}/p\mathbb{Z})[X]$ pour tout nombre premier p.

EXERCICE 1.7. *Montrer que -1 est une puissance 4ème modulo p si, et seulement si, on a $p \equiv 1 \bmod 8$.*

EXERCICE 1.8. (Carrés modulo p de l'intervalle $\{1, \dots, \frac{p-1}{2}\}$). *Soit C le nombre de carrés modulo p appartenant à l'intevalle $\{1, \dots, \frac{p-1}{2}\}$, et soit N celui des non-carrés, de sorte que l'on ait $C + N = \frac{p-1}{2}$.*

(i) Montrer que $p \equiv 1 \bmod 4$ entraîne $C = \frac{p-1}{4}$.

(ii) Montrer que l'on a $C = N$ si, et seulement si, $p \equiv 1 \bmod 4$.

On se propose de montrer que si $p \equiv 3 \bmod 8$ et $p \neq 3$ alors $C \equiv N \bmod 3$. On introduit les entiers

$$\alpha = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) a, \quad \beta = \sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right) a \quad \text{et} \quad \gamma = \sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right).$$

(iii) Montrer $\alpha = (1 - \left(\frac{-1}{p}\right))\beta + p\left(\frac{-1}{p}\right)\gamma$.

(iv) Montrer $\alpha = \left(\frac{2}{p}\right)\left[2\,(1 - \left(\frac{-1}{p}\right))\beta + p\left(\frac{-1}{p}\right)\gamma\right]$.

(v) En déduire que si $p \equiv 3 \bmod 8$ alors on a $p\gamma = 3\beta$.

(vi) Conclure et donner quelques exemples.

EXERCICE 1.9. *Soient $\alpha, \beta \in (\mathbb{Z}/p\mathbb{Z})^\times$. On se propose de calculer le nombre S des solutions $(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2$ de l'équation $\alpha x^2 + \beta y^2 = 1$.*

(i) Soit $a \in \mathbb{Z}/p\mathbb{Z}$. Montrer le nombre $\mathrm{N}(x^2 = a)$ des $x \in \mathbb{Z}/p\mathbb{Z}$ tels que $x^2 = a$ vaut $1 + \left(\frac{a}{p}\right)$.

(ii) En déduire $S = \sum_{a,b \in \mathbb{Z}/p\mathbb{Z}, \alpha a + \beta b = 1} \mathrm{N}(x^2 = a)\mathrm{N}(x^2 = b)$, puis $S = p + \left(\frac{\beta}{p}\right) J$ où $J = \sum_{a \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{a(1-\alpha a)}{p}\right)$.

(iii) Montrer $J = \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{a^{-1}-\alpha}{p}\right)$, puis $S = p - \left(\frac{-\alpha\beta}{p}\right)$.

(iv) En déduire $S \neq 0$.

(v) Que dire du nombre des solutions $(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2$ de l'équation $\alpha x^2 + \beta y^2 = 0$?

EXERCICE 1.10. *Soient $m, n \in \mathbb{Z}$ avec n impair positif. Montrer que si le symbole de Jacobi $\left(\frac{m}{n}\right)$ vaut -1 alors m n'est pas un carré modulo n.*

EXERCICE 1.11. (Test de primalité de Solovay-Strassen) *Soit n un entier impair positif.*

(i) Montrer que n est premier si, et seulement si, $x^{\frac{n-1}{2}} \equiv \left(\frac{x}{n}\right) \bmod n$ pour tout $x \in (\mathbb{Z}/n\mathbb{Z})^\times$.

(ii) En déduire que si n n'est pas premier, au moins la moitié des $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ vérifient $x^{\frac{n-1}{2}} \not\equiv \left(\frac{x}{n}\right) \bmod n$.

EXERCICE 1.12. *Soit $0 \leq i \leq p-1$. Montrer que la somme $\sum_{a\in\mathbb{Z}/p\mathbb{Z}} \left(\frac{a}{p}\right) a^i$ vaut 0 si $i \neq \frac{p-1}{2}$, -1 sinon.*

EXERCICE 1.13. *Si G désigne la somme de Gauss relative à p, montrer l'identité $G = \sum_{a=0}^{p-1} \zeta^{a^2}$.*

EXERCICE 1.14. (Le signe de la somme de Gauss,[5] d'après Dirichlet) *Soient $N \geq 1$ et $G_N = \sum_{a=0}^{N-1} e^{\frac{2i\pi a^2}{N}}$.*

(i) Soient $a < b$ deux entiers et $f : [a, b] \to \mathbb{C}$ une fonction continue et $\mathcal{C}^1$ par morceaux. Montrer

$$\frac{f(a)+f(b)}{2} + \sum_{k=a+1}^{b-1} f(k) = \sum_{n\in\mathbb{Z}} \int_a^b f(t)e^{2i\pi nt}dt.$$

(ii) Montrer $G_N = (1 + i^{-N})N^{\frac{1}{2}}I$ où $I = \int_{-\infty}^{+\infty} e^{2i\pi t^2}dt$.

(iii) En déduire $I = \frac{1+i}{2}$ (intégrale de Gauss) et

$$G_N = \begin{cases} (1+i)N^{\frac{1}{2}} & \text{si } N \equiv 0 \bmod 4, \\ N^{\frac{1}{2}} & \text{si } N \equiv 1 \bmod 4, \\ 0 & \text{si } N \equiv 2 \bmod 4, \\ iN^{\frac{1}{2}} & \text{si } N \equiv 3 \bmod 4. \end{cases}$$

EXERCICE 1.15. *(i) Montrer que si $a \in \mathbb{Z}$ est un carré modulo p, alors a n'est pas une racine primitive modulo p.*

(ii) On suppose de plus que $\frac{p-1}{2}$ est premier. Montrer que $a \in \mathbb{Z}$ est une racine primitive modulo p si, et seulement si, $\left(\frac{a}{p}\right) = -1$ et $a \not\equiv \pm 1 \bmod p$.

EXERCICE 1.16. *On suppose que p est un nombre premier de Fermat[6], c'est-à-dire de la forme $2^{2^m} + 1$. Par exemple, $p = 3, 5, 17, 257$ ou 65537.*

5. Lorsque N est premier impair, cette somme est bien la somme de Gauss relative à N d'après l'exercice 1.13.

6. Fermat avait conjecturé que tous les nombres de la forme $F_m = 2^{2^m} + 1$ sont des nombres premiers. Euler a remarqué qu'il n'en est rien car 641 divise F_5. En fait, les seuls F_m premiers connus actuellement sont F_0 à F_4 cités ci-dessus.

(i) Montrer que $a \in \mathbb{Z}$ est une racine primitive modulo p si, et seulement si, $\left(\frac{a}{p}\right) = -1$.

(ii) En déduire que 3 est une racine primitive modulo p dès que $p \neq 3$.

EXERCICE 1.17. *Quelle est la période du décimal $\frac{1}{65537}$?*

EXERCICE 1.18. *Montrer que le groupe multiplicatif du corps (non-commutatif) des quaternions de Hamilton contient un sous-groupe fini non-cyclique.*

EXERCICE 1.19. *(i) Montrer que si G est un groupe cyclique et si q divise $|G|$, alors G a un unique sous-groupe de cardinal q, qui est cyclique.*

(ii) En déduire que $(\mathbb{Z}/N\mathbb{Z})^\times$ est cyclique si, et seulement si, $N = 2, 4, p^m, 2p^m$ où p est premier impair et $m \geq 0$.

EXERCICE 1.20. *Soient $N \geq 2$ un entier et soit $\mathcal{Q}$ la réunion de l'ensemble des nombres premiers impairs et de $\{4, 8\}$. Soient s le nombre d'éléments de $\mathcal{Q}$ divisant N et $C(N)$ l'ensemble des carrés de $(\mathbb{Z}/N\mathbb{Z})^\times$.*

(i) Montrer $|C(N)| = \frac{\varphi(N)}{2^s}$ et $(\mathbb{Z}/N\mathbb{Z})^\times/C(N) \simeq (\mathbb{Z}/2\mathbb{Z})^s$.

(ii) Montrer que si $a \in C(N)$, il existe exactement 2^s éléments $b \in (\mathbb{Z}/N\mathbb{Z})^\times$ tels que $a = b^2$.

EXERCICE 1.21. *Soit $N \geq 2$ un entier. Montrer que $\overline{\mathbb{Z}}/N\overline{\mathbb{Z}}$ est infini.*

EXERCICE 1.22. (Une démonstration géométrique de la loi de réciprocité quadratique, d'après Eisenstein [7]) *Soit p un nombre premier impair et soit $q \geq 1$ un entier impair premier à p. On se propose de montrer, suivant Eisenstein, la relation*

$$\left(\frac{q}{p}\right) = (-1)^e,$$

où e désigne le nombre des points de coordonnées entières à l'intérieur du triangle OP'S' (figure 1).

(i) En déduire la loi de réciprocité quadratique.

On suppose d'abord simplement l'entier $q \geq 1$ premier à p. On pose $X = \{2, 4, \ldots, p-1\}$ et on note $R \subset \{1, \ldots, p-1\}$ l'ensemble des restes de la division par p des qx, pour $x \in X$.

(ii) Vérifier que l'application $\{1, \ldots, p-1\} \to X$, définie par

$$r \mapsto \begin{cases} r & \text{si } r \text{ est pair,} \\ p - r & \text{sinon,} \end{cases}$$

induit une bijection de R sur X.

7. *Geometrischer Beweis des Fundamentaltheorems für die quadratischen Reste*, Crelle's Journal 28, 246–249 (1844).

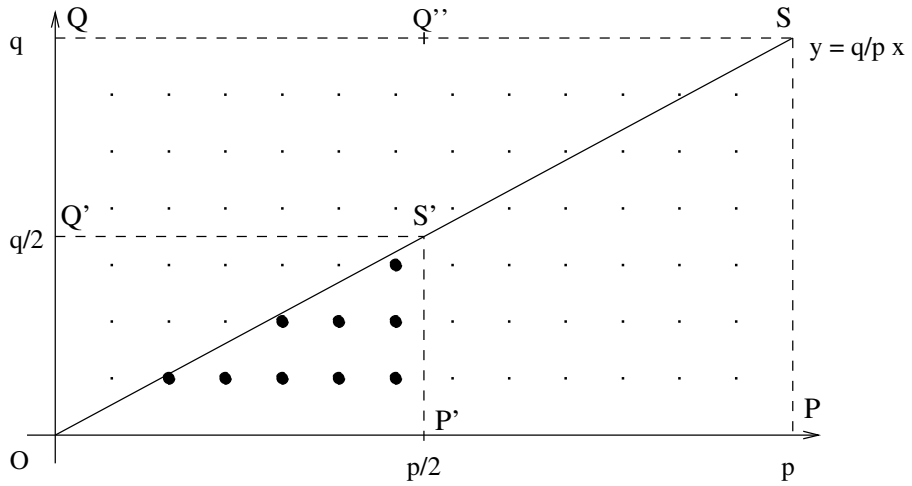

FIGURE 1. $\left(\frac{q}{p}\right) = (-1)^e$ où e est le nombre de points noirs (Eisenstein)

(iii) En déduire $\left(\frac{q}{p}\right) = (-1)^{\sum r}$, *la somme portant sur les* $r \in R$. *(On pourra considérer le produit des éléments de* X *modulo* p*)*

(iv) Vérifier que si $x \in X$, *et si* r *est le reste de la division de* qx *par* p, *on a* $r \equiv [qx/p] \bmod 2$.

(v) En déduire $\left(\frac{q}{p}\right) = (-1)^f$ *où* f *désigne le nombre des points à l'intérieur du triangle OPS dont les coordonnées sont entières, et d'abscisse paire.*

(vi) On suppose q *impair. Soit* A *(resp.* B*) le nombre des points à coordonnées entières et d'abscisse paire à l'intérieur du trapèze* $P'PSS'$ *(resp. du triangle* $S'SQ''$*). Montrer* $A \equiv B \bmod 2$.

(vii) En déduire la relation d'Eisenstein.

(viii) Montrer aussi $\left(\frac{2}{p}\right) = (-1)^f$ *où* f *désigne le nombre d'entiers pairs compris entre* $p/2$ *et* p, *puis* $f \equiv \frac{p^2-1}{8} \bmod 2$.

Chapitre 2

Géométrie des nombres

Ce chapitre a pour but d'introduire la *géométrie des nombres*. Inventée[1] par Minkowski en 1896, elle consiste à donner une minoration du nombre des points d'un réseau de l'espace euclidien $\mathbb{R}^n$ appartenant à une partie convexe donnée, et ce en fonction de leurs volumes. Appliquées à certains réseaux de nature arithmétique, ces estimations ont des conséquences nombreuses et spectaculaires appartenant à la théorie des nombres. En guise d'illustrations, nous retrouverons dans ce chapitre les deux résultats classiques suivants, et bien d'autres du même genre :

THÉORÈME 2.1. (Fermat, Euler) *Tout nombre premier congru à* 1 *modulo* 4 *est la somme de deux carrés d'entiers.*

THÉORÈME 2.2. (Lagrange) *Tout entier est la somme de quatre carrés d'entiers.*

Les démonstrations originales de ces deux résultats (par Euler et Lagrange) étaient basées notamment sur un argument de "descente infinie". Il y en a eu depuis beaucoup d'autres. Dans la suite du cours, la théorie de Minkowski aura une autre application importante : elle nous permettra de borner de manière efficace le *nombre de classes* d'un corps de nombres. Elle permettrait aussi de démontrer le "sens difficile" du *théorème des unités* de Dirichlet.

RÉFÉRENCES : P. Samuel, *Théorie algébrique des nombres*, Éd. Hermann, chapitre 4.1.

I. Stewart & D. Tall, *Algebraic number theory*, Éd. Chapman & Hall, chapitres 6 et 7. Les preuves que nous donnerons des deux théorèmes ci-dessus sont notamment issues du chapitre 7 de ce livre.

1. Réseaux de $\mathbb{R}^n$

Fixons $n \geq 1$ un entier. Dans tout ce chapitre, V désignera l'espace vectoriel $\mathbb{R}^n$ muni d'une norme $|.|$ fixée quelconque. Rappelons qu'une partie $D \subset V$ est *discrète* si pour tout réel $r > 0$, l'ensemble $\{v \in D, |v| \leq r\}$ est fini. Cette propriété ne dépend pas du choix de $|.|$ par équivalence des normes sur V.

DÉFINITION 2.3. *Un réseau de V est un sous-groupe discret qui engendre V comme $\mathbb{R}$-espace vectoriel.*

1. Minkowski, "Geometrie der Zahlen", http://www.archive.org/details/geometriederzahl00minkrich.

Autrement dit, c'est une partie discrète $L \subset V$ telle que pour tout $a, b \in L$ alors $a - b \in L$, et telle qu'il existe $e_1, \ldots, e_n \in L$ qui est une base du $\mathbb{R}$-espace vectoriel V. L'exemple typique est le sous-groupe $\mathbb{Z}^n$ des éléments à coordonnées entières. En guise d'autre exemple, l'ensemble

$$L_0 := \{(a, b) \in \mathbb{Z}^2, a \equiv 2b \bmod 3\}$$

est aussi un réseau de $\mathbb{R}^2$. En effet, il est discret (car inclus dans $\mathbb{Z}^2$) et contient une base de $\mathbb{R}^2$, par exemple $(3, 0)$, $(0, 3)$.

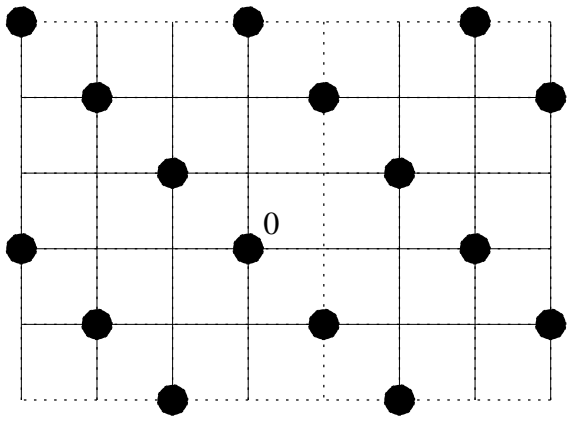

FIGURE 1. Le réseau L_0

On rappelle qu'une famille $e_1, \ldots, e_r$ d'un groupe abélien G est dite $\mathbb{Z}$-génératrice (ou simplement génératrice si le contexte ne prête pas à confusion) si tout élément de g s'écrit sous la forme $\sum_{i=1}^{r} m_i e_i$ avec $m_i \in \mathbb{Z}$ pour $i = 1, \ldots, r$. On dit que c'est une $\mathbb{Z}$-base si de plus une telle écriture est unique.

THÉORÈME 2.4. *(Caractérisation algébrique des réseaux) Soit $L \subset V$ un sous-groupe. Les conditions suivantes sont équivalentes.*

(i) L est un réseau.

(ii) L admet une famille finie $\mathbb{Z}$-génératrice qui est une $\mathbb{R}$-base de V.

En particulier, tout réseau de $\mathbb{R}^n$ admet une $\mathbb{Z}$-base à n éléments.

Donnons quelques exemples avant d'entamer la démonstration. Tout d'abord, il est évident que la base canonique $e_1, \ldots, e_n$ de $\mathbb{R}^n$ est une $\mathbb{Z}$-base de son sous-groupe $\mathbb{Z}^n$: on a $(m_i) = \sum_i m_i e_i$ pour tout $m_1, \ldots, m_n \in \mathbb{Z}$. De plus, remarquons aussi que $(1, -1)$ et $(2, 1)$ forment une $\mathbb{Z}$-base du réseau L_0 ci-dessus, de même que $(3, 0)$ et $(2, 1)$. Cela résulte en effet des écritures :

$$(a, b) = \frac{a - 2b}{3}\,(3, 0) + b\,(2, 1), \quad \text{et} \quad (a, b) = \frac{a - 2b}{3}\,(1, -1) + \frac{a + b}{3}\,(2, 1).$$

Le sens (ii) implique (i) du théorème est le plus simple, résulte de la proposition-definition qui suit.

PROPOSITION-DÉFINITION 2.5. *Soit $e = \{e_1, \dots, e_n\}$ une base de l'espace vectoriel V, on note*

$$L(e) = \{m_1 e_1 + m_2 e_2 + \cdots + m_n e_n, \quad m_1, m_2, \dots, m_n \in \mathbb{Z}\}$$

le sous-groupe engendré par e, c'est un réseau de V.

Notons qu'il est évident que e est aussi une $\mathbb{Z}$-base de $L(e)$. En considérant la norme $|\sum_i v_i e_i| = \sup_i |v_i|$ sur V, il est clair que $L(e)$ est une partie discrète de V : $L(e)$ est bien un réseau. Le théorème ci-dessus affirme que tout réseau est de la forme $L(e)$ pour une certaine $\mathbb{R}$-base e de V.

Nous serons amené à introduire le *pavé fondamental* de V associé à la base $e = \{e_1, \dots, e_n\}$: c'est l'ensemble

$$\Pi(e) = \{\sum_{i=1}^{n} v_i e_i, v_i \in [0, 1[\} \subset V.$$

Sa propriété principale est la suivante :

LEMME 2.6. *Soit $e = \{e_1, \dots, e_n\}$ une base de V. Tout $v \in V$ s'écrit de manière unique sous la forme $\lambda + x$ avec $\lambda \in L(e)$ et $x \in \Pi(e)$.*

DÉMONSTRATION — Désignons par $[t] \in \mathbb{Z}$ la partie entière inférieure du nombre réel t : c'est l'unique entier relatif m tel que $m \leq t < m + 1$. Si $v = \sum_{i=1}^{n} v_i e_i \in V$ alors $v = \lambda + x$ avec $\lambda = \sum_i [v_i] e_i \in L$ et $x = \sum_i (v_i - [v_i]) e_i \in \Pi(e)$. L'unicité de cette écriture se déduit coordonnée par coordonnée de celle de la partie entière inférieure, car (e_i) est une base de V. □

Le théorème résultera du lemme et de la proposition suivants.

LEMME 2.7. *Soient L un réseau de V et $e_1, \dots, e_n$ une base de $\mathbb{R}^n$ telle que $e_i \in L$ pour tout i. Alors $L(e)$ est d'indice fini dans L et il existe un entier $N \geq 1$ tel que $L \subset \frac{1}{N} L(e)$.*

DÉMONSTRATION — Il est clair que l'on a $L(e) \subset L$. Vérifions tout d'abord que $L/L(e)$ est fini. En effet, d'après le lemme 2.6 tout élément $v \in V$ s'écrit de manière unique sous la forme $v = \lambda(v) + x(v)$ où $\lambda(v) \in L(e)$ et $x(v) \in \Pi(e)$. Comme $L(e) \subset L$, on en tire que $x(v) = v - \lambda(v) \in L \cap \Pi(e)$ si $v \in L$. Mais L est discret et $\Pi(e)$ est borné, et donc $L \cap \Pi(e)$ est fini ! En particulier, $|L/L(e)| \leq |L \cap \Pi(e)| < +\infty$.

D'après le théorème de Lagrange appliqué au groupe quotient fini $L/L(e)$, on constate que si l'on pose $N := |L/L(e)|$ alors $N \cdot L/L(e) = 0$, c'est-à-dire que $NL \subset L(e)$. □

PROPOSITION 2.8. *Soit L un réseau de V et soit $\mathcal{B}$ l'ensemble des bases $e = \{e_1, \dots, e_n\}$ de V telles que $e_i \in L$ pour tout i. Alors il existe $e \in \mathcal{B}$ telle que $|\det(e_1, \dots, e_n)|$ est minimal, et pour tout tel e on a $L = L(e)$.*

Le déterminant de la famille de vecteurs e_i ci-dessus est pris de manière sous-entendue relativement à la base canonique de $V = \mathbb{R}^n$.

DÉMONSTRATION — Comme L engendre l'espace vectoriel V, il contient une base de V, et donc $\mathcal{B}$ est non vide. Fixons $e \in \mathcal{B}$. Il est clair que $L(e) \subset L$. Soit $N \geq 1$ tel que $L \subset \frac{1}{N} L(e)$ (Lemme 2.7). Tout élément de L s'écrit donc sous la forme $\sum_i \frac{m_i}{N} e_i$ avec $m_i \in \mathbb{Z}$ pour tout i. En particulier, pour tout $f = \{f_1, \dots, f_n\} \in \mathcal{B}$, on a par multi-linéarité de det

$$\det(f) \in N^{-n} \det(e)\mathbb{Z}.$$

Cet ensemble de valeurs est discret dans $\mathbb{R}$, on peut donc bien choisir $e \in \mathcal{B}$ tel que $|\det(e)|$ est minimal (nécessairement non nul).

Comme nous l'avons vu plus haut, tout élément $v \in L$ se décompose sous la forme $\lambda + x$ avec $\lambda \in L(e)$ et $x \in \Pi(e) \cap L$. Il suffit donc de voir $\Pi(e) \cap L = \{0\}$. Soit $v = \sum_i v_i e_i \in \Pi(e) \cap L$, de sorte que $v_i \in [0, 1[$ pour tout i. On cherche à montrer $v_i = 0$ pour tout i. Soit $1 \leq i \leq n$. Si $v_i \neq 0$, alors $v, e_1, \dots, \hat{e_i}, \dots, e_n$ est dans $\mathcal{B}$. Mais le caractère multi-linéaire alterné du déterminant entraîne

$$|\det(e_1, \dots, e_{i-1}, v, e_{i+1}, \dots, e_n)| = v_i |\det(e_1, \dots, e_n)| < |\det(e_1, \dots, e_n)|,$$

ce qui est absurde par minimalité de $\det(e)$. □ □

PROPOSITION 2.9. *Soient $L \subset \mathbb{R}^n$ un réseau et $e = \{e_1, \dots, e_m\}$ une famille $\mathbb{Z}$-génératrice de L. Alors $m \geq n$. De plus, les conditions suivantes sont équivalentes :*

(i) e est une $\mathbb{Z}$-base de L,

(ii) e est une base de l'espace vectoriel $\mathbb{R}^n$,

(iii) $m = n$.

En particulier, toutes les $\mathbb{Z}$-bases de L ont même cardinal n.

DÉMONSTRATION — En effet, comme L engendre l'espace vectoriel $\mathbb{R}^n$, e est une famille génératrice de ce dernier, et donc $m \geq n$. L'équivalence de (ii) et (iii) est alors bien connue. De plus, (ii) implique trivialement (i).

Montrons enfin que (i) entraîne (iii). Si e est une $\mathbb{Z}$-base de L, alors $\psi : \mathbb{Z}^m \to L$, $(m_i) \mapsto \sum_i m_i e_i$ est un isomorphisme de groupes. Soit f une $\mathbb{Z}$-base de L à n éléments (Théorème 2.4). Il vient que $\psi^{-1}(f)$ est une $\mathbb{Z}$-base de $\mathbb{Z}^m$ à n éléments. Mais $\mathbb{Z}^m$ est un réseau de $\mathbb{R}^m$ de manière naturelle, donc la première inégalité démontrée entraîne que $n \geq m$, et donc $n = m$. □

On se propose enfin de décrire toutes les $\mathbb{Z}$-bases d'un réseau à partir d'une seule. Considérons

$$\mathrm{GL}_n(\mathbb{Z}) := \{M \in \mathrm{M}_n(\mathbb{Z}) \mid \exists N \in \mathrm{M}_n(\mathbb{Z}), MN = \mathrm{I}_n\}.$$

Autrement dit, $\mathrm{GL}_n(\mathbb{Z})$ est le sous-groupe de $\mathrm{GL}_n(\mathbb{R})$ constitué des matrices à coefficients entiers, et dont l'inverse aussi est à coefficients entiers.

PROPOSITION 2.10. *(i)* $\mathrm{GL}_n(\mathbb{Z}) = \{M \in \mathrm{M}_n(\mathbb{Z}),\ \det(M) = \pm 1\}$.

(ii) Soient $e = (e_1, \ldots, e_n)$ et $f = (f_1, \ldots, f_n)$ deux bases de V, et soit $P = (p_{i,j})$ la matrice des vecteurs f_j dans la base e_i, i.e. $f_j = \sum_i p_{i,j} e_i$. Alors e et f engendrent le même réseau, c'est-à-dire $L(e) = L(f)$, si, et seulement si, on a $P \in \mathrm{GL}_n(\mathbb{Z})$.

DÉMONSTRATION — Vérifions le (i). Si $M, N \in \mathrm{M}_n(\mathbb{Z})$ satisfont $MN = \mathrm{I}_n$, alors $\det(M)\det(N) = 1$ avec $\det(M), \det(N) \in \mathbb{Z}$, donc $\det(M) = \pm 1$. Réciproquement, si $M \in \mathrm{M}_n(\mathbb{Z})$ et $\det(M) = \pm 1$, la relation $M {}^t\mathrm{Co}(M) = \det(M)\mathrm{I}_n$ assure que $M^{-1} = {}^t\mathrm{Co}(M)\det(M)^{-1} \in \mathrm{M}_n(\mathbb{Z})$.

Montrons le (ii). Remarquons que f_j appartient au réseau engendré par les e_i si, et seulement si, la j-ième colonne de P est à coefficients entiers. Introduisons par symmétrie la matrice $Q \in \mathrm{GL}_n(\mathbb{R})$ des vecteurs e_j dans la base f_i, on a donc $PQ = \mathrm{I}_n$. D'après la remarque ci-dessus, les e_i et les f_j engendrent le même réseau si, et seulement si, P et Q sont à coefficients entiers, c'est-à-dire si $P \in \mathrm{GL}_n(\mathbb{Z})$. □

EXEMPLE 2.11. *Les éléments (a, b) et (c, d) de $\mathbb{Z}^2$ engendrent $\mathbb{Z}^2$ si, et seulement si, on a $ad - bc = \pm 1$.*

2. Lemme du corps convexe de Minkowski

Nous aurons besoin de considérer le volume (ou "mesure") de certaines parties de $\mathbb{R}^n$. On munit donc dans ce qui suit l'espace vectoriel $V = \mathbb{R}^n$ de la mesure de Lebesgue [2] que l'on notera μ, vérifiant $\mu([0,1]^n) = 1$.

DÉFINITION 2.12. *Soient L un réseau de $\mathbb{R}^n$ et X un sous-ensemble mesurable de $\mathbb{R}^n$. On dit que X est un* domaine fondamental *(pour l'action) de L si tout $v \in \mathbb{R}^n$ s'écrit de manière unique sous la forme $\lambda + x$ avec $\lambda \in L$ et $x \in X$.*

Il existe des domaines fondamentaux, d'après la caractérisation algébrique des réseaux et le :

LEMME 2.13. *Si e est une base de V alors $\Pi(e)$ est un domaine fondamental de $L(e)$ de mesure $|\det(e_1, \ldots, e_n)| \in \mathbb{R}_{>0}$.*

DÉMONSTRATION — La mesurabilité de $\Pi(e)$ et la formule donnée pour sa mesure sont conséquences de la formule du jacobien ("changement de variables") en théorie de l'intégration. Le reste se déduit du lemme 2.6. □

2. Nous renvoyons par exemple au cours de W. Rudin *Real and complex analysis* pour la construction de la mesure de Lebesgue.

On constate, en considérant par exemple les pavés associés à différentes $\mathbb{Z}$-bases d'un réseau L, qu'il existe une multitude de domaines fondamentaux différents. Il en existe en fait encore bien plus qui ne sont pas des pavés (pourquoi ?). Remarquons cependant que les différents pavés fondamentaux de L ont tous même mesure. En effet, observons que si e et f sont des bases de V, et $P \in \mathrm{GL}_n(\mathbb{R})$ est la matrice des f_j dans la base e_i comme dans la proposition 2.10, le lemme ci-dessus entraîne

$$\mu(\Pi(f))) = |\det(P)|\mu(\Pi(e)) \tag{1}$$

En particulier, si $L(e) = L(f)$ alors $\det(P) = \pm 1$ car $P \in \mathrm{GL}_n(\mathbb{Z})$, et donc $\mu(\Pi(f)) = \mu(\Pi(e))$ comme il était annoncé. Cette observation est en fait un cas particulier du résultat suivant :

Lemme 2.14. (Blichfeldt) *Soient L un réseau de V, et $X, Y \subset V$ deux parties mesurables. On suppose que X est un domaine fondamental de V, et que $\forall x, y \in Y$, $x - y \in L \Rightarrow x = y$. Alors $\mu(Y) \leq \mu(X)$.*

En particulier, tous les domaines fondamentaux de L ont même mesure, égale à celle d'un pavé fondamental de L, et qui est donc finie et non nulle.

Il sera commode d'adopter la notation suivante : pour toute partie $A \subset V$ et pour $v \in V$, on notera $A + v = \{a + v, a \in A\}$. De même, $A - v = A + (-v)$.

Démonstration — En effet, X étant un domaine fondamental de L, V admet la décomposition en réunion dénombrable disjointe [3]

$$V = \coprod_{\lambda \in L} (X + \lambda).$$

En prenant l'intersection avec Y, on obtient $Y = \coprod_{\lambda \in L} Y \cap (X + \lambda)$. La relation évidente

$$(Y \cap (X + \lambda)) - \lambda = X \cap (Y - \lambda),$$

combinée avec l'invariance par translation de la mesure de Lebesgue, assure

$$\mu(Y) = \sum_{\lambda \in L} \mu(X \cap (Y - \lambda)).$$

Mais par hypothèse sur Y, les $Y - \lambda$ sont des parties disjointes de V quand λ varie dans L, de sorte que la somme de droite dans l'égalité ci-dessus est $\leq \mu(X)$, ce qui conclut. □

Définition 2.15. (Covolume d'un réseau) *Le covolume* $\mathrm{covol}(L)$ *d'un réseau $L \subset V$ est la mesure commune des domaines fondamentaux de L, c'est un élément de $\mathbb{R}_{>0}$.*

La proposition suivante est un résultat fondamental en géométrie des nombres. On rappelle qu'une partie $C \subset V$ est dite convexe si pour tous $v, v' \in C$, et tout $\lambda \in [0, 1]$, on a $\lambda v + (1 - \lambda)v' \in C$. Elle est dite symétrique si pour tout $v \in C$, alors $-v \in C$. L'exemple typique de partie convexe symétrique est obtenu en considérant une boule de V centrée en l'origine, relativement à une norme quelconque

3. Le symbole $\coprod$ désigne une réunion disjointe.

de l'espace V. Remarquons que si C est convexe symétrique, et si $x, y \in C$, alors $\frac{x-y}{2} = \frac{1}{2}x + \frac{1}{2}(-y) \in C$.

PROPOSITION 2.16. *(Lemme du corps convexe de Minkowski) Soit $C \subset V$ une partie mesurable symétrique convexe et soit L un réseau de V. Si* $\mathrm{covol}(L) < \frac{\mu(C)}{2^n}$, *ou si C est compact et* $\mathrm{covol}(L) \leq \frac{\mu(C)}{2^n}$, *alors il existe un élément non nul dans $L \cap C$.*

DÉMONSTRATION — En effet, $L' := 2L \subset L$ est un réseau de V : si la base (e_i) engendre L alors la base $(2e_i)$ engendre L'. La formule du jacobien (1) montre $\mathrm{covol}(L') = 2^n \mathrm{covol}(L)$.

Supposons pour commencer $\mathrm{covol}(L') < \mu(C)$. Le lemme de Blichfeldt assure alors qu'il existe $x, y \in C$ distincts tels que $x - y \in 2L$. Mais C est convexe symétrique, donc l'élément $(x-y)/2$ est dans $C \cap L$ et non nul, ce que l'on cherchait.

Supposons maintenant $\mathrm{covol}(L') \leq \mu(C)$ mais que C est compact. Pour tout réel $\varepsilon > 0$, on considère

$$C_\varepsilon = \{v \in V \mid \exists x \in C, |v - x| < \varepsilon\}.$$

On vérifie immédiatement que c'est un ouvert borné convexe symétrique de mesure $> \mu(C)$. Le cas précédent montre donc $(L\backslash\{0\}) \cap C_\varepsilon \neq \emptyset$. Comme L est discret et C_ε est borné, $(L\backslash\{0\}) \cap C_\varepsilon$ est fini. Enfin, il décroît (pour l'inclusion) avec ε : il est donc constant pour ε assez petit, nécessairement égal à $(L\backslash\{0\}) \cap C$ car $\cap_\varepsilon C_\varepsilon = C$ (C est fermé), ce qui termine la preuve. □

Le lemme suivant est utile au calcul du covolume de certains réseaux.

PROPOSITION 2.17. *Soient L un réseau de $\mathbb{R}^n$ et $L' \subset L$ un sous-groupe. Les assertions suivantes sont équivalentes :*

(i) L' est un réseau,

(ii) L' est d'indice fini dans L.

Si elles sont satisfaites, alors $\mathrm{covol}(L') = |L/L'| \,\mathrm{covol}(L)$.

DÉMONSTRATION — Le sous-groupe L' est discret car L l'est. Supposons qu'il est d'indice fini dans L, disons h. Le théorème de Lagrange montre $hL \subset L'$. Comme L engendre $\mathbb{R}^n$ comme espace vectoriel, il en va de même pour hL puis de L'. Cela montre que (ii) entraîne (i). La réciproque se déduit du lemme 2.7. Vérifions maintenant l'assertion sur le covolume. Soit $h = |L/L'|$. Par définition il existe des éléments $\lambda_1, \ldots, \lambda_h \in L$ tels que

$$L = \coprod_{i=1}^{h} (L' + \lambda_i).$$

Soit X un domaine fondamental pour L. Considérons $X' = \coprod_{i=1}^{h}(\lambda_i + X)$. Il est mesurable de mesure $\mu(X') = h\mu(X)$ par invariance de la mesure par translations. On conclut car c'est un domaine fondamental [4] pour L. En effet,

$$\mathbb{R}^n = \coprod_{\lambda\in L}(X+\lambda) = \coprod_{i=1}^{h}\coprod_{\lambda'\in L'}(X+\lambda_i+\lambda') = \coprod_{\lambda'\in\Lambda'}(X'+\lambda').$$

□

Calculons par exemple, le covolume du réseau $L_0 = \{(a,b)\in\mathbb{Z}^2, a\equiv 2b \bmod 3\}$ considéré au premier paragraphe. Soit on invoque le fait que $(1,-1)$, $(2,1)$ en est une $\mathbb{Z}$-base, et donc que l'on a

$$\mathrm{covol}(L) = |\det\begin{pmatrix} 1 & 2 \\ -1 & 1\end{pmatrix}| = 3$$

par le lemme 2.13, soit on constate que le morphisme de groupes : $\mathbb{Z}^2 \to \mathbb{Z}/3\mathbb{Z}$, $(a,b)\mapsto a-2b$, est surjectif de noyau L, de sorte que l'on a un isomorphisme de groupes $\mathbb{Z}^2/L \simeq \mathbb{Z}/3\mathbb{Z}$, et on applique la proposition précédente.

3. Quelques applications arithmétiques

THÉORÈME 2.18. (Fermat, Euler) *Soit p nombre premier $\equiv 1 \bmod 4$. Il existe $a,b\in\mathbb{Z}$ tels que $p = a^2+b^2$.*

Fixons donc un nombre premier $p\equiv 1 \bmod 4$. Le point de départ est le résultat de Fermat-Euler suivant, démontré au premier chapitre.

LEMME 2.19. *-1 est un carré modulo p.*

Nous allons considérer maintenant un réseau judicieux du plan euclidien $\mathbb{R}^2$. D'après le lemme, il existe un entier $u\in\mathbb{Z}$ tel que $u^2\equiv -1 \bmod p$.

LEMME 2.20. *Soit $L = \{(a,b)\in\mathbb{Z}^2, a\equiv ub \bmod p\}$. C'est un réseau de $\mathbb{R}^2$ de covolume p. De plus, pour tout $(a,b)\in L$ on a la congruence $a^2+b^2\equiv 0 \bmod p$.*

DÉMONSTRATION — Considérons en effet l'application $\psi : \mathbb{Z}^2\to\mathbb{Z}/p\mathbb{Z}$ envoyant (a,b) sur $a-bu \bmod p$. C'est un morphisme de groupes manifestement surjectif (considérer par exemple les $(a,0)$), dont le noyau est exactement L par définition. Ainsi, ψ induit un isomorphisme $\mathbb{Z}^2/L\simeq\mathbb{Z}/p\mathbb{Z}$, et le premier point découle donc de la proposition 2.17. Pour le second point, on constate que si $(a,b)\in L$, on a $a^2+b^2\equiv(u^2+1)b^2\equiv 0 \bmod p$. □

4. Remarquons que ce n'est pas nécessairement un pavé, même si X en est un !

On considère maintenant le disque euclidien $C(r) = \{(x, y) \in \mathbb{R}^2,\ x^2 + y^2 < r\}$. Il est clair que $C(r)$ est un ouvert convexe, symétrique, de mesure πr.

LEMME 2.21. *$L \cap C(2p) \neq \{0\}$.*

DÉMONSTRATION — En effet, d'après le lemme du corps convexe de Minkowski il suffit de voir $2p\pi > 4\text{covol}(L) = 4p$; on conclut car $\pi > 2$. □

Terminons la démonstration du théorème. Soit $(a, b) \in L \cap C(2p)\backslash\{0\}$. Alors d'une part $0 < a^2 + b^2 < 2p$ et d'autre part $a^2 + b^2 \equiv 0 \bmod p$: la seule possibilité est donc $p = a^2 + b^2$!

THÉORÈME 2.22. (Lagrange) *Tout entier ≥ 0 est somme de quatre carrés.*

Il suffit évidemment de le démontrer pour les entiers $n \geq 1$ qui sont sans facteur carré, ce que nous supposons désormais. [5]

LEMME 2.23. *Si $n \in \mathbb{Z}$ est sans facteur carré alors -1 est somme de deux carrés dans $\mathbb{Z}/n\mathbb{Z}$.*

DÉMONSTRATION — Le théorème des restes chinois permet de se ramener au cas où n est un nombre premier. En effet, supposons $-1 \equiv x^2 + y^2 \bmod M$ et $-1 \equiv (x')^2 + (y')^2 \bmod N$ avec $(M, N) = 1$. On peut trouver d'après les restes chinois $x'' \in \mathbb{Z}$ tels que $x'' \equiv x \bmod M$ et $x'' \equiv x' \bmod N$. De même, il existe $y'' \in \mathbb{Z}$ tel que $y'' \equiv y \bmod M$ et $y'' \equiv y' \bmod M$. On constate alors que $(x'')^2 + (y'')^2 \equiv -1 \bmod M$, $\bmod N$ et donc $\bmod MN$.

Comme le lemme est évident si $p = 2$ (et faux si $p = 4$!), on suppose maintenant p impair. Dans ce cas, cela résulte par exemple de l'exercice 1.9 (prendre $\alpha = \beta = -1$). On peut aussi raisonner comme suit. Soit $C = \{x^2, x \in \mathbb{Z}/p\mathbb{Z}\}$ l'ensemble des carrés de $\mathbb{Z}/p\mathbb{Z}$ (zéro inclus). D'après la proposition 1.2, $|C| = \frac{p+1}{2}$. On en déduit que C, ainsi que son "opposé translaté " $-1 - C = \{-1 - c, c \in C\}$ ont tous deux $\frac{p+1}{2}$ éléments, et ne peuvent donc être disjoints, il existe donc $x^2, y^2 \in C$ tels que $-1 - x^2 = y^2$. □

D'après ce lemme, on peut trouver $u, v \in \mathbb{Z}$ tels que $-1 + u^2 + v^2 \equiv 0 \bmod n$.

LEMME 2.24. *Soit $L = \{(a, b, c, d) \in \mathbb{Z}^4, c \equiv au + bv \bmod n, d \equiv av - bu \bmod n\}$. C'est un réseau de $\mathbb{R}^4$ de covolume n^2. De plus, pour tout $(a, b, c, d) \in L$ on a $a^2 + b^2 + c^2 + d^2 \equiv 0 \bmod n$.*

DÉMONSTRATION — En effet, L est le noyau du morphisme de groupes $\psi : \mathbb{Z}^4 \longrightarrow (\mathbb{Z}/n\mathbb{Z})^2$ défini par $(a, b, c, d) \mapsto (c - au - bv, d - av + bu)$. Comme ψ est clairement surjectif, L est d'indice n^2 dans $\mathbb{Z}^4$, ce qui prouve le premier point. Enfin, si $(a, b, c, d) \in L$, alors $a^2 + b^2 + c^2 + d^2 \equiv a^2(1 + u^2 + v^2) + b^2(1 + v^2 + u^2) \equiv 0 \bmod n$. □

5. D'après une identité remarquable classique due à Lagrange, que l'on peut aussi voir comme conséquence de la "multiplicativité de la norme des quaternions de Hamilton", il suffirait de le démontrer pour les nombres premiers. Cette réduction ne sera en fait pas nécessaire.

On rappelle que si $r \geq 0$, le disque euclidien $C(r) = \{(x_1, x_2, x_3, x_4) \in \mathbb{R}^4,\ \sum_i x_i^2 < r\}$ est de mesure $\frac{\pi^2}{2} r^2$ (voir l'exercice 2.12).

LEMME 2.25. *$L \cap C(2n) \neq 0$.*

DÉMONSTRATION — En effet, $C(r)$ est un ouvert convexe symétrique de mesure $\pi^2 r^2/2$. On déduit du lemme de Minkowski que si $\frac{\pi^2 r^2}{2} > 16p^2$, c'est-à-dire si $r > \frac{4\sqrt{2}}{\pi}\, p$, alors $C(r) \cap L$ contient un élément non nul. On conclut car $\frac{4\sqrt{2}}{\pi} < 2$. □

Soit $(a, b, c, d) \in L \cap C(2n)$ non nul. On a alors $0 < a^2 + b^2 + c^2 + d^2 < 2n$ et $a^2 + b^2 + c^2 + d^2 \equiv 0 \bmod n$, puis $n = a^2 + b^2 + c^2 + d^2$, ce qui conclut la démonstration du théorème de Lagrange. □

Ces deux démonstrations présentent des similarités frappantes. Elles sont en fait tout à fait typiques de nombreuses démonstrations en théorie des nombres : elles comportent tout d'abord un argument de congruence (dit aussi "local" dans le jargon) qui consiste ici à établir l'identité cherchée modulo un entier bien choisi, et il y a ensuite un argument "global", ici de géométrie des nombres, nous permettant de passer d'une solution modulaire à une vraie solution. La définition du réseau L à partir de $\mathbb{Z}^2$ ou $\mathbb{Z}^4$ pourrait paraître astucieuse, notamment dans le second cas ; elle s'expliquerait en fait très simplement dans le language de la théorie des formes quadratiques sur $\mathbb{Z}/p\mathbb{Z}$. Au final, on constate que la "raison" pour laquelle les deux résultats forts célèbres ci-dessus sont vrais est que les nombres $\frac{4}{\pi}$ et $\frac{4\sqrt{2}}{\pi}$ sont tous deux < 2 !

4. Les nombres premiers de la forme $a^2 + db^2$

Soit $d \geq 1$ un entier, un problème bien naturel dans la continuité des précédents théorèmes est d'essayer de décrire les nombres premiers p de la forme $a^2 + db^2$. Comme les carrés modulo 8 sont $\equiv 0, 1, 4$, un tel nombre satisfera en général des congruences particulières modulo 8. Il satisfera aussi les conditions suivantes :

PROPOSITION 2.26. *Si un entier n sans facteur carré est de la forme $a^2 + db^2$, alors n est un carré modulo d et $-d$ est un carré modulo n.*

DÉMONSTRATION — Il est évident que si $n = a^2 + db^2$ alors n est un carré modulo d. De plus, n et b sont premiers entre eux, car si p premier divise b et n, alors p divise a^2, puis p divise a, et donc p^2 divise n : absurde. On en déduit $b \in (\mathbb{Z}/n\mathbb{Z})^\times$ puis $-d \equiv (ab^{-1})^2 \bmod n$. □

Remarquons que les résultats du premier chapitre, notamment la loi de réciprocité quadratique, nous permettent de décrire très simplement ces conditions. Sur le problème nettement plus difficile de la réciproque, la méthode du chapitre précédent conduit au résultat général suivant.

THÉORÈME 2.27. *Soient $d \geq 1$ un entier et p un nombre entier > 0 tel que $-d$ est un carré modulo p. Alors l'un au moins des nombres*

$$p,\ 2p,\ 3p,\ \ldots,\ hp$$

est de la forme $a^2 + db^2$, où h désigne la partie entière inférieure de $4\frac{\sqrt{d}}{\pi}$.

Notons que p n'est pas nécessairement un nombre premier dans cet énoncé.

DÉMONSTRATION — En effet, on imite essentiellement verbatim la démonstration donnée au chapitre précédent dans le cas $d = 1$. Par hypothèse, il existe $u \in \mathbb{Z}$ tel que $u^2 \equiv -d \bmod p$ et on considère

$$L = \{(a, b) \in \mathbb{Z}^2, a \equiv ub \bmod p\}.$$

C'est un réseau de covolume p tel que $a^2 + db^2 \equiv 0 \bmod p$ pour tout $(a, b) \in L$. Soit

$$C_d(r) = \{(x, y) \in \mathbb{R}^2, x^2 + dy^2 \leq r\},$$

c'est l'image du disque euclidien de rayon $\sqrt{r}$ par la dilatation $(x, y) \mapsto (x, y/\sqrt{d})$, sa surface est donc $\frac{\pi r}{\sqrt{d}}$ (remarquer d'ailleurs que cela tend vers 0 quand d grandit).

Le lemme de Minkowski assure alors l'existence d'un élément non nul dans $L \cap C_d(\frac{4\sqrt{d}}{\pi}p)$. Si $(a, b) \in \mathbb{Z}^2$ est un tel élément, alors $a^2 + db^2 = kp$ où k est un entier tel que $0 < k \leq \frac{4\sqrt{d}}{\pi}$, ce qui conclut. (En fait, $\frac{4\sqrt{d}}{\pi}$ n'est jamais entier car π est transcendant, mais nous n'avons pas besoin de ceci). □

d	1 et 2	3 à 5	6 à 9	10 à 15	16 à 22	23 à 30	31 à 39	40 à 49
h	1	2	3	4	5	6	7	8

TABLE 1. Quelques valeurs de $h := \frac{4}{\pi}\sqrt{d}$.

Le théorème 2.27 a de nombreuses conséquences, et nous allons en explorer quelques-unes.

COROLLAIRE 2.28. (Gauss) *Un nombre premier impair est de la forme $a^2 + 2b^2$ si, et seulement si, il est $\equiv 1, 3 \bmod 8$.*

Par exemple, on a $3 = 1 + 2.1$, $11 = 9 + 2.1$, $17 = 9 + 2.4$, $19 = 1 + 2.9$...

DÉMONSTRATION — La loi de réciprocité quadratique montre que -2 est un carré modulo p si, et seulement si, $p \equiv 1, 3 \bmod 8$. Le théorème 2.27 conclut car $h = 1$ pour $d = 2$. □

COROLLAIRE 2.29. (Euler, Lagrange) *Un nombre premier $\neq 3$ est de la forme $a^2 + 3b^2$ si et seulement s'il est $\equiv 1 \bmod 3$.*

DÉMONSTRATION — En effet, $\left(\frac{-3}{p}\right) = 1$ si, et seulement si, $p \equiv 1 \bmod 3$ d'après la loi de réciprocité quadratique. Le théorème 2.27 montre donc que si $p \equiv 1 \bmod 3$, soit p soit $2p$ est de la forme $a^2 + 3b^2$ car $h = 2$. Mais $2p = a^2 + 3b^2$ est absurde modulo 4. □

L'énoncé particulièrement beau suivant fait suite à la discussion précédent le théorème. On prétend qu'Euler en aurait longtemps cherché une démonstration sans jamais y parvenir !

COROLLAIRE 2.30. (Lagrange, Gauss) *Soit $p \neq 2, 5$ un nombre premier. Alors p (resp. $2p$) est de la forme $a^2 + 5b^2$ si, et seulement si, $p \equiv 1, 9 \bmod 20$ (resp. $p \equiv 3, 7 \bmod 20$).*

DÉMONSTRATION — La loi de réciprocité quadratique assure que $\left(\frac{-5}{p}\right) = 1$ si, et seulement si,

$$p \equiv 1, 3, 7, 9 \bmod 20.$$

Le théorème 2.27 assure alors que pour ces p, soit p soit $2p$ est de la forme $a^2 + 5b^2$. Mais si $n = a^2 + 5b^2$ est impair, on constate que $n \equiv 1 \bmod 4$. Si $2n = a^2 + 5b^2$ avec n impair, on constate aussi que a et b sont impairs, puis que $2n \equiv 6 \bmod 8$, c'est-à-dire $n \equiv 3 \bmod 4$. Le résultat s'en déduit. □

Ce résultat admet un addendum intéressant. Remarquons que si $2p = a^2 + 5b^2$ avec p impair, nous avons vu que a et b sont impairs. On peut donc écrire $a = b + 2c$, puis $2p = (b + 2c)^2 + 5b^2 = 2(2c^2 + 2bc + 3b^2)$, et enfin $p = 2c^2 + 2bc + 3b^2$. Comme l'argument se renverse, on constate que :

REMARQUE 2.31. *(suite) De plus, $2p$ est de la forme $a^2 + 5b^2$ si et seulement si p est de la forme $2a^2 + 2ab + 3b^2$.*

Nous verrons au chapitre suivant que l'apparition ici des deux formes quadratiques $a^2 + 5b^2$ et $2a^2 + 2ab + 3b^2$ n'est pas un hasard !

Par des arguments tout à fait similaires à ceux que nous venons d'introduire, et que nous laissons au lecteur le soin de vérifier, on pourrait démontrer les énoncés suivants, tous dûs à Gauss.

COROLLAIRE 2.32. *Soit p un nombre premier tel que $\left(\frac{-6}{p}\right) = 1$. Alors p (resp. $2p$) est de la forme $a^2 + 6b^2$ si et seulement si $p \equiv \pm 1 \bmod 8$ (resp $p \equiv \pm 3 \bmod 8$). De plus, $2p$ est de la forme $a^2 + 6b^2$ si, et seulement si, p est de la forme $2a^2 + 3b^2$.*

COROLLAIRE 2.33. *Un nombre premier p est de la forme $a^2 + 7b^2$ si, et seulement si, $p = 7$ ou $p \equiv 1, 2, 4 \bmod 7$.*

COROLLAIRE 2.34. *Soit p un nombre premier impair. Alors p (resp. $2p$) est de la forme $a^2 + 8b^2$ si, et seulement si, $p \equiv 1 \bmod 8$ (resp. $p \equiv 3 \bmod 8$). De plus, $2p$ est de la forme $a^2 + 8b^2$ si, et seulement si, p est de la forme $3a^2 + 2ab + 3b^2$.*

COROLLAIRE 2.35. *Soit $p > 3$ un nombre premier. Alors p (resp. $2p$) est de la forme $a^2 + 9b^2$ si, et seulement si, $p \equiv 1 \bmod 12$ (resp. $p \equiv 5 \bmod 12$). De plus, $2p$ est de la forme $a^2 + 9b^2$ si, et seulement si, p est de la forme $2a^2 + 2ab + 5b^2$.*

COROLLAIRE 2.36. *Soit p un nombre premier tel que $\left(\frac{-10}{p}\right) = 1$. Alors p (resp. $2p$) est de la forme a^2+10b^2 si, et seulement si, $p \equiv 1, 3 \bmod 8$ (resp $p \equiv -1, -3 \bmod 8$). De plus, $2p$ est de la forme a^2+10b^2 si, et seulement si, p est de la forme $2a^2+5b^2$.*

Le cas $d = 11$ réserve cependant une surprise. On doit en effet a priori se contenter du résultat suivant :

COROLLAIRE 2.37. *Soit $p > 2$ un nombre premier tel que $\left(\frac{-11}{p}\right) = 1$. Alors soit p, soit $3p$, est de la forme a^2+11b^2. De plus, le second cas se produit si, et seulement si, p est de la forme $3a^2 + 2ab + 4b^2$.*

La différence essentielle avec les cas précédemment étudiés, notamment le cas $d = 5$, est que l'analyse des congruences ne semble pas permettre de trancher entre les deux possibilités. Nous verrons en fait dans l'exercice 2.10 que pour tout entier $N \geq 2$, un élément de $(\mathbb{Z}/N\mathbb{Z})^\times$ est de la forme $a^2 + 11b^2$, avec $a, b \in \mathbb{Z}/N\mathbb{Z}$, si et seulement s'il est de la forme $3u^2 + 2uv + 4v^2$, avec $u, v \in \mathbb{Z}/N\mathbb{Z}$. Ce que le corollaire ne nous dit pas mais que nous démontrerons plus tard, c'est que les deux possibilités sont exclusives (choses que nous avions conclues dans les cas précédents par un argument de congruence) : p et $3p$ ne peuvent pas être simultanément de la forme $a^2 + 11b^2$.

La table suivante donne, parmi les nombres premiers p tels que $\left(\frac{-11}{p}\right) = 1$, c'est-à-dire $p \equiv 1, 3, 4, 5, 9 \bmod 11$, ceux de la forme $a^2 + 11b^2$ (type A), et ceux tels que $3p$ est de la forme $a^2 + 11b^2$ (type B).

p	3	5	23	31	37	47	53	59	67	71	89	97	103	113	137	157	163
type	B	B	B	B	B	A	A	B	B	B	B	B	A	B	B	B	A
p	179	181	191	199	223	229	251	257	269	311	313	317	331	353	367	379	383
type	B	B	B	A	B	B	B	A	A	A	B	B	B	B	B	B	B
p	389	397	401	419	421	433	443	449	463	467	487	499	509	521	577	587	599
type	B	A	A	A	A	B	B	B	B	B	B	A	B	B	B	A	A

TABLE 2. Nombres premiers < 600 de type A ou B

La théorie de la multiplication complexe (Kronecker) fait apparaître un lien tout particulier (mais bien caché !) avec le polynôme $x^3 - x^2 + x + 1$, duquel on pourrait déduire le théorème suivant :

THÉORÈME 2.38. *Soit p un nombre premier $\equiv 1, 3, 4, 5, 9 \bmod 11$. Alors p est de type A si, et seulement si, le polynôme $x^3 - x^2 + x + 1$ admet une racine dans $\mathbb{Z}/p\mathbb{Z}$.*

La démonstration de ce résultat va cependant au-delà des méthodes développées dans ce cours. Il serait facile de le vérifier à l'aide d'un ordinateur pour tous les nombres premiers du tableau ci-dessus. Remarquons enfin que parmi les 51 nombres premiers étudiés, on constate que 15 sont de type A, soit une proportion d'environ $1/3$. On pourrait en fait démontrer que la densité de Dirichlet (voir les exercices

du Chapitre 9 pour cette notion) de l'ensemble des nombres premiers p de type A parmi ceux $\equiv 1, 3, 4, 5, 9 \bmod p$ est exactement $1/3$, mais c'est aussi au-delà des thèmes abordés dans ce cours : c'est une conséquence du théorème ci-dessus et du théorème de Cebotarev.

En revanche, nous allons expliquer plus loin dans ce cours, suivant Gauss et sa théorie du genre des formes binaires, pourquoi cet exemple d'apparence pourtant bien similaire aux précédents (par exemple au cas $d = 5$) est en fait radicalement différent !

Notons que nous pourrions étendre sans trop de difficulté l'analyse précédente à une poignée de $d \geq 15$, bien que ce soit de plus en plus fastidieux quand h grandit. Nous verrions que les disjonctions des cas grandissent et qu'il y a de plus en plus de possibilités distinctes, parfois déterminées par des congruences, parfois non. La théorie des formes quadratiques binaires (Lagrange, Gauss, Legendre) étudiée au chapitre qui suit s'avèrera un outil bien plus efficace pour toutes ces questions.

5. Exercices

EXERCICE 2.1. *Soient $m, n \in \mathbb{Z}$ avec $n \geq 1$ et soit le réseau $L = \{(a, b) \in \mathbb{Z}^2,\ a \equiv mb \bmod n\}$ de $\mathbb{R}^2$. Donner une $\mathbb{Z}$-base de L.*

EXERCICE 2.2. *Montrer que $\{(a, b, c) \in \mathbb{Z}^3, a \equiv b \bmod 5, b \equiv a + c \bmod 2\}$ est un réseau de $\mathbb{R}^3$, calculer son covolume, et en donner une $\mathbb{Z}$-base.*

EXERCICE 2.3. *Montrer qu'un element $(a, b) \in \mathbb{Z}^2$ se complète en une $\mathbb{Z}$-base de $\mathbb{Z}^2$ si, et seulement si, a et b sont premiers entre eux.*

EXERCICE 2.4. *Donner un exemple de famille génératrice du groupe $\mathbb{Z}$ dont on ne peut extraire aucune $\mathbb{Z}$-base.*

EXERCICE 2.5. *Soit $L \subset \mathbb{R}^n$ un réseau et soit $e_1, \ldots, e_n$ une famille d'éléments de L. Montrer que c'est une $\mathbb{Z}$-base de L si, et seulement si, $|\det(e_1, \ldots, e_n)| = \mathrm{covol}(L)$.*

EXERCICE 2.6. *Soit G un groupe abélien. Si $N \geq 1$ on pose $NG = \{Ng, g \in G\}$, c'est un sous-groupe de G.*

(i) On suppose $G = \mathbb{Z}^n$. Montrer que $2G$ est d'indice 2^n dans G.

(ii) En déduire que si $m, n \geq 1$, alors $\mathbb{Z}^n \simeq \mathbb{Z}^m$ entraîne $n = m$.

(iii) Re-démontrer à l'aide de ce résultat la proposition 2.9.

EXERCICE 2.7. *Soit V un $\mathbb{Q}$-espace vectoriel et soit $A \subset V$ un sous-groupe finiment engendré. On se propose de démontrer que A admet une $\mathbb{Z}$-base de cardinal égal à la dimension du $\mathbb{Q}$-espace vectoriel $\mathrm{Vect}_{\mathbb{Q}}(A)$ engendré par A.*

(i) Expliquer pourquoi $\mathrm{Vect}_{\mathbb{Q}}(A)$ *est de dimension finie. On notera* n *cette dimension.*

(ii) Montrer qu'il existe une injection $\mathbb{Q}$*-linéaire* $f : \mathbb{Q}^n \to V$ *et un entier* $N \geq 1$ *tels que*

$$f(\mathbb{Z}^n) \subset A \subset f(\frac{1}{N}\mathbb{Z}^n).$$

(iii) En déduire que le groupe abélien A *est isomorphe à un réseau de* $\mathbb{R}^n$ *et conclure.*

(iv) (Application) Montrer que tout sous-groupe finiment engendré de $\mathbb{C}$ *admet une* $\mathbb{Z}$*-base finie.*

EXERCICE 2.8. *Démontrer le corollaire 2.32.*

EXERCICE 2.9. (Retour sur le cas $d = 11$).

(i) Soit n *un entier. Montrer que* $3n$ *(resp.* $4n$*) est de la forme* $a^2 + 11b^2$ *si, et seulement si,* n *est de la forme* $3a^2 + 2ab + 4b^2$ *(resp.* $a^2 + ab + 3b^2$*).*

(ii) Montrer que si un entier impair est de la forme $a^2+ab+3b^2$*, alors il est soit de la forme* $3a^2 + 2ab + 4b^2$*, soit de la forme* $a^2 + 11b^2$ *(non nécessairement exclusivement).*

On pourra remarquer les identités $(b+3a)^2+11b^2 = 3(3a^2+2ab+4b^2)$ *et* $(a+\frac{b}{2})^2+\frac{11}{4}b^2 = a^2 + ab + 3b^2 = (a + b)^2 - (a + b)b + 3b^2$.

(iii) Démontrer le corollaire 2.37 .

(iv) En déduire que si p *est premier tel que* $\left(\frac{-11}{p}\right) = 1$*, alors* p *est de la forme* $a^2 + ab + 3b^2$.

EXERCICE 2.10. *Si* $N \geq 1$ *est un entier, on considère l'ensemble* $P(N)$ *(resp.* $Q(N)$*) des éléments de* $(\mathbb{Z}/N\mathbb{Z})^\times$ *qui sont de la forme* a^2+11b^2 *(resp.* $3a^2+2ab+4b^2$*) avec* $a, b \in \mathbb{Z}/N\mathbb{Z}$.

(i) Montrer que $P(N)$ *et* $Q(N)$ *sont non vides.*

(ii) Montrer $P(N) = Q(N)$ *pour tout* N *en utilisant (et vérifiant ?) les identités :*

$$(a^2 + 11b^2)(\alpha^2 + 11\beta^2) = (a\alpha + 11b\beta)^2 + 11(a\beta - b\alpha)^2,$$

$$(3a^2 + 2ab + 4b^2)(3\alpha^2 + 2\alpha\beta + 4\beta^2) = (3a\alpha + a\beta + b\alpha + 4b\beta)^2 + 11(a\beta - b\alpha)^2,$$

$$(a^2 + 11b^2)(3\alpha^2 + 2\alpha\beta + 4\beta^2) = 3A^2 + 2AB + 4B^2,$$

$$(3a^2 + 2ab + 4b^2)(3\alpha^2 + 2\alpha\beta + 4\beta^2) = 3C^2 + 2CD + 4D^2,$$

où $A = a\alpha + b\alpha + 4b\beta$*,* $B = a\beta - 3\alpha b - b\beta$*,* $C = a\alpha + 2a\beta + 2\alpha b$ *et* $D = a\alpha - a\beta - \alpha b - 2b\beta$.

(iii) Donner une autre démonstration de ce résultat en utilisant le résultat de l'exercice 1.9. On montrera en fait que l'on a $P(N) = Q(N) = (\mathbb{Z}/N\mathbb{Z})^\times$, *à moins que* 11 *ne divise* N *auquel cas* $P(N) = Q(N)$ *est l'ensemble des éléments de* $(\mathbb{Z}/N\mathbb{Z})^\times$ *qui sont des carrés modulo* 11.

EXERCICE 2.11. *Soit* p *un nombre premier.*

(i) Vérifier que si $p \neq 2$ *alors* $\left(\frac{-14}{p}\right) = (-1)^{\frac{p^2-1}{8}} \left(\frac{p}{7}\right)$.

On suppose désormais[6] $\left(\frac{-14}{p}\right) = 1$.

(ii) Montrer que p, $2p$ *ou* $3p$ *est de la forme* $a^2 + 14b^2$.

(iii) Vérifier par des exemples que les trois cas sont possibles, et que pour chaque nombre premier testé un seul de p, $2p$ *ou* $3p$ *est de la forme* $a^2 + 14b^2$.

(iv) Montrer que $3p$ *est de la forme* $a^2 + 14b^2$ *si, et seulement si,* $p \equiv \pm 3 \bmod 8$, *et qu'il est équivalent au fait que* p *soit de la forme* $3a^2 + 2ab + 5b^2$.

(v) Montrer que $2p$ *est de la forme* $a^2 + 14b^2$ *si, et seulement si,* p *est de la forme* $2a^2 + 7b^2$.

EXERCICE 2.12. (Volume des sphères euclidiennes) *Soit* $n \geq 1$ *un entier. Pour* $r > 0$ *réel on pose*

$$C_n(r) = \{(x_1, \ldots, x_n) \in \mathbb{R}^n, \sum_i x_i^2 < r^2\}.$$

(i) Soit $c_n = \mu(C_n(1))$. *Montrer* $\mu(C_n(r)) = c_n r^n$, *et pour* $n > 1$ *la relation* $c_n = 2c_{n-1}I_n$ *où* $I_n = \int_0^{\pi/2} \cos(t)^n dt$ *(intégrale de Wallis).*

(ii) Montrer $(n+1)I_{n+1} = nI_{n-1}$ *pour tout* $n \geq 2$, *puis* $nI_nI_{n-1} = \pi/2$.

(iii) En déduire le calcul de c_n, *et notamment* $c_{2n} = \frac{\pi^n}{n!}$.

(iv) Montrer $c_n \to 0$ *quand* $n \to \infty$.

n	1	2	3	4	5	6	7	8	9	10
c_n	2	3.141	4.188	4.934	5.263	5.167	4.724	4.058	3.298	2.550

TABLE 3. Volume c_n de la sphère euclidienne de rayon 1 dans $\mathbb{R}^n$ à 10^{-3} près.

EXERCICE 2.13. *(Réseaux entiers unimodulaires de petite dimension) On munit* $\mathbb{R}^n$ *du produit scalaire euclidien standard* $(x_i)\cdot(y_i) = \sum_i x_i y_i$. *On suppose que* $L \subset \mathbb{R}^n$ *est un réseau de covolume* 1, *et que de plus* $v \cdot w \in \mathbb{Z}$ *pour tout* $v, w \in L$ *(réseau dit* "entier"*).*

6. D'après la question précédente, c'est équivalent à $p \equiv 1, 3, 5, 9, 13, 15, 19, 23, 25, 27, 39, 45 \bmod 56$.

(i) Montrer que si $n \leq 4$*, il existe* $v \in L$ *tel que* $v \cdot v = 1$*.*

(ii) On suppose qu'il existe $v \in L$ *tel que* $v \cdot v = 1$*. Montrer que tout élément de* L *sécrit de manière unique sous la forme* $mv + u$ *avec* $m \in \mathbb{Z}$ *et* $u \in L \cap v^\perp$*.*

(iii) (suite) Montrer que $L \cap v^\perp$ *est un réseau entier de covolume* 1 *dans l'espace euclidien* $v^\perp$ *(muni du produit scalaire induit de* $\mathbb{R}^n$*).*

(iv) En déduire que si $n \leq 4$*, il existe* $g \in \mathrm{O}_n(\mathbb{R})$ *tel que* $L = g(\mathbb{Z}^n)$*.*

En utilisant d'autres techniques, il est possible de démontrer que ce résultat subsiste jusqu'en dimension $n = 7$*. L'exercice suivant donne un contre-exemple fameux en dimension* 8*.*

Exercice 2.14. (Le réseau E_8) *Soit* $\mathrm{D}_8 = \{(x_1, \ldots, x_8) \in \mathbb{Z}^8, \sum_i x_i \equiv 0 \bmod 2\}$ *et soit* $e \in \mathbb{R}^8$ *le vecteur* $\frac{1}{2}(1,1,1,1,1,1,1,1)$*. On munit* $\mathbb{R}^8$ *du produit scalaire euclidien standard.*

(i) Montrer que D_8 *est un réseau de* $\mathbb{R}^8$ *de covolume* 2*.*

(ii) En déduire que $\mathrm{E}_8 := \mathbb{Z}e + \mathrm{D}_8$ *est un réseau de* $\mathbb{R}^8$ *de covolume* 1*.*

(iii) Vérifier que pour tout $v, w \in \mathrm{E}_8$*, on a* $v \cdot v \in 2\mathbb{Z}$ *et* $v \cdot w \in \mathbb{Z}$*.*

(iv) En déduire que E_8 *n'est pas de la forme* $g(\mathbb{Z}^8)$ *pour* $g \in \mathrm{O}_8(\mathbb{R})$*.*

Chapitre 3

Formes quadratiques binaires entières

RÉFÉRENCE : Le livre de Gauss déjà cité.

1. Vocabulaire des formes

DÉFINITION 3.1. *Une forme quadratique binaire entière est une fonction* $q : \mathbb{Z}^2 \to \mathbb{Z}$ *telle qu'il existe* $a, b, c \in \mathbb{Z}$ *vérifiant*

$$q(x, y) = ax^2 + bxy + cy^2, \ \ \forall x, y \in \mathbb{Z}.$$

Dans tout ce chapitre, nous appellerons simplement "forme" une "forme quadratique binaire entière". Remarquons que si q est comme dans la définition ci-dessus, on a

$$a = q(1, 0), \ b = q(0, 1), \text{ et } \ a + b + c = q(1, 1).$$

La forme q est donc uniquement déterminée par le triplet $(a, b, c) \in \mathbb{Z}^3$, c'est pourquoi nous la désignerons souvent simplement par le symbole (a, b, c), à la manière de Gauss [1]. On note $\mathcal{Q}(\mathbb{Z}^2)$ l'ensemble des formes, c'est un groupe abélien pour l'addition évidente des fonctions.

La forme (a, b, c) est dite *primitive* si a, b, c sont premiers entre eux dans leur ensemble. Autrement dit, une forme est primitive si elle n'est pas égale à nq où $n \geq 2$ et $q \in \mathrm{Q}(\mathbb{Z}^2)$. L'étude de toutes les formes se ramenant trivialement à celle des formes primitives, on se concentrera parfois sur ces dernières, notamment lorsque cela allègera les énoncés.

DÉFINITION 3.2. *On dit que la forme* q *représente l'entier* $n \in \mathbb{Z}$ *s'il existe* $(x, y) \in \mathbb{Z}^2$, *avec* $(x, y) \neq (0, 0)$, *vérifiant* $q(x, y) = n$. *On dit que* q *représente primitivement l'entier* $n \in \mathbb{Z}$ *s'il existe* $x, y \in \mathbb{Z}$ *premiers entre eux avec* $q(x, y) = n$.

Déterminer l'ensemble des entiers représentés par une forme donnée est la motivation principale de ce chapitre. Pour les formes du type $x^2 + dy^2$, ce problème a été soulevé au chapitre précédent, et d'autres formes quadratiques annexes sont alors apparues, ce qui justifie en partie (suivant Lagrange) que l'on s'y intéresse dans cette généralité. Par exemple, la forme $x^2 + 5y^2$ s'est trouvée accompagnée de la forme $2x^2 + 2xy + 3y^2$, l'une et l'autre représentant alors exclusivement les premiers p tels que $\left(\frac{-5}{p}\right) = 1$.

Notons que si l'on connaît tous les entiers primitivement représentés par q, alors on connaît tous les entiers représentés par q, de sorte que l'on se concentrera souvent sur ceux-ci. Une forme peut cependant représenter un même entier primitivement

1. Le lecteur qui étudiera Gauss prendra garde qu'il ne considère que des formes du type $ax^2 + 2bxy + cy^2$ avec $a, b, c \in \mathbb{Z}$, et qu'il note donc (a, b, c) ce que nous notons $(a, 2b, c)$.

et non primitivement : la forme $(1,0,1)$ représente 25 primitivement et non primitivement (et 4 uniquement non primitivement). Remarquons enfin que si un nombre premier est représenté par q, il l'est nécessairement primitivement.

Une quantité fondamentale attachée à une forme est son discriminant.

DÉFINITION 3.3. *Le discriminant de la forme $q = (a,b,c)$ est l'entier* $\mathrm{disc}(q) = b^2 - 4ac$.

Par exemple, le discriminant de x^2+dy^2 est $-4d$. On constate aussi que x^2+5y^2 et $2x^2+2xy+3y^2$ sont toutes deux de discriminant -20. De même, les formes $(1,0,11)$ et $(3,2,4)$ rencontrées dans l'étude des premiers de la forme x^2+11y^2 sont toutes deux de discriminant -44.

Nous verrons par la suite que le discriminant d'une forme détermine grandement les propriétés des entiers qu'elle représente. La question la plus élémentaire est celle de leur signe.

PROPOSITION 3.4. (Signe du trinôme) *Soit q une forme de discriminant D.*

(i) q représente 0 si, et seulement si, D est un carré,

(ii) $D \leq 0$ si, et seulement si, les entiers non nuls représentés par q sont tous de même signe.

DÉMONSTRATION — Écrivons $q = (a,b,c)$. Supposons d'abord $a = 0$. Dans ce cas q représente 0, $D = b^2$ est un carré, et $q(x,y) = bxy + cy^2$. Cela montre (i). De plus on a $D \leq 0$ si, et seulement si, on a $b = 0$, soit $q(x,y) = cy^2$, ce qui entraîne (ii).

Supposons maintenant $a \neq 0$. En particulier $q(x,y) = 0$ avec $(x,y) \neq 0$ entraîne $y \neq 0$. Considérons l'identité remarquable ("forme canonique")

$$4aq(x,y) = (2ax+by)^2 - Dy^2. \tag{2}$$

On en déduit que q représente 0 si, et seulement si, D est un carré dans $\mathbb{Q}$, ou ce qui revient au même si D est un carré dans $\mathbb{Z}$ (car $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$!). Le sens $\Rightarrow$ du (ii) s'ensuit également car si $D \leq 0$ et $q(x,y) \neq 0$ alors $aq(x,y) > 0$. Pour la réciproque, on considère $(x,y) = (-b, 2a)$. □

Cela nous conduit à une discussion sur l'involution sur les formes $q = (a,b,c) \mapsto -q = (-a,-b,-c)$. Bien sûr, $\mathrm{disc}(q) = \mathrm{disc}(-q)$ et cette involution échange formes à valeurs ≥ 0 et formes à valeurs ≤ 0. Ainsi, dans l'étude des formes de discriminant < 0 (qui ne représentent pas 0), on ne perdra rien à ne considérer que des formes (a,b,c) à valeurs positives, ou ce qui revient au même telles que $a > 0$.

Convention : *dorénavant, nous supposerons toujours qu'une forme de discriminant < 0 est positive. Autrement dit, si (a,b,c) est une forme telle que $b^2 - 4ac < 0$, on supposera toujours $a > 0$.*

La théorie des formes de discriminant < 0 s'avèrera sensiblement plus simple. En effet, considérons par exemple le problème algorithmique consistant à déterminer

tous les entiers positifs représentés par une forme $q = (a, b, c)$ de discriminant $D < 0$. L'identité (2) montre que $q(x, y) = n$ entraîne

$$|y| \leq \sqrt{\frac{4an}{-D}} \text{ et } |2ax + by| \leq \sqrt{4an},$$

en particulier il n'y a qu'un nombre fini de couples (x, y) à tester pour résoudre $q(x, y) = n$. Quand $D > 0$ ce n'est plus vrai. Par exemple l'équation de "Pell-Fermat" $x^2 - 2y^2 = 1$ admet une infinité de solutions $(x, y) \in \mathbb{Z}^2$ (Exercice 3.7).

2. Notions d'équivalence entre deux formes

Suivant Lagrange, étudions maintenant les formes obtenues par changement de variables à coefficients entiers à partir d'une forme donnée. C'est une question tout à fait importante car les entiers représentés par la forme obtenue seront évidemment parmi ceux représentés par la forme dont on est parti, et qu'en particulier deux formes obtenues par changement de variable réversible représentent les même entiers.

Fixons donc q une forme, ainsi que u, v deux éléments de $\mathbb{Z}^2$. La fonction

$$(x, y) \mapsto q(xu + yv),\ \mathbb{Z}^2 \to \mathbb{Z},$$

est alors une nouvelle forme. Concrètement, si l'on écrit $u = (\alpha, \gamma)$ et $v = (\beta, \delta)$, on trouve simplement la forme $q(\alpha x + \beta y, \gamma x + \delta y)$, de sorte que l'on a simplement opéré le changement de variables $(x, y) \mapsto (\alpha x + \beta y, \gamma x + \delta y)$. La notation matricielle suivante sera parfois commode.

NOTATION : Si $(x, y) \in \mathbb{Z}^2$, on pose $q(\begin{pmatrix} x \\ y \end{pmatrix}) = q(x, y)$, autrement dit on voit les éléments de $\mathbb{Z}^2$ comme des vecteurs colonnes. Si u et v sont comme ci-dessus on a donc la relation

$$q(xu + yv) = q(x \begin{pmatrix} \alpha \\ \gamma \end{pmatrix} + y \begin{pmatrix} \beta \\ \delta \end{pmatrix}) = q(P \begin{pmatrix} x \\ y \end{pmatrix})$$

où $P = \mathrm{Mat}(u, v) = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ est la matrice des vecteurs u et v dans la base canonique de $\mathbb{Z}^2$.

PROPOSITION-DÉFINITION 3.5. *Si $q \in \mathrm{Q}(\mathbb{Z}^2)$ et $M \in \mathrm{M}_2(\mathbb{Z})$ on note $q \cdot M$ la forme $(x, y) \mapsto q(M \begin{pmatrix} x \\ y \end{pmatrix})$. Pour tout $M, N \in \mathrm{M}_2(\mathbb{Z})$ et tout $q \in \mathrm{Q}(\mathbb{Z}^2)$, on a les relations $(q \cdot M) \cdot N = q \cdot (MN)$ et $\mathrm{q} \cdot \mathrm{I}_2 = q$.*

Le cas le plus important de changement de coordonnées est celui où u, v est une $\mathbb{Z}$-base de $\mathbb{Z}^2$, ou ce qui revient au même si le déterminant de $P = \mathrm{Mat}(u, v)$ vaut ± 1 (i.e. $P \in \mathrm{GL}_2(\mathbb{Z})$), car alors ce changement de variables est réversible : $q = (q \cdot P) \cdot P^{-1}$. Dans ce cas, la forme obtenue renferme à bien des égards la même information que la forme q, et selon la définition suivante sera dite *équivalente* à q. On rappelle que

$$\mathrm{SL}_2(\mathbb{Z}) := \{P \in \mathrm{GL}_2(\mathbb{Z}) \mid \det(P) = 1\},$$

c'est donc un sous-groupe distingué d'indice 2 de $\mathrm{GL}_2(\mathbb{Z})$. On dira qu'une $\mathbb{Z}$-base u, v de $\mathbb{Z}^2$ est directe si $\det(u, v) = +1$.

DÉFINITION 3.6. *Deux formes q et q' sont dites équivalentes (resp. proprement équivalentes) s'il existe une $\mathbb{Z}$-base u, v de $\mathbb{Z}^2$ (resp. une $\mathbb{Z}$-base directe) telle que $q'(x,y) = q(xu+vy)$ pour tout $x, y \in \mathbb{Z}$. Il revient au même de dire qu'il existe $P \in \mathrm{GL}_2(\mathbb{Z})$ (resp. $P \in \mathrm{SL}_2(\mathbb{Z})$) tel que $q' = q \cdot P$.*

On notera $q \sim q'$ (resp. $q \overset{+}{\sim} q'$) si q et q' sont équivalentes (resp. proprement équivalentes). Ce sont des relations d'équivalence sur $\mathrm{Q}(\mathbb{Z}^2)$. En effet, la relation (3.5) signifie que $(P,q) \mapsto q \cdot P$ est une action à droite du groupe $\mathrm{GL}_2(\mathbb{Z})$ (resp. $\mathrm{SL}_2(\mathbb{Z})$) sur $\mathrm{Q}(\mathbb{Z}^2)$ dont les orbites sont les classes d'équivalence (resp. d'équivalence propre). Notons que $q \overset{+}{\sim} q'$ entraîne évidemment $q \sim q'$. En particulier, l'ensemble des classes d'équivalence (resp. d'équivalence propre) de formes est une partition de $\mathrm{Q}(\mathbb{Z}^2)$.

La notion d'équivalence est due à Lagrange et celle d'équivalence propre à Gauss. Même si la première est la plus naturelle dans les questions de représentation des entiers, c'est la seconde qui permettra de comprendre les propriétés les plus fines des formes, comme l'a vu Gauss. L'intérêt des de la notion d'équivalence propre n'apparaîtra clairement que plus tard dans le cours, lorsque sera discutée la notion de composition des formes.

LEMME 3.7. (Équivalences élémentaires) *Pour tout $a, b, c \in \mathbb{Z}$, on a $(a,b,c) \sim (a,-b,c)$ et*

$$(a,b,c) \overset{+}{\sim} (c,-b,a) \overset{+}{\sim} (a,b+2a,c+b+a) \overset{+}{\sim} (a,b-2a,c-b+a).$$

DÉMONSTRATION — En effet, cela découle des changements de variables $(x,y) \mapsto (x,-y)$ (qui change l'orientation), $(x,y) \mapsto (y,-x)$, $(x+y,y)$ et $(x-y,y)$ (qui la préservent), qui correspondent aussi respectivement aux matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ et } \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}.$$

□

Par exemple, la forme $(5,6,2)$ est proprement équivalente à $(1,0,1)$. On peut en effet le voir en appliquant les équivalences élémentaires suivantes : $(5,6,2) \overset{+}{\sim} (2,-6,5) \overset{+}{\sim} (2,-2,1) \overset{+}{\sim} (1,2,2) \overset{+}{\sim} (1,0,1)$.

PROPOSITION 3.8. *Deux formes équivalentes représentent les mêmes entiers, primitivement ou non, et ce le même nombre de fois. De plus, elles sont simultanément primitives. Enfin, deux formes équivalentes ont même discriminant.*

DÉMONSTRATION — Le premier point de la proposition est évident : si $P \in \mathrm{GL}_2(\mathbb{Z})$ alors

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto P^{-1} \begin{pmatrix} x \\ y \end{pmatrix}$$

définit une bijection entre les $(x,y) \in \mathbb{Z}^2$ tels que $q(x,y) = n$ et les $(x',y') \in \mathbb{Z}^2$ tels que $(q \cdot P)(x',y') = n$, son inverse étant $\begin{pmatrix} x' \\ y' \end{pmatrix} \mapsto P \begin{pmatrix} x' \\ y' \end{pmatrix}$. Comme $u \in \mathbb{Z}^2$ est primitif si et seulement s'il n'est pas de la forme mv avec $v \in \mathbb{Z}^2$ et $m \geq 2$,

on voit de plus que u est primitif si, et seulement si, Pu l'est. La seconde assertion découle de ce que si $m \in \mathbb{Z}$, $q \in \mathrm{Q}(\mathbb{Z}^2)$ et $M \in \mathrm{M}_2(\mathbb{Z})$, alors $(mq) \cdot P = m(q \cdot P)$. La dernière assertion découle de la proposition suivante et de ce que le déterminant d'un élément de $\mathrm{GL}_2(\mathbb{Z})$ est toujours ± 1. □

PROPOSITION 3.9. *Si q est une forme et $P \in \mathrm{M}_2(\mathbb{Z})$, alors* $\mathrm{Mat}(q \cdot P) = {}^tP \,\mathrm{Mat}(q)\, P$. *En particulier,* $\mathrm{disc}(q \cdot P) = \det(P)^2 \mathrm{disc}(q)$.

DÉMONSTRATION — Si $q = (a, b, c)$, posons $\mathrm{Mat}(q) = \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}$. On a $\mathrm{disc}(q) = -\det(\mathrm{Mat}(q))$. On conclut par l'identité matricielle $2q(x, y) = {}^t\begin{pmatrix} x \\ y \end{pmatrix} \mathrm{Mat}(q) \begin{pmatrix} x \\ y \end{pmatrix}$, valable pour tout $x, y \in \mathbb{Z}$. □

Observons que deux formes de même discriminant ne sont pas nécessairement équivalentes. Par exemple, les deux formes $(1, 0, 5)$ et $(2, 2, 3)$ ont même discriminant -20. La seconde représente 2 mais pas la première, car 2 n'est pas de la forme x^2+5y^2 avec $x, y \in \mathbb{Z}$.

3. Entiers représentés par une forme, d'après Lagrange

THÉORÈME 3.10. (Lagrange) *Soient $D, n \in \mathbb{Z}$. Il y a équivalence entre :*

(i) D est un carré modulo $4n$,

(ii) il existe une forme de discrimininant D qui représente primitivement n.

En effet, supposons que D est un carré modulo $4n$. On peut donc trouver $b, c \in \mathbb{Z}$ tels que $D = b^2 - 4nc$. Mais alors la forme $q = (n, b, c)$ est de discrimimant D, et représente primitivement $n = q(1, 0)$. On a montré (i) implique (ii).

La réciproque, d'apparence moins intéressante, est plus difficile. Nous aurons besoin des deux lemmes suivants. On dira qu'un vecteur $(x, y) \in \mathbb{Z}^2$ est primitif si x et y sont premiers entre eux.

LEMME 3.11. *Tout vecteur primitif $u \in \mathbb{Z}^2$ se complète en une $\mathbb{Z}$-base directe u, v de $\mathbb{Z}^2$.*

DÉMONSTRATION — En effet, écrivons $u = (x, y)$. Soient $\alpha, \beta \in \mathbb{Z}$ tels que $\alpha x + \beta y = 1$ (Bézout). On constate que

$$\det \begin{pmatrix} x & -\beta \\ y & \alpha \end{pmatrix} = 1$$

donc (x, y) et $(-\beta, \alpha)$ forment une $\mathbb{Z}$-base directe de $\mathbb{Z}^2$. □

LEMME 3.12. (Lemme clé) *L'entier $n \in \mathbb{Z}$ est primitivement représenté par la forme q si, et seulement si, $q \overset{+}{\sim} (n, b, c)$, avec de plus $-|n| < b \leq |n|$ si $n \neq 0$.*

DÉMONSTRATION — Une forme du type (n, b, c) représente primitivement l'entier n car $q(1, 0) = n$, ainsi donc que toute forme équivalente. Réciproquement, soient q une forme et $n = q(u)$ avec u primitif. D'après le lemme précédent, on peut compléter le vecteur u en une $\mathbb{Z}$-base u, v de $\mathbb{Z}^2$ telle que $\det(u, v) = 1$. Si q' est la forme $q'(x, y) = q(ux + vy)$ alors $q' \overset{+}{\sim} q$ et $q' = (n, *, *)$. Cela conclut le cas $n = 0$, puis le cas $n \neq 0$ en appliquant de manière répétée les équivalences propres élémentaires (Lemme 3.7). □

Terminons la démonstration du théorème de Lagrange. Supposons que n est primitivement représenté par une forme q. Le lemme précédent assure que l'on a $q \overset{+}{\sim} (n, b, c)$ pour certains $b, c \in \mathbb{Z}$. D'après la proposition 3.8, $\mathrm{disc}(q) = b^2 - 4nc$. En particulier, $\mathrm{disc}(q)$ est un carré modulo $4n$. □

Le théorème de Lagrange se précise quand n est un nombre premier. Rappelons que si une forme représente un nombre premier, elle le représente primitivement : si $q(x, y)$ est premier alors (x, y) est nécessairement primitif.

THÉORÈME 3.13. *Soient $D \in \mathbb{Z}$ et p un nombre premier tels que D est un carré modulo $4p$. Alors p est représenté par une forme de discriminant D, et une telle forme est unique à équivalence près.*

DÉMONSTRATION — Soit q une forme qui représente p (une telle forme existe d'après Lagrange). D'après la remarque ci-dessus, q représente p primitivement. Le lemme 3.11 montre donc l'existence de $b, c \in \mathbb{Z}$ tels que $q \sim (p, b, c)$ et $0 \leq b \leq p$ (utiliser $(u, v, w) \sim (u, -v, w)$). De même, si q' représente p alors on a $q' \sim (p, b', c')$ et $0 \leq b' \leq p$. Si q et q' ont même discriminant D on a de plus

$$D = b^2 - 4pc = (b')^2 - 4pc'.$$

Nous allons montrer $b = b'$, ce qui entraînera $c = c'$, puis $q \sim q'$, et donc l'assertion d'unicité de l'énoncé. On a $b^2 = (b')^2 \bmod 4p$. Les carrés de $0, 1, 2$ étant distincts modulo 8, le théorème est vrai pour $p = 2$. La relation $b^2 \equiv (b')^2 \bmod p$ entraîne $b' \equiv \pm b \bmod p$ car p est premier. Les inégalités $0 \leq b, b' \leq p$ assurent alors $b = b'$ ou $b = p - b'$. Ce dernier cas ne se produit pas si $p > 2$ car la congruence $b^2 \equiv (b')^2 \bmod 4$ entraîne $b \equiv b' \bmod 2$. □

Ces résultats justifient grandement une étude plus fine des classes d'équivalence de formes de discriminant donné, qui sera l'objet du paragraphe suivant.

REMARQUE 3.14. Si p est impair alors D est un carré modulo $4p$ si, et seulement si, $D \equiv 0, 1 \bmod 4$ et D est un carré modulo p. Enfin, D est un carré modulo 8 si, et seulement si, $D \equiv 0, 1, 4 \bmod 8$.

4. L'ensemble des classes de formes de discriminant donné

Constatons que si D est le discriminant d'une forme, on a la congruence

$$D \equiv 0, 1 \bmod 4.$$

Réciproquement, si $D \equiv 0, 1 \bmod 4$, alors D est le discriminant de la forme

$$\begin{cases} x^2 - \frac{D}{4}y^2, & \text{si } \ D \equiv 0 \bmod 4, \\ \\ x^2 + xy + \frac{1-D}{4}y^2, & \text{si } \ D \equiv 1 \bmod 4. \end{cases}$$

Cette forme est appelée *forme principale* de discriminant D. Il y a bien sûr beaucoup d'autres formes de discriminant D, par exemple toutes celles équivalentes à la forme principale. La question restante abordée ici est de classifier à équivalence près toutes les formes de discriminant D. La forme principale se distingue par la propriété suivante.

PROPOSITION 3.15. *Une forme représente* 1 *si, et seulement si, elle est équivalente à la forme principale de même discriminant.*

DÉMONSTRATION — Il est évident que la forme principale représente 1. Réciproquement, si une forme q de discriminant D représente 1 elle le représente primitivement, et elle est donc équivalente à $(1, b, c)$ avec $b \in \{0, 1\}$ par le lemme 3.12. Cette forme est aussi de discriminant D, d'où la congruence $b \equiv D \bmod 2$. Il y a donc une seule possibilité pour b, et donc une seule pour $c = \frac{b^2-D}{4}$: c'est la forme principale. □

On fixe dorénavant un entier $D \equiv 0, 1 \bmod 4$. On conserve de plus la convention du paragraphe précédent : si $D < 0$ on ne considère que des formes positives. Le résultat suivant, dû à Lagrange, est central dans la théorie des formes.

THÉORÈME 3.16. (Lagrange) *Soit $D \in \mathbb{Z}$ non nul. À équivalence (propre ou non) près, il n'y a qu'un nombre fini de formes de discriminant D.*

Nous supposerons que D n'est pas un carré, cas en fait beaucoup plus simple et pour lequel nous renvoyons aux exercices. Il suffit de démontrer le lemme de réduction suivant.

LEMME 3.17. (Réduction de Lagrange) *Toute forme de discriminant D non carré est proprement équivalente à une forme (a, b, c) avec $|b| \leq |a| \leq |c|$. Une telle forme satisfait $1 \leq |a| \leq \sqrt{\frac{|D|}{3}}$.*

Le théorème 3.16 s'ensuit car il n'y a qu'un nombre fini de triplets (a, b, c) satisfaisant les conditions ci-dessus et la relation $b^2 - 4ac = D$. Observons de plus que si on a $-|a| \leq b \leq |a| \leq |c|$ et $D = b^2 - 4ac$, on a alors $4|a|^2 \leq 4|ac| = |b^2 - D| \leq |a|^2 + |D|$, ce qui montre la seconde assertion du lemme.

DÉMONSTRATION — (du lemme 3.17) Soit q une forme de discriminant D. Soit $\mathcal{V}$ l'ensemble des valeurs absolues des entiers représentés primitivement par q. Comme D n'est pas un carré, on a $0 \notin \mathcal{V}$ d'après la proposition 3.4, et il est de plus évident

que $\mathcal{V} \neq \emptyset$. Il existe donc $u \in \mathbb{Z}^2$ primitif tel que $a = q(u)$ satisfait $|a| = \mathrm{Min}\mathcal{V}$. Le lemme 3.10 assure alors qu'il existe $b, c \in \mathbb{Z}$ tels que

$$q \overset{+}{\sim} (a, b, c) \quad \text{et} \quad |b| \leq |a|.$$

Mais c est représenté primitivement par (a, b, c), et donc par q, d'où l'inégalité $|a| \leq |c|$. □

En guise de seconde démonstration du théorème ci-dessus, donnons un algorithme permettant, étant donnée une forme (a, b, c), de trouver une forme (a', b', c') qui lui est proprement équivalente et qui satisfait de plus $|b'| \leq |a'| \leq |c'|$. On suppose donc que ces inégalités ne sont pas toutes satisfaites ; nous allons définir une forme (a', b', c') qui est élémentairement proprement équivalente à (a, b, c) et telle que $|a'| + |b'| < |a| + |b|$, ce qui concluera :

- Si $|c| < |a|$ on pose $(a', b', c') = (c, -b, a)$.
- Si $|c| \geq |a|$ et $|b| > |a|$, on pose $(a', b', c') = (a, b \pm 2a, c + a \pm b)$ le signe $\pm$ étant uniformément choisi, et choisi de sorte que $|b \pm a| < |b|$. C'est possible car $a \neq 0$ (D n'est pas un carré).

Définition 3.18. *On désigne par* $\mathrm{Cl}(D)$ (resp. $\mathrm{P}(D)$) *l'ensemble des classes d'équivalence propre de formes (resp. de formes primitives) de discriminant D, supposées de plus positives si $D < 0$. On note enfin* $\mathrm{h}(D) = |\mathrm{P}(D)|$.

En particulier, on a $\mathrm{h}(D) = 1$ si, et seulement si, toute forme primitive de discriminant D est proprement équivalente à la forme principale. Observons que si d est le pgcd de a, b, c, alors d divise tous les entiers représentés par (a, b, c) et d^2 divise D. En particulier, si un nombre premier p est représenté par une forme non primitive de discriminant D, alors p divise D. On déduit de cela, du théorème 3.13, et de la remarque 3.14 le :

Corollaire 3.19. *Supposons* $\mathrm{h}(D) = 1$. *Alors tout nombre premier impair p tel que* $\left(\frac{D}{p}\right) = 1$ *est représenté par la forme principale de discriminant D.*

Proposition 3.20. *Si* $|D| \leq 11$ *et D n'est pas un carré alors on a* $\mathrm{h}(D) = 1$.

Comme D n'est pas un carré et $D \equiv 0, 1 \bmod 4$, l'hypothèse $|D| \leq 11$ affirme simplement que D est dans la liste $\{-11, -8, -7, -4, -3, 5, 8\}$.

Démonstration — La seconde assertion découle du théorème 3.13. Vérifions la première. Si $|D| < 12$ alors $\sqrt{\frac{|D|}{3}} < 2$. Toute forme de discriminant D est donc équivalente à une forme (a, b, c) avec $a = \pm 1$. Si $a = 1$, et en particulier si $D < 0$ par convention, une telle forme représente 1 et le corollaire découle alors de la proposition 3.15. Il ne reste donc qu'à traiter les cas $D > 0$, i.e. $D = 5, 8$, et $a = -1$.

Si $D = 5$, cela conduit aux deux formes $(1, 1, -1)$ et $(-1, 1, 1)$, qui sont en fait proprement équivalentes car $(a, b, c) \overset{+}{\sim} (c, -b, a)$ en général. Si $D = 11$, on obtient

les deux formes $(1,0,-2)$ et $(-1,0,2)$, qui sont aussi proprement équivalentes ! En effet, le lemme 3.7 justifie la suite d'équivalences propres suivante :

$$(-1,0,2) \overset{+}{\sim} (-1,-2,1) \overset{+}{\sim} (1,2,-1) \overset{+}{\sim} (1,0,-2).$$

□

Notons que cela fournit une autre démonstration du théorème des deux carrés de Fermat, qui en est le cas $D=-4$. Cela montre aussi qu'un nombre premier impair p est de la forme $a^2+ab+3b^2$ (resp. $a^2+ab+2b^2$, resp. a^2+ab+b^2) si, et seulement si, -11 (resp. -7, resp. -3) est un carré modulo p.

Le problème de déterminer si deux formes satisfaisant les conditions du lemme 3.17 sont équivalentes ou non est en fait sensiblement plus simple lorsque $D<0$, et nous allons nous concentrer sur ce cas par la suite.

5. Détermination de Cl(D) lorsque le discriminant D est négatif, d'après Gauss

DÉFINITION 3.21. (Gauss) *Une forme (a,b,c) de discriminant <0 est dite* réduite *(au sens de Gauss) si elle vérifie $-a<b\leq a\leq c$, et si on a de plus $b\geq 0$ dans le cas où $a=c$.*

On rappelle que par convention on a toujours $a>0$ et $c>0$ pour une forme (a,b,c) de discriminant <0. Les équivalences élémentaires $(a,-a,c) \overset{+}{\sim} (a,a,c)$ et $(a,b,a) \overset{+}{\sim} (a,-b,a)$, ainsi que le lemme 3.17, entraînent que toute forme de discriminant <0 est proprement équivalente à une forme réduite. L'algorithme du paragraphe précédent donne même une suite d'équivalences propres élémentaires permettant de passer d'une forme quelconque à une forme réduite.

THÉORÈME 3.22. (Réduction de Gauss) *Une forme de discriminant <0 est proprement équivalente à une unique forme réduite.*

L'existence a déjà été justifiée ci-dessus, il n'y a donc qu'à vérifier l'unicité.

LEMME 3.23. *(Les deux premières valeurs primitives d'une forme réduite) Soit $q=(a,b,c)$ une forme réduite. L'entier a est le plus petit entier (primitivement) représenté par q, de plus il y a deux cas :*

(i) Si $a<c$ alors $a=q(u)$ pour exactement 2 vecteurs $u\in\mathbb{Z}^2$, à savoir $u=\pm(1,0)$. Dans ce cas, c est la seconde valeur représentée primitivement par q. De plus, $c=q(v)$ pour exactement 2 vecteurs primitifs $v\in\mathbb{Z}^2$, à moins que $b=a$ auquel cas il y en a 4.

(ii) Si $a=c$ alors $a=q(u)$ pour exactement 4 vecteurs primitifs $u\in\mathbb{Z}^2$, à moins que $b=a$ auquel cas il y en a 6.

Démonstration — Observons déjà que le seul vecteur $(x, y) \in \mathbb{Z}^2$ primitif tel que $y = 0$ est $\pm(1, 0)$ et qu'alors $q(\pm 1, 0) = a$. Considérons maintenant l'identité

$$4aq(x, y) = (2ax + by)^2 - Dy^2$$

pour $(x, y) \in \mathbb{Z}^2$. Si $|y| \geq 2$, on constate que $aq(x, y) \geq -D = 4ac - b^2$. Mais $b^2 \leq a^2 \leq ac$ comme q est réduite, et donc $q(x, y) \geq 3c > c$ dès que $|y| \geq 2$. Considérons donc pour finir le cas $y = \pm 1$, qui se ramène à $y = 1$. Comme $-a < b \leq a$, on a $|2ax + b| \geq |b|$ pour tout $x \in \mathbb{Z}$, avec égalité si, et seulement si, $x = 0$, ou $b = a$ et $x = -1$. Ainsi, pour tout $x \in \mathbb{Z}$,

$$q(x, 1) \geq \frac{b^2 - D}{4a} = c,$$

avec égalité si, et seulement si, $x = 0$, ou $b = a$ et $x = -1$. Le lemme en découle. □

Retournons à la démonstration de l'unicité dans le théorème 3.22. Soient $q = (a, b, c)$ et $q' = (a', b', c')$ deux formes réduites. On suppose d'abord seulement q et q' équivalentes. Comme deux formes équivalentes représentent primitivement les même valeurs, et chacune le même nombre de fois, on a $a = a'$ (même minimum). De plus, on a $c = c'$. En effet, soit a est représenté exactement deux fois auquel cas $c = c'$ est la seconde valeur primitive de q et q' d'après le lemme ci-dessus (i), soit a est représenté 4 ou 6 fois auquel cas on a $c = a = a' = c'$ d'après le (ii). En prenant le discriminant, on obtient de plus $b^2 = (b')^2$, et donc $b = \pm b'$.

Si l'on a $c = a$, l'inégalité $b, b' \geq 0$ entraîne $b = b'$. On peut donc supposer $a < c$: q et q' sont dans le cas (i) du lemme ci-dessus. On en déduit que l'on a $b = a$ si, et seulement si, $b' = a'$, et on peut donc supposer enfin que l'on a $b, b' \neq a$. Ainsi,a et c sont représentés primitivement par q et q', et ce exactement deux fois chacun, nécessairement par $\pm(1, 0)$ pour a et $\pm(0, 1)$ pour c. On a donc $q'(x, y) = q(xu + yv)$ avec $u = \pm(1, 0)$ et $v = \pm(0, 1)$. Comme $q'(x, y) = q'(-x, -y)$, on peut supposer que l'on a $u = (1, 0)$. Supposons enfin que q et q' sont *proprement* équivalentes. On a alors de plus $\det(u, v) = 1$. Cela entraîne $v = (0, 1)$, et donc $q = q'$. □

Remarque 3.24. On pourra consulter les exercices pour un point de vue plus "géométrique" sur ce résultat, basé sur l'action de $\mathrm{SL}_2(\mathbb{Z})$ sur le demi-plan de Poincaré.

Ce résultat a de multiples applications. Il permet tout d'abord de parler de *la forme réduite* d'une classe d'équivalence propre de formes, puisqu'elle est unique. Il donne surtout un algorithme simple pour calculer $\mathrm{Cl}(D)$ pour $D < 0$ donné : il suffit de déterminer le nombre de triplets $(a, b, c) \in \mathbb{Z}^3$ définissant une forme réduite de discriminant D. On pourra procéder comme suit : pour chaque $b \in \mathbb{Z}$ tel que $b \equiv D \bmod 2$ et tel que $|b| \leq \sqrt{\frac{-D}{3}}$ on factorisera $\frac{b^2-D}{4}$ sous la forme ac avec $|b| \leq a \leq c$.

Par exemple, nous avons vu que $\mathrm{h}(D) = 1$ si $|D| \leq 11$. D'après l'algorithme ci-dessus, nous pouvons maintenant calculer sans difficulté $\mathrm{h}(D)$ pour des petites valeurs de $|D|$.

EXEMPLE 3.25. Prenons l'exemple $D = -20$, de sorte que $\sqrt{\frac{-D}{3}} < 3$. Les formes réduites (a, b, c) de ce discriminant satisfont donc $|b| \leq 2$ et b pair. Si $b = 0$ alors $-4ac = -20$ et donc $a = 1$ et $c = 5$: c'est la forme principale $(1, 0, 5)$. Sinon $a = 2$ et donc $b = 2$, puis $c = \frac{b^2-D}{4a} = 3 \geq a$: c'est la forme $(2, 2, 3)$. Ces deux formes sont bien réduites, et donc non proprement équivalentes d'après Gauss. On aurait pu arguer plus directement ici que $(1, 0, 5)$ et $(2, 2, 3)$ sont non équivalentes car 2 est représenté par la seconde et non par la première. En guise d'application du théorème 3.13, on retrouve le fait que si p est premier impair, $D = -20$ est un carré modulo p (i.e. -5 est un carré modulo p), si, et seulement si, p est de la forme $x^2 + 5y^2$ ou $2x^2 + 2xy + 3y^2$, et que ces deux cas se produisent exclusivement.

D	h(D)	Formes réduites primitives
-15	2	$(1, 1, 4)$, $(2, 1, 2)$
-20	2	$(1, 0, 5)$, $(2, 2, 3)$
-23	3	$(1, 1, 6)$, $(2, \pm 1, 3)$
-24	2	$(1, 0, 6)$, $(2, 0, 3)$
-31	3	$(1, 1, 8)$, $(2, \pm 1, 4)$
-32	2	$(1, 0, 8)$, $(3, 2, 3)$
-35	2	$(1, 1, 9)$, $(3, 1, 3)$
-36	2	$(1, 0, 9)$, $(2, 2, 5)$
-39	4	$(1, 1, 10)$, $(2, \pm 1, 5)$, $(3, 3, 4)$
-40	2	$(1, 0, 10)$, $(2, 0, 5)$
-44	3	$(1, 0, 11)$, $(3, \pm 2, 4)$
-47	5	$(1, 1, 12)$, $(2, \pm 1, 6)$, $(3, \pm 1, 4)$
-48	2	$(1, 0, 12)$, $(3, 0, 4)$

TABLE 1. Formes réduites primitives de discriminant $-48 \leq D < 0$ tel que h(D) $\neq 1$

Étant donné le critère 3.19, il est naturel de se demander quels sont les $D < 0$ tels que h(D) $= 1$. Nous avons déjà vu que c'est toujours le cas si $|D| \leq 11$, on vérifie de même que :

PROPOSITION 3.26. *On a* h(D) $= 1$ *pour tout discriminant D dans la liste suivante :*

$$\{-3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163\}.$$

DÉMONSTRATION — On peut supposer $|D| \geq 12$. Soit (a, b, c) une forme réduite d'un tel discriminant. On a $b \equiv D \bmod 2$ et $b^2 \leq a^2 \leq -D/3$. Notons que $[\sqrt{\frac{-D}{3}}]$ vaut 7 si $D = -163$, 4 si $D = -67$, 3 si $D = -43$, 2 si $D = -19$. Si $D = -19, -27, -43, -47$ et -163, on vérifie que pour tout b tel que $b^2 \leq -D/3$ et $b \equiv D \bmod 2$, le nombre

$\frac{b^2-D}{4}$ est premier, ce qui force $a = 1$. Par exemple pour $D = -163$ on a $b \in \{\pm 1, \pm 3, \pm 5, \pm 7\}$ et on constate que

$$\frac{1+163}{4} = 41, \quad \frac{9+163}{4} = 43, \quad \frac{25+163}{4} = 47, \quad \text{et} \quad \frac{49+163}{4} = 53$$

qui sont tous premiers. Si $D = 12, -16, -28$, donc $b = 0, \pm 2$, on constate que dans tous les cas $\frac{b^2-D}{4}$ est soit premier soit une puissance de 2, ce qui force encore $a = 1$. □

On prétend que Gauss, par examen de ses tables, avait conjecturé que les $D < 0$ tels que $\mathrm{h}(D) = 1$ sont ceux de la proposition précédente. Ce problème, dit "du nombre de classes 1", a par la suite suscité une multitude de recherches en théorie des nombres. Il a été démontré 150 ans plus tard par Heegner, en 1952. Sa démonstration comportait certains points obscurs, éclaircis par Stark en 1967. Baker en a donné aussi une démonstration différente en 1966. Ces démonstrations dépassent malheureusement le cadre de ce cours.

THÉORÈME 3.27. *(Stark, Heegner,Baker) Si $D < 0$, alors $\mathrm{h}(D) = 1$ si, et seulement si, D est l'un des treize discriminants de la proposition 3.26.*

Gauss avait aussi conjecturé $\mathrm{h}(D) \to \infty$ si $D \to -\infty$, ce qui a aussi été démontré (et bien avant le résultat ci-dessus !) par Hecke-Deuring-Heilbronn. Siegel a même démontré

$$\log \mathrm{h}(D) \underset{-D\to+\infty}{\sim} \frac{1}{2}\log(|D|).$$

Mentionnons enfin que le cas $D > 0$ est assez différent : on conjecture depuis Gauss que l'on a $\mathrm{h}(D) = 1$ pour une infinité de $D > 0$, mais c'est un problème toujours ouvert.

6. Classes ambiguës de discriminant négatif

Terminons ce chapitre par une discussion sur la différence entre équivalence et équivalence propre. On définit *l'opposée de la forme* $q = (a, b, c)$ comme étant la forme de même discriminant

$$q^{\mathrm{opp}} = (a, -b, c) = q \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Bien sûr $(q^{\mathrm{opp}})^{\mathrm{opp}} = q$. Comme $\mathrm{SL}_2(\mathbb{Z})$ est distingué dans $\mathrm{GL}_2(\mathbb{Z})$, on constate que $q \overset{+}{\sim} q'$ entraîne $q^{\mathrm{opp}} \overset{+}{\sim} (q')^{\mathrm{opp}}$, de sorte que si C est une classe d'équivalence propre de formes alors $C^{\mathrm{opp}} = \{q^{\mathrm{opp}}, q \in C\}$ en est aussi une.

LEMME 3.28. *$C \mapsto C^{\mathrm{opp}}$ est une involution de $\mathrm{Cl}(D)$ dont les orbites sont exactement les classes d'équivalence de formes de discriminant D.*

DÉMONSTRATION — Il est évident que l'application $C \mapsto C^{\mathrm{opp}}$ est involutive : $(C^{\mathrm{opp}})^{\mathrm{opp}} = C$. Ses orbites sont alors par définition de la forme $C \cup C^{\mathrm{opp}}$. Mais une telle partie est la classe d'équivalence toute entière de n'importe qu'elle forme de C car $\mathrm{GL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z}) \cup \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \mathrm{SL}_2(\mathbb{Z})$. □

DÉFINITION 3.29. *Une forme est dite*[2] *ambiguë si elle est proprement équivalente à son opposée. Une classe $C \in \mathrm{Cl}(D)$ est dite ambiguë si $C^{\mathrm{opp}} = C$.*

Il découle de cette définition qu'une forme primitive est ambiguë si, et seulement si, sa classe d'équivalence propre est ambiguë. Le lemme élémentaire précédent montre que pour déterminer les classes d'équivalence (non propre) de formes primitives de discriminant D il suffit de déterminer les classes d'équivalence propre de discriminant D et parmi celles-ci de regrouper chaque classe non ambiguë avec son opposée. En particulier, le nombre de classes d'équivalence de formes primitives de discriminant D vaut

$$\frac{\mathrm{h}(D) + a(D)}{2}$$

où $a(D)$ désigne le nombre de classes ambiguës de $\mathrm{P}(D)$. Gauss a déterminé $a(D)$ pour tout D, mais nous nous restreindrons pour simplifier au cas où $D < 0$. Nous désignerons par $t(N)$ le nombre de diviseurs premiers distincts de l'entier N. Par exemple, on a $t(12) = 2$.

THÉORÈME 3.30. (Gauss) *On suppose $D < 0$.*

(i) Une forme réduite (a, b, c) de discriminant D est ambiguë si, et seulement si, on a $b = 0$, $b = a$ ou $c = a$.

(ii) Il y a exactement 2^{t-1} classes ambiguës dans $\mathrm{P}(D)$ où $t = t(D)$, à moins que $D \equiv 4 \bmod 16$ (resp. $D \equiv 0 \bmod 32$) auquel cas $t = t(D) - 1$ (resp. $t = t(D) + 1$).

DÉMONSTRATION — En effet, soit (a, b, c) la forme réduite d'une classe ambiguë. Elle est donc proprement équivalente à son opposée, qui est $(a, -b, c)$. Si $c > a$ et $b \neq a$ c'est encore une forme réduite, ce qui force $b = -b$ par le théorème 3.22, et donc $b = 0$. Ainsi, soit $b = a$, soit $b = 0$, soit $c = a$. Réciproquement $(a, 0, c)$ est égale à son opposée, $(a, a, c) \overset{+}{\sim} (a, a - 2a, c + a - a) = (a, -a, c)$, et $(a, b, a) \overset{+}{\sim} (a, -b, a)$, ce qui conclut le premier point.

Comme toute classe ambiguë contient une et une seule forme réduite ambiguë par le théorème 3.22, il ne reste qu'à dénombrer les formes réduites primitives décrites au (i). Constatons que $(a, b, a) \overset{+}{\sim} (a, b - 2a, 2a - b) \overset{+}{\sim} (2a - b, 2a - b, a)$, de sorte que les formes réduites (a, b, c) telles que $b = a$ ou $c = a$ sont en bijection naturelle avec les formes (a, a, c) telles que $1 \leq a \leq 2c$. Écartons enfin définitivement le cas $D = -4$ qui est trivial car $\mathrm{h}(-4) = 1$.

Soit $S(D)$ l'ensemble des couples (u, v) d'entiers positifs premiers entre eux tels que $-D = 4uv$. Cet ensemble est non vide si et seulement si $D \equiv 0 \bmod 4$, auquel cas il a exactement $|S(D)| = 2^{t(\frac{D}{4})}$ éléments (pourquoi ?). Notons que si $(u, v) \in S(D)$, alors $(v, u) \in S(D)$, et que de plus $(u, v) \neq (v, u)$ car $D \neq -4$, il y a donc exactement $\frac{|S(D)|}{2}$ formes réduites primitives du type $(a, 0, c)$.

2. On prendra garde, si l'on lit Gauss, que sa définition d'une forme ambiguë n'est pas équivalente à celle donnée ici. Pour lui, une forme (a, b, c) est dite ambiguë si $b \equiv 0 \bmod a$; par exemple (a, b, a) n'est pas en général ambiguë dans son sens mais elle l'est avec la définition ici. Par contre, les deux définitions de classe ambiguë coïncident.

Afin d'étudier le nombre des formes primitives de discriminant D du type (a,a,c) avec $1 \leq a \leq 2c$, considérons l'ensemble $T(D)$ des couples (u,v) d'entiers positifs premiers entre eux tels que $-D = u(4v-u)$. Si $D \equiv 1 \bmod 4$, on constate que toute décomposition $-D = rs$ avec r et s positifs premiers entre eux satisfait $-r \equiv s \bmod 4$ et $\mathrm{pgcd}(r, \frac{r+s}{4}) = 1$, de sorte que $|T(D)| = 2^{t(D)}$. On verifierait de même au cas par cas que : (i) si $D \equiv 4, 8 \bmod 16$, ou si $D \equiv 16 \bmod 32$, alors $T(D) = \emptyset$, (ii) si $D \equiv 12 \bmod 16$ alors $|T(D)| = 2^{t(D)-1}$, et (iii) si $D \equiv 0 \bmod 32$ alors $|T(D)| = 2^{t(D)}$.

Considérons l'involution $(u,v) \mapsto (4v-u, v)$ de $T(D)$. Elle n'a pas de point fixe car $D \neq -4$. Il en résulte qu'exactement la moitié des $(u,v) \in T(D)$ satisfont $u < 4v-u$, c'est-à-dire $u < 2v$. Comme $D \neq -4$, la forme $(2c, 2c, c)$ n'est pas primitive et donc l'ensemble des formes réduites primitives de discriminant D du type (a,a,c) ou (a,b,a) a exactement $\frac{|T(D)|}{2}$ éléments. Le nombre total de formes réduites ambiguës est donc dans tous les cas

$$a(D) = \frac{|S(D)| + |T(D)|}{2},$$

d'où l'on déduit le théorème. □

Ainsi que nous le verrons plus tard, Gauss a défini une loi de groupe abélien naturelle sur $\mathrm{P}(D)$, basée sur sa *composition des formes*. Elle s'exprime naturellement grâce à l'arithmétique des corps quadratiques, c'est pourquoi nous repoussons temporairement sa description. L'élément neutre s'avèrera être la classe d'équivalence propre de la forme principale, et C^{opp} l'inverse de la classe C. Le résultat ci-dessus s'interprêtera alors comme la détermination des éléments de carré 1 de $\mathrm{P}(D)$, en particulier $t = 1$ si, et seulement si, $\mathrm{h}(D)$ est impair !

Exemple 3.31. Soit $D = -44$. La méthode de Gauss démontre que les formes réduites de discriminant -44 sont $(1,0,11)$, $(2,2,6)$ et $(3,\pm 2,4)$. En particulier $|\mathrm{Cl}(-44)| = 4$. La forme $(2,2,6)$ n'est pas primitive, de sorte que $\mathrm{h}(-44) = 3$. La forme $(1,0,11)$ est évidemment ambiguë, et les deux formes $(3,\pm 2,4)$ sont opposées l'une de l'autre. À équivalence près il y a donc exactement deux formes de discriminant -44 : $(1,0,11)$ et $(3,2,4)$. On déduit du théorème 3.13 le résultat suivant, annoncé au chapitre précédent : si $p > 2$ est un nombre premier tel que $\left(\frac{-11}{p}\right) = 1$ alors p est exclusivement de la forme $x^2 + 11y^2$ ou de la forme $3x^2 + 2xy + 4y^2$, avec $x, y \in \mathbb{Z}$. Comme nous l'avions observé, il y a statistiquement $2/3$ de ces nombres premiers qui sont du second type : bien que nous ne pourrons le démontrer ici, ce phénomène est en fait relié à l'apparition des deux formes équivalentes $(3,\pm 2,4)$ mais non proprement équivalentes.

7. Exercices

Exercice 3.1. *Montrer que tout nombre premier $\equiv 1 \bmod 4$ est de la forme $5x^2 + 16xy + 13y^2$ avec $x, y \in \mathbb{Z}$.*

Exercice 3.2. (Discriminants fondamentaux) *Soit $D \in \mathbb{Z}$ un entier non nul. On dit que D est un discriminant si c'est le discriminant d'une forme. On dit que D est un discriminant fondamental si de plus toute forme de discriminant D est primitive.*

(i) Montrer que D est un discriminant si, et seulement si, $D \equiv 0, 1 \bmod 4$.

(ii) Montrer que D est un discriminant fondamental si, et seulement si, :
(a) $D \equiv 1 \bmod 4$ et D est sans facteur carré,
(b) $D \equiv 0 \bmod 4$, $D/4 \equiv 2, 3 \bmod 4$, et $D/4$ est sans facteur carré.

(iii) Montrer que $|\mathrm{Cl}(D)| = \sum_{D'} \mathrm{h}(D')$ où D' parcourt les discriminant d divisant D et tels que D/d est un carré.

EXERCICE 3.3. *(i) Déterminer (des représentants de) $\mathrm{Cl}(-20)$ ainsi que ses classes ambiguës.*

(ii) Soit p un nombre premier impair tel que $\left(\frac{-5}{p}\right) = 1$. Montrer que p est soit de la forme $a^2 + 5b^2$, soit de la forme $2a^2 + 2ab + 3b^2$, et ce exclusivement.

(iii) (suite) Montrer que le premier cas se produit si, et seulement si, $p \equiv 1 \bmod 4$.

(iv) Donner des exemples.

EXERCICE 3.4. *(i) Déterminer $\mathrm{Cl}(-44)$ ainsi que ses classes ambiguës.*

(ii) Soit p un nombre premier impair tel que $\left(\frac{-11}{p}\right) = 1$. Montrer que p est soit de la forme $a^2 + 11b^2$, soit de la forme $3a^2 + 2ab + 4b^2$, et ce exclusivement.

(iii) Donner des exemples.

EXERCICE 3.5. *Démontrer que si p est un nombre premier tel que $\left(\frac{-84}{p}\right) = 1$ alors p est représenté par une et une seule des formes $(1, 0, 21)$, $(2, 2, 11)$, $(5, 4, 5)$ et $(3, 0, 7)$.*

EXERCICE 3.6. *Déterminer $\mathrm{Cl}(-56)$ ainsi que les classes ambiguës de ce discriminant. Comparer avec l'exercice 2.11.*

EXERCICE 3.7. *(i) On suppose $D < 0$. Trouver toutes les representations de 1 par la forme principale de discriminant D.*

(ii) En considérant les entiers $a_n, b_n \in \mathbb{Z}$ tels que $(1+\sqrt{2})^n = a_n + b_n\sqrt{2}$, montrer que $x^2 - 2y^2$ représente une infinité de fois 1 et -1.

EXERCICE 3.8. *Soit $\mathrm{G} \subset \mathrm{SL}_2(\mathbb{Z})$ le sous-groupe engendré par les éléments $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ et $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. On se propose de montrer que $\mathrm{G} = \mathrm{SL}_2(\mathbb{Z})$.*

(i) En utilisant l'algorithme de réduction de Lagrange, et que $|\mathrm{Cl}(-4)| = 1$, montrer que toute matrice dans $\mathrm{M}_2(\mathbb{Z})$ symétrique positive et de déterminant 1 est de la forme ${}^tPP$ où $P \in \mathrm{G}$.

(ii) Montrer que si $P \in \mathrm{SL}_2(\mathbb{Z})$ est tel que ${}^tPP = \mathrm{I}_2$ alors $P \in \mathrm{G}$.

(iii) Conclure.

EXERCICE 3.9. *Soit* $\mathbb{H} = \{\tau \in \mathbb{C}, \mathrm{Im}(\tau) > 0\}$ *le demi-plan de Poincaré. Si* g *désigne l'élément* $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *de* $\mathrm{SL}_2(\mathbb{R})$*, et si* τ *est dans* $\mathbb{H}$*, on pose* $g \cdot \tau = \frac{a\tau+b}{c\tau+d}$*.*

(i) Montrer la relation $\mathrm{Im}\ g \cdot \tau = \frac{\mathrm{Im}\,\tau}{|c\tau+d|^2}$*.*

(ii) Vérifier que $(g, \tau) \mapsto g \cdot \tau$ *définit une action de* $\mathrm{SL}_2(\mathbb{R})$ *sur* $\mathbb{H}$*.*

(iii) Vérifier que les transformations de $\mathbb{H}$ *définies par* $\tau \mapsto \tau + 1$ *et* $\tau \mapsto -\frac{1}{\tau}$ *sont induites par des éléments de* $\mathrm{SL}_2(\mathbb{Z})$*.*

Soit D *l'ensemble des éléments* τ *de* $\mathbb{H}$ *vérifiant soit* $-\frac{1}{2} < \mathrm{Re}\,\tau \leq \frac{1}{2}$ *et* $|\tau| > 1$*, soit* $0 \leq \mathrm{Re}\,\tau \leq \frac{1}{2}$ *et* $|\tau| = 1$ *(faire un dessin).*

(iv) Montrer que pour tout $\tau \in \mathbb{H}$*, l'orbite de* τ *sous l'action de* $\mathrm{SL}_2(\mathbb{Z})$ *rencontre* D*. On pourra considérer* $g \in \mathrm{SL}_2(\mathbb{Z})$ *tel que* $\mathrm{Im}\ g \cdot \tau$ *est maximal.*

(v) Soient $\tau \in \mathrm{D}$ *et* $g \in \mathrm{SL}_2(\mathbb{Z})$ *tels que* $g \cdot \tau \in \mathrm{D}$*. Vérifier que l'on a* $g \cdot \tau = \tau$*.*

(vi) En déduire que pour tout $\tau \in \mathbb{H}$*, l'orbite de* τ *sous l'action de* $\mathrm{SL}_2(\mathbb{Z})$ *rencontre un et un seul point dans* D*.*

(vii) Si $q = (a, b, c)$ *est une forme de discriminant* < 0*, montrer qu'il existe un unique* $\tau(q) \in \mathbb{H}$ *tel que* $q(x, y) = a(x - \tau(q)y)(x - \overline{\tau(q)}y)$ *pour tout* $(x, y) \in \mathbb{Z}^2$*.*

(viii) Vérifier que si $P \in \mathrm{SL}_2(\mathbb{Z})$ *et* $\mathrm{disc}\, q < 0$ *on a* $\tau(q \cdot P) = P^{-1} \cdot \tau(q)$*.*

(ix) En déduire une autre démonstration du théorème 3.22.

EXERCICE 3.10. (Polarisation d'une forme) *Soit* q *une forme. Si* $u, v \in \mathbb{Z}^2$ *on note* $f(u, v) \in \mathbb{Z}$ *l'unique élément tel que* $q(xu + yv) = q(u)x^2 + f(u, v)xy + q(v)y^2$*, autrement dit*

$$f(u, v) = q(u + v) - q(u) - q(v).$$

Montrer que $f : \mathbb{Z}^2 \times \mathbb{Z}^2 \to \mathbb{Z}, (u, v) \mapsto f(u, v)$ *est une application* $\mathbb{Z}$*-bilinéaire, symétrique et paire (i.e.* $f(u, u) \in 2\mathbb{Z}\ \forall u \in \mathbb{Z}$*), qui détermine* q *en retour par la formule* $q(u) = \frac{f(u,u)}{2}$ *pour tout* $u \in \mathbb{Z}^2$*.*

EXERCICE 3.11. (Formes de discriminant carré)

(i) Montrer qu'une forme de discriminant k^2 *avec* $k \geq 1$ *entier est équivalente à* $(0, k, c)$ *pour un unique entier* $0 \leq c \leq k - 1$*.*

(ii) Montrer qu'une forme de discriminant 0 *est équivalente à* $(0, 0, c)$ *pour un unique entier* $c \in \mathbb{Z}$*.*

EXERCICE 3.12. (Groupe orthogonal d'une forme) *Si* q *est une forme, on définit son groupe orthogonal par* $\mathrm{O}(q) = \{P \in \mathrm{GL}_2(\mathbb{Z}), q \cdot P = q\}$*, ainsi que* $\mathrm{SO}(q) = \mathrm{O}(q) \cap \mathrm{SL}_2(\mathbb{Z})$*.*

(i) Vérifier que $\mathrm{O}(q)$ *est un sous-groupe de* $\mathrm{GL}_2(\mathbb{Z})$ *contenant* $\pm\mathrm{I}_2$*.*

(ii) Montrer que $\mathrm{O}(q) \neq \mathrm{SO}(q)$ *si, et seulement si,* q *est ambiguë.*

(iii) Comparer $\mathrm{O}(q)$ *et* $\mathrm{O}(q')$ *si* q *et* q' *sont équivalentes, ou si* $q' = mq$ *avec* $m \neq 0$.

On suppose maintenant $D = \mathrm{disc}(q) < 0$.

(iv) Montrer que $\mathrm{O}(q)$ *est discret dans* $\mathrm{M}_2(\mathbb{R})$ *et qu'il est conjugué à un sous-groupe de* $\mathrm{O}_2(\mathbb{R})$.

(v) En déduire que $\mathrm{O}(q)$ *est fini, et que si* q *est ambiguë alors* $\mathrm{O}(q)$ *est un produit semi-direct de* $\mathbb{Z}/2\mathbb{Z}$ *par son sous-groupe* $\mathrm{SO}(q)$.

(vi) Montrer que si $P \in \mathrm{SO}(q)$ *fixe un élément non nul de* $\mathbb{Z}^2$ *alors* $P = \mathrm{I}_2$.

(vii) Supposons q *primitive et réduite. Montrer que* $\mathrm{SO}(q) = \{\pm I_2\}$ *à moins que* $D = -3$ *(resp.* $D = -4$*) auquel cas il est cyclique d'ordre* 6 *(resp.* 4*).*

(viii) Décrire explicitement $\mathrm{O}(q)$ *si* q *est réduite.*

Exercice 3.13. *Soient* p *un nombre premier et* q *une forme de discriminant* $D < 0$ *représentant* p. *On se propose de déterminer l'ensemble* $R = \{u \in \mathbb{Z}^2, q(u) = p\}$ *de toutes les représentations de* p *par* q. *Soit* b *l'unique entier tel que* $b^2 \equiv D \bmod 4p$ *et* $0 \leq b \leq p$ *(justifier).*

(i) Montrer que $\forall u \in R$, *il existe un unique* $P \in \mathrm{GL}_2(\mathbb{Z})$ *tel que* $q \cdot P = (p, b, \frac{b^2-D}{4p})$ *et* $P((1,0)) = u$.

(ii) Vérifier que l'action de $\mathrm{GL}_2(\mathbb{Z})$ *sur* $\mathbb{Z}^2$ *induit une action de* $\mathrm{O}(q)$ *sur* R.

(iii) En déduire que si $u \in R$, *alors* $R = \{P(u) \mid P \in \mathrm{O}(q)\}$.

(iv) En déduire que $|R| = |\mathrm{O}(q)|$, *à moins que* q *ne soit ambiguë et qu'il existe une symétrie* $s \in \mathrm{O}(q)$ *fixant un élément de* R, *auquel cas* $|R| = |\mathrm{SO}(q)|$.

(v) (suite) Montrer que ce second cas se produit si, et seulement si, p *divise* D.

Chapitre 4

Arithmétique des entiers quadratiques imaginaires

Le but de ce chapitre est d'introduire l'arithmétique des anneaux engendrés par des entiers algébriques (l'*arithmétique transcendante*, selon Gauss) en étudiant de manière détaillée le cas des anneaux $\mathbb{Z}[\sqrt{d}]$, où $d < 0$ est entier, et $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ lorsque de plus $d \equiv 1 \bmod 4$. Nous en donnerons aussi quelques applications à l'étude des équations diophantiennes.

Cette famille infinie d'exemples, historiquement la première étudiée, permet déjà de rendre compte de la diversité des phénomènes qui distinguent l'arithmétique de $\mathbb{Z}$ de celle des anneaux plus généraux. Même dans ce cas particulier, il est important pour ne pas s'y perdre de commencer par dégager les propriétés fondamentales que peut posséder la relation de divisibilité dans un anneau commutatif général, et c'est par là que nous commencerons. C'est de toutes façon une étape incontournable avant de dégager les propriétés plus fines de factorisation des idéaux démontrées par Kummer et Dedekind, qui feront l'objet d'un chapitre ultérieur.

Références : On pourra consulter le chapitre 4 du livre de Stewart & Tall, le chapitre 1 du livre de Samuel, où encore le chapitre du *Cours d'algèbre* de Perrin concernant l'arithmétique des anneaux.

1. Vocabulaire de l'arithmétique des anneaux

Dans tout ce paragraphe, A désigne un anneau commutatif unitaire. On supposera que A est *intègre*, ce qui signifie qu'il est non nul, et que pour tout $a, b \in A$, $ab = 0$ entraîne $a = 0$ ou $b = 0$.

1.1. Divisibilité. Si $a, b \in A$, on dit que a divise b, ou que b est multiple de a, et on écrit $a|b$, s'il existe $c \in A$ tel que $b = ac$. L'intégrité de A assure que c est alors unique si $a \neq 0$. La relation de divisibilité est une relation de préordre sur A au sens de Bourbaki : pour tout $a, b, c \in A$, alors $a|a$, et si $a|b$ et $b|c$ alors $a|c$. L'étude de cette relation est appelée parfois *arithmétique de* A.

1.2. Unités. Les diviseurs de 1 jouent un rôle particulier puisqu'ils divisent tous les éléments de A ; ils sont appelés *unités* ou *inversibles* de A. L'ensemble des unités de A est noté $A^\times$ (à ne pas confondre avec $A\backslash\{0\}$), c'est un groupe (commutatif) pour la multiplication de A.

1.3. Éléments associés. Par intégrité de A, on constate que si $a, b \in A$, on a $a|b$ et $b|a$ si, et seulement si, $a = bu$ avec $u \in A^\times$. On dit alors que a et b sont *associés*, c'est une relation d'équivalence sur A, que l'on notera $a \sim b$. Par exemple, l'arithmétique d'un corps est inintéressante, car tous les éléments non nuls sont associés...

1.4. Pgcd, ppcm. Si $a_1, \ldots, a_n$ est une famille d'éléments de A, on appelle *plus grand diviseur commun* (ou pgcd) des a_i un élément $d \in A$ tel que d divise a_i pour tout i, et tel que si $b \in A$ divise a_i pour tout i alors b divise d.

Autrement dit, c'est un élément maximal de A parmi les éléments inférieurs aux a_i pour la relation d'ordre de divisibilité. De même on définit un plus petit multiple commun (ou ppcm) des a_i comme étant un élément minimal parmi les éléments plus grands que les a_i pour la relation de divisibilité.

En toute généralité, pgcd et ppcm n'existent pas toujours : nous verrons des exemples de ce phénomène dans l'exercice 4.10. En revanche, il découle de la définition que si deux pgcd (resp. ppcm) existent alors il sont associés.

1.5. Éléments premiers entre eux. Des éléments $a_1, \ldots, a_n \in A$ sont dits premiers entre eux si leurs seuls diviseurs communs sont les unités, ou ce qui revient au même si l'élément 1 est un pgcd des a_i.

1.6. Éléments irréductibles. Un élément *non nul* $\pi \in A$ est dit irréductible si ce n'est pas une unité, et si pour tout $a, b \in A$, la relation $\pi = ab$ entraîne que a ou b est une unité. Autrement dit, aux unités près, ce sont les éléments ayant exactement deux diviseurs, à savoir 1 et eux-même.

Si π est irréductible, il en va de même de tout élément associé. Il est souvent commode de choisir un ensemble de représentants des éléments irréductibles pour la relation d'association. Par exemple, les unités de $\mathbb{Z}$ sont ± 1, et les irréductibles de $\mathbb{Z}$ sont les $\pm p$ avec p un nombre premier (sous entendu positif), un système de représentants étant précisément donné par l'ensemble des nombres premiers. *Par la suite, on désignera par* P *un tel ensemble fixé de représentants.*

1.7. Anneaux factoriels. La définition suivante est fondamentale.

Définition 4.1. *On dit que A a la propriété de factorisation si pour tout $a \in A$ ni nul ni inversible, alors il existe $u \in A^\times$, $n \geq 1$ et $\pi_1, \ldots, \pi_n \in \mathrm{P}$ tels que $a = u\pi_1 \cdots \pi_n$. On dit que A est factoriel si de plus, pour tout a comme précédemment, une telle écriture est unique à permutation près.*

Autrement dit, cette seconde propriété est que si $u\pi_1 \cdots \pi_n = u'\pi'_1 \cdots \pi'_m$ avec $u, u' \in A^\times$, $\pi_i, \pi'_j \in \mathrm{P}$, alors $m = n$, $\exists \sigma \in \mathfrak{S}_n$ tel que $\pi'_i = \pi_{\sigma(i)}$ pour tout $i = 1, \cdots, n$, et donc $u = u'$. Il est facile de voir qu'autant la propriété de factorisation que celle d'être factoriel ne dépendent pas du choix de l'ensemble de représentants P des irréductibles de A.

1.8. Arithmétique des anneaux factoriels. Supposons A factoriel. Si $a \in A$ est non nul et si $\pi \in \mathrm{P}$, le caractère factoriel assure que le nombre $v_\pi(a) \in \mathbb{N}$ d'occurences de π dans l'écriture de a comme produit d'une unité et d'éléments de P est bien défini, on l'appelle la valuation en π de A. Par définition, $v_\pi(a) = 0$ pour tout π sauf un nombre fini et il y a donc un sens a écrire

$$a = u \prod_{\pi \in \mathrm{P}} \pi^{v_\pi(a)}$$

avec $u \in A^\times$, avec la convention $a^0 = 1$ pour tout $a \in A - \{0\}$.

La propriété d'unicité entraîne $v_\pi(ab) = v_\pi(a) + v_\pi(b)$ pour tout $a, b \in A\backslash\{0\}$. En particulier, $a|b$ si et seulement si $v_\pi(a) \leq v_\pi(b)$ pour tout $\pi \in \mathrm{P}$, de sorte que l'arithmétique de A est essentiellement triviale.

On en déduit par exemple que pgcd et ppcm existent dans un anneau factoriel. En effet, un pgcd de $a_1, \ldots, a_n$ est $\prod_{\pi \in \mathrm{P}} \pi^{\mathrm{Min_i v_\pi(a_i)}}$, et un ppcm s'obtient de même en remplaçant le Min par un Max.

1.9. Éléments premiers. Un élément non nul $\pi \in A$ est dit premier si ce n'est pas une unité et s'il satisfait à la propriété d'Euclide-Gauss : pour tout $a, b \in A$, π divise ab entraîne π divise a ou π divise b.

Un élément premier est irréductible. En effet, si $\pi = ab$ alors π divise a ou b. Si par exemple $\pi|a$, de sorte que $a = \pi c$ où $c \in A$, alors $\pi = \pi cb$ puis $1 = cb$, et donc b est une unité.

1.10. Caractérisation d'Euclide-Gauss des anneaux factoriels. Il n'est pas vrai en général qu'un irréductible est premier. C'est vrai toutefois si A est factoriel, car si $\pi \in \mathrm{P}$ divise ab, alors $1 \leq v_\pi(ab) = v_\pi(a) + v_\pi(b)$ et donc soit $v_\pi(a) \geq 1$ soit $v_\pi(b) \geq 1$. Plus précisément, on a la propriété suivante :

Proposition 4.2. *Si A satisfait la propriété de factorisation alors A est factoriel si, et seulement si, tout irréductible de A est premier.*

Démonstration — Supposons que tout irréductible de A est premier. Supposons qu'il existe $u, u' \in A^\times$, $n, m \geq 1$, ainsi que $\pi_1, \ldots, \pi_n, \pi'_1, \ldots, \pi'_m \in \mathrm{P}$ tels que

$$u\pi_1 \ldots \pi_n = u'\pi'_1 \ldots \pi'_m.$$

Alors π_1 divise $u'\pi'_1 \ldots \pi'_m$. Si π_1 ne divise aucun des π'_i alors π_1 divise u' par la propriété d'Euclide-Gauss appliquée m fois, et donc π_1 est une unité : absurde. Quitte à permuter les π'_i on peut donc supposer que π_1 divise π'_1, c'est-à-dire $\pi_1 = \pi'_1$ car π'_1 est irréductible, et donc associé à π_1. Ainsi, on peut diviser l'égalité ci-dessus par π_1 (A intègre). On conclut par récurrence sur n à moins que $m > n$ et qu'un produit de $m - n$ éléments parmi les π'_i soit une unité, ce qui est impossible car un diviseur d'une unité est une unité. □

1.11. Idéaux. On rappelle qu'un idéal est un sous-groupe additif $I \subset A$ tel que $aI \subset I$ pour tout $a \in A$. L'ensemble aA des multiples de a dans A est un idéal appelé idéal principal engendré par $a \in A$. On note aussi $(a) = aA$. On a $bA \subset aA$ si et seulement $b \in aA$, i.e. si, et seulement si, $a|b$ ("contenir c'est diviser"). En particulier $aA = A$ si, et seulement si, $a \in A^\times$.

Si $(I_j)_{j\in J}$ sont des idéaux, on désigne par $\sum_j I_j$ le plus petit idéal contenant les I_j, c'est-à-dire l'ensemble des sommes finies d'éléments de $\bigcup_j I_j$. Si $a_1, \ldots, a_n \in A$ on pose aussi

$$(a_1, \ldots, a_n) = a_1A + a_2A + \cdots + a_nA = \{\sum_{i=1}^{n} a_i x_i, x_i \in A \ \forall i\},$$

Un idéal est dit finiment engendré ou de type fini s'il est de la forme $(a_1, \ldots, a_n)$.

De même, $\cap_j I_j$ est un idéal : c'est le plus grand idéal inclus dans chacun des I_j. Les notions de somme et d'intersection sont donc les analogues dans le langage des d'idéaux des notions respectives de pgcd et ppcm pour les éléments.

1.12. Anneaux noethérien. Un anneau est dit noethérien si tout idéal de A est finiment engendré. Une propriété importante (en fait caractéristique) des anneaux noethériens est que toute suite $(I_m)_{m\geq 1}$ d'idéaux qui est croissante, c'est-à-dire $I_m \subset I_{m+1}$ pour tout $m \geq 1$, est constante à partir d'un certain rang.

En effet, on vérifie immédiatement que $I = \bigcup_{m\geq 1} I_m$ est un idéal de A, donc de la forme $(a_1, \ldots, a_n)$ pour certains éléments $a_i \in A$. Si N est assez grand de sorte que $a_i \in I_N$ pour $i = 1, \ldots, n$, on constate que $I_m \subset I \subset I_N$ pour tout $m \geq 1$, d'où l'on tire $I_m = I_N$ si $m \geq N$.

PROPOSITION 4.3. *Si A est noethérien alors A admet la propriété de factorisation.*

DÉMONSTRATION — Soit $S \subset A\backslash\{0\}$ l'ensemble des éléments qui sont produits d'unités et d'irréductibles. Si $a \notin S$, alors a n'est pas irréductible en particulier, et donc il est de la forme bc avec b et c non unités. Comme S est stable par produits, soit b soit c n'est pas dans S ! Si $S \neq A\backslash\{0\}$, on construit donc récursivement une suite d'éléments non nuls $(a_m)_{m\geq 1}$ avec $a_m \in A\backslash S$, a_{m+1} divise a_m, et a_m non associé à a_{m+1}. Ainsi, $I_m = (a_m)$ est une suite strictement croissante d'idéaux de A, ce qui est absurde par noethérianité . □

1.13. Anneaux principaux. Un anneau est dit principal si tous ses idéaux sont principaux.

LEMME 4.4. (Relation de Bézout) *Si A est principal, et si $a, b \in A$, alors a et b admettent un pgcd d et il existe $u, v \in A$ tels que $au + bv = d$.*

En effet, il existe $d \in A$ tel que l'idéal $Aa + Ab$ (donc principal) soit de la forme Ad. Un tel d est évidemment un pgcd de a, b, et de la forme $au + bv$ avec $u, v \in A$.

PROPOSITION 4.5. *Un anneau principal est factoriel.*

Démonstration — Un anneau principal est évidemment noethérien, de sorte que A satisfait la propriété de factorisation. Il suffit de vérifier la caractérisation d'Euclide-Gauss. Soit π un irréductible. Supposons $\pi|ab$ avec $a, b \in A$. Si π ne divise pas a alors a et π sont premiers entre eux, et donc il existe $u, v \in A$ tels que $au + \pi v = 1$ d'après le lemme ci-dessus. Mais alors $abu + \pi bv = b$ et donc π divise b. □

1.14. Anneaux euclidiens. L'anneau A est dit euclidien s'il possède une fonction $\varphi : A\backslash\{0\} \to \mathbb{N}$ telle que $\forall a, b \in A\backslash\{0\}$, il existe q et $r \in A$ tels que :

(i) $a = bq + r$,

(ii) on a soit $r = 0$, soit $\varphi(r) < \varphi(b)$.

Pour des raisons que l'auteur ignore, une telle fonction s'appelle un *stathme euclidien*. Les deux exemples fondamentaux d'anneaux euclidiens sont les anneaux $\mathbb{Z}$ et $k[X]$ quand k est un corps. Un stathme euclidien sur $\mathbb{Z}$ est donné par $\varphi(a) = |a|$ (valeur absolue) et un stathme euclidien sur $k[X]$ étant la fonction degré d'un polynôme non nul. La vérification de (i) et (ii) dans les deux cas est le fruit de l'algorithme classique de division euclidienne.

Théorème 4.6. (Gauss) *Un anneau euclidien est principal, et donc factoriel.*

Démonstration — L'idéal nul étant principal, il suffit de voir que tout idéal non nul I de A est principal. Soit φ un stathme euclidien sur A, la partie $\varphi(I\backslash\{0\}) \subset \mathbb{N}$ est non vide, on peut donc trouver un élément $b \in I\backslash\{0\}$ pour lequel $\varphi(b)$ soit minimal. Bien entendu, $bA \subset I$ et nous allons vérifier l'inclusion réciproque. Mais si $a \in I$, il existe $q, r \in A$ tels que $a = bq + r$, et que de plus si $r \neq 0$ alors $\varphi(r) < \varphi(b)$. Mais $r = a - bq \in I$ car I est un idéal, donc ce second cas ne se produit pas par minimalité de $\varphi(b)$. Ainsi, $a = bq$ puis $I \subset bA$ et $I = bA$. □

Corollaire 4.7. *Les anneaux $\mathbb{Z}$ et $k[X]$ quand k est un corps sont principaux, et donc factoriels.*

Les inversibles de $k[X]$ quand k est un corps étant les constantes dans $k^\times$, on prend en général les polyômes unitaires non constants comme ensemble P des représentants des irréductibles dans ce cas. De la factorialité de $k[X]$ et du lemme du contenu de Gauss on déduit aussi la proposition importante suivante, pour laquelle nous renvoyons à l'exercice 4.12. On rappelle qu'un polynôme $P \in A[X]$ est dit primitif si ses coefficients sont premiers entre eux dans leur ensemble. On note aussi $K = \mathrm{Frac}(A)$ le corps de fractions [1] de A.

1. Lorsque A est un sous-anneau d'un corps C, on rappelle que le corps de fractions de A est simplement l'ensemble des $\frac{a}{b} \in C$ avec $a, b \in A$ et $b \neq 0$. C'est un sous-corps de C noté $\mathrm{Frac}(A)$. En général, on considère l'ensemble X des couples $(a, b) \in A^2$ tels que $b \neq 0$. La relation $(a, b) \sim (a', b') \Leftrightarrow ab' = ba'$ est une relation d'équivalence sur X dont l'ensemble des classes est noté Frac$A$. La classe de $(a, b) \in X$ est notée $\frac{a}{b}$. On munit $\mathrm{Frac}(A)$ d'une structure de corps en posant $\frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}$ et $\frac{a}{b} + \frac{a'}{b'} = \frac{ab'+ba'}{bb'}$. C'est un exercice de vérifier que ces lois sont bien définies indépendamment des choix de représentants et qu'elle définissent une loi de corps sur $\mathrm{Frac}(A)$. L'anneau A se plonge alors dans K via $\iota : a \mapsto \frac{a}{1}$ (un morphisme injectif d'anneau), et tout élément de $\mathrm{Frac}(A)$ est de la forme $\frac{\iota(a)}{\iota(b)} = \frac{a}{b}$ pour certains $a, b \in A$ et $b \neq 0$. Dans les fondements des mathématiques, c'est ainsi que l'on définit $\mathbb{Q}$ à partir de $\mathbb{Z}$!

PROPOSITION 4.8. (Gauss) *Si A est factoriel alors $A[X]$ est factoriel. De plus, les irréductibles de $A[X]$ sont exactement les irréductibles de A ainsi que les polynômes primitifs irréductibles dans $K[X]$.*

2. Anneaux d'entiers quadratiques imaginaires euclidiens

Fixons $D \equiv 0, 1 \bmod 4$ un entier que l'on supposera < 0. On considère le nombre complexe α défini par $\alpha = \sqrt{D/4}$ si $D \equiv 0 \bmod 4$, ou $\alpha = \frac{1+\sqrt{D}}{2}$ si $D \equiv 1 \bmod 4$. Pour lever l'ambiguïté sur la racine carrée intervenant dans sa définition nous supposerons que l'on choisit celle de partie imaginaire > 0. C'est un entier algébrique : on a $\alpha^2 = D/4 \in \mathbb{Z}$ dans le premier cas, et $\alpha^2 - \alpha + \frac{1-D}{4} = 0$ dans le second. On considère alors le réseau $A_D \subset \mathbb{C}$ de base $1, \alpha$, i.e.

$$A_D = \mathbb{Z} + \mathbb{Z}\alpha.$$

La remarque précédente montre que *c'est un sous-anneau de* $\mathbb{C}$, ou encore que $A_D = \mathbb{Z}[\alpha]$ au sens du premier chapitre. Par exemple, $A_{-4} = \mathbb{Z}[i]$ (entiers de Gauss) et $A_{-3} = \mathbb{Z}[j]$ où $j = e^{2i\pi/3} = \frac{1+\sqrt{-3}}{2} - 1$ (entiers d'Eisenstein). Nous allons nous intéresser à l'arithmétique de l'anneau A_D.

Une application qui jouera un rôle important par la suite est l'application norme. Si $z \in \mathbb{C}$, on pose $\mathrm{N}(z) = z\overline{z} \in \mathbb{R}_{\geq 0}$: c'est le carré de la norme usuelle. Bien sûr, $\mathrm{N}(zz') = \mathrm{N}(z)\mathrm{N}(z')$ pour tout $z, z' \in \mathbb{C}$ et on constate de plus que pour tout $x, y \in \mathbb{Z}$, alors

$$\mathrm{N}(x + y\alpha) = \begin{cases} x^2 - \frac{D}{4}y^2, & \text{si } D \equiv 0 \bmod 4, \\ x^2 + xy + \frac{1-D}{4}y^2, & \text{si } D \equiv 1 \bmod 4. \end{cases}$$

La fonction $(x, y) \mapsto \mathrm{N}(x + y\alpha)$ est donc la forme principale de discriminant D. En particulier, $\mathrm{N}(\mathbb{Z}[\alpha]) \subset \mathbb{N}$. Notons de plus que $z \mapsto \overline{z}$ préserve $\mathbb{Z}[\alpha]$, car $\overline{\alpha}$ vaut $-\alpha$ ou $1 - \alpha$.

PROPOSITION 4.9. *(i) Les unités de A_D sont les éléments $u \in A_D$ tels que $\mathrm{N}(u) = 1$. En particulier, hormis les exceptions $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ et $\mathbb{Z}[j]^\times = \{\pm 1, \pm j, \pm j^2\}$ on a $A_D = \{\pm 1\}$.*

(ii) Soient $a, b \in A_D$ non nuls tels que $a \mid b$ dans $\mathbb{Z}[\alpha]$. Alors $\mathrm{N}(a) \mid \mathrm{N}(b)$ dans $\mathbb{Z}$, et $\mathrm{N}(a) = \mathrm{N}(b)$ si et seulement si a et b sont associés.

(iii) Pour que $\pi \in A_D$ non nul et non unité soit irréductible, il suffit qu'aucun diviseur propre de $\mathrm{N}(\pi)$ ne soit de la forme $\mathrm{N}(z)$ avec $z \in A_D$. C'est en particulier le cas si $\mathrm{N}(\pi)$ est premier.

DÉMONSTRATION — Soient $a, b \in A_D$ tels que $ab = 1$. Alors $\mathrm{N}(a), \mathrm{N}(b) \in \mathbb{N}$ et $\mathrm{N}(a)\mathrm{N}(b) = 1$, donc $\mathrm{N}(a) = 1$. Réciproquement, si $a \in A_D$ est tel que $\mathrm{N}(a) = 1$ alors $a\overline{a} = 1$ mais $\overline{a} \in A_D$ et donc $a \in A_D^\times$. Le "en particulier" découle de l'étude des représentations de 1 par une forme principale, déjà traitée en exercice.

Si $a = bc$ avec $a, b, c \in A_D$ non nuls, alors $\mathrm{N}(a) = \mathrm{N}(b)\mathrm{N}(c)$ et donc $\mathrm{N}(b) \mid \mathrm{N}(a)$ dans $\mathbb{Z}$. Il y a égalité si, et seulement si, $\mathrm{N}(c) = 1$, i.e. $c \in A_D^\times$. Le (iii) en découle immédiatement. □

COROLLAIRE 4.10. *A_D a la propriété de factorisation.*

DÉMONSTRATION — En effet, on constate que si $a, b \in A_D$ sont non nuls et tels que a est un diviseur propre de b (i.e. $b = ac$ avec ni a ni c une unité), alors $N(a) < N(b)$. On conclut donc par récurrence sur la norme de l'élément. □

THÉORÈME 4.11. *Si $D \in \{-3, -4, -7, -8, -11\}$ alors A_D est euclidien pour le stathme* N. *En particulier, il est principal et factoriel. Pour les autres valeurs de D, l'anneau A_D n'est pas euclidien (pour aucun stathme).*

La première partie du théorème est due à Gauss, la dernière à P. Samuel [2].

DÉMONSTRATION — Commençons par vérifier le premier point. Il suffit de montrer la propriété d'approximation suivante : si $z \in \mathbb{C}$, il existe un $t \in A_D$ tel que $|z - t| < 1$. En effet, si a et b sont non nuls et dans A_D, et si $t \in A_D$ est tel que $\mathrm{N}(\frac{a}{b} - t) < 1$, alors $\mathrm{N}(a - tb) < \mathrm{N}(b)$ (multiplicativité de N), et donc $\mathrm{N} : A_D \to \mathbb{N}$ définit un stathme euclidien. Il ne reste qu'à vérifier la propriété d'approximation ci-dessus pour les valeurs de l'énoncé. Il ne serait pas difficile de procéder géométriquement. Donnons un argument algébrique.

Soit q la forme principale de discriminant $D < 0$. Soient $x, y \in \mathbb{R}$ fixés. On cherche $u, v \in \mathbb{Z}$ tels que $q(x - u, y - v) < 1$. Supposons $D \equiv 0 \bmod 4$. On peut choisir $u, v \in \mathbb{Z}$ tels que $|x - u|, |y - v| \leq \frac{1}{2}$, auquel cas

$$q(x - u, y - v) = (x - u)^2 - \frac{D}{4}(y - v)^2 \leq \frac{1 - D/4}{4}$$

qui est < 1 si $D = -4, -8$. Supposons $D \equiv 1 \bmod 4$, auquel cas on rappelle l'identité $4q(\alpha, \beta) = (2\alpha + \beta)^2 - D\beta^2$. On choisit alors $v \in \mathbb{Z}$ tel que $|y - v| \leq 1/2$, puis $u \in \mathbb{Z}$ tel que $|2u + \frac{v - 2x - y}{2}| \leq 1$, c'est bien sur possible ! On a alors $4q(x - u, y - v) \leq 1 - \frac{D}{4}$ qui est < 4 dès que $-D < 12$, ce qui conclut le premier point.

Pour voir que A_D n'est pas euclidien nous avons besoin de la proposition suivante.

PROPOSITION 4.12. *(i) Tout idéal non nul de A_D admet une $\mathbb{Z}$-base à deux éléments. En particulier, A_D est noethérien.*

(ii) Tout idéal non nul I de A_D est d'indice fini dans A_D, noté $\mathrm{N}(I)$ *("norme de I").*

(iii) Si $z \in A_D$ est non nul, alors $\mathrm{N}((z)) = \mathrm{N}(z)$.

DÉMONSTRATION — Si I est un idéal de A_D, il est donc discret dans $\mathbb{C} \simeq \mathbb{R}^2$, comme partie d'un réseau. C'est en fait un réseau s'il est non nul. En effet, si $x \neq 0 \in I$ on constate que $x, \alpha x \in I$ est encore une $\mathbb{R}$-base de $\mathbb{C}$, ce qui conclut. En particulier, I admet une $\mathbb{Z}$-base à deux éléments (c'est la caractérisation algébrique des réseaux, i.e. le théorème 2.4) et est d'indice fini dans A_D (Proposition 2.17). De plus, on a $|A_D/I| = \mathrm{covol}\, I \,/\, \mathrm{covol} A_D$. Mais la multiplication par $z \in \mathbb{C}^\times$ est la composée d'une rotation et d'une homothétie de rapport $|z|$, qui multiplie donc les covolumes par $|z|^2 = N(z)$. En particulier, on a l'égalité $\mathrm{N}((z)) = \mathrm{N}(z)$. □

2. P. Samuel, *About euclidean rings*, Journal of Algebra 19, 282-301 (1971).

Terminons la démonstration du théorème. Supposons que A_D admette un stathme euclidien φ. Soit $x \in A$ qui n'est ni nul, ni une unité, et tel que $\varphi(x)$ est minimal. On en déduit que tout $a \in A_D$ est de la forme $bx + r$ avec $r = 0$ ou $r \in A_D^\times$. En particulier $1 < \mathrm{N}(x) = \mathrm{N}((x)) \leq 1 + |A_D^*|$. Mais $|D| > 4$, donc $A_D^* = \{\pm 1\}$, puis $\mathrm{N}(x) \in \{2, 3\}$. En particulier la forme principale de discriminant $-D$ représente 2 ou 3. Il est clair que cela entraîne $|D/4| \leq 3$ si $D \equiv 0 \bmod 4$, et $|D| \leq 12$ si $D \equiv 1 \bmod 4$ (car $4(x^2 + xy + \frac{1-D}{4}) = (2x + y)^2 - Dy^2$)). Il ne reste qu'à exclure $A_{-12} = \mathbb{Z}[\sqrt{-3}]$, mais il n'est pas euclidien car non factoriel (voir §4). □

3. Digression : application aux équations diophantiennes

Avant de continuer notre analyse, donnons une application typique de la factorialité des anneaux de la forme $\mathbb{Z}[\alpha]$ à l'étude des équations diophantiennes. La proposition suivante avait été formulée par Fermat, on prétend qu'il l'avait lancée en défi aux mathématiciens anglais de son époque (le milieu du 17$^{\text{eme}}$ siècle). Nombreux sont les contemporains de Fermat qui considéraient ce problème comme étant insoluble !

PROPOSITION 4.13. *Les seules solutions $x, y \in \mathbb{Z}$ de l'équation $y^2 = x^3 - 2$ sont $(x, y) = (\pm 5, 3)$.*

DÉMONSTRATION — Soient $x, y \in \mathbb{Z}$ tels que $y^2 = x^3 - 2$. Comme 2 n'est pas un cube dans $\mathbb{Z}/4\mathbb{Z}$, on constate que x et y sont impairs. On déduit de $y^2 = x^3 - 2$ qu'ils sont en fait premiers entre eux. Considérons la factorisation

$$(y + i\sqrt{2})(y - i\sqrt{2}) = x^3$$

dans $\mathbb{Z}[i\sqrt{2}] = A_{-8}$. Ce dernier est euclidien d'après la proposition précédente, donc factoriel. Vérifions que $y + i\sqrt{2}$ et $y - i\sqrt{2}$ sont premiers entre eux dans $\mathbb{Z}[i\sqrt{2}]$. Il suffit de voir qu'il n'y a pas d'irréductible π divisant $y + i\sqrt{2}$ et $y - i\sqrt{2}$. Mais un tel π diviserait $2i\sqrt{2} = -(i\sqrt{2})^3$, et donc $i\sqrt{2}$ (car π est également premier), et donc y. Mais alors $\mathrm{N}(i\sqrt{2}) = 2$ diviserait $N(y) = y^2$, ce qui est absurde.

Si dans un anneau factoriel A, on a une relation $a^n = bc$ avec b et c premier entre eux, et n un entier ≥ 1, on constate en décomposant b et c en irréductibles qu'il existe $d \in A$ et $u \in A^\times$ tels que $b = d^n u$. Comme $\mathbb{Z}[\sqrt{-2}]^\times = \{\pm 1\}$, on en déduit l'existence de $u, v \in \mathbb{Z}$ tels que

$$\pm(y + i\sqrt{2}) = (u + iv\sqrt{2})^3 = u^3 - 6uv^2 + (3u^2v - 2v^3)i\sqrt{2}.$$

En prenant la coordonnée en $i\sqrt{2}$, on obtient $\pm 1 = v(3u^2 - 2v^2)$, d'où l'on tire $v = \pm 1$ puis $3u^2 = \pm v + 2$ et donc $u = 1$ et $v = \pm 1$. En particulier, $\pm y = u^3 - 6uv^2 = -5$, ce qui conclut ! □

Cette méthode admet de multiples applications. La plus célèbre est certainement la stratégie qu'elle fournit pour montrer que l'équation de Fermat $x^n + y^n = z^n$, qui s'écrit aussi

$$x^n = \prod_{i=0}^{n-1} (z - \zeta^i y)$$

où $\zeta = e^{\frac{2i\pi}{n}}$, n'a pas de solution non triviale ($xyz = 0$) quand $n \neq 2$. Si l'on sait que $\mathbb{Z}[\zeta]$ est factoriel, et si l'on arrive à se ramener au cas où les $z-\zeta^i y$ sont premiers entre eux, cela fournit un point de départ pour l'étude de l'équation, à savoir que $z - \zeta y$ est une puissance n^{ieme} dans $\mathbb{Z}[\zeta]$ fois une unité de $\mathbb{Z}[\zeta]$, ce qui fournit $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ identités distinctes au lieu d'une !

L'idée même que $\mathbb{Z}[\alpha]$ avec $\alpha \in \overline{\mathbb{Z}}$ puisse ne pas être factoriel a en fait mis très longtemps à émerger dans l'esprit des mathématiciens. Sous une autre forme peut-être, c'est aussi l'erreur présumée de la démonstration jamais retrouvée par Fermat de son "théorème" ("cette marge est trop petite pour la contenir."...). Fermat en a vraiment démontré le cas $n = 4$ par sa méthode de descente infinie, et le cas second cas historiquement effectivement démontré, à savoir $n = 3$ a dû attendre Euler. Dans ce cas, $\mathbb{Z}[j] = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ est factoriel d'après le théorème ci-dessus, et la stratégie fonctionne en effet : nous renvoyons au chapitre 17 du livre de Ireland et Rosen pour une démonstration utilisant ces idées. Cette stratégie a aussi ses limites, on peut en fait montrer que le plus petit entier n impair tel que $\mathbb{Z}[\zeta]$ n'est pas factoriel est $n = 23$, et aussi qu'il n'y a qu'un nombre fini d'entiers n tels que $\mathbb{Z}[\zeta]$ est factoriel ! Il faut alors se plonger dans les travaux de Kummer pour aller plus loin dans cette direction... Mais ceci anticipe sur le cheminement du cours... revenons donc à l'anneau $\mathbb{Z}[\alpha]$ étudié ici.

4. Anneaux d'entiers quadratiques imaginaires factoriels

Donnons des exemples de D pour lesquels $A_D = \mathbb{Z}[\alpha]$ n'est pas factoriel. Vérifions par exemple que $\mathbb{Z}[\sqrt{-3}]$ n'est pas factoriel. En effet, on a la relation

$$2 \cdot 2 = 4 = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

bien que 2 et $1 \pm \sqrt{-3}$ soient des irréductibles non associés dans $\mathbb{Z}[\sqrt{3}]$. Le seul point non trivial est cette dernière assertion, vérifions-là à l'aide de la proposition 4.9. Les unités de $\mathbb{Z}[\sqrt{-3}]$ étant ± 1, il sont deux à deux non associés. Ils sont aussi irréductibles. En effet, chacun est de norme 4 et 2 n'est pas une norme de $\mathbb{Z}[\sqrt{-3}]$, i.e. n'est pas de la forme $a^2 + 3b^2$ avec $a, b \in \mathbb{Z}$. Cela conclut. De même, on vérifierait que les factorisations

$$2 \cdot 2 = -(2i)^2, \;\; 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}), \;\; 2 \cdot 3 = -\sqrt{-6}^2$$

entraînent que $\mathbb{Z}[\sqrt{-3}]$, $\mathbb{Z}[\sqrt{-4}] = \mathbb{Z}[2i]$, $\mathbb{Z}[\sqrt{-5}]$ et $\mathbb{Z}[\sqrt{-6}]$ ne sont pas factoriels. Par exemple, 2, 3 et $1 \pm \sqrt{-5}$ sont de normes respectives 4, 9 et 6, ils sont donc irréductibles car il n'y a pas d'élément de norme 2 ou 3 dans $\mathbb{Z}[\sqrt{-5}]$, non associés car $\mathbb{Z}[\sqrt{-5}]^\times = \{\pm 1\}$. Un premier résultat général est le suivant, englobant notamment les exemples précédents sauf $d = -5$.

Proposition 4.14. *Si A_D est factoriel, alors D est sans facteur carré, à moins que l'on ait $D \equiv 0 \bmod 4$ auquel cas $D/4$ est sans facteur carré et n'est pas congru à 1 modulo 4.*

Un entier $D \equiv 0, 1 \bmod 4$ satisfaisant les conclusions de cette proposition est appelé *discriminant fondamental*. Il est équivalent de demander que D n'est pas de la forme $N^2 D'$ avec $D \equiv 0, 1 \bmod 4$ et $N \in \mathbb{Z}$, ou encore que toutes les formes binaires de discriminant D sont primitives (comparer avec l'exercice 3.2).

La première observation, cruciale, est dûe à Dedekind. Soit A un anneau intègre de corps de fractions K. On dit que A est *intégralement clos* (ou *normal*) si pour tout élément de K qui est entier sur A est en fait dans A. Autrement dit, si pour tout $x \in K$ tel qu'il existe $P \in A[X]$ unitaire vérifiant $P(x) = 0$ alors $x \in A$.

PROPOSITION 4.15. *Si A est factoriel alors A est intégralement clos.*

DÉMONSTRATION — En effet, supposons que $x \in K$ et qu'il existe un entier $n \geq 1$ et des éléments $a_0, a_1, \ldots, a_{n-1} \in A$ tels que

$$a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} = x^n.$$

Comme A est factoriel on peut écrire $x = \frac{p}{q}$ avec $p, q \in A$ premiers entre eux, $q \neq 0$. Mais alors en multipliant l'équation par q^n on conclut que q divise p^n. Si π est un irréductible divisant q, il divise donc p car π est premier, ce qui est absurde car p et q sont premiers entre eux. Ainsi, q est une unité, et donc $x \in A$. □

Cette proposition généralise l'égalité $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$ démontrée au premier chapitre. Un autre exemple important d'anneau intégralement clos est donné par la proposition suivante :

PROPOSITION 4.16. *L'anneau $\overline{\mathbb{Z}}$ est intégralement clos.*

DÉMONSTRATION — Soit $x \in \mathbb{C}$ et soit $P \in \overline{\mathbb{Z}}[X]$ unitaire de degré n satisfaisant $P(x) = 0$. Il faut montrer $x \in \overline{\mathbb{Z}}$. Soient $a_0, a_1, \ldots, a_{n-1} \in \overline{\mathbb{Z}}$ les coefficients de P, $A = \mathbb{Z}[a_0, \ldots, a_{n-1}]$ et $B = \mathbb{Z}[a_0, \ldots, a_{n-1}, x]$. On a $xB \subset B$. Il suffit donc de montrer que le groupe additif B est finiment engendré (Proposition 1.16 (ii)).

D'après la proposition 1.16 (i), le groupe additif de A est finiment engendré. Il suffit donc de montrer que tout élément de B est de la forme $\sum_{i=0}^{n} a_i x^i$ avec $a_i \in A$. Soit $y \in B$. On peut donc écrire $y = Q(x)$ avec $Q \in A[X]$. Comme P est unitaire à coefficients dans $\mathbb{Z}$, donc dans l'anneau A, on peut effectuer la division euclidienne de Q par P dans $A[X]$: on peut écrire $Q = SP + R$ avec $S, R \in A[X]$ et $\deg R < n$. On a alors $y = Q(x) = R(x)$, ce que l'on voulait démontrer. □

PROPOSITION 4.17. *A_D est intégralement clos si, et seulement si, D est un discriminant fondamental.*

DÉMONSTRATION — Nous ne démontrerons pour l'instant que la condition nécessaire, qui est celle dont on a besoin pour démontrer la proposition 4.14. La condition suffisante sera démontré au chapitre suivant.

Supposons $A_D = \mathbb{Z}[\alpha]$ intégralement clos. Il contient en particulier $\overline{\mathbb{Z}} \cap \mathbb{Q}(\sqrt{d})$. Écrivons $d = d'm^2$ avec $m \geq 1$ et d' sans facteur carré. On a donc $\sqrt{d'} = \frac{1}{m}\sqrt{d} \in \mathbb{Z}[\alpha]$. En considérant la $\mathbb{Z}$-base $1, \alpha$ de $\mathbb{Z}[\alpha]$, on constate que cela entraîne $m = 1$, donc $d = d'$ est sans facteur carré. Dans le cas $\alpha = \frac{1+\sqrt{d}}{2}$, observera pour cela que $\frac{1}{m}\sqrt{d} = \frac{2}{m}\alpha - \frac{1}{m}$, donc $1/m \in \mathbb{Z}$. Enfin, si $d \equiv 1 \bmod 4$, on observe de plus $\frac{1+\sqrt{d}}{2} \in \overline{\mathbb{Z}} \cap \mathbb{Q}(\sqrt{d}) \subset \mathbb{Z}[\alpha]$, et donc $\alpha = \frac{1+\sqrt{d}}{2}$. □

La proposition 4.14 peut en fait être sensiblement améliorée. Nous devons au préalable faire une remarque sur les différences entre "factoriel" et "principal" pour les anneaux $\mathbb{Z}[\alpha]$. Bien qu'il ne soit pas vrai en général qu'un anneau noethérien factoriel est principal (par exemple l'idéal $(2, X)$ de l'anneau factoriel $\mathbb{Z}[X]$ n'est pas principal), cela vaut pour les anneaux qui nous intéresseront majoritairement dans le cours, à savoir les $\mathbb{Z}[\alpha]$ avec $\alpha \in \overline{\mathbb{Z}}$. Nous reportons la vérification de ce fait à un chapitre ultérieur.

Il se trouve que la question de la principalité de $\mathbb{Z}[\alpha]$ est intimement reliée à la théorie des formes binaires étudiée au chapitre précédent. Ce lien peut-être inattendu sera étudié en détail un peu plus loin dans le cours. Le théorème suivant en sera un cas particulier.

THÉORÈME 4.18. *Soit $D < 0$ un discriminant fondamental. L'anneau A_D est principal si, et seulement si, on a $\mathrm{h}(D) = 1$.*

Notre étude des formes binaires admet alors la conséquence suivante.

COROLLAIRE 4.19. *Soit d un entier < 0.*

(i) L'anneau $\mathbb{Z}[\sqrt{d}]$ est principal si, et seulement si, $d = -1$ ou -2.

(ii) On suppose $d \equiv 1 \bmod 4$. L'anneau $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ est principal si, et seulement si, l'entier d est dans l'ensemble $\{-3, -7, -11, -19, -43, -67, -163\}$.

DÉMONSTRATION — Supposons que $\mathbb{Z}[\sqrt{d}]$ est principal. La proposition 4.14 entraîne que d est sans facteur carré ainsi que la congruence $d \equiv 3 \bmod 4$ si d est impair. Si on a $d = ab$ avec $a < b$, la forme binaire $(a, 0, b)$ est de discriminant $4d$, réduite au sens de Gauss, et primitive : c'est donc la forme principale par le théorème 4.18, *i.e.* $a = 1$. On a donc soit $d = -1$, soit $-d$ est un nombre premier. Si c'est un premier impair, on observe de même que la forme binaire $(2, 2, \frac{1-d}{2})$ est de discriminant $4d$, réduite au sens de Gauss, et primitive car on a $d \equiv 3 \bmod 4$, ce n'est donc pas la forme principale : c'est absurde par le théorème 4.18. Les seules possibilités sont donc $d = -1$ ou $d = -2$. Réciproquement, on a déjà vu que pour ces valeurs de d l'anneau $\mathbb{Z}[\sqrt{d}]$ est euclidien, donc principal.

De même, la condition suffisante du (ii) se déduit du théorème 4.18 et de la proposition 3.26. La condition nécessaire, la plus intéressante peut-être, est par contre absolument non élémentaire : elle se déduit du théorème 3.27 de Heegner-Stark-Baker. Un argument élémentaire semblable à celui du (i), consistant à considérer des formes réduites ambiguës, démontre par contre que si $\mathrm{h}(d) = 1$ avec $d \equiv 1 \bmod 4$ sans facteur carré, alors d est premier. □

Nous renvoyons à l'exercice 4.6 pour une démonstration du (i) qui ne repose pas sur le théorème 4.18. Observons que si l'on a $d = -19, -43, -67, -163$ alors l'anneau $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ est principal mais non euclidien, d'après le théorème 4.11 (Samuel).

Le théorème 4.18 conclut ce chapitre sur une note un peu pessimiste : il n'y a en particulier qu'un nombre fini d'entiers quadratiques imaginaires α tels que $\mathbb{Z}[\alpha]$ est un anneau factoriel. Cependant, comme Dedekind et Kummer l'ont remarqué,

et comme nous le verrons ultérieurement, tous ceux d'entre eux qui sont intégralement clos (classifiés par la proposition 4.17) possèdent la propriété de factorisation unique de leurs idéaux en produit d'idéaux premiers. Comme on le verra aussi, cette propriété sera souvent suffisante pour les applications arithmétiques !

REMARQUE 4.20. (D'après le livre de Stewart et Tall, chapitre 4) La détermination des entiers $d > 0$ et $\alpha = \sqrt{d}$ ou $\frac{1+\sqrt{d}}{2}$ et $d \equiv 1 \bmod 4$ tels que $\mathbb{Z}[\alpha]$ est euclidien est en fait un problème ouvert. Par exemple, il n'est pas difficile de vérifier que $\mathbb{Z}[\sqrt{2}]$ est euclidien pour la valeur absolue de la norme de $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. Un résultat plus profond est que les seuls autres α tels que $\mathbb{Z}[\alpha]$ est euclidien pour la norme sont $\alpha = \sqrt{3}, \sqrt{6}$ et les $\alpha = \frac{1+\sqrt{d}}{2}$ avec

$$d = 5, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 55, 73$$

(Chatland-Davenport, Inkeri). Il semble que l'on ne connaisse pas d'exemple de $\mathbb{Z}[\alpha]$ qui soit euclidien et mais pour lequel la valeur absolue de la norme de $\mathbb{Q}(\alpha)/\mathbb{Q}$ ne soit pas un stathme euclidien, un candidat selon Samuel est $\mathbb{Z}[\sqrt{14}]$ (qui est principal).

5. Exercices

Les quatre premiers exercices concernent l'arithmétique de l'anneau $\mathbb{Z}[i]$ avec $i^2 = -1$ (anneau des "entiers de Gauss"). On rappelle que cet anneau est euclidien.

EXERCICE 4.1. (Irréductibles de $\mathbb{Z}[i]$)

(i) Montrer que $1 + i$ est irréductible dans $\mathbb{Z}[i]$ et que $2 = -i(1 + i)^2$.

(ii) Montrer que si $p \equiv 1 \bmod 4$ est un nombre premier, alors $p = \pi\overline{\pi}$ où π et son conjugué complexe $\overline{\pi}$ sont des irréductibles non associés de $\mathbb{Z}[i]$.

(iii) Montrer que si $p \equiv 3 \bmod 4$ est un nombre premier, alors p est irréductible dans $\mathbb{Z}[i]$.

(iv) Montrer que si π est un irréductible de $\mathbb{Z}[i]$ alors $\pi\mathbb{Z}[i] \cap \mathbb{Z}$ est un idéal de $\mathbb{Z}$ engendré par un nombre premier. En déduire que si π est un irréductible de $\mathbb{Z}[i]$ alors π divise un et un seul nombre premier usuel.

(v) En déduire une classification des irréductibles de $\mathbb{Z}[i]$.

EXERCICE 4.2. *Montrer que si $p \equiv 1 \bmod 4$ est un nombre premier, il existe exactement 8 couples $(a, b) \in \mathbb{Z}^2$ tels que $p = a^2 + b^2$.*

EXERCICE 4.3. *Factoriser $-3 + 15i$ en irréductibles dans $\mathbb{Z}[i]$.*

EXERCICE 4.4. (Un choix de représentants des irréductibles)

(i) Montrer que l'idéal $(2(1 + i))$ de $\mathbb{Z}[i]$ admet pour $\mathbb{Z}$-base $4, 2(1 + i)$.

(ii) En déduire un isomorphisme de groupes abéliens $\mathbb{Z}[i]/2(1+i)\mathbb{Z}[i] = \mathbb{Z}/4\mathbb{Z}\cdot\overline{1} \oplus \mathbb{Z}/2\mathbb{Z}\cdot\overline{1+i}$. À quelle condition sur $a, b \in \mathbb{Z}$ est-ce que $a+bi \equiv 3 \bmod 2(1+i)$?

(iii) Montrer qu'un ensemble de représentants des irréductibles de $\mathbb{Z}[i]$ est donné par $1 + i$ et l'ensemble des irréductibles de $\mathbb{Z}[i]$ congrus à 3 modulo $2(1 + i)$.

EXERCICE 4.5. *Soit p un nombre premier et soit $\alpha = \sqrt{-p}$.*

(i) Montrer que $\alpha\,\mathbb{Z}[\alpha] = \{a + b\alpha \mid a, b \in \mathbb{Z}, a \equiv 0 \bmod p\}$.

(ii) En déduire que α est un élément premier de $\mathbb{Z}[\alpha]$.

EXERCICE 4.6. Soient d un entier < 0 et $A = \mathbb{Z}[\sqrt{d}]$. On se propose de démontrer que si l'anneau A est principal alors on a $d = -1$ ou -2. *Soient $a, b \in \mathbb{Z}$ avec $a > 0$; on note $\mathrm{I}_{a,b}$ le sous-groupe $a\mathbb{Z} + (b + \sqrt{d})\mathbb{Z} \subset A$.*

(i) Montrer que $\mathrm{I}_{a,b}$ est un idéal de A si, et seulement si, a divise $b^2 - d$.

(ii) Montrer $|A/\mathrm{I}_{a,b}| = a$.

(iii) Montrer que si I est un idéal principal de A, alors $|A/I|$ est soit $\geq |d|$, soit un carré.

(iv) Conclure.

Dans l'esprit de l'exercice précédent, le lecteur pourra essayer de démontrer que si $d \equiv 1 \bmod 4$ et si $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ est principal, alors d est un nombre premier. Pour cela, on pourra considérer un facteur premier minimal p de d et observer que l'idéal de $\mathbb{Z}[\alpha]$ engendré par p et $\frac{p+\sqrt{d}}{2}$ est de norme p.

EXERCICE 4.7. *(Points entiers d'une certaine courbe elliptique) On se propose de montrer que les $x, y \in \mathbb{Z}$ tels que $y^2 + y = x^3 - 2$ sont exactement $(x, y) = (2, 2)$ ou $(2, -3)$.*

(i) Montrer que $\sqrt{-7}$ est premier dans $\mathbb{Z}[\alpha]$ où $\alpha = \frac{1+\sqrt{-7}}{2}$.

(ii) Montrer que si $y^2 + y = x^3 - 2$ alors $y + \alpha$ n'est pas divisible par $\sqrt{-7}$ dans $\mathbb{Z}[\alpha]$.

(iii) Conclure.

On peut démontrer qu'il y a une infinité de $x, y \in \mathbb{Q}$ tels que $y^2 + y = x^3 - 2$. Par exemple, en considérant la tangente à la courbe $y^2 + y = x^3 - 2$ au point $(2, 2)$ on constate que l'autre point d'intersection, à savoir $(x, y) = (\frac{44}{25}, \frac{178}{125})$, est aussi solution ! On peut itérer ce procédé et les solutions deviennent vite gigantesques, par exemple au deuxième coup on obtient la solution

$$\left(\frac{13373096}{5784025}, \frac{38354841394}{13910580125}\right).$$

EXERCICE 4.8. *(i) Trouver toutes les solutions $x, y \in \mathbb{Z}$ de $y^2 + y = x^3 - k$ sous l'hypothèse que $p = 4k - 1$ est un nombre premier > 3 et que $\mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$ est factoriel.*

(ii) (difficile) Étudier le cas $k = 1$ (attention aux unités de $\mathbb{Z}[j]$).

Dans ce qui suit, A désignera un anneau commutatif unitaire intègre, sauf mention du contraire.

EXERCICE 4.9. (Pgcd et ppcm : quelques généralités) *Soient $a, b \in A$ non nuls.*

(i) Montrer que l'idéal $(a) \cap (b)$ est principal engendré par $m \in A$ si, et seulement si, m est un ppcm de a et b.

(ii) On suppose a premier et que a ne divise pas b, montrer que ab est un ppcm de a et b.

(iii) On suppose que $(a) + (b) = (d)$. Montrer que d est un pgcd de a et b.

(iv) On suppose a irréductible et que a ne divise pas b. Montrer que 1 est un pgcd de a et b.

EXERCICE 4.10. (Pgcd et ppcm : exemples et contre-exemples dans l'anneau non factoriel $\mathbb{Z}[\sqrt{-5}]$).

(i) Montrer que $\sqrt{-5}$ et $1 + \sqrt{-5}$ admettent un ppcm et un pgcd.

(ii) Montrer que 2 et $1 + \sqrt{-5}$ n'admettent pas de ppcm. On pourra remarquer qu'un tel ppcm m satisferait $12 \,|\, \mathrm{N}(m)$, puis qu'il serait associé à $2 + 2\sqrt{-5}$.

(iii) Montrer que $3(1+\sqrt{-5})$ et $3(1-\sqrt{-5}) = (1+\sqrt{-5})(-2-\sqrt{-5})$ n'admettent pas de pgcd.

Soit I l'idéal $(2, 1 + \sqrt{-5})$ de $\mathbb{Z}[\sqrt{-5}]$.

(iv) Montrer que I admet pour $\mathbb{Z}$-base $2, 1 + \sqrt{-5}$.

(v) En déduire que $\mathrm{N}(I) = 2$, puis que I n'est pas principal.

(vi) En déduire que la réciproque du (iii) de l'exercice précédent est fausse.

(vii) Montrer que $(2) \cap (1 + \sqrt{-5}) = (1 + \sqrt{-5}) \cdot I$.

EXERCICE 4.11. *Soient A un anneau intègre et $\varphi : A\backslash\{0\} \to \mathbb{N}$ un stathme euclidien. On dit que φ est* fort *si $\forall a, b \in A$, "$a \neq 0$ et b divise a" entraîne "$\varphi(b) \leq \varphi(a)$". Si I est un idéal non nul de A, on pose $\mathrm{m}_\varphi(I) = \mathrm{Min}\{\varphi(a), a \in I - \{0\}\}$ (justifier).*

(i) Vérifier que les stathmes euclidiens rencontrés jusque-là sont forts.

(ii) On suppose φ fort. Soient $I \neq 0$ un idéal de A et $x \in I - \{0\}$. Montrer que l'on a $I = Ax$ si, et seulement si, $\varphi(x) = \mathrm{m}_\varphi(I)$.

(iii) Montrer que tout anneau euclidien admet un stathme euclidien fort (Motzkin). *Un stathme euclidien φ étant donné, on pourra considérer $a \mapsto \mathrm{m}_\varphi(aA)$.*

EXERCICE 4.12. (Lemme du contenu de Gauss) *Soit A un anneau factoriel de corps de fractions K. Si $P \in A[X]$ est non nul, on note $\mathrm{c}(P)$ le pgcd des coefficients de P, c'est un élément de A bien défini aux unités près. On dit que P est primitif si $\mathrm{c}(P)$ est une unité.*

(i) Montrer que $A[X]^\times = A^\times$.

(ii) Montrer que si $P, Q \in A[X]$ sont primitifs alors PQ est primitif.

(iii) En déduire que si $P, Q \in A[X]$ sont non nuls, alors $\mathrm{c}(PQ) = \mathrm{c}(P)\mathrm{c}(Q)$ (aux unités près).

(iv) Montrer que si $P \in A[X]$ est non constant, alors P est irréductible dans $A[X]$ si, et seulement si, $\mathrm{c}(P) = 1$ et P est irréductible dans $K[X]$.

(v) En déduire que les irréductibles de $A[X]$ sont les irréductibles de A et les polynômes primitifs non constants qui sont irréductibles dans $K[X]$.

(vi) Montrer que $A[X]$ est factoriel.

(vii) En déduire que $\mathbb{Z}[X_1, \ldots, X_n]$ et $k[X_1, \ldots, X_n]$ sont factoriels si $n \geq 1$ et si k est un corps.

(viii) Vérifier que $\mathbb{Z}[X]$ n'est pas principal (bien que factoriel par le (vii)).

EXERCICE 4.13. *Soit A l'anneau des fonctions holomorphes sur $\mathbb{C}$ tout entier.*

(i) Montrer que A est intègre.

(ii) Montrer que les unités de A sont les fonctions holomorphes sur $\mathbb{C}$ qui ne s'annulent pas, et que les irréductibles de A sont, aux unités près, les $z - a$ avec $a \in \mathbb{C}$.

(iii) En déduire que A n'a pas la propriété de factorisation (en particulier, A n'est pas noethérien).

Chapitre 5

L'anneau des entiers d'un corps de nombres

Ce chapitre a pour but d'introduire l'anneau $\mathcal{O}_K$ des entiers algébriques d'un corps de nombres K, tel qu'il a été défini en toute généralité en 1877 par Richard Dedekind, le dernier élève de Gauss, dans son livre "*Sur la théorie des nombres entiers algébriques*" (en français !). Cette définition englobe notamment les anneaux introduits par Gauss et Eisenstein dans leurs études des *lois de réciprocité supérieures*, à savoir $\mathbb{Z}[i]$ et $\mathbb{Z}[\frac{1+i\sqrt{3}}{2}]$, et plus généralement celui des entiers cyclotomiques $\mathbb{Z}[e^{\frac{2i\pi}{n}}]$, étudié en détail par Kummer dans ses travaux sur le grand théorème de Fermat. Elle contient aussi certains anneaux d'entiers quadratiques étudiés au chapitre précédent, ce qui a par exemple permis à Dedekind de découvrir un point de vue plus simple sur la loi de Gauss de composition des formes binaires, que nous exposerons par ailleurs plus tard.

Nous commençons par développer les outils fondamentaux nécessaires à l'étude des nombres algébriques, à savoir les notions de trace, norme et discriminant. Cela nous obligera à commencer par quelques rappels de théorie des extensions de corps et de leurs plongements, avec lesquels nous supposerons une certaine familiarité, bien que les démonstrations ici soient complètes. Le résultat central de ce chapitre est un théorème de structure du groupe additif de $\mathcal{O}_K$. L'étude arithmétique de ce dernier fera l'objet des chapitres suivants.

Références : Nous renvoyons par exemple au livre *Algebra* de Serge Lang pour les rudiments de théorie des corps. En ce qui concerne les entiers des corps de nombres, on pourra consulter le chapitre 12 du livre de Ireland et Rosen, le chapitre 2 du livre de Samuel, ou le livre sus-cité de Dedekind !

1. Les corps de nombres et leurs plongements

Si L est un corps et si $K \subset L$ en est un sous-corps, l'addition de L et l'application $K \times L \to L$ induite par la multiplication de L définissent une structure de K-espace vectoriel sur L. En particulier, tout sous-corps L de $\mathbb{C}$ admet ainsi une structure naturelle de $\mathbb{Q}$-espace vectoriel : $1 \in L$ par définition, et donc $\mathbb{Q} \subset L$.

Définition 5.1. *Un corps de nombres est un sous-corps de $\mathbb{C}$ qui est de dimension finie comme $\mathbb{Q}$-espace vectoriel.*

Une *extension L/K de corps de nombres* est la donnée de deux corps de nombres L et K tels que $K \subset L$. Toute famille génératrice de L comme $\mathbb{Q}$-espace vectoriel en est encore une comme K-espace vectoriel, et donc L est alors de dimension finie comme K-espace vectoriel. On note $[L : K]$ cette dimension, que l'on appelle *degré de L sur K*. Lorsque $K = \mathbb{Q}$ on parle simplement du degré $[L : \mathbb{Q}]$ du corps de nombres L. Évidemment, $[L : \mathbb{Q}] = 1$ si, et seulement si, $L = \mathbb{Q}$, qui est le plus simple des corps de nombres. De même, $[L : K] = 1$ si, et seulement si, $L = K$.

On rappelle que $x \in \mathbb{C}$ est *algébrique* s'il existe un polynôme non nul $P \in \mathbb{Q}[X]$ tel que $P(x) = 0$. On note $\overline{\mathbb{Q}} \subset \mathbb{C}$ l'ensemble des nombres algébriques. Si K est un corps de nombres de degré n, et si $x \in K$, la famille $1, x, \ldots, x^n$ a $n+1$ éléments : elle est donc $\mathbb{Q}$-liée et $x \in \overline{\mathbb{Q}}$. Autrement dit :

PROPOSITION 5.2. *Tout corps de nombres est inclus dans* $\overline{\mathbb{Q}}$.

Si $x \in \mathbb{C}$ et si K est un sous-corps de $\mathbb{C}$, on note $K[x] = \{P(x), P \in K[X]\}$ la sous-K-algèbre de $\mathbb{C}$ engendrée par x.

PROPOSITION-DÉFINITION 5.3. *Si K est un corps de nombres et si $x \in \overline{\mathbb{Q}}$, alors $K[x]$ est un corps de nombres, que l'on notera aussi $K(x)$.*

Une manière de voir ceci est de considérer l'ensemble $I_{x,K} = \{P \in K[X], P(x) = 0\}$ des polynômes annulateurs de x à coefficients dans K. C'est clairement un idéal de $K[X]$, donc principal, qui est non nul car $x \in \overline{\mathbb{Q}}$: il est donc engendré par un unique polynôme unitaire

$$\Pi_{x,K} \in K[X].$$

Par définition, c'est le polynôme annulateur de x unitaire, de degré minimal, à coefficients dans K, et il est appelé *polynôme minimal de x sur K*. En particulier, il est irréductible dans $K[X]$. Le morphisme surjectif d'anneaux $K[X] \to K[x]$, $P \mapsto P(x)$, a pour noyau $I_{x,K} = (\Pi_{x,K})$, et induit donc un isomorphisme d'anneaux

$$K[X]/(\Pi_{x,K}) \xrightarrow{\sim} K[x].$$

On en déduit d'une part que si $n = \deg(\Pi_{x,K})$ alors $1, x, \ldots, x^{n-1}$ est une K-base de $K[x]$ ("division euclidienne et unicité du reste dans $K[X]$"). On en déduit aussi que $K[x]$ est un corps. En effet, tout élément non nul de $K[X]/(\Pi_{x,K})$ est représenté par un polynôme $P \in K[X]$ non nul tel que $\deg(P) < n$. Comme $\Pi_{x,K}$ est irréductible, il est premier avec P, et donc il existe $U, V \in K[X]$ tels que $PU + \Pi_x V = 1$ (Bézout dans $K[X]$), et donc $PU \equiv 1 \bmod \Pi_{x,K}$: P est inversible dans $K[X]/(\Pi_{x,K})$. □

Le cas le plus important de cette définition est celui où $K = \mathbb{Q}$. Nous verrons en fait plus loin que tout corps de nombres K est de la forme $\mathbb{Q}(x)$ pour (une infinité de) $x \in K$ (théorème de l'élément primitif).

EXEMPLE 5.4. (Corps quadratiques et cyclotomiques) Parmi les exemples historiquement importants de corps de nombres, mentionnons les *corps cyclotomiques*, qui sont les $\mathbb{Q}(\zeta)$ où ζ est une racine de l'unité, ainsi que les *corps quadratiques*, de la forme $\mathbb{Q}(\sqrt{d})$ où $d \in \mathbb{Q}$ n'est pas un carré.

Si K est un corps de nombres et si $x_1, \ldots, x_n \in \overline{\mathbb{Q}}$, on note aussi $K(x_1, \ldots, x_n)$ le corps de nombres défini récursivement comme étant $(K(x_1, \ldots, x_{n-1}))(x_n)$. C'est le plus petit corps de nombres contenant K et les x_i, il ne dépend en particulier pas de l'ordre des x_i. En particulier, si $x, y \in \overline{\mathbb{Q}}$ alors $\mathbb{Q}(x, y)$ est un corps de nombres. Comme xy et $x - y \in \mathbb{Q}(x, y)$, on en déduit le fait bien connu suivant, qui se déduirait aussi très simplement de la proposition 1.15 :

COROLLAIRE 5.5. $\overline{\mathbb{Q}}$ *est un sous-corps de* $\mathbb{C}$.

La proposition suivante, dite "de la base télescopique", est bien connue.

PROPOSITION 5.6. *Si $K \subset L \subset M$ sont des corps de nombres alors $[M : K] = [M : L][L : K]$.*

DÉMONSTRATION — On vérifie immédiatement que si $e_1, \ldots, e_n$ est une base du L-espace vectoriel M, et si $f_1, \ldots, f_m$ est une base du K-espace vectoriel L, alors les éléments $e_i f_j$, avec $1 \leq i \leq n$ et $1 \leq j \leq m$, forment une base du K-espace vectoriel M. □

DÉFINITION 5.7. *Si K est un corps de nombres on note $\Sigma(K)$ l'ensemble des morphismes de corps $K \to \mathbb{C}$, appelés aussi plongements, ou plongements complexes, de K.*

Si L/K est une extension de corps de nombres, on note $\Sigma(L/K)$ l'ensemble des plongements K-linéaires $L \to \mathbb{C}$. Autrement dit, $\Sigma(L/K) = \{\sigma \in \Sigma(L), \sigma_{|K} = \mathrm{id}\}$. En particulier, $\Sigma(L/\mathbb{Q}) = \Sigma(L)$.

La notion de plongement est une vaste généralisation de la notion de conjugaison complexe, ingrédient crucial dans la théorie de Galois. Elle est étroitement liée à celle de conjugué d'un nombre algébrique. On rappelle que si $x \in \overline{\mathbb{Q}}$ et si K est un corps de nombres, les K-conjugués de x sont les racines dans $\mathbb{C}$ du polynôme $\Pi_{x,K}$. Le lemme suivant montre qu'il y en a exactement $\deg(\Pi_{x,K})$.

LEMME 5.8. *Si $K \subset \mathbb{C}$ est un sous-corps et si $P \in K[X]$ est irréductible (donc non constant) alors P est scindé à racines simples dans $\mathbb{C}[X]$.*

DÉMONSTRATION — En effet, P est scindé car $\mathbb{C}$ est algébriquement clos. D'autre part, $P' \in K[X]$ est un polynôme non nul de degré $< \deg(P)$, et donc premier à P dans $K[X]$, de sorte que P et P' n'ont pas de racine commune dans $\mathbb{C}$ (relation de Bézout). □

Les propriétés principales des plongements se résument en la proposition qui suit.

PROPOSITION 5.9. *(i) (Lemme de prolongement) Soient $K \subset L$ des corps de nombres. L'application de restriction $\Sigma(L) \to \Sigma(K)$, $\sigma \mapsto \sigma_{|L}$, est surjective, chaque élément de $\Sigma(K)$ ayant exactement $[L : K]$ antécédents. En particulier $|\Sigma(L/K)| = [L : K]$.*

(ii) (Conjugués et plongements) Soit $x \in \overline{\mathbb{Q}}$, l'application $\Sigma(K(x)/K) \to \mathbb{C}$, $\sigma \mapsto \sigma(x)$, induit une injection d'image l'ensemble des K-conjugués de x.

DÉMONSTRATION — Vérifions d'abord le (i) quand L est de la forme $K(x)$, où $x \in \overline{\mathbb{Q}}$. Fixons $\tau \in \Sigma(K)$. L'isomorphisme d'anneaux naturel $K[X]/(\Pi_{x,K}) \xrightarrow{\sim} K(x)$ entraîne que l'application

$$T = \{\sigma \in \Sigma(K(x)), \sigma_{|K} = \tau\} \longrightarrow \mathbb{C}, \sigma \mapsto \sigma(x),$$

est une injection, d'image l'ensemble des $y \in \mathbb{C}$ tels que $\Pi_{x,K}^{\tau}(y) = 0$. Rappelons que la notation Q^{τ}, pour $Q \in K[X]$ et $\tau \in \Sigma(K)$, désigne le polynôme Q auquel on a appliqué τ à tous les coefficients, en particulier $Q^{\tau} \in \tau(K)[X]$. On vérifie immédiatement que

$$(PQ)^{\tau} = P^{\tau} Q^{\tau} \quad \text{si} \quad P, Q \in K[X].$$

En particulier, $\Pi^{\tau}_{x,K}$ est irréductible dans $\tau(K)[X]$, car $\Pi_{x,K}$ l'est dans $K[X]$. Il a donc exactement $[K(x) : K]$ racines distinctes dans $\mathbb{C}$ par le lemme 5.8, et donc $|T| = [K(x) : K]$. Notons que le (ii) en découle : c'est le cas où τ est l'identité. Pour le cas général du (i), on se ramène au cas $L = K(x)$ par induction en écrivant $L = K(x_1, \ldots, x_r)$, l'assertion sur le nombre d'antécédents résultant de la base télescopique. □

COROLLAIRE 5.10. (Théorème de l'élément primitif) *Tout corps de nombres est de la forme $\mathbb{Q}(x)$ pour un $x \in \overline{\mathbb{Q}}$.*

DÉMONSTRATION — En effet, si K est un corps de nombres et si $L \subset K$ en est un sous-corps, le plongement $\mathrm{id} \in \Sigma(L)$ se prolonge à K de $[K : L]$-manières différentes d'après le lemme 5.9 (i). Si $L \neq K$ alors $[K : L] \geq 2$, et on peut donc trouver un tel prolongement $\sigma \in \Sigma(K)\backslash\{\mathrm{id}\}$. En particulier, le sous-$\mathbb{Q}$-espace vectoriel strict $H_\sigma = \{x \in K, \sigma(x) = x\}$ contient L. Mais comme $\mathbb{Q}$ est infini, la réunion finie des H_σ avec $\sigma \in \Sigma(K)\backslash\{\mathrm{id}\}$ n'est pas K tout entier : n'importe quel élément hors de cette réunion est donc primitif. Mieux, les H_σ introduits ci-dessus sont clairement des sous-corps stricts de K, de sorte que

$$K \setminus \bigcup_{\sigma \in \Sigma(K)\backslash\{\mathrm{id}\}} H_\sigma$$

est exactement l'ensemble des éléments primitifs de K. □

2. Trace, norme et discriminant : préliminaires algébriques

Dans tout ce paragraphe, on fixe L/K une extension de corps de nombres. Le lecteur ne perdrait pas grand chose à supposer $K = \mathbb{Q}$, mais cela ne simplifierait aucun des arguments qui vont suivre.

Si $x \in L$, considérons l'application de multiplication par x :

$$m_x : L \to L, y \mapsto xy.$$

C'est une application K-linéaire, autrement dit c'est un endomorphisme du K-espace vectoriel L. On note $\chi_{x,L/K} \in K[X]$ son polynôme caractéristique, $\mathrm{Tr}_{L/K}(x)$ sa trace, et $\mathrm{N}_{L/K}(x)$ son déterminant. Notons que ces deux derniers éléments sont dans K.

PROPOSITION-DÉFINITION 5.11. *L'application $\mathrm{Tr}_{L/K} : L \to K$ ainsi définie est K-linéaire, on l'appelle la trace de L/K. De même, l'application $\mathrm{N}_{L/K} : L \to K$ est multiplicative : $\mathrm{N}_{L/K}(xy) = \mathrm{N}_{L/K}(x)\mathrm{N}_{L/K}(y)$ pour tout $x, y \in L$, on l'appelle la norme de L/K.*

DÉMONSTRATION — En effet, la première assertion découle de la linéarité de la trace et de ce que pour tout $x, y \in L$ et $\lambda \in K$, on a l'identité $m_{\lambda x+y} = \lambda m_x + m_y$ dans les endomorphismes du K-espace vectoriel L. De même, la seconde assertion découle de la multiplicativité du déterminant et de l'identité, pour tout $x, y \in L$, $m_{xy} = m_x \cdot m_y$ dans les endomorphismes du K-espace vectoriel L. □

EXEMPLE 5.12. Considérons par exemple le cas du corps quadratique $L = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Q}$ non carré, et $K = \mathbb{Q}$. Alors $1, \sqrt{d}$ est une $\mathbb{Q}$-base de $\mathbb{Q}(\sqrt{d})$. La matrice de la multiplication par $x = a + b\sqrt{d}$ avec $a, b \in \mathbb{Q}$ dans cette base est visiblement

$$\begin{pmatrix} a & db \\ b & a \end{pmatrix}$$

et donc $\mathrm{Tr}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(x) = 2a$ et $\mathrm{N}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(x) = a^2 - db^2$. Remarquons que la multiplicativité de la norme explique notamment l'identité remarquable $(a^2 - db^2)(\alpha^2 - d\beta^2) = (a\alpha + b\beta d)^2 - d(a\beta + \alpha b)^2$ pour tout $a, b, \alpha, \beta \in \mathbb{Q}$, car $(a + b\sqrt{d})(\alpha + \beta\sqrt{d}) = (a\alpha + b\beta d) + (a\beta + b\alpha)\sqrt{d}$.

Le théorème de Cayley-Hamilton assure que $\chi_{L/K}(m_x) = 0$ dans $\mathrm{End}_K(L)$, ce qui revient en fait au même que $\chi_{x,L/K}(x) = 0$: le polynôme $\chi_{x,L/K}$ est un polynôme annulateur de x dans $K[X]$. Cela fournit notamment un algorithme simple pour trouver un polynôme annulateur d'un élément $x \in L$ si l'on connaît une K-base de L et la décomposition de x dans cette base : on calcule le polynôme caractéristique de m_x. La relation entre $\chi_{x,L/K}$ et $\Pi_{x,K}$ est donnée par la proposition suivante :

PROPOSITION 5.13. *Si $x \in L$ alors $\chi_{x,L/K} = \Pi_{x,K}^r$ où $r = [L : K(x)]$.*

DÉMONSTRATION — Soient $n = [K(x) : K]$, $r = [L : K(x)]$, et $e_1, \ldots, e_r$ une base de L comme $K(x)$-espace vectoriel. Par la base télescopique, les éléments

$$e_1, xe_1, \ldots, x^{n-1}e_1, e_2, xe_2, \ldots, x^{n-1}e_2, \ldots, e_r, xe_r, \ldots, x^{n-1}e_r$$

forment une K-base de L. Mais pour chaque $1 \leq i \leq r$, la multiplication par x préserve le sous-espace $\oplus_{k=0}^{n-1} Ke_i x^k$. Sa matrice dans la base $e_i, xe_i, \ldots, x^{n-1}e_i$ est visiblement

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \ddots & \vdots & -a_1 \\ 0 & 1 & \ddots & 0 & -a_2 \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & -a_{n-1} \end{pmatrix},$$

où $\Pi_{x,K} = X^n + \sum_{i=0}^{n-1} a_i X^i$ (c'est la matrice compagnon de $\Pi_{x,K}$). Un développement par rapport à la dernière colonne montre que le polynôme caractéristique d'une telle matrice est exactement $X^n + \sum_{i=0}^{n-1} a_i X^i$, ce qui conclut. □

PROPOSITION 5.14. *Soient L/K une extension de corps de nombres et $x \in L$.*

(i) $\mathrm{Tr}_{L/K}(x) = \sum_{\sigma \in \Sigma(L/K)} \sigma(x)$.

(ii) $\mathrm{N}_{L/K}(x) = \prod_{\sigma \in \Sigma(L/K)} \sigma(x)$.

(iii) $\chi_{x,L/K} = \prod_{\sigma \in \Sigma(L/K)} (X - \sigma(x))$ *dans* $\mathbb{C}[X]$.

DÉMONSTRATION — Les relations (i) et (ii) se déduisent de la troisième, sur laquelle nous nous concentrons donc. Partons du fait que

$$\Pi_{x,K} = \prod_{\sigma \in \Sigma(K(x)/K)} (X - \sigma(x))$$

d'après la proposition 5.9 (ii). Mais pour tout $\sigma \in \Sigma(K(x)/K)$ il existe exactement $[L : K(x)]$ éléments $\sigma' \in \Sigma(L/K)$ tels que $\sigma'(x) = \sigma(x)$, d'après la proposition 5.9 (i) et (ii). On en déduit

$$\prod_{\sigma \in \Sigma(L/K)} (X - \sigma(x)) = \Pi_{x,K}^{[L:K(x)]} = \chi_{x,L/K},$$

la dernière égalité venant de la proposition 5.13. □

EXEMPLE 5.15. Continuons l'exemple de $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ avec $d \in \mathbb{Q}$ non carré. On a $\Sigma(\mathbb{Q}(\sqrt{d})) = \{\mathrm{id}, a + b\sqrt{d} \mapsto a - b\sqrt{d}\}$. On retrouve bien que $\mathrm{Tr}_{K/\mathbb{Q}}(a + b\sqrt{d}) = 2a$ et $\mathrm{N}_{K/\mathbb{Q}}(a + b\sqrt{d}) = a^2 - db^2$.

La forme K-linéaire trace $\mathrm{Tr}_{L/K} : L \to K$ nous permet de considérer l'application

$$L \times L \to K, (x, y) \mapsto \mathrm{Tr}_{L/K}(xy),$$

qui est donc K-bilinéaire et symétrique. Elle est même non dégénérée : pour tout $x \in L$ non nul, il existe $y \in L$ tel que $\mathrm{Tr}_{L/K}(xy) = 1$. En effet, il suffit de considérer l'élément $y = \frac{1}{[L:K]x} \in L$.

Soit $n = [L : K]$ et soit $e_1, \ldots, e_n$ une famille d'éléments de L. Si $x_1, \ldots, x_n \in K$ on considère l'élement $x = \sum_{j=1}^n x_j e_j$. En multipliant par e_i pour tout i et en prenant la trace on obtient un système linéaire à coefficients dans K :

$$\left(\mathrm{Tr}_{L/K}(e_i e_j)\right)_{1 \le i,j,\le n} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \mathrm{Tr}_{L/K}(xe_1) \\ \mathrm{Tr}_{L/K}(xe_2) \\ \vdots \\ \mathrm{Tr}_{L/K}(xe_n) \end{pmatrix}. \tag{3}$$

Cela conduit à poser la définition suivante.

DÉFINITION 5.16. *Soit L/K une extension de corps de nombres de degré n. Le discriminant relatif à K d'une famille $e_1, \ldots, e_n$ d'éléments de L est le déterminant de la matrice*

$$(\mathrm{Tr}_{L/K}(e_i e_j))_{1 \le i,j,\le n} \in \mathrm{M}_n(K).$$

On le note $\mathrm{disc}_{L/K}(e_1, \ldots, e_n)$*, c'est un élément de K.*

On rappelle que si $P \in \mathbb{C}[X]$ est unitaire, le discriminant de P est traditionnellement le nombre complexe $\mathrm{disc}(P) = \prod_{i<j}(x_i - x_j)^2$ où $P = \prod_i (X - x_i)$.

PROPOSITION 5.17. *Soit L/K une extension de degré n et soit $e_1, \cdots, e_n \in L$.*

(i) $\mathrm{disc}_{L/K}(e_1, \ldots, e_n) \neq 0$ *si, et seulement si, $e_1, \ldots, e_n$ est une K-base de L.*

(ii) Si $P = (p_{i,j}) \in \mathrm{M}_n(K)$, et si l'on pose $f_j = \sum_i p_{i,j} e_i$ pour $j = 1, \cdots, n$, alors

$$\mathrm{disc}_{L/K}(f_1, \ldots, f_n) = \det(P)^2 \mathrm{disc}_{L/K}(e_1, \ldots, e_n).$$

(iii) $\mathrm{disc}_{L/K}(e_1, \ldots, e_n) = \det((\sigma_i(e_j))_{1 \le i,j \le n})^2$ *où* $\Sigma(L/K) = \{\sigma_1, \ldots, \sigma_n\}$.

(iv) Si $L = K(x)$, et si $x_1, \ldots, x_n \in \mathbb{C}$ sont les K-conjugués de x, alors

$$\mathrm{disc}_{K(x)/K}(1, x, x^2, \ldots, x^{n-1}) = \prod_{i<j}(x_i - x_j)^2 = (-1)^{\frac{n(n-1)}{2}} \mathrm{N}_{K(x)/K}(\Pi'_{x,K}(x)).$$

Démonstration — Vérifions le (i). Si les e_i sont K-liés il existe des $x_i \in K$ non tous nuls tels que $\sum_i x_i e_i = 0$, la relation (3) appliquée à $x = 0$ assure donc que $\mathrm{disc}_{L/K}(e_1, \ldots, e_n) = 0$. Réciproquement, soit ${}^t(x_1, \ldots, x_n)$ dans le noyau de la matrice $(\mathrm{Tr}_{L/K}(e_i e_j))_{1 \leq i,j, \leq n}$, et soit $x = \sum_i x_i e_i$. La relation (3) assure que $\mathrm{Tr}_{L/K}(x e_i) = 0$ pour tout i, et donc $e_1, \ldots, e_n$ n'est pas K-génératrice de L par non dégénéscence de $\mathrm{Tr}_{L/K}$.

Le (ii) est une propriété générale des formes bilinéaires : pour tout $x_i, y_j \in K$ on a la relation

$$\mathrm{Tr}_{L/K}((\sum_{i=1}^{n} x_i e_i)(\sum_{j=1}^{n} y_j e_j)) = {}^t \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} (\mathrm{Tr}_{L/K}(e_i e_j))_{1 \leq i,j, \leq n} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

Dans les notations de l'énoncé on a donc $(\mathrm{Tr}_{L/K}(f_i f_j))_{1 \leq i,j, \leq n} = {}^t P (\mathrm{Tr}_{L/K}(e_i e_j))_{1 \leq i,j, \leq n} P$, ce qui conclut en prenant le déterminant.

Pour le (iii), on rappelle que $\mathrm{Tr}_{L/K} = \sum_{k=1}^{n} \sigma_k$. On constate alors que

$$(\mathrm{Tr}(e_i e_j))_{1 \leq i,j \leq n} = {}^t(\sigma_i(e_j))(\sigma_i(e_j)),$$

ce qui implique conclut en prenant le déterminant. La première égalité du (iv) s'en déduit (déterminant de Vandermonde). La seconde découle de la proposition 5.14 (ii) appliquée à l'élément $\Pi'_{x,K}(x)$.

Observons enfin que (i) et (iv) donnent une nouvelle démonstration du lemme 5.8. □

La formule (iv) s'écrit donc encore $\mathrm{disc}_{K(x)/K}(1, x, x^2, \ldots, x^{n-1}) = \mathrm{disc}(\Pi_{x,K})$, ce qui explique un peu la terminologie employée ! On rappelle les formules classiques $\mathrm{disc}(X^2 + aX + b) = a^2 - 4b$, $\mathrm{disc}(X^3 + aX + b) = -4a^3 - 27b^2$, et plus généralement

$$\mathrm{disc}(X^n + aX + b) = (-1)^{\frac{n(n-1)}{2}} (n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1} a^n).$$

Les coefficients de $\mathrm{disc}(P)$ sont toujours des polynômes universels à coefficients entiers en les coefficients de P (pourquoi ?), cependant assez compliqués quand $\deg(P)$ grandit, par exemple :

$$\mathrm{disc}(X^3 + aX^2 + bX + c) = -4a^3 c + a^2 b^2 + 18abc - 4b^3 - 27c^2.$$

En pratique, P étant donné, on calcule son discriminant à l'aide de l'ordinateur !

3. Entiers d'un corps de nombres

Dans tout ce paragraphe K est un corps de nombres fixé.

Définition 5.18. *(Dedekind) L'anneau des entiers du corps de nombres K est l'anneau $\mathcal{O}_K = K \cap \overline{\mathbb{Z}}$.*

C'est bien un anneau, comme intersection de deux anneaux (Proposition 1.15). À bien des égards, l'anneau $\mathcal{O}_K$ est à K ce que $\mathbb{Z}$ est à $\mathbb{Q}$. Par exemple, la proposition 1.14 du chapitre 1 se traduit en

$$\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}.$$

On commence par observer que $\mathcal{O}_K$ est toujours "assez gros".

LEMME 5.19. *Pour tout $x \in K$, il existe un entier non nul $m \in \mathbb{Z}$ tel que $mx \in \mathcal{O}_K$. En particulier, $\mathcal{O}_K$ engendre K comme $\mathbb{Q}$-espace vectoriel.*

DÉMONSTRATION — En effet, soient $x \in K$ et $n = [\mathbb{Q}(x) : \mathbb{Q}]$. En nettoyant les dénominateurs de l'équation algébrique $\Pi_{x,\mathbb{Q}}(x) = 0$ on constate qu'il existe des entiers $a_0, a_1, \ldots, a_n \in \mathbb{Z}$ avec $a_n \neq 0$ tels que $\sum_{i=0}^{n} a_i x^i = 0$. En multipliant cette égalité par a_n^{n-1} on en déduit que $(a_n x)^n + \sum_{i=0}^{n-1} a_i a_n^{n-i} (a_n x)^i = 0$, et donc $m = a_n$ convient. □

Par construction, l'anneau $\mathcal{O}_K$ est intégralement clos.

PROPOSITION 5.20. *Pour tout corps de nombres K, l'anneau $\mathcal{O}_K$ est intégralement clos.*

DÉMONSTRATION — C'ést une conséquence de la définition $\mathcal{O}_K = K \cap \overline{\mathbb{Z}}$ et du fait que $\overline{\mathbb{Z}}$ est intégralement clos (Théorème 4.16). □

La détermination exacte de $\mathcal{O}_K$ est un problème difficile en général que nous allons maintenant aborder. Nous aurons besoin pour cela de critères simples caractérisant les entiers algébriques.

THÉORÈME 5.21. *(Critère d'intégralité) Soit $x \in K$, il y a équivalence entre :*

(i) $x \in \mathcal{O}_K$,

(ii) $\Pi_{x,\mathbb{Q}} \in \mathbb{Z}[X]$,

(iii) $\chi_{x,K/\mathbb{Q}} \in \mathbb{Z}[X]$.

En particulier, si $x \in \mathcal{O}_K$ alors $\mathrm{Tr}_{K/\mathbb{Q}}(x) \in \mathbb{Z}$ et $\mathrm{N}_{K/\mathbb{Q}}(x) \in \mathbb{Z}$.

DÉMONSTRATION — En effet, la dernière assertion découle de (i) ⇒ (iii). De plus, la relation $\chi_{x,K/\mathbb{Q}} = \Pi_{x,K/\mathbb{Q}}^{[K:\mathbb{Q}(x)]}$ assure que (ii) ⇒ (iii) ⇒ (i). Le point crucial, à savoir (i) ⇒ (ii), découle du lemme suivant. □

LEMME 5.22. *(i) Si x est dans $\mathcal{O}_K$ et si $\sigma \in \Sigma(K)$, alors $\sigma(x) \in \overline{\mathbb{Z}}$.*

(ii) Si L/K est une extension finie de corps de nombres, et si $x \in \mathcal{O}_L$, alors $\Pi_{x,L}$ et $\chi_{L/K}$ sont dans $\mathcal{O}_L[X]$. En particulier, $\mathrm{Tr}_{L/K}(x)$ et $\mathrm{N}_{L/K}(x)$ sont dans $\mathcal{O}_L$.

DÉMONSTRATION — Pour le (i), on constate que si $x \in \mathcal{O}_K$, il existe par définition $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}$ tels que $x^n + \sum_{i=0}^{n-1} a_i x^i = 0$. En appliquant un élément $\sigma \in \Sigma(K)$, on a $\sigma(x)^n + \sum_{i=0}^{n-1} a_i \sigma(x)^i = 0$, et donc $\sigma(x) \in \overline{\mathbb{Z}}$.

Pour le (ii), on rappelle que si $x \in L$ alors $\Pi_{x,K} = \prod_{\sigma \in \Sigma(K(x)/K)} (X - \sigma(x)) \in K[X]$. Mais si $x \in \mathcal{O}_L$ alors $\Pi_{x,K} \in \overline{\mathbb{Z}}[X]$ d'après le (i), et donc $\Pi_{x,K} \in \mathcal{O}_K[X]$. On conclut car $\chi_{x,L/K} = \Pi_{x,K}^{[L:K(x)]}$. □

Utilisons ce critère pour déterminer l'anneau des entiers des corps quadratiques, cas le plus simple après $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.

PROPOSITION 5.23. *Soient $d \in \mathbb{Z}\backslash\{0,1\}$ sans facteur carré et $K = \mathbb{Q}(\sqrt{d})$. Alors*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{d} & \text{si } d \equiv 2, 3 \bmod 4, \\ \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2} & \text{si } d \equiv 1 \bmod 4 \end{cases}$$

DÉMONSTRATION — Il est clair que $\sqrt{d} \in \mathcal{O}_K$ et on a déjà observé que $\alpha = \frac{1+\sqrt{d}}{2} \in \mathcal{O}_K$ si $d \equiv 1 \bmod 4$, car on a la relation $\alpha^2 - \alpha + \frac{1-d}{4} = 0$. Cela démontre les inclusions $\supset$ de l'énoncé. Observons aussi que $d \not\equiv 0 \bmod 4$ car d est sans facteur carré.

Réciproquement, soit $x = a + b\sqrt{d} \in \mathcal{O}_K$ avec $a, b \in \mathbb{Q}$. On a déjà vu que $\chi_{x,K/\mathbb{Q}} = T^2 - 2aT + (a^2 - db^2)$, i.e. $\mathrm{Tr}_{K/\mathbb{Q}}(x) = 2a$ et $\mathrm{N}_{K/\mathbb{Q}}(x) = a^2 - db^2$. Le théorème 5.21 entraîne donc que $2a, a^2 - db^2 \in \mathbb{Z}$. En particulier, $(2a)^2 - d(2b)^2 \in 4\mathbb{Z}$, donc $d(2b)^2 \in \mathbb{Z}$, puis $2b \in \mathbb{Z}$ car d est sans facteur carré. De même si $a \in \mathbb{Z}$ alors $b \in \mathbb{Z}$ et on a gagné. On peut donc supposer $2a$ impair. Dans ce cas, la relation $(2a)^2 \equiv d(2b)^2 \bmod 4$ entraîne que $2b$ est impair et que $d \equiv 1 \bmod 4$. Mézalors $x - \frac{1+\sqrt{d}}{2} = a' + b'\sqrt{d} \in \mathcal{O}_K$ avec $a' \in \mathbb{Z}$, et on conclut par le cas précédent. □

En particulier, on trouve que $\mathcal{O}_{\mathbb{Q}(i)}$ est l'anneau $\mathbb{Z}[i]$ des entiers de Gauss, et $\mathcal{O}_{\mathbb{Q}(j)}$, où $j = e^{2i\pi/3} = \frac{-1+i\sqrt{3}}{2}$, est celui des entiers d'Eisenstein $\mathbb{Z}[j]$. Nous sommes maintenant en mesure de terminer la démonstration de la proposition 4.17. En effet, elle découle du calcul précédent et de la proposition 5.20.

Si $\alpha \in \mathbb{C}$, on rappelle que l'on note $\mathbb{Z}[\alpha] = \{P(\alpha), P \in \mathbb{Z}[X]\}$. C'est le plus petit sous-anneau de $\mathbb{C}$ contenant α. Un sous-anneau $A \subset \mathbb{C}$ sera dit *monogène* si $A = \mathbb{Z}[\alpha]$ pour un certain $\alpha \in \mathbb{C}$. Nous verrons beaucoup d'exemples de corps de nombres K tels que $\mathcal{O}_K$ est monogène : c'est par exemple le cas des corps quadratiques comme on vient de le voir. Il ne faut pas croire cependant que c'est un phénomène général. Par exemple, nous verrons dans l'exercice 5.9 que si $d, d' \in \mathbb{Z}\backslash\{0,1\}$ sont distincts, sans facteur carré, tous deux $\equiv 1 \bmod 8$, et si $K = \mathbb{Q}(\sqrt{d}, \sqrt{d'})$ $(= \mathbb{Q}(\sqrt{d} + \sqrt{d'}))$, alors $\mathcal{O}_K$ n'est pas monogène.

Une propriété importante des sous-anneaux monogènes de $\overline{\mathbb{Z}}$ est la suivante.

COROLLAIRE 5.24. *Si $\alpha \in \overline{\mathbb{Z}}$ alors le morphisme d'anneaux $\mathbb{Z}[X] \to \mathbb{Z}[\alpha]$, $P \mapsto P(\alpha)$, induit un isomorphisme d'anneaux*

$$\mathbb{Z}[X]/(\Pi_{x,\mathbb{Q}}) \xrightarrow{\sim} \mathbb{Z}[\alpha].$$

En particulier, $1, x, \ldots, x^{n-1}$ est une $\mathbb{Z}$-base de $\mathbb{Z}[\alpha]$ où $n = [\mathbb{Q}(x) : \mathbb{Q}]$.

DÉMONSTRATION — L'application de l'énoncé est clairement un morphisme surjectif d'anneaux, de noyau $I = \{P \in \mathbb{Z}[X], P(\alpha) = 0\}$. La proposition précédente entraîne $\Pi_{x,\mathbb{Q}} \in I$, donc $(\Pi_{x,\mathbb{Q}}) \subset I$. Réciproquement, si $P \in I$ alors $P = \Pi_{x,\mathbb{Q}} Q$ où $Q \in \mathbb{Q}[X]$ par la propriété du polynôme minimal de x. Mais la division euclidienne d'un polynôme de $\mathbb{Z}[X]$ par un polynôme *unitaire* dans $\mathbb{Z}[X]$ a toujours un reste et un quotient dans $\mathbb{Z}[X]$, et donc $Q \in \mathbb{Z}[X]$, par unicité de la division euclidienne dans $\mathbb{Q}[X]$, ce qu'il fallait démontrer. Le dernier point découle encore de l'existence et unicité du reste et du quotient de la division euclidienne d'un $P \in \mathbb{Z}[X]$ par un $Q \in \mathbb{Z}[X]$ unitaire. □

4. Structure additive de $\mathcal{O}_K$ et discriminant de K

Soit K un corps de nombres.

THÉORÈME 5.25. *(Dedekind) Le groupe additif de $\mathcal{O}_K$ admet une $\mathbb{Z}$-base à $n = [K : \mathbb{Q}]$ éléments. En particulier, il existe $e_1, \dots, e_n \in \mathcal{O}_K$ tels que $\mathcal{O}_K = \sum_{i=1}^n \mathbb{Z}e_i$.*

Autrement dit, $\mathcal{O}_K \simeq \mathbb{Z}^n$ comme groupe abélien. Si $\mathcal{O}_K$ est monogène, cela découle du Cor. 5.24.

DÉMONSTRATION — D'après le théorème de l'élément primitif, il existe $x \in K$ tel que $K = \mathbb{Q}(x)$. Quitte à multiplier x par un entier $m \in \mathbb{Z}$, on peut de plus supposer que $x \in \overline{\mathbb{Z}}$ (Lemme 5.19). En particulier, $\mathbb{Z}[x] \subset \mathcal{O}_K$. Réciproquement, soit $z \in \mathcal{O}_K$. Si $n = [\mathbb{Q}(x) : \mathbb{Q}]$ alors $z = \sum_{i=0}^{n-1} z_i x^i$ où $z_i \in \mathbb{Q}$ pour tout i. Mais $\mathrm{Tr}_{K/\mathbb{Q}}(x^j z), \mathrm{Tr}_{K/\mathbb{Q}}(x^j x^k) \in \mathbb{Z}$ pour tout $j, k \in \mathbb{N}$ car $x, z \in \mathcal{O}_K$ (Théorème 5.21). En particulier, $d = \mathrm{disc}_{K/\mathbb{Q}}(1, x, \dots, x^{n-1})$ est un entier non nul par la proposition 5.17, et l'inversion du système linéaire (3) entraîne que les z_i sont dans $\frac{1}{d}\mathbb{Z}$, i.e.

$$\mathbb{Z}[x] \subset \mathcal{O}_K \subset \frac{1}{d}\mathbb{Z}[x].$$

Mais $\frac{1}{d}\mathbb{Z}[x]$ est un groupe abélien libre de rang n d'après le lemme 5.24, dont $\mathcal{O}_K$ peut donc être vu comme sous-réseau par la propriété d'inclusion ci-dessus, il est donc également libre de rang n d'après la caractérisation algébrique des réseaux (Thm. 2.4). □

Notons que cette démonstration fournit un algorithme pour calculer $\mathcal{O}_K$ en général. En effet, on commence par choisir un $x \in \overline{\mathbb{Z}}$ tel que $K = \mathbb{Q}(x)$ (un multiple d'un élément primitif), et on calcule $d = \mathrm{disc}_{K/\mathbb{Q}}(1, x, \dots, x^{n-1})$ où $n = [\mathbb{Q}(x) : \mathbb{Q}]$. On cherche alors à determiner le groupe abélien fini

$$\mathcal{O}_K/\mathbb{Z}[x] \subset (\frac{1}{d}\mathbb{Z}[x])/\mathbb{Z}[x] \simeq (\mathbb{Z}/d\mathbb{Z})^n.$$

Pour chacun des d^n représentants z du groupe quotient $\frac{1}{d}\mathbb{Z}[x]/\mathbb{Z}[x]$ on détermine si $z \in \mathcal{O}_K$, en vérifiant que son polynôme caractéristique est dans $\mathbb{Z}[X]$. Ceci étant fait, $\mathcal{O}_K$ est le groupe abélien engendré par $\mathbb{Z}[x]$ et l'ensemble des représentants de $\frac{1}{d}\mathbb{Z}[x]/\mathbb{Z}[x]$ qui sont des éléments de $\mathcal{O}_K$.

Cet algorithme résoud en théorie le problème de déterminer $\mathcal{O}_K$, mais il est souvent inefficace en pratique à cause du trop grand nombre de vérifications à effectuer. On peut en court-circuiter certaines étapes en étudiant directement l'équation $\chi_{x,K/\mathbb{Q}} \in \mathbb{Z}[X]$, mais cela s'avère fastidieux même dans les exemples les plus simples. Nous renvoyons à l'exercice 5.7 pour l'exemple de $\mathbb{Q}(\sqrt[3]{2})$ traité par cette méthode directe.

Observons qu'une $\mathbb{Z}$-base de $\mathcal{O}_K$ est nécessairement une $\mathbb{Q}$-base de K d'après le lemme 5.19. Comme on vient de l'expliquer, K étant donné il est en général difficile d'exhiber une $\mathbb{Z}$-base de $\mathcal{O}_K$. Des considérations de discriminant peuvent être cependant très utiles pour ces questions.

PROPOSITION 5.26. *Soit $e_1, \cdots, e_n \in \mathcal{O}_K$ une $\mathbb{Q}$-base de K alors $\mathrm{disc}_{K/\mathbb{Q}}(e_1, \cdots, e_n)$ est un entier non nul. Soit (f_i) une autre famille ayant la même propriété et soit P la matrice des f_i dans la base (e_i). On suppose $f_j \in \sum_i \mathbb{Z}e_i$ pour tout j, i.e. $P \in \mathrm{M}_n(\mathbb{Z})$. Alors*

$$\mathrm{disc}_{K/\mathbb{Q}}(f_1, \cdots, f_n) = \det(P)^2 \mathrm{disc}_{K/\mathbb{Q}}(e_1, \cdots, e_n)$$

et $\sum_i \mathbb{Z}f_i$ est d'indice fini égal à $|\det(P)|$ dans $\sum_i \mathbb{Z}e_i$.

DÉMONSTRATION — En effet, si $e_1, \cdots, e_n \in \mathcal{O}_K$ alors $(\mathrm{Tr}_{L/\mathbb{Q}}(e_i e_j)_{1 \leq i,j \leq n}) \in \mathrm{M}_n(\mathbb{Z})$, d'après le théorème 5.21, et donc $\mathrm{disc}_{K/\mathbb{Q}}(e_1, \ldots, e_n) \in \mathbb{Z}$. Il est non nul si (e_i) est une $\mathbb{Q}$-base de K d'après la proposition 5.17. Le premier point du lemme se déduit alors de la proposition 5.17 (ii). Le second découle de la proposition 2.17, après avoir identifié le groupe abélien $\sum_i \mathbb{Z}e_i$ au réseau $\mathbb{Z}^n$ de $\mathbb{R}^n$ via l'application linéaire $\sum_i x_i e_i \mapsto (x_i)$. □

En appliquant ce lemme à deux $\mathbb{Z}$-bases de $\mathcal{O}_K$, de sorte que $\det(P) = \pm 1$, on donne sens à la définition suivante.

DÉFINITION 5.27. *Soit K un corps de nombres. Le discriminant relatif à $K/\mathbb{Q}$ d'une $\mathbb{Z}$-base de $\mathcal{O}_K$ est un entier non nul qui ne dépend pas du choix de la base en question. On l'appelle le discriminant de K.*

La proposition ci-dessus révèle aussi que les $\mathbb{Z}$-bases de $\mathcal{O}_K$ sont exactement les familles $e_1, \ldots, e_n \in \mathcal{O}_K$ telles que $|\mathrm{disc}_{K/\mathbb{Q}}(e_1, \ldots, e_n)|$ est non nul et minimal. Nous verrons dans les exercices comment l'utiliser pour déterminer $\mathcal{O}_K$ dans des cas particuliers.

5. Entiers des corps cyclotomiques

Nous allons conclure ce chapitre en déterminant l'anneau des entiers de certains corps cyclotomiques. Soit $n \geq 1$ un entier et soit $\zeta = e^{2i\pi/n}$. On rappelle que le n-ième polynôme cyclotomique est le polynôme

$$\Phi_n(X) = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} (X - \zeta^k) \in \mathbb{C}[X].$$

Il est donc de degré $\varphi(n)$. Il est bien connu que ce polynôme est dans $\mathbb{Z}[X]$ et qu'il est irréductible dans $\mathbb{Q}[X]$ (Gauss). Autrement dit, $\Phi_n = \Pi_{\zeta,\mathbb{Q}}$. Le théorème suivant est dû à Kummer.

THÉORÈME 5.28. *Si $K = \mathbb{Q}(\zeta)$ avec $\zeta \in \mathbb{C}$ une racine de l'unité, alors $\mathcal{O}_K = \mathbb{Z}[\zeta]$.*

Pour simplifier nous ne démontrerons ce résultat que lorsque ζ est une racine de l'unité d'ordre p^r avec p un nombre premier. Dans ce cas, $\Phi_{p^r}(X) = \frac{X^{p^r}-1}{X^{p^{r-1}}-1} = \sum_{i=0}^{p-1} X^{ip^{r-1}} \in \mathbb{Z}[X]$. De plus, l'irréductibilité de Φ_{p^r} dans $\mathbb{Q}[X]$ est une conséquence du critère d'Eisenstein, rappelons pourquoi.

On rappelle qu'un polynôme unitaire $P = X^n + \sum_{i=0}^{n-1} a_i X^i \in \mathbb{Z}[X]$ est un *polynôme d'Eisenstein en le nombre premier* p si p divise $a_0, \ldots, a_{n-1}$ mais p^2 ne divise pas a_0. Le *critère d'Eisenstein* assure alors que P est irréductible [1] dans $\mathbb{Q}[X]$.

Vérifions que le polynôme $\Phi_{p^r}(X+1)$ est d'Eisenstein en p. En effet, le petit théorème de Fermat entraîne

$$\Phi_{p^r}(X+1) \equiv X^{p^r - p^{r-1}} \bmod p\mathbb{Z}[X].$$

On conclut car $\Phi_{p^r}(0) = p$ (règle de l'Hôpital !). L'irréductibilité de $\Phi_{p^r}(\mathrm{X}{+}1)$ dans $\mathbb{Q}[X]$ découle alors du critère d'Eisenstein, ainsi que celle de son translaté $\Phi_{p^r}(X)$.

Observons de plus que si $x = \zeta - 1$ alors (voir l'exercice 5.4)

$$\mathrm{disc}_{K/\mathbb{Q}}(1, x, \ldots, x^{\varphi(p^r)-1}) = \mathrm{disc}(\Phi_{p^r}(X+1)) = \mathrm{disc}(\Phi_{p^r}) \mid \mathrm{disc}(X^{p^r} - 1) = \pm p^{rp^r}.$$

En particulier $\pm\mathrm{disc}(K)$ est une puissance de p d'après la proposition 5.26. Il suffit donc pour conclure de démontrer que $\mathbb{Z}[\zeta] = \mathbb{Z}[\zeta - 1]$ est d'indice premier à p dans $\mathcal{O}_K$. Cela découle de la proposition suivante.

PROPOSITION 5.29. *Soit $K = \mathbb{Q}(x)$ un corps de nombres avec $x \in \overline{\mathbb{Z}}$. On suppose que $\Pi_{x,\mathbb{Q}}$ est un polynôme d'Eisenstein en le nombre premier p. Alors $\mathbb{Z}[x]$ est d'indice premier à p dans $\mathcal{O}_K$.*

DÉMONSTRATION — On a déjà vu que le groupe abélien $\mathcal{O}_K/\mathbb{Z}[x]$ est fini (démonstration du théorème 5.25). Supposons que son cardinal soit multiple de p. Le lemme de Cauchy entraîne alors qu'il existe $z \in \mathcal{O}_K \backslash \mathbb{Z}[x]$ tel que $pz \in \mathbb{Z}[x]$. Ainsi, $pz = \sum_{i=0}^{n-1} b_i x^i \in p\mathcal{O}_K$ où les b_i sont $\mathbb{Z}$ et non tous dans $p\mathbb{Z}$. Nous allons contredire ceci en montrant que p divise b_i pour tout i. On part pour cela de la congruence dans $\overline{\mathbb{Z}}$

$$\sum_{i=0}^{n-1} b_i x^i \equiv 0 \bmod p. \tag{4}$$

Pour $i \geq n$, on a de plus $x^i \equiv 0 \bmod p$ par hypothèse sur $\Pi_{x,\mathbb{Q}}$. Ainsi, si l'on multiplie l'équation (4) par x^{n-1}, il ne reste que $b_0 x^{n-1} \equiv 0 \bmod p$. Autrement dit, on a $b_0 x^{n-1} = pa$ avec $a \in \mathcal{O}_K$. En prenant la norme on trouve $b_0^n \mathrm{N}_{K/\mathbb{Q}}(x)^{n-1} \equiv 0 \bmod p^n$. Mais $\mathrm{N}_{K/\mathbb{Q}}(x) = \pm a_0$ car $\chi_{x,K/\mathbb{Q}} = \Pi_{x,\mathbb{Q}}$, qui est divisible par p mais non par p^2 par hypothèse. Il vient que p divise b_0. En multipliant ensuite (4) successivement par $x^{n-2}, \ldots, x, 1$ on déduit de même successivement $b_1 \equiv \cdots \equiv b_{n-2} \equiv b_{n-1} \equiv 0 \bmod p$. □

EXEMPLE 5.30. En guise d'exemple, vérifions que si $K = \mathbb{Q}(x)$ avec $x = \sqrt[3]{2}$, alors $\mathcal{O}_K = \mathbb{Z}[x]$. En effet, $\mathrm{disc}_{K/\mathbb{Q}}(1, x, x^2) = \mathrm{disc}(P) = -2^2 \cdot 3^3$ où $P = X^3 - 2$. En particulier, $|\mathcal{O}_K/\mathbb{Z}[x]|$ divise $2^2 \cdot 3^3$. Mais P et $P(X-1) = (X-1)^3 - 2 = X^3 - 3X^2 + 3X - 3$ sont des polynômes d'Eisenstein respectivement pour $p = 2$ et 3. Comme $\mathbb{Z}[x] = \mathbb{Z}[x-1]$, la proposition montre que $|\mathcal{O}_K/\mathbb{Z}[x]|$ est premier à 2 et à 3, c'est donc 1. On pourra comparer avec la méthode directe de l'exercice 5.7.

1. Donnons-en une démonstation. D'après le lemme de Gauss, il suffit de voir qu'il est irréductible dans $\mathbb{Z}[X]$ (voir l'exercice 5.13). Soit $P = AB$ avec $A, B \in \mathbb{Z}[X]$. On peut supposer que A et B sont unitaires quitte à écrire $P = (-A)(-B)$. On a $P \equiv X^n \equiv AB$ dans $(\mathbb{Z}/p\mathbb{Z})[X]$. Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, cela entraîne $A \equiv X^i$ et $B \equiv X^j$ avec $i + j = n$. Si $i, j \geq 1$, alors p divise $A(0)$ et $B(0)$, et donc p^2 divise $P(0) = A(0)B(0)$: absurde, donc $i = 1$ ou $j = 1$. Mais comme A et B sont unitaires cela entraîne $A = 1$ ou $B = 1$.

6. Exercices

EXERCICE 5.1. *Montrer qu'un corps de nombres de degré* 2 *est de la forme* $\mathbb{Q}(\sqrt{d})$ *pour un unique* $d \in \mathbb{Z}\backslash\{0,1\}$ *sans facteur carré.*

EXERCICE 5.2. *Montrer que tout corps quadratique est inclus dans un corps cyclotomique.*

EXERCICE 5.3. *Soit* $d \in \mathbb{Z}$. *Montrer que le produit de deux nombres de la forme* $a^3+db^3+d^2c^3-3abcd$, *avec* $a,b,c \in \mathbb{Z}$, *est encore de cette forme. On pourra d'abord supposer que* d *n'est pas un cube et considérer le corps de nombres* $\mathbb{Q}(\sqrt[3]{d})$.

EXERCICE 5.4. *Soient* $P, Q \in \mathbb{Z}[X]$ *des polynômes unitaires. On suppose* $\mathrm{disc}(Q) \neq 0$. *Montrer que si* P *divise* Q *dans* $\mathbb{Q}[X]$ *alors* $\mathrm{disc}(P)$ *divise* $\mathrm{disc}(Q)$ *dans* $\mathbb{Z}$.

EXERCICE 5.5. *Soit* $K = \mathbb{Q}(\sqrt{d})$ *avec* $d \in \mathbb{Z}\backslash\{0,1\}$ *sans facteur carré. Montrer que* $\mathrm{disc}(K) = d$ *ou* $4d$, *selon que* $d \equiv 1 \bmod 4$ *ou non.*

EXERCICE 5.6. *(i) Soient* K *un corps de nombres et* $e_1, \ldots, e_n \in \mathcal{O}_K$ *tels que* $\mathrm{disc}_{K/\mathbb{Q}}(e_1, \ldots, e_n)$ *est non nul et sans facteur carré. Montrer que* $e_1, \ldots, e_n$ *est une* $\mathbb{Z}$*-base de* $\mathcal{O}_K$.

(ii) Soit $K = \mathbb{Q}(x)$ *où* $x \in \mathbb{C}$ *satisfait* $x^3 - x + 1 = 0$. *Montrer que* $[K : \mathbb{Q}] = 3$ *puis que* $\mathcal{O}_K = \mathbb{Z}[x]$.

EXERCICE 5.7. *On se propose de montrer sans utiliser la proposition 5.29 que si* $K = \mathbb{Q}(\sqrt[3]{2})$ *alors* $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$. *On pose* $x = \sqrt[3]{2}$ *et on fixe* $z = a + bx + cx^2 \in K$ *avec* $a, b, c \in \mathbb{Q}$.

(i) Vérifier que $\chi_{z,K/\mathbb{Q}} = X^3 - 3aX^2 + 3(a^2 - 2bc)X - (a^3 + 2b^3 + 4c^3 - 6abc)$.

On suppose dorénavant $z \in \mathcal{O}_K$.

(ii) En considérant $\mathrm{Tr}_{K/\mathbb{Q}}(x^i z)$, *montrer que* $6b,\ 6c \in \mathbb{Z}$.

(iii) En déduire que $3a, 3b, 3c \in \mathbb{Z}$. *On pourra multiplier* $a^3 + 2b^3 + 4c^3 - 6abc$ *par* 2.3^3 *puis* 3^3.

On pose $3a = \alpha$, $3b = \beta$ *et* $3c = \gamma$, *de sorte que* $\alpha, \beta, \gamma \in \mathbb{Z}$.

(iv) Vérifier que $\alpha^2 \equiv 2\beta\gamma \bmod 3$, $\alpha - \beta + \gamma \equiv 0 \bmod 3$, *puis que* $\alpha \equiv \gamma \equiv -\beta \bmod 3$.

(v) Vérifier que $\pm\frac{1}{3}(1 - x + x^2) \notin \mathcal{O}_K$ *et conclure.*

EXERCICE 5.8. *Soient* $m, n \in \mathbb{Z}\backslash\{0,1\}$ *des entiers distincts, sans facteur carré, et tels que* $m \equiv n \equiv 1 \bmod 4$. *On se propose de montrer que si* $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ *alors* $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\beta + \mathbb{Z}\alpha\beta$ *où* $\alpha = \frac{1+\sqrt{n}}{2}$ *et* $\beta = \frac{1+\sqrt{m}}{2}$.

(i) Montrer $[K : \mathbb{Q}] = 4$ *et déterminer* $\Sigma(K)$.

(ii) Vérifier $\mathrm{disc}_{K/\mathbb{Q}}(1, \alpha, \beta, \alpha\beta) = m^2n^2$.

(iii) Montrer $4\mathcal{O}_K \subset \mathbb{Z}+\mathbb{Z}\sqrt{n}+\mathbb{Z}\sqrt{m}+\mathbb{Z}\sqrt{mn}$ *(utiliser des traces sur* $\mathbb{Q}(\sqrt{n}), \mathbb{Q}(\sqrt{m}), \mathbb{Q}(\sqrt{mn})$*,*

(iv) Conclure.

EXERCICE 5.9. *(Un exemple d'anneau des entiers non monogène) On considère* $K = \mathbb{Q}(\sqrt{n}, \sqrt{m})$ *avec* $m, n \in \mathbb{Z}\backslash\{0, 1\}$ *sans facteur carré, distincts, et tels que* $m \equiv n \equiv 1 \bmod 8$. *On va montrer qu'il n'existe pas d'élément* $x \in \mathcal{O}_K$ *tel que* $\mathcal{O}_K = \mathbb{Z}[x]$.

(i) En utilisant le résultat de l'exercice 5.8, montrer que l'anneau $\mathcal{O}_K/2\mathcal{O}_K$ *est isomorphe à*

$$A = (\mathbb{Z}/2\mathbb{Z})[X, Y]/(X^2 - X, Y^2 - Y).$$

(ii) Vérifier que l'anneau A *admet exactement quatre morphismes d'anneaux distincts* $A \to \mathbb{Z}/2\mathbb{Z}$.

(iii) En déduire que l'anneau A *n'est pas isomorphe à* $(\mathbb{Z}/2\mathbb{Z})[X]/(P)$ *où* $P \in (\mathbb{Z}/2\mathbb{Z})[X]$ *est de degré* 4. *On pourra constater que les morphismes d'anneaux* $(\mathbb{Z}/2\mathbb{Z})[X]/(P) \to \mathbb{Z}/2\mathbb{Z}$ *sont en bijection avec l'ensemble des racines de* P *dans* $\mathbb{Z}/2\mathbb{Z}$.

(iv) Conclure.

EXERCICE 5.10. *Soit* K *un corps de nombres. Montrer* $\mathcal{O}_K^\times = \{x \in \mathcal{O}_K, \mathrm{N}_{K/\mathbb{Q}}(x) = \pm 1\}$.

EXERCICE 5.11. *Soit* $K \subset \mathbb{C}$ *un corps de nombres. On note* $\mu(K) \subset \mathcal{O}_K^\times$ *l'ensemble des racines de l'unité appartenant à* K *et on pose* $U(K) = \{z \in \mathcal{O}_K, |\sigma(z)| = 1 \ \forall\ \sigma \in \Sigma(K)\}$.

(i) Montrer que $U(K)$ *est un sous-groupe de* $\mathcal{O}_K^\times$ *contenant* $\mu(K)$.

(ii) Montrer que $\{\chi_{x,K/\mathbb{Q}}, x \in U(K)\} \subset \mathbb{Q}[X]$ *est un ensemble fini.*

(iii) En déduire que $U(K)$ *est fini, puis* $U(K) = \mu(K) = \{\zeta \in \mathbb{C}, \zeta^n = 1\}$ *où* $n = |U(K)|$.

(iv) (suite) Montrer $\varphi(n) \,|\, [K : \mathbb{Q}]$.

(v) (Kronecker) Montrer que si $x \in \overline{\mathbb{Z}}$ *a tous ses* $\mathbb{Q}$*-conjugués de module* 1 *alors* x *est une racine de l'unité.*

EXERCICE 5.12. *Soit* $\alpha \in \overline{\mathbb{Z}}$. *Montrer que* $\mathbb{Z}[\alpha]$ *est intégralement clos si, et seulement si,* $\mathbb{Z}[\alpha]$ *est l'anneau des entiers de* $\mathbb{Q}(\alpha)$.

L'exercice suivant donne un autre point de vue sur un théorème de Gauss (Exercice 4.12).

EXERCICE 5.13. (Irréductibilité dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$)

(i) Soient $P, Q, R \in \mathbb{Q}[X]$ des polynômes unitaires tels que $P = QR$. Montrer que si $P \in \mathbb{Z}[X]$ alors $Q, R \in \mathbb{Z}[X]$. On pourra observer que les racines de P dans $\mathbb{C}$ sont dans $\overline{\mathbb{Z}}$.

(ii) En déduire que si $P \in \mathbb{Z}[X]$ est irréductible et unitaire, alors P est irréductible dans $\mathbb{Q}[X]$.

(iii) (Application) Montrer que si $P \in \mathbb{Z}[X]$ est unitaire, et s'il existe un entier $N \geq 1$ tel que $P \bmod N$ est irréductible dans $(\mathbb{Z}/N\mathbb{Z})[X]$, alors P est irréductible dans $\mathbb{Q}[X]$.

EXERCICE 5.14. *Soit p un nombre premier impair et $\zeta = e^{\frac{2i\pi}{p}}$. Montrer que* $\mathrm{disc}(\mathbb{Q}(\zeta)) = (-1)^{\frac{p-1}{2}} p^{p-2}$.

EXERCICE 5.15. (Signe du discriminant) *Soit K un corps de nombres. Montrer que le signe de* $\mathrm{disc}(K)$ *est $(-1)^s$ où $2s$ est le nombre des $\sigma \in \Sigma(K)$ tels que $\sigma(K) \not\subset \mathbb{R}$.*

EXERCICE 5.16. (Théorème de Stickelberger) *Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire.*

(i) On suppose $P = \prod_{i=1}^{n}(X - x_i)$ dans $\mathbb{C}[X]$, montrer $\prod_{1 \leq i < j \leq n}(x_i + x_j) \in \mathbb{Z}$.

(ii) En déduire $\mathrm{disc}(P) \equiv 0, 1 \bmod 4$.

En déduire que si K est un corps de nombres alors $\mathrm{disc}(K) \equiv 0, 1 \bmod 4$.

PROBLÈME 5.1. *Soient M/L et L/K des extensions de corps de nombres. Montrer que :*

(i) $\mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L} = \mathrm{Tr}_{M/K}$,

(ii) $\mathrm{N}_{L/K} \circ \mathrm{N}_{M/L} = \mathrm{N}_{M/K}$.

Chapitre 6

Finitude du nombre des classes d'idéaux d'un anneau de nombres

Dans ce chapitre, nous poursuivons notre étude de l'arithmétique des anneaux de nombres algébriques comme $\mathcal{O}_K$ ou $\mathbb{Z}[\alpha]$ avec $\alpha \in \overline{\mathbb{Z}}$. L'exemple des entiers quadratiques imaginaires nous a montré que ces anneaux ont une forte tendance à ne pas être factoriels ou principaux. [1] Nous étudions ici en général leur défaut de principalité, en introduisant la notion centrale de classes d'idéaux dans un anneau. Le résultat principal est alors que l'ensemble de ces classes est toujours fini, ce qui n'est pas sans rappeler la finitude des classes de formes de discriminant donné. Suivant Minkowski, nous verrons que la géométrie des nombres fournit un algorithme efficace pour déterminer cet ensemble de classes, en particulier pour montrer qu'un anneau de nombres est principal.

Références : Le chapitre IV paragraphes 2 et 3 du livre de Samuel. Le chapitre 12 du livre de Ireland et Rosen.

1. L'ensemble des classes d'idéaux d'un anneau intègre

Soit A un anneau intègre de corps de fractions K. Si I est un idéal de A et si $x \in K$, on note

$$xI = \{xa, a \in I\} \subset K.$$

Une partie de K de cette forme est appelée [2] *idéal fractionnaire de* K. C'est un sous-groupe additif de K stable par multiplication par tout élément de A. En particulier, xI est un idéal de A si de plus $xI \subset A$. C'est notamment le cas si $x \in A$.

Définition 6.1. *Deux idéaux I et J de A sont dits* équivalents*, et l'on note $I \sim J$, s'il existe $x, y \in A$ non nuls tels que $xI = yJ$, ou ce qui revient au même s'il existe $z \in K^\times$ tel que $zI = J$. C'est une relation d'équivalence sur l'ensemble des idéaux non nuls de A dont on note* $\mathrm{Cl}(A)$ *l'ensemble des classes.*

La vérification que c'est une relation d'équivalence est immédiate. On note $[I]$ la classe dans $\mathrm{Cl}(A)$ de l'idéal non nul I de A. L'ensemble $\mathrm{Cl}(A)$ mesure le défaut de principalité de l'anneau A :

Proposition 6.2. *Un idéal non nul I de A est principal si, et seulement si, on a $I \sim A$. En particulier,* $\mathrm{Cl}(A)$ *est de cardinal* 1 *si, et seulement si, A est principal.*

1. En fait, pour ces anneaux il est équivalent d'être factoriel et principal. Cela provient de l'exercice 7.5 combiné au théorème 6.15 (i).

2. Bien que couramment adoptée, c'est une très mauvaise terminologie car en général ce ne sont pas des ideaux de K (dont les seuls idéaux 0 et K, puisque c'est un corps).

Démonstration — On a bien sûr $xA \sim A$ pour tout $x \in A$ non nul. Réciproquement, soit I un idéal de A et $z \in K^*$ tels que $I = zA$. On a $z \cdot 1 \in I \subset A$, et donc I est principal. □

L'ensemble $\mathrm{Cl}(A)$ est muni d'une loi de composition interne intéressante qu'elle hérite du produit des idéaux que nous décrivons maintenant.

Définition 6.3. *Si I et J sont deux idéaux de A. On note IJ l'idéal de A engendré par les éléments de la forme xy avec $x \in I$ et $y \in J$.*

Évidemment, on a $(a)(b) = (ab)$ pour tout $a, b \in A$. Plus généralement, si $I = (a_1, \ldots, a_n)$ et si $J = (b_1, \ldots, b_m)$, alors IJ est l'idéal engendré par les nm éléments $a_i b_j$. L'anneau A étant commutatif par hypothèse, on a $IJ = JI$. Le produit des idéaux est associatifs : $(HI)J = H(IJ)$ est simplement l'idéal engendré par les $xyz = x(yz) = (xy)z$ avec $x \in H$, $y \in I$ et $z \in J$. On définit plus généralement le produit $I_1 \cdots I_n$ de $n \geq 2$ idéaux de A par la relation récursive $I_1 \cdots I_n = (I_1 \cdots I_{n-1})I_n$. Si I, I', J, J' sont des idéaux de A, on constate enfin que les relations $I \sim I'$ et $J \sim J'$ entraînent $IJ \sim I'J'$. Nous avons donc vérifié la proposition suivante.

Proposition 6.4. *La multiplication des idéaux induit une loi de composition sur* $\mathrm{Cl}(A)$. *Cette loi est commutative et associative. La classe de A, i.e. celle des idéaux principaux, en est un élément neutre.*

Ce qui manque en général à $\mathrm{Cl}(A)$ pour être un groupe (muni de cette loi) est donc l'inversibilité de ses éléments. Remarquons qu'il est équivalent de dire que la classe de l'idéal non nul I est inversible et de dire qu'il existe un idéal non nul J de A tel que IJ est principal. Un tel idéal I sera dit simplement inversible.

2. Finitude du nombre des classes d'idéaux

Commençons par une définition importante.

Définition 6.5. *Un ordre du corps de nombres K est un sous-anneau $A \subset \mathcal{O}_K$ contenant une $\mathbb{Q}$-base de K.*

Par exemple, si $\alpha \in \overline{\mathbb{Z}}$ alors $\mathbb{Z}[\alpha]$ est un ordre de $\mathbb{Q}(\alpha)$. De plus, $\mathcal{O}_K$ est également un ordre de K (Lemme 5.19). L'intêret de cette notion pour nous est essentiellement d'englober ces deux cas importants. Notre objectif principal dans ce chapitre est de démontrer le théorème suivant.

Théorème 6.6. (Finitude du nombre des classes) *Si A est un ordre du corps de nombres K, alors* $\mathrm{Cl}(A)$ *est fini.*

Il s'avère que bien qu'un tel A n'est pas toujours principal comme nous l'avons déjà vu, il n'en est pas très loin. En effet, la proposition suivante affirme que tout idéal de I contient un idéal principal qui est très gros, à savoir d'indice dans I inférieur à une constante ne dépendant que de A :

Proposition 6.7. *Soit A un ordre du corps de nombres K. Il existe un entier $C \geq 1$ tel que pour tout idéal I de A, il existe un élément $x \in I$ tel que $|I/Ax| \leq C$.*

Vérifions que cela entraîne le théorème. En effet, soit I un idéal non nul de A, et soit $x \in I$ comme dans l'énoncé de la proposition (en particulier, on a $x \neq 0$ car I est infini). Si N désigne le cardinal du groupe abélien fini I/Ax, alors N annule I/Ax d'après Lagrange, c'est-à-dire $NI \subset Ax$. On constate donc que

$$NA \subset \frac{N}{x} I \subset A$$

(l'inclusion de gauche vient de ce que $x \in I$, donc $N = \frac{N}{x} x \in \frac{N}{x} I$). En particulier, $J = \frac{N}{x} I$ est un idéal de A qui est équivalent à I, car $xJ = NI$, et qui est compris entre NA et A. Rappelons que $N \leq C$ d'après la proposition. Il ne reste donc qu'à vérifier que pour tout entier $N \geq 1$ il n'existe qu'un nombre fini d'idéaux de A contenant N. Cela se déduit par exemple du lemme suivant.

LEMME 6.8. *Pour tout entier $N \geq 1$, l'anneau A/NA est fini, et a $N^{[K:\mathbb{Q}]}$ éléments.*

DÉMONSTRATION — En effet, le groupe additif de A admet une $\mathbb{Z}$-base $e_1, \ldots, e_n$ à $n = [K : \mathbb{Q}]$ éléments. Nous l'avons déjà vu si $A = \mathbb{Z}[\alpha]$ (Proposition 5.24) où $A = \mathcal{O}_K$ (existence de $\mathbb{Z}$-bases de $\mathcal{O}_K$) et nous le démontrerons pour tout A au théorème 6.15. Soit $e_1, \ldots, e_n \in A$ une telle base. On constate alors que $NA = \oplus_{i=1}^{n} N\mathbb{Z}e_i$, puis que l'ensemble quotient A/NA a exactement N^n éléments. [3] □

Cela termine la démonstration de la finitude du nombre de classes à partir de la proposition 6.7. Observons au passage que nous avons démontré le corollaire suivant.

COROLLAIRE-DÉFINITION 6.9. *Soit A un ordre d'un corps de nombres. On note $C(A)$ le plus petit entier C satisfaisant la proposition 6.7. Tout idéal non nul de A est équivalent à un idéal de A contenant un entier N tel que $1 \leq N \leq C(A)$.*

Il ne reste donc qu'à vérifier la proposition 6.7. Elle pourrait se démontrer à l'aide du principe des tiroirs en étudiant le défaut d'euclidianité de A, nous renvoyons à l'exercice 6.13 pour cette approche. L'inconvénient de cette méthode est qu'elle fournit une majoration de $C(A)$ assez mauvaise (bien qu'explicite) qui rend son utilisation peu commode. Dans un paragraphe suivant, nous la déduirons plutôt de la géométrie des nombres, qui donnera un renseignement nettement plus precis et fondamental dans l'optique du calcul effectif de $\mathrm{Cl}(A)$ dans les exemples.

3. Digression : idéaux contenant un nombre premier

Avant de se concentrer sur la preuve de la proposition 6.7, qui nous occupera par la suite jusqu'à la fin du chapitre, remarquons qu'il nous faudra de plus, pour déterminer des représentants de $\mathrm{Cl}(A)$, être capable de déterminer les idéaux de A contenant un entier $N \geq 2$ donné. Ces idéaux sont chacun l'image réciproque d'un idéal de l'anneau fini A/NA, et peuvent donc tous être énumérés en théorie si A est explicite. Lorsque N est premier et A est monogène, on dispose de la recette suivante.

3. Mieux le groupe additif A/NA est isomorphe à $(\mathbb{Z}/N\mathbb{Z})^n$. Attention, il s'agit seulement d'un isomorphisme additif, et l'anneau quotient A/NA n'est pas en général isomorphe à l'anneau produit $(\mathbb{Z}/N\mathbb{Z})^n$.

PROPOSITION 6.10. *Soient $\alpha \in \overline{\mathbb{Z}}$, $A = \mathbb{Z}[\alpha]$, p un nombre premier et $P = \overline{\Pi}_{\alpha,\mathbb{Q}} \in (\mathbb{Z}/p\mathbb{Z})[X]$ la réduction modulo p du polynôme minimal de α sur $\mathbb{Q}$.*

(i) Si $Q \in (\mathbb{Z}/p\mathbb{Z})[X]$ est un diviseur de P, et si $\widetilde{Q} \in \mathbb{Z}[X]$ est un polynôme tel que $\widetilde{Q} \bmod p = Q$, alors $\mathrm{I}(Q) := pA + \widetilde{Q}(\alpha)A$ est un idéal de A contenant p qui ne dépend pas du choix de $\widetilde{Q}$.

(ii) L'application $Q \mapsto \mathrm{I}(Q)$ est une bijection entre facteurs unitaires de P et idéaux de A contenant p ; elle satisfait $Q|Q' \Leftrightarrow \mathrm{I}(Q') \subset \mathrm{I}(Q)$.

(iii) L'anneau $A/\mathrm{I}(Q)$ est isomorphe à $(\mathbb{Z}/p\mathbb{Z})[X]/(Q)$. En particulier, on a

$$|A/\mathrm{I}(Q)| = p^{\deg(Q)}.$$

Ce résultat jouera un rôle important dans les applications. Considérons par exemple $\alpha = \sqrt{-5}$, de sorte que $\Pi_{\alpha,\mathbb{Q}} = X^2 + 5$, et cherchons les idéaux de $A = \mathbb{Z}[\alpha]$ contenant 2. On a $X^2 + 5 \equiv (X+1)^2 \bmod 2$, les idéaux de $\mathbb{Z}[\alpha]$ contenant 2 sont donc $2A$, $2A + (\alpha+1)A$ et A. De même, comme $X^2 + 5 \equiv (X-1)(X+1) \bmod 3$, les idéaux de A contenant 3 sont $3A$, A, $3A + (\alpha-1)A$ et $3A + (\alpha+1)A$. Enfin, si -5 n'est pas un carré modulo p, les idéaux de A contenant p sont simplement A et pA.

DÉMONSTRATION — Il est clair que $pA + \widetilde{Q}(\alpha)A$ est un idéal de A contenant p. Si $\widetilde{Q}', \widetilde{Q} \in \mathbb{Z}[X]$ sont congrus modulo $p\mathbb{Z}[X]$ alors $\widetilde{Q}'(\alpha) - \widetilde{Q}(\alpha) \in p\mathbb{Z}[\alpha] = pA$ et donc les idéaux $pA + \widetilde{Q}(\alpha)A$ et $pA + \widetilde{Q}'(\alpha)A$ sont les mêmes, ce qui démontre le (i).

Avant de démontrer le (ii) faisons quelques rappels généraux. Soit A un anneau commutatif unitaire.

(a) Soit I un idéal de A. L'application $J \mapsto J/I$ est une bijection entre l'ensemble ordonné (pour l'inclusion) des idéaux de A contenant I et celui des idéaux de A/I, la bijection inverse étant l'application $I' \mapsto \{x \in A, x + I \in I'\}$.

(b) Si $I \subset J$ sont deux idéaux de A, la surjection canonique $A/I \to A/J$ a pour noyau I/J et induit donc un isomorphisme d'anneaux $(A/I)/(J/I) \xrightarrow{\sim} A/J$.

(c) En particulier, si I' et J' sont des idéaux de A, le (ii) appliqué aux idéaux $I = I'$ et $J = I' + J'$ montre que l'application naturelle $A/I' \to A/(I' + J')$ induit un isomorphisme canonique $(A/I')/((I' + J')/I') \xrightarrow{\sim} A/(I' + J')$.

Nous cherchons à appliquer le (a) à $A = \mathbb{Z}[\alpha]$ et $I = pA$, et il faut donc étudier l'anneau A/pA dans ce cas. Nous allons démontrer qu'il existe un isomorphisme canonique

$$A/pA \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})[X]/(P).$$

Il s'agit d'une vérification relativement formelle, mais instructive !, que nous allons justifier lourdement.

Soient B l'anneau $\mathbb{Z}[X]$, $I = \Pi_{x,\mathbb{Q}}B$ et $J = pB$. Soit $\varphi : B \to A$ la surjection canonique $Q \mapsto Q(\alpha)$. On sait que φ induit un isomorphisme $\varphi' : B/I \xrightarrow{\sim} A$, d'après la proposition 5.24. D'autre part, on a clairement les égalités $\varphi(I + J) = \varphi(pB) =$

$p\varphi(B) = pA$. Autrement dit, φ' induit une bijection $(J+I)/I \xrightarrow{\sim} pA$, puis par passage aux quotients un isomorphisme

$$\varphi'' : (B/I)/((I+J)/I) \xrightarrow{\sim} A/pA.$$

D'autre part, le (c) des rappels ci-dessus montre que l'anneau de gauche de cet isomorphisme s'identifie naturellement à $B/(I+J)$, soit encore à $(B/J)/((I+J)/J)$, en appliquant encore le (c) en échangeant les rôles de I et J. Considérons d'autre part la surjection canonique $\psi : B \to (\mathbb{Z}/p\mathbb{Z})[X]$, $Q \mapsto \overline{Q} := Q \bmod p$. Elle est de noyau $J = pB$ et induit donc un isomorphisme $\psi' : B/J \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})[X]$. On a de plus clairement les égalités $\psi(I+J) = \psi(I) = (P)$, de sorte que ψ' induit une bijection $(J+I)/J \xrightarrow{\sim} (P)$, puis un isomorphisme

$$\psi'' : (B/J)/((I+J)/J) \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})[X]/(P).$$

Au final, on a détaillé une suite d'isomorphismes canoniques

$$(\mathbb{Z}/p\mathbb{Z})[X]/(P) \underset{\psi''}{\xleftarrow{\sim}} (B/J)/((I+J)/J) \underset{\text{can}}{\xrightarrow{\sim}} B/(I+J) \underset{\text{can}}{\xleftarrow{\sim}} (B/I)/((I+J)/I) \underset{\varphi''}{\xrightarrow{\sim}} A/pA.$$

Concrètement, l'isomorphisme $A/pA \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})[X]/(P)$ qui s'en déduit est l'unique morphisme d'anneaux envoyant, pour tout $Q \in \mathbb{Z}[X]$, l'élément $Q(\alpha) \bmod pA$ vers $\overline{Q}(X) \bmod P$. Cet isomorphisme envoie en particulier l'idéal $\mathrm{I}(Q)/pA$ sur (Q). Cela démontre le (iii) de la proposition, car $((\mathbb{Z}/p\mathbb{Z})[X]/(P))/(Q) \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})[X]/(Q)$ si $Q|P$, d'après le point (b) du rappel appliqué aux idéaux $(P) \subset (Q)$ de $(\mathbb{Z}/p\mathbb{Z})[X]$.

Démontrons maintenant le point (ii) de la proposition. Par la caractérisation des idéaux d'un quotient rappelée au (a) ci-dessus l'ensemble ordonné des idéaux de $k[X]/(P)$, où k est un corps et $P \in k[X]$, est en bijection naturelle avec celui des idéaux de $k[X]$ contenant P. Par principalité de $k[X]$, les idéaux de $k[X]$ contenant P sont les (Q) avec $Q \in k[X]$ divisant P, le générateur Q étant même unique s'il est choisi unitaire, et de plus $(Q) \subset (Q')$ si et seulement si $Q'|Q$. Le point (ii) de la proposition résulte donc du fait que l'isomorphisme $A/pA \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})[X]/(P)$ décrit plus haut envoie $\mathrm{I}(Q)/pA$ sur (Q).

□

4. Réalisation géométrique de $\mathcal{O}_K$: le plongement canonique

Fixons K un corps de nombres. Nous allons commencer par montrer comment réaliser $\mathcal{O}_K$ de manière naturelle comme un réseau d'un certain espace vectoriel réel de dimension $n = [K : \mathbb{Q}]$. Cela nous permettra non seulement de mieux comprendre sa structure, par exemple de retrouver l'existence de bases entières, mais aussi de lui appliquer la géométrie des nombres de Minkowski, d'où l'on tirera notamment la proposition 6.7.

Le premier exemple est le cas de $\mathbb{Z}$, qui est naturellement un réseau de $\mathbb{R}$. Un second exemple est celui des corps quadratiques imaginaires $K = \mathbb{Q}(\sqrt{d})$ avec d un rationnel < 0. En effet, on a vu que $\mathcal{O}_K$ est de la forme $\mathbb{Z} + \mathbb{Z}\alpha$ avec $\alpha \notin \mathbb{R}$: c'est en particulier un réseau de $\mathbb{C}$ (identifié à $\mathbb{R}^2$). Cette observation a par ailleurs été très utile à la compréhension des anneaux d'entiers quadratiques imaginaires.

Considérons maintenant le cas $K = \mathbb{Q}(\sqrt{2})$, pour lequel on a vu que $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}] = \mathbb{Z} + \mathbb{Z}\sqrt{2}$. On constate que $K \subset \mathbb{R}$, mais $\mathbb{Z} + \mathbb{Z}\sqrt{2}$ n'est pas discret dans

$\mathbb{R}$. En effet, sinon ce serait un réseau, donc de la forme $a\mathbb{Z}$ pour un réel $a > 0$. Mais les conditions $1 \in a\mathbb{Z}$ et $\sqrt{2} \in a\mathbb{Z}$ entraînent par quotient que $\sqrt{2} \in \mathbb{Q}$ ce qui est absurde. Il n'est pas difficile de vérifier qu'un sous-groupe de $\mathbb{R}$ qui n'est pas discret est en fait dense, de sorte que $\mathbb{Z}[\sqrt{2}]$ est en fait dense dans $\mathbb{R}$, ce qui n'est pas très commode pour visualiser ses éléments. On peut rétablir le caractère discret en considérant les deux plongements de $\mathbb{Q}(\sqrt{2})$ dans $\mathbb{R}$, à savoir l'identité et $a + b\sqrt{2} \mapsto a - b\sqrt{2}$. En effet, considérons l'application

$$\iota : \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{R}^2, a + b\sqrt{2} \mapsto (a + b\sqrt{2}, a - b\sqrt{2}),$$

a, b désignant ici des nombres rationnels. Cette application est injective et $\mathbb{Q}$-linéaire. Alors $\iota(\mathbb{Z} + \mathbb{Z}\sqrt{2}) = \mathbb{Z}\iota(1) + \mathbb{Z}\iota(\sqrt{2})$. Mais $\iota(1) = (1, 1)$ et $\iota(\sqrt{2}) = (\sqrt{2}, -\sqrt{2})$ sont non proportionnels dans $\mathbb{R}^2$, donc une $\mathbb{R}$-base, et $\iota(\mathbb{Z}[\sqrt{2}])$ est un réseau de $\mathbb{R}^2$. On peut donc voir via l'isomorphisme de groupes ι l'anneau $\mathbb{Z}[\sqrt{2}]$ comme un réseau de $\mathbb{R}^2$. Cette construction s'étend verbatim à tous les $\mathbb{Q}(\sqrt{d})$ avec $d > 0$.

Notons que si $d < 0$, il ne faut pas considérer les deux plongements complexes de $\mathbb{Q}(\sqrt{d})$ mais bien un seul. Par exemple, l'image de $\mathbb{Z}[i] \to \mathbb{C} \times \mathbb{C}$ par l'application $z \mapsto (z, \overline{z})$ est bien un sous-groupe discret mais ce n'est pas un réseau : il est engendré par 2 éléments dans un espace vectoriel réel de dimension 4.

Ces constructions se généralisent comme suit. On considère l'ensemble $\Sigma(K)$ des $n = [K : \mathbb{Q}]$ plongements de K dans $\mathbb{C}$. Si $\sigma \in \Sigma(K)$, on définit son conjugué complexe $\overline{\sigma} : x \mapsto \overline{\sigma(x)}$ ($z \mapsto \overline{z}$ désignant la conjugaison complexe dans $\mathbb{C}$), c'est encore un élément de $\Sigma(K)$. Par définition, l'application $\sigma \mapsto \overline{\sigma}$ est une involution de $\Sigma(K)$. Les points fixes de cette involution, disons Σ_1, sont les *plongements réels de* K, c'est-à-dire les $\sigma \in \Sigma(K)$ tels que $\sigma(K) \subset \mathbb{R}$. Par exemple, si $K = \mathbb{Q}(x)$ avec $x \in \overline{\mathbb{Q}}$ les plongements réels de K sont en bijection naturelle avec les conjugués de x qui sont des nombres réels (Lemme 5.9). Les plongements non réels venant par paires conjuguées, il sera commode de choisir une partie $\Sigma_2 \subset \Sigma(K) \backslash \Sigma_1$ telle que

$$\Sigma(K) = \Sigma_1 \coprod \Sigma_2 \coprod \overline{\Sigma}_2.$$

Il n'y a pas de choix de Σ_2 plus naturel que les autres a priori, et chacun ferait l'affaire dans la construction qui suit. Il sera même commode d'ordonner les éléments de Σ_1 et Σ_2. On pose traditionnellement

$$r_1(K) = |\Sigma_1|, \;\; r_2(K) = |\Sigma_2|$$

et on notera même $r_1 = r_1(K)$ et $r_2 = r_2(K)$ dans ce qui suit pour alléger les notations. On numérote enfin $\Sigma_1 = \{\sigma_1, \ldots, \sigma_{r_1}\}$ et $\Sigma_2 = \{\sigma_{r_1+1}, \ldots, \sigma_{r_1+r_2}\}$. On a $|\Sigma(K)| = n = r_1 + 2r_2$ (Lemme 5.9).

Définition 6.11. *Le plongement canonique de K est l'application $\iota : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ définie par*

$$\iota(x) = (\sigma_i(x))_{i=1,\ldots,r_1+r_2}.$$

C'est une application $\mathbb{Q}$-linéaire injective.

Notons que la $\mathbb{Q}$-linéarité de ι découle de celle des $\sigma \in \Sigma(K)$, ainsi que l'injectivité (une coordonnée suffirait d'ailleurs !). L'observation importante de ce paragraphe est alors la suivante.

Théorème 6.12. *$\iota(\mathcal{O}_K)$ est un réseau de $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$.*

Dans la suite, nous identifions $\mathbb{C}$ à $\mathbb{R}^2$ au moyen de la $\mathbb{R}$-base $1, i$. Cela nous donne une identification de $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ à $\mathbb{R}^n$ et y fixe également la mesure de Lebesgue.

LEMME 6.13. *Soit $e_1, \dots, e_n$ une $\mathbb{Q}$-base de K. Alors $\iota(e_1), \dots, \iota(e_n)$ est une $\mathbb{R}$-base de $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ qui engendre un réseau de covolume $2^{-r_2}|\mathrm{disc}_{K/\mathbb{Q}}(e_1, \dots, e_n)|^{\frac{1}{2}}$.*

DÉMONSTRATION — On considère la $\mathbb{R}$-base f de $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ constituée des $(0, \dots, 0, *, 0, \dots, 0)$ où $* = 1$ (resp. 1 ou i) s'il est à une place d'indice $\leq r_1$ (resp. sinon). Si $x \in K$, le vecteur $\iota(x)$ décomposé dans cette base est donc de la forme

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

Soit P la matrice des vecteurs $\iota(e_j)$ dans la base f. Si $r_2 = 0$, c'est-à-dire $\Sigma_1 = \Sigma(K)$, on constate que $|\det(P)| = |\det(\sigma_j(e_i))| = |\mathrm{disc}_{K/\mathbb{Q}}(e_1, \dots, e_n)|^{\frac{1}{2}} \neq 0$ (Proposition 5.17 (i) et (iii)), ce qui conclut dans ce cas. En général, on constate que si $\sigma \in \Sigma_2(K)$, on a la relation

$$\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix} \begin{pmatrix} \mathrm{Re}\ \sigma(e_1) & \cdots & \mathrm{Re}\ \sigma(e_n) \\ \mathrm{Im}\ \sigma(e_1) & \cdots & \mathrm{Im}\ \sigma(e_n) \end{pmatrix} = \begin{pmatrix} \sigma(e_1) & \cdots & \sigma(e_n) \\ \overline{\sigma}(e_1) & \cdots & \overline{\sigma}(e_n) \end{pmatrix}.$$

La relation $|\det \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}| = 2$ montre que l'on a

$$|\det(P)| = 2^{-|\Sigma_2|}|\det(\sigma_i(e_j))| = 2^{-r_2}|\mathrm{disc}_{K/\mathbb{Q}}(e_1, \dots, e_n)|^{\frac{1}{2}}.$$

□

DÉMONSTRATION — Démontrons maintenant le théorème 6.12. D'après le lemme 5.19, $\mathcal{O}_K$ contient une $\mathbb{Q}$-base de K, et l'image par ι d'une telle base est une $\mathbb{R}$-base de $V = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ d'après le lemme 6.13, donc le sous-groupe $\iota(\mathcal{O}_K)$ engendre V. Il ne reste qu'à vérifier que $\iota(\mathcal{O}_K)$ est discret.

Munissons V de sa norme sup. dans la base f de la démonstration du lemme 6.13. Soit $r > 0$ un réel. Si $x \in \mathcal{O}_K$ est tel que $|\iota(x)| < r$, alors $|\sigma(x)| < r$ pour tout $\sigma \in \Sigma_1$ et $|\mathrm{Re}\ \sigma(x)|, |\mathrm{Im}\ \sigma(x)| < r$ pour tout $\sigma \in \Sigma_2$. En particulier, $|\sigma(x)| < \sqrt{2}\,r$ pour tout $\sigma \in \Sigma(K)$. Mais x est annulé par

$$\chi_{x,K/\mathbb{Q}} = \prod_{\sigma \in \Sigma(K)} (X - \sigma(x)) \in \mathbb{Z}[X].$$

La borne précédente montre que les coefficients d'un tel polynôme sont bornés par un réel ne dépendant que de r. Comme ils sont de plus entiers, il n'y a qu'un nombre fini de $\chi_{x,K/\mathbb{Q}}$ possibles pour $x \in \mathcal{O}_K$ tel que $|\iota(x)| < r$, et donc qu'un nombre fini de tels x (qui sont racines de tels polynômes) : $\iota(\mathcal{O}_K)$ est discret. □

Mentionnons qu'à ce stade, nous obtenons une autre démonstration de l'existence d'une $\mathbb{Z}$-base à n éléments du groupe additif $\mathcal{O}_K$. En effet, ι étant injective elle définit un isomorphisme (additif) de $\mathcal{O}_K$ sur $\iota(\mathcal{O}_K)$. Mais ce dernier est un réseau de l'espace vectoriel réel $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \simeq \mathbb{R}^n$, on conclut donc par le théorème 2.4 de caractérisation algébrique des réseaux. En fait, cette preuve est essentiellement la même que celle donnée au chapitre 4, même si le point de vue plus géométrique de ce chapitre l'éclaircit substantiellement.

Via l'isomorphisme additif $\iota : \mathcal{O}_K \xrightarrow{\sim} \iota(\mathcal{O}_K)$, la théorie des réseaux admet des conséquences immédiates à la structure de $\mathcal{O}_K$ et de ses ordres. On observe notamment que si $A \subset \mathcal{O}_K$ est un sous-groupe quelconque contenant une $\mathbb{Q}$-base de K (par exemple un ordre), alors $\iota(A)$ est un sous-réseau de $\iota(\mathcal{O}_K)$ d'après la proposition 5.17. En particulier, A est d'indice fini $\frac{\mathrm{covol}(\iota(A))}{\mathrm{covol}(\iota(\mathcal{O}_K))}$ dans $\mathcal{O}_K$ et admet une $\mathbb{Z}$-base à n éléments. Cela justifie le (i) de la proposition-définition suivante.

PROPOSITION-DÉFINITION 6.14. *Soit K un corps de nombres et soit $A \subset \mathcal{O}_K$ un sous-groupe additif contenant une $\mathbb{Q}$-base de K.*

(i) A admet une $\mathbb{Z}$-base à $n := [K : \mathbb{Q}]$ éléments.

On note $\mathrm{disc}(A) \in \mathbb{Z}$ *le discriminant d'une $\mathbb{Z}$-base quelconque de A.*

(ii) On a la relation $|\mathrm{disc}(A)|^{1/2} = \mathrm{covol}(\iota(A))\ 2^{r_2(K)}$.

(iii) Si B est un sous-groupe de $\mathcal{O}_K$ contenant A alors A est d'indice fini dans B égal à $\frac{|\mathrm{disc}(A)|^{1/2}}{|\mathrm{disc}(B)|^{1/2}}$. En particulier, $\frac{|\mathrm{disc}(A)|}{|\mathrm{disc}(B)|} = |B/A|^2$ est le carré d'un entier.

DÉMONSTRATION — Le fait que $\mathrm{disc}(A)$ ainsi défini est indépendant du choix de la $\mathbb{Z}$-base de A découle des propositions 2.10 (ii) et 5.17 (ii). Il est entier d'après la dernière assertion du théorème 5.21 et donné par la formule (ii) par le lemme 6.13. Le (iii) est conséquence de la proposition 2.17. □

Notons en particulier la relation $\mathrm{covol}(\iota(\mathcal{O}_K))2^{r_2(K)} = |\mathrm{disc}(\mathcal{O}_K)|^{1/2}$ conséquence du (ii). Le résultat suivant généralise la proposition 4.12.

THÉORÈME 6.15. *Soient K un corps de nombres, A un ordre de K et $I \subset A$ un idéal non nul. Alors I est d'indice fini dans A et admet une $\mathbb{Z}$-base à $[K : \mathbb{Q}]$ éléments. En particulier, A est un anneau noethérien.*

DÉMONSTRATION — En effet, il suffit de voir que I contient une $\mathbb{Q}$-base de K par la proposition qui précède. Mais comme A est un ordre de K, il contient une $\mathbb{Q}$-base de K, disons $e_1, \ldots, e_n \in A$. Soit $x \in I$ non nul, alors $xe_1, \ldots, xe_n$ est une $\mathbb{Q}$-base de K constituée d'éléments de I. □

Ce théorème justifie l'importante définition qui suit.

DÉFINITION 6.16. *Si I est un idéal non nul de l'ordre A, on définit sa* norme $\mathrm{N}(I)$ *par la formule $\mathrm{N}(I) = |A/I|$. C'est un entier ≥ 1.*

La terminologie norme vient du lien qu'elle partage avec la norme de $K/\mathbb{Q}$. En effet, notons aussi $\mathrm{N} = \mathrm{N}_{K/\mathbb{Q}} : K \to \mathbb{Q}$ la norme de $K/\mathbb{Q}$. On rappelle que $\mathrm{N}(zz') = \mathrm{N}(z)\mathrm{N}(z')$ et que $\mathrm{N}(\mathcal{O}_K) \subset \mathbb{Z}$. De plus, $\mathrm{N}(z) = 0$ si, et seulement si, $z = 0$ car si $z \neq 0$ alors $1 = \mathrm{N}(1) = \mathrm{N}(z)\mathrm{N}(1/z)$.

PROPOSITION 6.17. *Pour tout idéal non nul $I \subset A$ et tout $z \in A$ non nul, $\mathrm{N}(zI) = |\mathrm{N}(z)|\mathrm{N}(I)$. En particulier, $\mathrm{N}(zA) = |\mathrm{N}(z)|$.*

Démonstration — (C'est une généralisation de la proposition 4.12) Soit

$$a = (a_1, \cdots, a_{r_1+r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$$

avec $a_i \neq 0$ pour tout i, et soit $d_a \in \mathrm{End}_{\mathbb{R}}(\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})$ la dilatation définie par $d_a((x_i)) = (a_i x_i)$. La formule du changement de variables montre que l'application d_a multiplie la mesure de Lebesgue par

$$n(a) := \prod_{i=1}^{r_1} |a_i| \prod_{i=1}^{r_2} |a_{r_1+i}|^2$$

(c'est évident !). Revenant aux notations de l'énoncé, on constate que $\iota(zI) = d_{\iota(z)}(\iota(I))$. Ainsi, $\mathrm{covol}(zI) = n(\iota(z))|\mathrm{covol}(\iota(I))$, mais $n(\iota(z))$ n'est autre que $|\mathrm{N}(z)|$. □

Nous avons tous les outils pour appliquer le lemme du corps convexe de Minkowski aux idéaux d'un ordre. Si $r \in \mathbb{R}$ et $n \geq 1$, on appelle *constante de Minkowski* la constante $C(r, n) = (\frac{4}{\pi})^r \frac{n!}{n^n}$.

Théorème 6.18. (Minkowski) *Soit A un ordre de K et soit I un idéal non nul de A. Il existe $x \in I$ non nul tel que $|\mathrm{N}(x)| \leq C(r_2, n) \cdot \mathrm{N}(I) \cdot |\mathrm{disc}(A)|^{1/2}$.*

Ce théorème entraîne la proposition 6.7 avec $C \leq C(r_2, n)|\mathrm{disc}(A)|^{1/2}$. En effet, le noyau de la projection canonique $A/xA \to A/I$ est exactement I/xA, de sorte que $|I/xA||A/I| = |A/xA|$. Mais $|A/I| = \mathrm{N}(I)$ et $|A/xA| = \mathrm{N}(xA) = |\mathrm{N}_{K/\mathbb{Q}}(x)|$ d'après la proposition 6.17, de sorte que l'énoncé ci-dessus s'écrit aussi $|I/Ax| \leq C(r_2, n)|\mathrm{disc}(A)|^{1/2}$. Le théorème entraîne donc également le corollaire :

Corollaire 6.19. (Borne de Minkowski) *Si A est un ordre d'un corps de nombres K alors*

$$C(A) \leq C(r_2, n)\, |\mathrm{disc}(A)|^{1/2}, \quad \text{où } n = [K : \mathbb{Q}] \text{ et } r_2 = r_2(K).$$

Démonstration — (du théorème) Nous allons appliquer le lemme du corps convexe de Minkowski au réseau $\iota(I)$ de $V = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Considérons la norme $|\cdot|$ sur V définie par

$$|(x_i)| = \sum_{i=1}^{r_1} |x_i| + 2 \sum_{i=r_1+1}^{r_1+r_2} |x_i|.$$

et pour tout réel $t > 0$ considérons $C_t = \{v \in V, |v| \leq t\}$ la boule fermée associée de centre 0 et de rayon t. Le fait qu'il s'agisse d'une norme est immédiat, et il en découle que C_t est convexe, compact et symétrique. Soit μ la mesure de Lebesgue sur V identifié à $\mathbb{R}^n$ comme plus haut.

Lemme 6.20. $\mu(C_t) = 2^{r_1}(\frac{\pi}{2})^{r_2} \frac{t^n}{n!}$.

Démonstration — En effet, désignons C_t par C_{t,r_1,r_2} pour bien mentionner la dépendance en r_1 et r_2, et posons $c(r_1, r_2) = \mu(C_{1,r_1,r_2})$ et $n = r_1 + 2r_2$. Par homothétie, $\mu(C_{t,r_1,r_2}) = c_{r_1,r_2} t^n$. De plus, si $r_1 > 0$ on constate par Fubini en intégrant selon la première coordonnée $x_1 \in [-1, 1]$ que

$$c_{r_1,r_2} = 2 \int_0^1 \mu(C_{1-t,r_1-1,r_2}) = 2c_{r_1-1,r_2} \int_0^1 (1-t)^{n-1} dt = \frac{2}{n} c_{r_1-1,r_2}.$$

Enfin, si $r_2 > 0$, on trouve de manière similaire en écrivant $x_{r_1+1} \in \mathbb{C}$ sous la forme $re^{i\theta}$:

$$c_{r_1,r_2} = 2\pi \int_0^{\frac{1}{2}} \mu(C_{1-2r,r_1,r_2-1}) r dr = 2\pi c_{r_1,r_2-1} \int_0^{\frac{1}{2}} (1-2r)^{n-2} r dr = \frac{\pi}{2n(n-1)} c_{r_1,r_2-1},$$

car $\int_0^1 (1-r) r^{n-2} dr = \frac{1}{n-1} - \frac{1}{n} = \frac{1}{n(n-1)}$. □

La pertinence de notre choix de $|.|$ vient de la relation qu'elle partage avec N. En effet, la moyenne arithmético-géométrique

$$(\prod_{i=1}^{r_1} |x_i| \prod_{i=r_1+1}^{r_1+r_2} |x_i|^2)^{\frac{1}{n}} \leq \frac{1}{n} (\sum_{i=1}^{r_1} |x_i| + 2 \sum_{i=r_1+1}^{r_1+r_2} |x_i|),$$

où les x_i sont dans $\mathbb{C}$, qui découle de la convexité de l'exponentielle réelle, entraîne

$$|\mathrm{N}(x)| \leq n^{-n} |\iota(x)|^n$$

pour tout $x \in K$. Pour conclure, on choisit $t > 0$ tel que $\mu(C_t) = 2^n \mathrm{covol}(\iota(I))$. Le lemme du corps convexe de Minkovski assure l'existence d'un élément de $\iota(x) \in \iota(I)$ non nul tel que $|\iota(x)| \leq t$, et donc tel que

$$|\mathrm{N}(x)| \leq n^{-n} t^n = \frac{n!}{2^{r_1} (\frac{\pi}{2})^{r_2} n^n} 2^n \mathrm{covol}(\iota(I)) = (\frac{4}{\pi})^{r_2} \frac{n!}{n^n} \mathrm{N}(I) 2^{r_2} \mathrm{covol}(\iota(A))$$

□

Terminons par un corollaire amusant du théorème 6.18, aussi dû à Minkowski.

COROLLAIRE 6.21. (Minkowski) *Si $K \neq \mathbb{Q}$ alors $|\mathrm{disc}(\mathcal{O}_K)| \geq \frac{\pi}{3} (\frac{3\pi}{4})^{n-1}$. En particulier, on a $\mathrm{disc}(\mathcal{O}_K) \neq \pm 1$.*

DÉMONSTRATION — On applique le théorème 6.18 à $A = I = \mathcal{O}_K$ et on utilise le fait que pour tout $x \in \mathcal{O}_K$ non nul, $\mathrm{N}(x)$ est entier non nul, et donc $|\mathrm{N}(x)| \geq 1$. Cela entraîne

$$|\mathrm{disc}(\mathcal{O}_K)| \geq C(r_2, n)^{-2} \geq a_n, \quad \text{avec} \quad a_n = C(\frac{n}{2}, n)^{-2},$$

car $r_2 \leq \frac{n}{2}$ et $\pi < 4$. Mais $a_2 = \frac{\pi^2}{4}$ et $\frac{a_{n+1}}{a_n} = \frac{\pi}{4}(1 + \frac{1}{n})^{2n} \geq \frac{3\pi}{4}$ pour $n > 1$, ce qui conclut. □

5. Exercices

D	2	9	22	39	61	88	120	157	199
h	0.90	1.90	2.98	3.97	4.97	5.97	6.97	7.97	8.98

TABLE 1. Quelques valeurs de $h = \frac{2}{\pi}\sqrt{D}$ à 10^{-2} près

EXERCICE 6.1. *(i) Soit D un entier $\equiv 0, 1 \bmod 4$ vérifiant $D < 0$. Vérifier que A_D est un ordre de $\mathbb{Q}(\sqrt{D})$ et que l'on a $\mathrm{disc}\, A_D = D$.*

(i) Soient $d \in \mathbb{Z}$, supposé < 0 et sans facteur carré, et $K = \mathbb{Q}(\sqrt{d})$. On pose $D = d$ si $d \equiv 1 \bmod 4$, et $D = 4d$ sinon. Rappeler pourquoi on a $\mathcal{O}_K = A_D$ et montrer plus généralement que les ordres de K sont exactement les anneaux de la forme A_{nD} avec $n \geq 1$.

EXERCICE 6.2. *On considère $\alpha = \frac{1+\sqrt{-19}}{2}$ et $A = \mathbb{Z}[\alpha]$.*

(i) Montrer que tout idéal de A est équivalent à un idéal contenant 1 ou 2.

(ii) En déduire que A est principal, bien que non euclidien.

EXERCICE 6.3. *On considère $\alpha = \sqrt{-5}$ et $A = \mathbb{Z}[\alpha]$.*

(i) Montrer que tout idéal de A est principal ou équivalent à l'idéal $I = 2A + (\alpha - 1)A$.

(ii) Montrer que I est non principal, en déduire que $|\mathrm{Cl}(A)| = 2$.

(iii) Montrer que $I^2 = (2)$ et en déduire que $\mathrm{Cl}(A) \simeq \mathbb{Z}/2\mathbb{Z}$.

(iv) En déduire que si J est un idéal non nul de A alors on a exclusivement soit J, soit IJ principal.

EXERCICE 6.4. *On considère $\alpha = \sqrt{-3}$ et $A = \mathbb{Z}[\alpha]$.*

(i) Montrer que tout idéal de A est principal ou équivalent à l'idéal $I = 2A + (\alpha - 1)A$.

(ii) Montrer que I est non principal, en déduire que $|\mathrm{Cl}(A)| = 2$.

(iii) Montrer que $I^2 = 2I$.

(iv) En déduire que $\mathrm{Cl}(A)$ n'est pas un groupe et décrire sa loi de composition.

(v) En déduire que si J est un idéal non nul de A alors IJ n'est jamais principal. Comparer avec l'exercice 6.3.

EXERCICE 6.5. *Soit $\alpha \in \mathbb{C}$ tel que $\alpha^3 = \alpha + 1$ et soit $A = \mathbb{Z}[\alpha]$.*

(i) Montrer que $\mathrm{disc}(A) = -23$.

(ii) En déduire que A est principal.

EXERCICE 6.6. *Montrer que $\mathrm{Cl}(\mathbb{Z}[\frac{1+\sqrt{-23}}{2}]) \simeq \mathbb{Z}/3\mathbb{Z}$.*

EXERCICE 6.7. *Soit $d \in \mathbb{Z}$ qui n'est pas un cube, soient $\alpha = \sqrt[3]{d}$ et $A = \mathbb{Z}[\alpha]$.*

(i) Montrer que $\mathrm{disc}(A) = -27d^2$.

On suppose maintenant $d = 2$. On donne la valeur $\frac{16}{\pi\sqrt{3}} \simeq 2.94$ à 10^{-2} près.

(ii) Montrer que tout idéal de A est soit principal soit équivalent à $I = 2A + \alpha A$ ou $J = 2A + \alpha^2 A$.

(iii) Montrer que I et J sont principaux.

(iv) En déduire que A est principal.

(v) En déduire que A est l'anneau des entiers de $\mathbb{Q}(\sqrt[3]{2})$.

EXERCICE 6.8. *Montrer que $\mathbb{Z}[e^{2i\pi/5}]$ est principal.*

EXERCICE 6.9. *Soit A un anneau intègre. Montrer que A est isomorphe à un ordre d'un corps de nombres si, et seulement si, le groupe additif de A est finiment engendré.*

EXERCICE 6.10. *On se propose de montrer que $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ est principal pour $d = -43, -67$ et -163.*

(i) Soient $P \in \mathbb{Z}[X]$ unitaire et p un nombre premier. On suppose que $P \bmod p$ est irréductible dans $(\mathbb{Z}/p\mathbb{Z})[X]$. Montrer que les idéaux de $A = \mathbb{Z}[X]/(P)$ contenant p^n sont les $p^i A$ avec $0 \leq i \leq n$.

(ii) Conclure.

EXERCICE 6.11. *Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire de degré > 1. On se propose de montrer que $\mathrm{disc}(P) \neq \pm 1$, à moins que $P = (X-n)(X-n+1)$ avec $n \in \mathbb{Z}$.*

(i) Montrer que si P est irréductible alors $\mathrm{disc}(P) \neq \pm 1$. On utilisera le Corollaire 6.21.

(ii) Conclure en utilisant l'exercice 5.4.

(iii) En déduire que $-4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 = \pm 1$ n'a pas de solution[4] $a, b, c \in \mathbb{Z}$.

(iv) Montrer que si P n'a pas de racine dans $\mathbb{Z}$, et si $\pm\mathrm{disc}(P)$ est premier, alors P est irréductible.

EXERCICE 6.12. (Principe des tiroirs) *On considère l'espace vectoriel $\mathbb{R}^n$ muni de la norme $|(x_i)| = \mathrm{Sup}_i |x_i|$ et on fixe un entier $N \geq 1$. Montrer que pour tout $v \in \mathbb{R}^n$, il existe un entier $1 \leq k \leq N^n$ et un $z \in \mathbb{Z}^n$ tels que $|kv - z| < \frac{1}{N}$. On pourra considérer l'application $\psi : \mathbb{R}^n \to [0,1[^n$, $(v_i) \mapsto (v_i - [v_i])$, et appliquer le principe des tiroirs aux éléments $\psi(kv)$ pour $k = 0, \ldots, N^n$.*

EXERCICE 6.13. *Soit A un ordre d'un corps de nombres K. On se propose de re-démontrer la finitude de $\mathrm{Cl}(A)$ en utilisant simplement le principe des tiroirs (Exercice 6.12). On fixe $e_1, \ldots, e_n \in A$ une $\mathbb{Q}$-base de K et on pose $\mathrm{N} = \mathrm{N}_{K/\mathbb{Q}}$.*

4. On pourrait vérifier qu'une telle équation a pourtant des solutions dans $\mathbb{Z}/N\mathbb{Z}$ pour tout entier N et dans $\mathbb{R}$! On pourrait également démontrer que les solutions rationnelles sont les $(a,b,c) = (3r, 3r^2 - 1, r^3 - r \pm 1/3)$ avec $r \in \mathbb{Q}$.

(i) Soit $C = \mathrm{Sup}_{i,\sigma\in\Sigma(K)}|\sigma(e_i)| \in \mathbb{R}_{>0}$. *Montrer que pour tout* $x_1, \ldots, x_n \in \mathbb{Q}$ *on a*

$$|\mathrm{N}(\sum_i x_i e_i)| \leq C \cdot (\mathrm{Sup}_i|x_i|)^n.$$

(ii) ("Division euclidienne approchée") Soit N *la partie entière supérieure de* $C^{1/n}$. *Montrer que pour tout* $z \in K$ *il existe* $u \in A$ *et* $1 \leq k \leq N^n$ *tels que* $|\mathrm{N}(kz - u)| < 1$.

(iii) En déduire que si I *est un idéal non nul de* A, *et si* $x \in I$ *est tel que* $|\mathrm{N}(x)|$ *est non nul minimal (justifier), alors* $(N^n)!I \subset xA \subset I$.

(iv) Conclure que $\mathrm{Cl}(A)$ *est fini.*

(v) On suppose par exemple $A = \mathbb{Z}[\sqrt{d}]$ *avec disons* $d < 0$. *Montrer que* $(N^2)!$ *vaut environ* $d!$ *et comparer avec la méthode du cours !*

Problème 6.1. (Lucy et Lily, d'après R. Schwartz)

Soit P *un pentagone régulier du plan (Lucy) dont on colorie les sommets de* 5 *couleurs différentes. On construit alors*[5] *une suite de polygones* $P_0, P_1, \ldots, P_n$ *telle que* $P_0 = P$ *et* P_{i+1} *est obtenu en faisant subir à* P_i *une réflexion d'axe l'un des côtés arbitraire de* P_i. *On ne note pas les étapes intermédiaires.*

Problème *: sachant que l'on connaît les coordonnées exactes du centre de* P_n, *comment faire pour le ramener à sa position initiale* P *?*

Pour formaliser le problème, on pourra supposer que $P \subset \mathbb{C}$ *a pour sommets les* ζ^k *avec* $\zeta = e^{\frac{2i\pi}{5}}$ *et* $k \in \mathbb{Z}$. *Dans ce cas, le centre de* P_n *est un élément donné de* $\mathbb{Z}[\zeta]$ *(pourquoi ?). On pourra introduire un plongement complexe* $\mathbb{Q}[\zeta] \to \mathbb{C}$ *qui n'est ni l'inclusion, ni la conjugaison complexe, ainsi que l'image de* P *par ce plongement (Lily), et utiliser que* $\iota(\mathbb{Z}[\zeta])$ *est discret !*

5. Voici une applet Java, par R. Schwartz, permettant de faire ceci : http://www.math.brown.edu/~res/Java/App12/test1.html.

Chapitre 7

Factorisation unique des idéaux

Nous avons constaté que bien peu d'anneaux de nombres algébriques sont factoriels. Leur défaut de factorialité se mesure notamment par la taille de l'ensemble $\mathrm{Cl}(A)$ des classes d'idéaux non nuls de l'anneau A, dont on a vu qu'il est toujours fini quand A est un ordre d'un corps de nombres. Nous poursuivons cette étude en montrant que si K est un corps de nombres, et si $A = \mathcal{O}_K$, la multiplication des idéaux sur $\mathrm{Cl}(A)$ définit une loi de groupe, ce qui en fait une structure très riche. Cela nous permettra notamment de démontrer le résultat central de la théorie : tout idéal non nul de $\mathcal{O}_K$ se factorise de manière unique comme produit d'idéaux premiers (Dedekind, Kummer).

Nous verrons que cette propriété rend parfois des services analogues à la propriété de factorialité. Son avantage est bien sûr qu'elle vaut pour tout corps de nombres K. C'est par exemple l'un des ingrédients essentiels dans la résolution par Kummer du problème de Fermat $x^n+y^n = z^n$ pour les exposants n qui sont des nombres premiers réguliers. Nous en donnerons des applications à l'étude des solutions entières de l'équation $y^2 = x^3 + k$, ainsi qu'à la détermination de $\mathrm{Cl}(\mathcal{O}_K)$.

Références : Les chapitres III et V du livre de Samuel. Le chapitre 12 du livre de Ireland et Rosen.

1. Le groupe des classes d'ideaux d'un corps de nombres

1.1. Groupe de Picard d'un anneau. Soit A un anneau commutatif unitaire intègre. Nous avons défini au chapitre précédent §1 l'ensemble $\mathrm{Cl}(A)$ des classes d'équivalence d'idéaux non nuls de A. Il est muni d'une loi de composition interne associative et commutative issue de la multiplication des idéaux, et la classe des idéaux principaux en est un élément neutre.

Définition 7.1. *Soit I un idéal non nul A. On dit que I est* inversible *si $[I]$ admet un inverse dans $\mathrm{Cl}(A)$, ou ce qui revient au même, s'il existe un idéal non nul J de A tel que IJ et principal.*

Par exemple, tout idéal principal non nul est inversible. On désigne par

$$\mathrm{Pic}(A) \subset \mathrm{Cl}(A)$$

le sous-ensemble des classes inversibles. Par construction, la multiplication des idéaux définit une structure de groupe abélien sur $\mathrm{Pic}(A)$, appelé *groupe de Picard de A*.

Si I et J sont des idéaux de A on dit que I divise J, et on écrit $I \mid J$, s'il existe un idéal $J' \subset A$ tel que $J = IJ'$. Si $I \mid J$ alors $J \subset I$, mais la réciproque ne vaut pas en général.

LEMME 7.2. *Soient I, J, J' des idéaux de A avec I inversible.*

(i) (Simplification) Si $IJ = IJ'$ alors $J = J'$.

(ii) (Contenir c'est diviser) $J \subset I$ si, et seulement si, I divise J, auquel cas il existe un unique idéal J' tel que $J = IJ'$.

DÉMONSTRATION — Soit I' est un idéal non nul tel que $II' = (\alpha)$ (et donc $\alpha \neq 0$). Si $IJ = IJ'$ alors en multipliant par I' on a $\alpha J = \alpha J'$ puis $J = J'$ en divisant par α. Cela montre le (i).

Pour le (ii), il est clair que si $J = IJ''$ pour un idéal $J'' \subset A$ alors $J \subset I$. Réciproquement soit $J \subset I$. On constate que

$$J = I(\alpha^{-1} I' J).$$

et que $\alpha^{-1} I' J$ est inclus dans A car $J \subset I$ et donc $JI' \subset II' = (\alpha)$. Ainsi, $J'' = \alpha^{-1} I' J$ est un idéal de A tel que $J = IJ''$. L'assertion d'unicité découle du (i). □

1.2. Cas des anneaux de nombres. Nous avons vu en exercices que

$$\mathrm{Cl}(\mathbb{Z}[\sqrt{-5}]) = \mathrm{Pic}(\mathbb{Z}[\sqrt{-5}]) = \mathbb{Z}/2\mathbb{Z},$$

l'idéal $(2, \sqrt{-5}+1)$ étant un générateur de carré (2). Cela fournit un premier exemple d'idéal inversible non principal. Nous avons vu aussi que $|\mathrm{Cl}(\mathbb{Z}[\sqrt{-3}])| = 2$, la classe non principale étant celle de l'idéal $I = (2, \sqrt{-3}+1)$, qui satisfait $I^2 = 2I$. L'idéal I est donc non inversible, car sinon on aurait $I = (2)$ ce qui est absurde car I n'est pas principal. Ainsi, $\mathrm{Pic}(\mathbb{Z}[\sqrt{-3}])$ est le groupe trivial.

THÉORÈME 7.3. *Si K est un corps de nombres alors tout idéal non nul de $\mathcal{O}_K$ est inversible, autrement dit $\mathrm{Cl}(\mathcal{O}_K) = \mathrm{Pic}(\mathcal{O}_K)$.*

Nous démontré au chapitre précédent que $\mathrm{Cl}(\mathcal{O}_K)$ est fini, il résulte donc de ce théorème que c'est un groupe abélien fini. On note

$$\mathrm{h}_K = |\mathrm{Cl}(\mathcal{O}_K)|$$

son cardinal et on l'appelle le *nombre de classes de K*. L'exemple de $\mathbb{Z}[\sqrt{-3}]$ montre que le théorème ci-dessus est spécifique à $\mathcal{O}_K$ et ne vaut pas pour les ordres généraux de K. On pourrait en fait démontrer que si A est un ordre de K dont tous les idéaux non nuls sont inversibles, alors $A = \mathcal{O}_K$!

Le lemme suivant est une forme faible provisoire du théorème ci-dessus, et sera un point clef de sa démonstration.

LEMME 7.4. *Si J, J' sont des idéaux non nuls de $\mathcal{O}_K$ tels que $JJ' = (\alpha)J'$ avec $\alpha \in \mathcal{O}_K$, alors $J = (\alpha)$.*

DÉMONSTRATION — Supposons pour commencer que $\alpha = 1$, i.e. $JJ' = J'$. Choisissons $f_1, \ldots, f_n$ une $\mathbb{Z}$-base de J', ce qui est loisible d'après le théorème 6.15. En écrivant $f_j \in JJ'$ on obtient des $m_{i,j} \in J$ avec $1 \leq i, j \leq n$ tels que $\forall j = 1, \ldots, n$, $f_j =$

$\sum_{i=1}^{n} m_{i,j} f_i$. C'est un système linéaire de taille n à coefficients complexes qui s'écrit aussi

$$(\mathrm{I}_n - (m_{i,j})) \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Comme les f_j sont non nuls on obtient que $\det(\mathrm{I}_n - (m_{i,j})) = 0$. Autrement dit $Q(1) = 0$ où Q est le polynôme caractéristique de $(m_{i,j})$. Mais J étant un idéal, on observe par un développement brutal que tous les coefficients non dominants de Q sont dans J, et donc $Q(1) \in 1 + J$. Comme $Q(1) = 0$, on a $1 \in J$, puis $J = A$, ce que l'on voulait démontrer (cet argument s'appelle le "lemme de Nakayama").

Retournons maintenant au cas d'un $\alpha \in \mathcal{O}_K$ général (observons que jusque là nous n'avons pas utilisé de spécificité de $\mathcal{O}_K$, l'argument ci-dessus étant valable dans tout ordre). Pour tout $y \in J$ on a $\frac{y}{\alpha} J' \subset J'$, donc $\frac{y}{\alpha} \in \overline{\mathbb{Z}} \cap K = \mathcal{O}_K$ d'après le critère d'intégralité du chapitre 1 (Proposition 1.16) et le fait que les idéaux de $\mathcal{O}_K$ admettent une $\mathbb{Z}$-base finie (Théorème 6.15). Ainsi, $J'' = \alpha^{-1} J$ est un idéal de $\mathcal{O}_K$, et la relation de l'énoncé s'écrit alors $J''J' = J'$. Le cas $\alpha = 1$ s'applique et donne $J'' = \mathcal{O}_K$, et donc $J = (\alpha)$. □

Démonstration — (du théorème) Soit I un idéal non nul de A. Pour voir qu'il est inversible, il suffit de démontrer qu'il existe un entier $n \geq 1$ tel que I^n est principal, car alors $[I][I^{n-1}] = [A]$. Mais les $\mathrm{h}_K + 1$ idéaux I^i avec $i = 0, \ldots, \mathrm{h}_K$ ne peuvent appartenir à des classes différentes, on peut donc trouver $0 \leq i < j \leq \mathrm{h}_K$ tels que

$$I^i \sim I^j.$$

Soient $x, y \in \mathcal{O}_K$ non nuls tels que $xI^i = yI^j$. On écrit ceci sous la forme $(yI^{j-i})I^i = (x)I^i$ et le lemme précédent conclut donc que $(y)I^{j-i} = (x)$, et donc que I^{j-i} est principal : l'entier $n = j - i$ convient. □

Le théorème 7.3 admet plusieurs corollaires fondamentaux dans l'étude de l'arithmétique de $\mathcal{O}_K$. D'une part, on déduit du lemme 7.2 que :

Corollaire 7.5. *Soient I, J, J' des idéaux non nuls de $\mathcal{O}_K$.*

(i) (Simplification) *Si $IJ = IJ'$ alors $J = J'$.*

(ii) (Contenir c'est diviser) *$I \subset J$ si et seulement J si divise I.*

D'autre part, le théorème de Lagrange appliqué au groupe abélien fini $\mathrm{Cl}(\mathcal{O}_K)$ entraîne que

Corollaire 7.6. *Pour tout idéal non nul I de $\mathcal{O}_K$, l'idéal I^{h_K} est principal où $\mathrm{h}_K = |\mathrm{Cl}(\mathcal{O}_K)|$.*

La détermination de h_K et de la structure de $\mathrm{Cl}(\mathcal{O}_K)$, K étant un corps de nombres donné, est très loin d'être résolue en général, malgrès ses multiples applications. Par exemple, $\mathrm{h}_K = 1$ si, et seulement si, $\mathcal{O}_K$ est factoriel, mais on ne sait toujours pas si une infinité de corps de nombres K ont cette propriété !

2. Idéaux premiers des ordres des corps de nombres

Notre objectif est désormais de démontrer que tout idéal de $\mathcal{O}_K$ admet une décomposition unique comme produit d'idéaux premiers. Cela nous oblige d'une part à quelques rappels et sorites généraux sur les idéaux premiers et maximaux, et d'autre part si possible de les déterminer dans le cas de $\mathcal{O}_K$. À ce stade il sera aussi instructif de travailler avec un ordre général. Fixons pour commencer un anneau commutatif unitaire A quelconque.

DÉFINITION 7.7. *Un idéal $P \subset A$ est dit premier si $P \neq A$ et si pour tout $a, b \in P$, la relation $ab \in P$ entraîne $a \in P$ ou $b \in P$. De manière équivalente, un idéal $P \subset A$ est premier si et seulement si l'anneau quotient A/P est intègre.*

Donnons quelques exemples :

(a) L'idéal nul $\{0\}$ est premier si, et seulement si, l'anneau A est intègre.

(b) Si A est intègre et si $\pi \in A$ est non nul, il suit immédiatement des définitions que πA est premier si, et seulement si, l'élément π est premier au sens du Chapitre 4 §1, de sorte que la notion d'idéal premier est la généralisation naturelle de celle d'élément premier dans un anneau.

(c) (suite) En particulier, dans un anneau principal (et donc factoriel) les idéaux premiers non nuls sont exactement ceux engendrés par un élément irréductible. Par exemple, les idéaux premiers non nuls de $\mathbb{Z}$ sont les $p\mathbb{Z}$ avec p premier, et ceux de $k[X]$ avec k un corps sont les (P) avec $P \in k[X]$ irréductible.

(d) Soient $\alpha \in \overline{\mathbb{Z}}$, $A = \mathbb{Z}[\alpha]$ et p un nombre premier. Soit $Q \in (\mathbb{Z}/p\mathbb{Z})[X]$ un diviseur de $\overline{\Pi}_{\alpha,\mathbb{Q}} \in (\mathbb{Z}/p\mathbb{Z})[X]$ et soit $\mathrm{I}(Q)$ l'idéal défini dans la proposition 6.10. Le (iii) de cette proposition affirme que $A/\mathrm{I}(Q) \simeq (\mathbb{Z}/p\mathbb{Z})[X]/(Q)$, ainsi $\mathrm{I}(Q)$ est premier si, et seulement si, Q est irréductible, d'après l'exemple (c).

REMARQUE 7.8. L'exemple (d) montre que les idéaux premiers de $\mathbb{Z}[\alpha]$ contenant un nombre premier p donné sont en bijection naturelle avec les facteurs irréductibles de $\overline{\Pi}_{\alpha,\mathbb{Q}}$ dans $(\mathbb{Z}/p\mathbb{Z})[X]$. On est donc ramené pour les déterminer à factoriser un polynôme $P \in \mathbb{Z}[X]$ donné dans $(\mathbb{Z}/p\mathbb{Z})[X]$, ce qui est un problème fini. Il existe un algorithme fameux pour cela dû à Berlekamp, qui permet par exemple de factoriser avec un ordinateur en moins d'une seconde un polynôme de degré 100 modulo un nombre premier à 40 chiffres. En revanche, un polynôme $P \in \mathbb{Z}[X]$ étant donné c'est en général un problème très difficile de répondre aux questions du type : "Quels sont les nombres premiers p tels que $P \bmod p$ admet une racine dans $\mathbb{Z}/p\mathbb{Z}$?". Par exemple, si $P = X^2 - a$ c'est essentiellement la loi de réciprocité quadratique ! Ce problème général, de formulation élémentaire, est l'un des problèmes centraux actuellement dans toute la théorie algébrique des nombres, et c'est d'ailleurs l'un des chemins qui mène au fameux "programme de Langlands".

Donnons deux propriétés importantes générales des idéaux premiers.

PROPOSITION 7.9. *Soit A un anneau et soit P un idéal premier de A.*

(i) Si I et J sont des idéaux de A tels que $P \supset IJ$, alors $P \supset I$ ou $P \supset J$.

(ii) Si B est un sous-anneau de A, alors $B \cap P$ est un idéal premier de B.

Démonstration — Si $I \not\subset P$, il existe $x \in I \backslash P$. Si $y \in J$, alors $xy \in P$, et donc $y \in P$: on a $J \subset P$, ce qui prouve le (i). Le (ii) est ... évident ! □

Une source générale d'idéaux premiers est la notion d'idéaux maximaux pour l'inclusion.

Définition 7.10. *Un idéal $I \subset A$ d'un anneau est dit maximal si $I \neq A$ et si les seuls idéaux $J \subset A$ contenant I sont A et I. Il est équivalent de demander que l'anneau A/I est un corps.*

Justifions la dernière assertion. Rappelons que $J \mapsto J/I$ induit une bijection entre idéaux de A contenant I et idéaux de l'anneau quotient A/I. Cette bijection préserve manifestement les inclusions : si $J, J' \supset I$ alors $J \subset J'$ si, et seulement si, $J/I \subset J'/I$. De plus, elle fait correspondre l'idéal trivial A avec l'idéal trivial A/I. Ainsi, $I \neq A$ est maximal pour l'inclusion si, et seulement si, l'anneau quotient A/I a pour seuls idéaux 0 et A/I. Mais les seuls anneaux commutatifs unitaires k qui ont exactement deux idéaux, à savoir 0 et k, sont les corps. En effet, si k est un corps tout élément non nul est inversible, donc engendre l'idéal k. Réciproquement, si les seuls idéaux de k sont 0 et k, tout $x \in k$ non nul engendre l'idéal k et donc il existe $y \in k$ tel que $xy = 1$: k est un corps.

Un corps étant intègre, c'est un fait général que *tout idéal maximal est premier*. La réciproque est toutefois fausse en général : dans un anneau intègre A qui n'est pas un corps, $\{0\}$ est premier mais n'est pas maximal. C'est cependant la seule nuance dans le cas des ordres des corps de nombres.

Proposition 7.11. *Soit A un ordre d'un corps de nombres.*

(i) (Existence) *Tout idéal de A distinct de A est inclus dans un idéal maximal (donc premier).*

(ii) (Maximalité) *Tout idéal premier non nul de A est maximal.*

Démonstration — Vérifions le (i). Soit $I \neq A$ un idéal non nul de A. On a déjà vu que A/I est fini (Thm. 6.15). En particulier, il n'a qu'un nombre fini d'idéaux, et tout idéal strict de A/I dont le cardinal maximal est un idéal maximal de A/I. Son image inverse dans A définit donc un idéal maximal de A contenant I. (En fait l'énoncé du (i) est vrai pour tout anneau A, mais sa démonstration nécessite l'axiome du choix.)

Montrons le (ii). Soit P un idéal premier non nul de A. Alors A/P est un anneau intègre fini : c'est donc un corps ! En effet, soit B un anneau intègre fini, et soit $b \in B$ non nul. La multiplication par b est une injection $B \to B$ par intégrité : c'est donc une bijection pour des raisons de cardinal. On peut donc trouver $b' \in B$ tel que $bb' = 1$. □

Le résultat suivant est une classification grossière des idéaux premiers des ordres des corps de nombres. Il peut être vu comme une généralisation de la détermination rappelée plus haut des idéaux premiers de $\mathbb{Z}$, ou encore de celle de $\mathbb{Z}[i]$ vue en exercices.

THÉORÈME 7.12. *Soit A un ordre d'un corps de nombres K.*

(i) Si P est un idéal premier non nul de A, alors P contient un unique nombre premier $p \in \mathbb{Z}$. On a $P \cap \mathbb{Z} = p\mathbb{Z}$ et A/P est un corps fini à p^n éléments avec $n \leq [K : \mathbb{Q}]$.

(ii) Réciproquement, pour tout nombre premier p l'ensemble des idéaux premiers de A contenant p est fini et non vide.

DÉMONSTRATION — Soit p un nombre premier. Les idéaux de A contenant p (i.e. pA) sont en bijection avec les idéaux de l'anneau A/pA. Ce dernier a exactement $p^{[K:\mathbb{Q}]}$ éléments d'après le lemme 6.8. Il est donc non nul et fini. Il n'y a donc qu'un nombre fini d'idéaux de A contenant p. L'idéal pA étant strict car $A/pA \neq 0$, il est contenu dans un idéal premier d'après la prop. 7.11 (i), ce qui démontre le (ii). De plus, si P est un idéal premier de A contenant p, l'homomorphisme d'anneaux canonique $A/pA \to A/P$ est surjectif, entre deux anneaux finis, donc $|A/P|$ divise $|A/pA| = p^{[K:\mathbb{Q}]}$ (Lemme 6.8). Il ne reste qu'à démontrer que tout idéal premier non nul de A contient un, et un seul, nombre premier.

Observons d'abord que si I est un idéal non nul de A, alors $I \cap \mathbb{Z} \neq \{0\}$. En effet, si $x \in I$ est non nul, il existe un polynôme unitaire $P \in \mathbb{Z}[X]$ tel que $P(x) = 0$ et $P(0) \neq 0$ (sans quoi on peut remplacer P par P/X^d où d est l'ordre d'annulation de P en 0). L'équation $P(x) = 0$ s'écrit alors aussi $P(0) = \sum_{i=1}^{m} a_i x^i$ où les a_i sont dans $\mathbb{Z}$, et donc $P(0) \in I$.

Ainsi, si P est un idéal premier de A, alors $P \cap \mathbb{Z}$ est un idéal premier de $\mathbb{Z}$ d'après le lemme 7.9, non nul d'après l'observation précédente : il est donc de la forme $p\mathbb{Z}$ avec p premier. Cet idéal contient un seul nombre premier : le nombre p. □

3. L'anneau $\mathcal{O}_K$ est de Dedekind.

3.1. Anneaux de Dedekind. On dira qu'un idéal I d'un anneau A est *strict* si $I \neq A$ et $I \neq 0$.

DÉFINITION 7.13. *Un anneau de Dedekind est un anneau intègre noethérien tel que pour tout idéal strict $I \subset A$, il existe un unique entier $n \geq 1$ et des idéaux premiers $P_1, \ldots, P_n$ uniques à permutation près tels que $I = P_1 \cdots P_n$.*

Cette propriété de factorisation des idéaux est aussi appelée *propriété de Dedekind*. Les anneaux principaux sont de Dedekind, mais il y en a bien d'autres. Du point de vue des idéaux, un anneau de Dedekind A se comporte de manière très similaire aux anneaux factoriels, les idéaux premiers jouant le rôle des éléments premiers. La situation est même plus simple car il n'y a pas dans le langage des idéaux à s'inquiéter des unités de A.

THÉORÈME 7.14. (Kummer, Dedekind) *Pour tout corps de nombres K, l'anneau $\mathcal{O}_K$ est de Dedekind.*

DÉMONSTRATION — On a déjà vu que $\mathcal{O}_K$ est noethérien (Théorème 6.15).

LEMME 7.15. *Soient A un ordre d'un corps de nombres, et $I \subset J$ deux idéaux non nuls de A. Alors $\mathrm{N}(J)$ divise $\mathrm{N}(I)$, et $\mathrm{N}(J) = \mathrm{N}(I)$ si, et seulement si, $I = J$.*

DÉMONSTRATION — En effet, la surjection canonique $A/I \to A/J$, qui est en particulier un morphisme de groupes additifs sous-jacents, a pour noyau J/I. On a donc $\mathrm{N}(I) = \mathrm{N}(J) \cdot |J/I|$, ce qui conclut. □

.

Vérifions tout d'abord l'existence. Supposons qu'il existe un idéal strict I de $\mathcal{O}_K$ qui n'est pas produit fini d'idéaux premiers. On peut alors considérer un tel idéal dont la norme est minimale. En particulier, I n'est pas maximal (car il serait premier). La proposition 7.11 montre qu'il existe un idéal maximal P de $\mathcal{O}_K$ contenant I. L'inversibilité de P montre qu'il existe un idéal Q de $\mathcal{O}_K$ tel que $I = QP$. On a évidemment $I \subset Q$, et même $I \neq Q$ par inversibilité de Q, le lemme ci-dessus assure donc $\mathrm{N}(Q) < \mathrm{N}(I)$. Mais Q n'est pas produit fini d'idéaux premiers car I le serait alors aussi, une contradiction.

Montrons l'unicité. Observons tout d'abord qu'un produit d'un nombre fini d'idéaux premiers est inclus dans chacun d'eux et en particulier toujours distinct de $\mathcal{O}_K$. Supposons donc $P_1 \cdots P_n = Q_1 \cdots Q_m$ où $m, n \geq 1$ sont des entiers et où les P_i et Q_j sont des idéaux premiers de $\mathcal{O}_K$. En particulier, $Q_1 \cdots Q_m \subset P_1$. Le lemme 7.9 entraîne donc qu'il existe $i \in \{1, \ldots, m\}$ tel que $P_1 \supset Q_i$. Mais Q_i est premier non nul donc maximal d'après la proposition 7.11 (ii), puis $P_1 = Q_i$. Mais on peut alors simplifier l'égalité par P_1. On en déduit par induction $m = n$ et qu'il existe $\sigma \in \mathfrak{S}_n$ tel que $Q_i = P_{\sigma(i)}$ pour tout $i = 1, \ldots, n$. □

Comme nous le verrons, ce théorème a de multiples conséquences. De manière similaire à la théorie des anneaux factoriels, il est parfois commode d'introduire la notion de valuation d'un idéal non nul I de $\mathcal{O}_K$ en un idéal premier P : c'est le nombre $v_P(I)$ de fois que l'idéal P intervient dans la décomposition de I. C'est donc 0 si, et seulement si, P ne divise pas I, ou ce qui revient au même, si $I \not\subset P$ (ce qui est le cas de tous les idéaux premiers exceptés un nombre fini par le théorème). On a toujours $I = \prod_P P^{v_P(I)}$ le produit étant fini en un sens évident. L'assertion d'unicité de la décomposition s'écrit alors $v_P(IJ) = v_P(I) + v_P(J)$ si I et J sont des idéaux non nuls. Enfin, I divise J si, et seulement si, $v_P(I) \leq v_P(J)$ pour tout idéal premier P non nul.

EXEMPLE 7.16. (pgcd et ppcm d'idéaux) Ces observations on notamment des conséquences sur les notions de pgcd et ppcm au sens des idéaux. En effet, soit I et J deux idéaux de $\mathcal{O}_K$, on constate que l'idéal $I + J$ est le plus petit idéal contenant (=divisant) I et J, il mérite alors bien son nom de pgcd de I et J. La propriété de Dedekind entraîne

$$I + J = \prod_P P^{\mathrm{Min}(v_P(I), v_P(J))}.$$

De même, $I \cap J$ apparaît comme le ppcm de I et J, et pour lequel on a une formule analogue avec des Max.

3.2. Application à la décomposition ... des nombres premiers ! Au point où nous en sommes, il nous reste à expliquer comment décomposer explicitement un idéal donné en produit d'idéaux premiers. Un cas particulièrement intriguant est de comprendre la décomposition de $p\mathcal{O}_K$ quand $p \in \mathbb{Z}$ est un nombre premier usuel. Nous avons vu dans les exercices que pour décomposer un élément en produit d'irréductibles dans un anneau de nombres, une bonne méthode consiste à déterminer la norme de l'élément, puis de chercher les diviseurs de cette norme qui sont des normes d'éléments de l'anneau. Une stratégie similaire fonctionne pour les idéaux. L'outil clé suivant éclaircit considérablement le problème, car on a vu que tout idéal premier non nul est de norme une puissance d'un nombre premier.

THÉORÈME 7.17. *(i)* (Multiplicativité de la norme) *Si I et J sont des idéaux non nuls de $\mathcal{O}_K$ alors* $\mathrm{N}(IJ) = \mathrm{N}(I)\mathrm{N}(J)$.

(ii) Si $P \neq 0$ est un idéal premier de $\mathcal{O}_K$ alors $\mathrm{N}(P)$ *est une puissance de l'unique nombre premier $p \in P$.*

(iii) Si $I \neq 0$ est un idéal, alors I divise l'idéal $(\mathrm{N}(I))$.

DÉMONSTRATION — Le (ii) est le point (iii) du théorème 7.12. Pour le (iii), on observe que le groupe abélien fini A/I est annulé par son cardinal $\mathrm{N}(I)$ (Lagrange), donc $\mathrm{N}(I).1 \in I$, puis I divise $\mathrm{N}(I)$ car I est inversible.

Il reste à vérifier le (i). D'après le théorème précédent, il suffit de démontrer que si les P_i sont des idéaux premiers non nuls (en nombre fini), alors on a $\mathrm{N}(\prod_i P_i) = \prod_i \mathrm{N}(P_i)$. Soient I et P des idéaux non nul de $\mathcal{O}_K$ avec P premier. Nous allons montrer $\mathrm{N}(IP) = \mathrm{N}(I)\mathrm{N}(P)$, ce qui conclura la démonstration.

L'inclusion $IP \subset I$ entraîne $\mathrm{N}(IP) = \mathrm{N}(I)|I/IP|$ d'après le Lemme 7.15, on veut donc montrer $\mathrm{N}(P) = |I/IP|$. Observons que les seuls idéaux Q de $\mathcal{O}_K$ tels que $I \,|\, Q \,|\, IP$, i.e. $IP \subset Q \subset I$, sont I et IP puisque P est premier. Ainsi, si l'on fixe $x \in I \backslash IP$ on a $IP + (x) = I$. On considère l'application

$$\mathcal{O}_K \to I/PI,\ a \mapsto ax + PI.$$

Cette application est additive, surjective, et son noyau est $S = \{a \in \mathcal{O}_K, ax \in PI\}$, qui est même un idéal de $\mathcal{O}_K$. Il contient P, c'est donc P ou $\mathcal{O}_K$ par maximalité de P. Mais $1 \notin S$ car $x \notin PI$, et donc $S = P$. Le morphisme de groupes ci-dessus se factorise donc en un isomorphisme de groupes additifs $\mathcal{O}_K/P \xrightarrow{\sim} I/PI$, d'où $\mathrm{N}(P) = |I/PI|$. □

THÉORÈME 7.18. *Soit $\alpha \in \overline{\mathbb{Z}}$. On suppose que l'anneau des entiers de $\mathbb{Q}(\alpha)$ est l'anneau $A = \mathbb{Z}[\alpha]$. Soient p un nombre premier et $P = \overline{\Pi_{\alpha,\mathbb{Q}}} \in (\mathbb{Z}/p\mathbb{Z})[X]$ la réduction modulo p de $\Pi_{\alpha,\mathbb{Q}}$. Écrivons $P = \prod_i P_i^{e_i}$ où les $P_i \in (\mathbb{Z}/p\mathbb{Z})[X]$ sont irréductibles unitaires deux à deux distincts. Alors les idéaux premiers de A contenant p sont les* $\mathrm{I}(P_i)$ (Prop. 6.10) *et $pA = \prod_i \mathrm{I}(P_i)^{e_i}$.*

DÉMONSTRATION — Rappelons que d'après la proposition 6.10, on dispose d'une bijection $Q \mapsto \mathrm{I}(Q)$ entre l'ensemble des diviseurs unitaires de P et celui des idéaux contenant, i.e. divisant, l'idéal pA. On a déjà observé que $\mathrm{I}(Q)$ est premier si, et

seulement si, Q est irréductible (exemple (d) §2). Ainsi, il existe des entiers $n_i \geq 1$ tels que

$$pA = \prod_i \mathrm{I}(P_i)^{n_i}$$

et il ne reste qu'à voir que $n_i = e_i$ pour tout i. Considérons l'ensemble X_i des idéaux I divisant pA tels que $I \subsetneq \mathrm{I}(P_j)$ pour $j \neq i$ (i.e. $\mathrm{I}(P_j)$ ne divise pas I si $i \neq j$). La propriété de Dedekind assure que X_i est la famille strictement croissante d'idéaux

$$\mathrm{I}(P_i)^{n_i} \subsetneq \mathrm{I}(P_i)^{n_i-1} \subsetneq \cdots \subsetneq \mathrm{I}(P_i).$$

Mais par construction, la bijection $Q \mapsto \mathrm{I}(Q)$ satisfait $\mathrm{I}(Q) \subset \mathrm{I}(Q')$ si, et seulement si, $Q'|Q$. On en déduit que X_i est également la famille croissante

$$\mathrm{I}(P_i^{e_i}) \subsetneq \mathrm{I}(P_i^{e_i-1}) \subsetneq \cdots \subsetneq \mathrm{I}(P_i),$$

et donc que $n_i = e_i$ et que pour tout $m \leq e_i$ on a $\mathrm{I}(P_i^m) = \mathrm{I}(P_i)^m$. □

Mentionnons que lorsque tous les e_i sont égaux à 1, la conclusion du théorème vaut encore même si A n'est pas supposé égal à l'anneau des entiers de $\mathbb{Q}(\alpha)$: voir le Problème 7.1 (i) et (ii) pour un démonstration très élémentaire de ce résultat.

Le polynôme $X^2 + aX + b \in \mathbb{Z}[X]$, de discriminant $D = a^2 - 4b$, est irréductible modulo p si, et seulement si, D est un carré modulo $4p$, et admet une racine double modulo p si, et seulement si, p divise D (Exercice 1.3). D'après la proposition 5.23, le théorème précédent s'applique donc aux corps quadratiques $\mathbb{Q}(\sqrt{d})$ où $d \in \mathbb{Z}\backslash\{0, 1\}$ est sans facteur carré, et s'écrit :

Corollaire 7.19. *Soit $K = \mathbb{Q}(\sqrt{d})$, $p \in \mathbb{Z}$ un nombre premier, et $D = \mathrm{disc}(\mathcal{O}_K)$, alors :*

(i) (Cas "ramifié") Si $p|D$, il existe un unique idéal premier $P \subset \mathcal{O}_K$ contenant p, et $(p) = P^2$.

(ii) (Cas "inerte") Si D n'est pas un carré modulo $4p$, l'idéal (p) est premier.

(iii) (Cas "décomposé") Si $(p, D) = 1$ et D est un carré modulo $4p$, alors $(p) = PP'$ où P et P' sont deux idéaux premiers distincts.

Ce dernier corollaire peut également se vérifier par calcul direct à partir de la proposition 6.10.

4. De l'utilité de la décomposition des idéaux

Il se trouve que cette décomposition des idéaux en produit d'idéaux premiers rend en pratique des services comparables à la propriété sensiblement plus forte de factorialité. Une illustration fameuse de ceci est le théorème suivant dû à Kummer :

Théorème 7.20. *(Kummer, 1850) Si le nombre premier impair p ne divise pas le nombre de classes de $\mathbb{Q}(e^{\frac{2i\pi}{p}})$ alors l'équation de Fermat $x^p + y^p = z^p$ n'admet pas de solution $x, y, z \in \mathbb{Z}$ avec $xyz \neq 0$.*

Nous ne démontrerons pas ce résultat qui est difficile. Une variante faible, dite aussi "premier cas de l'équation de Fermat", qui exclut seulement les solutions telles que $xyz \neq 0 \bmod p$ est cependant tout à fait accessible à ce stade du cours (voir le chapitre 17 du livre de Ireland et Rosen).

DÉFINITION 7.21. *Un nombre premier p tel que p divise $\mathrm{h}_{\mathbb{Q}(e^{\frac{2i\pi}{p}})}$ est appelé irrégulier.*

Une seconde découverte majeure de Kummer est d'avoir démontré le critère surprenant suivant d'irrégularité : le nombre premier $p > 3$ est irrégulier si et seulement s'il divise le numérateur de l'un au moins des nombres de Bernoulli $\mathrm{B}_2, \mathrm{B}_4, \ldots, \mathrm{B}_{p-3}$. On rappelle que ces nombres B_k peuvent être définis par la série génératrice

$$\frac{t}{e^t - 1} = \sum_{k \geq 0} \mathrm{B}_k \frac{t^k}{k!}.$$

Les B_k s'annulent si k est impair > 1, et sont intimement liés à la fonction ζ de Riemann par la formule d'Euler $\zeta(k) = (-1)^{k/2+1} \frac{\mathrm{B}_k (2\pi)^k}{2\, k!}$ pour tout entier $k \geq 2$ pair.

Je renvoie à la table qui suit pour les premières valeurs. Le premier nombre premier irrégulier qui apparaît est donc 691, qui divise B_{12}. Ce n'est pas le plus petit... qui est d'après cette table le nombre 37, divisant B_{32}. Il est aisé de vérifier que les nombres premiers irréguliers plus petits que 200 sont exactement $37, 59, 67, 101, 103, 131, 149$ et 157. On voit alors que le théorème de Kummer entraîne celui de Fermat pour de nombreux exposants p ! On peut montrer en revanche que $\mathrm{h}_{\mathbb{Q}(e^{\frac{2i\pi}{p}})} = 1$ si, et seulement si, $p < 23$ (voir les exercices pour les cas $p \leq 7$ et $p = 23$) : on voit bien l'intêret des résultats de Kummer. Les nombres premiers irréguliers sont encore l'objet de nombreuses recherches. On sait par exemple qu'il y en a une infinité mais on ne sait pas s'il y a un nombre infini de nombre premiers qui ne sont pas irréguliers. On ne sait pas non plus s'il existe des nombres premiers p tels que p^2 divise le numérateur de B_k pour $2 \leq k \leq p - 3$.

k	B_k	k	B_k	k	B_k	k	B_k
2	$\frac{1}{6}$	10	$\frac{5}{66}$	18	$\frac{43867}{798}$	26	$\frac{13 \cdot 657931}{6}$
4	$-\frac{1}{30}$	12	$-\frac{691}{2730}$	20	$-\frac{283 \cdot 617}{330}$	28	$-\frac{7 \cdot 9349 \cdot 362903}{870}$
6	$\frac{1}{42}$	14	$\frac{7}{6}$	22	$\frac{11 \cdot 131 \cdot 593}{138}$	30	$\frac{5 \cdot 1721 \cdot 1001259881}{14322}$
8	$-\frac{1}{30}$	16	$-\frac{3617}{510}$	24	$-\frac{103 \cdot 2294797}{2730}$	32	$-\frac{37 \cdot 683 \cdot 305065927}{510}$

TABLE 1. Les nombres B_k pour $k \leq 32$, avec leurs numérateurs factorisés.

Plutôt que d'étudier l'équation de Fermat et le théorème de Kummer, ce qui nous conduirait à l'étude des corps cyclotomiques que nous n'avons guère approchée, nous allons nous pencher sur l'équation diophantienne $y^2 = x^3 + k$ chère à Fermat et Mordell, ayant des liens avec l'arithmétique des corps quadratiques. Mordell a démontré que cette équation n'a qu'un nombre fini de solutions $x, y \in \mathbb{Z}$ si $k \in \mathbb{Z}$ est non nul. Nous l'avons déjà vérifié dans le cas $k = -2$.

THÉORÈME 7.22. *On suppose $k < 0$ sans facteur carré, $k \equiv 2, 3 \bmod 4$, et que $\mathrm{h}_{\mathbb{Q}(\sqrt{k})}$ n'est pas multiple de 3. Alors l'équation $y^2 = x^3 + k$ a au plus deux solutions.*

Nous allons voir qu'en fait il n'y a pas de solution si $-k$ n'est pas de la forme $3m^2 \pm 1$, et que s'il est de cette forme les solutions sont $(x, y) = (m^2 - k, \pm(m^3 + 3km))$. Par exemple, si $k = -13 = -(3 \cdot 2^2 + 1)$, cela s'applique car $\mathrm{h}_{\mathbb{Q}(\sqrt{-13})} = 2$ (voir l'exercice 7.4) et les solutions entières sont $(17, \pm 70)$ (solution qui ne sautait d'ailleurs pas aux yeux a priori).

La similarité avec l'énoncé du théorème de Kummer est grosso-modo que "si un certain nombre de classes a une certaine propriété alors une certaine équation diophantienne n'a pas de solution entière". À l'aide des résultats du chapitre suivant, il serait facile de vérifier au cas par cas que les premiers $k < 0$ sans facteur carré tels que $3 \mid \mathrm{h}_{\mathbb{Q}(\sqrt{k})}$ sont ceux de la table suivantes.

$-k$	23	26	29	31	38	53	59	61	83	87	89	106	107	109	110
$\mathrm{h}_{\mathbb{Q}(\sqrt{k})}$	3	6	6	3	6	6	3	6	3	6	12	6	3	6	12

TABLE 2. Les $-111 < k < 0$ sans facteur carré tels que 3 divise $\mathrm{h}_{\mathbb{Q}(\sqrt{k})}$.

DÉMONSTRATION — Soit $A = \mathbb{Z}[\sqrt{k}]$, c'est l'anneau des entiers de $\mathbb{Q}(\sqrt{k})$ car $k \not\equiv 1 \bmod 4$. L'équation se factorise dans A sous la forme $(y + \sqrt{k})(y - \sqrt{k}) = x^3$, que l'on peut aussi voir sous la forme d'un produit d'idéaux principaux

$$II' = (x)^3$$

où $I = (y + \sqrt{k})$ et $I' = (y - \sqrt{k})$.

Vérifions d'abord que I et I' sont premiers entre eux. Soit $D = I + I'$ leur pgcd. Il contient $y \pm \sqrt{k} \in D$ ainsi donc que $2y$ et $2k$. Comme k est sans facteur carré, on constate que x, y et k sont deux à deux premiers entre eux. En particulier le pgcd de $2y$ et $2k$ est 2, puis $2 \in D$ par Bézout. Les idéaux de A contenant 2 sont $2A$, A et un idéal premier $P = 2A + \sqrt{k}A$ ou $2A + (\sqrt{k} + 1)A$ selon que k est pair ou non, avec de plus $P^2 = (2)$. Le cas $D = 2A$ est absurde car $y + \sqrt{k} \notin 2A$, donc $D = P$. Comme $P^2 = (2)$, et $y \pm \sqrt{k} \notin 2A$, on a dans ce cas $v_P(I) = v_P(I') = 1$. Mais alors $v_P(II') = 3v_P(x) = v_P(I) + v_P(I') = 2$ est contradictoire. La seule possibilité est donc $D = A$.

Ainsi I et I' sont premiers entre eux. Comme II' est le cube d'un idéal de A, on en déduit que I est aussi le cube d'un idéal de A par factorisation unique des idéaux en produit d'idéaux premiers (par exemple, on constate que $v_P(I)$ est multiple de 3 pour tout idéal premier P de A). Ainsi, $I = J^3$ pour un certain idéal $J \subset A$. Mais $I = J^3$ est principal, donc l'ordre de $[J]$ dans $\mathrm{Cl}(A)$ divise 3. Comme il divise aussi $\mathrm{h}_{\mathbb{Q}(\sqrt{k})}$ qui est premier à 3, cet ordre est 1 : l'idéal J est principal.

On conclut alors comme dans l'étude du cas $k = 2$: soient $a, b \in \mathbb{Z}$ tels que $J = (a + b\sqrt{k})$. L'identité $I = J^3$ entraîne que $y + \sqrt{k}$ et le cube de l'élément $a + b\sqrt{k}$ diffèrent multiplicativement d'une unité de A. Mais tout unité de A est un cube car $k \neq 3$. Quitte à remplacer $a + b\sqrt{k}$ par un multiple par une unité, on a donc une identité dans A :

$$y + \sqrt{k} = (a + b\sqrt{k})^3 = a^3 + 3kab^2 + (3a^2b + kb^3)\sqrt{k}.$$

En particulier, $1 = b(3a^2 + kb^2)$ puis $b = \pm 1$ et $-k = 3a^2 - b$. Il n'y a donc pas de solution si $-k$ n'est pas de cette forme. S'il est de cette forme, il l'est pour exactement une valeur de b et deux valeurs de a car $b \equiv k \bmod 3$. La relation $y = a^3 + 3ka$ donne deux valeurs possibles opposées pour y, et donc une seule pour $y^2 - k = x^3$, ainsi que pour $x = (a + b\sqrt{k})(a - b\sqrt{k}) = a^2 - k$. Les deux solutions obtenues au final sont

$$(x, y) = (a^2 - k, \pm(a^3 + 3ka)),$$

qui sont bien solutions.

□

5. Application à la détermination de $\mathrm{Cl}(\mathcal{O}_K)$ sur un exemple

On se propose dans ce paragraphe de voir sur un exemple comment ces résultats fournissent des méthodes pour déterminer le groupe $\mathrm{Cl}(\mathcal{O}_K)$. Précisément, on se propose de démontrer

$$\mathrm{Cl}(\mathbb{Z}[\frac{1+\sqrt{-47}}{2}]) \simeq \mathbb{Z}/5\mathbb{Z}.$$

Tout d'abord, comme -47 est sans facteur carré et $\equiv 1 \bmod 4$, l'anneau $A := \mathbb{Z}[\frac{1+\sqrt{-47}}{2}]$ est l'anneau des entiers du corps de nombres $K = \mathbb{Q}(\sqrt{-47})$, de sorte que A est de Dedekind et $\mathrm{Cl}(A)$ est bien un groupe.

On a $A = A_{-47}$, donc $\mathrm{disc}(A) = -47$, et le théorème de Minkowski assure que toute classe d'idéaux non nuls de A contient un idéal contenant un entier $1 \leq N \leq C(1,2)\sqrt{47} < 5$ (table 5).

Considérons le problème de trouver tous les idéaux I contenant $1, 2, 3$ ou 4. Comme $A = \mathcal{O}_K$, "contenir c'est diviser", et il suffit donc de déterminer les idéaux divisant 3 ou $4 = 2^2$. On détermine d'abord les idéaux premiers de A contenant 2 ou 3 (ceux contenant 4 contiennent 2). Soient $\alpha = \frac{1+\sqrt{-47}}{2}$ et $P = \Pi_{\alpha,\mathbb{Q}} = X^2 - X + 12$. Les congruences

$$P \equiv X(X-1) \bmod 2, 3$$

montrent qu'il y a deux idéaux premiers contenant 2 (resp. 3), qui sont $D = (2, \alpha)$ et $D' = (2, \alpha - 1)$ (resp. $T = (3, \alpha)$ et $T' = (3, \alpha - 1)$). On a alors $(2) = DD'$ et $(3) = TT'$. Ainsi les idéaux contenant $(4) = D^2D'^2$ sont $4A$, A, D^2, D'^2, $D^2D' = 2D'$ et $2D$. Les idéaux contenant 3 sont $3A$, A, T et T'. Au final, on voit en particulier que $\mathrm{Cl}(A)$ est engendré par les classes de D, D', T et T'.

Mais on a $(2) = DD'$ et $(3) = TT'$, de sorte que $[D']$ est l'inverse de $[D]$ et $[T']$ est l'inverse de $[T]$: le groupe $\mathrm{Cl}(A)$ est donc engendré par les classes de D et T.

Une manière de trouver des relations multiplicatives entre ces classes, c'est-à-dire des idéaux principaux de la forme D^aT^b, est de trouver d'abord des éléments de A de norme 2^a3^b puis de décomposer les idéaux principaux qu'ils engendrent : ce sont des monômes en D, D', T et T'. Cette méthode s'appelle la "méthode des éléments de petite norme". On rappelle que

$$\mathrm{N}(x + y\alpha) = x^2 + xy + 12y^2 = \frac{1}{4}(2x + y)^2 + \frac{47}{4}y^2$$

(forme principale de discriminant -47) et constate notamment que $\mathrm{N}(\alpha) = 12$ et $\mathrm{N}(4+\alpha) = 32$ (plus petite puissance de 2 qui est une norme). Observons que l'on a $\alpha \in D, \alpha \in T$ mais $\alpha \notin D'$ (car sinon on aurait $D = D'$), d'où l'égalité $(\alpha) = D^2T$. Ainsi, $[T] = [D]^{-2}$ dans $\mathrm{Cl}(A)$, qui est donc engendré comme groupe par la classe de D. De même, $(4+\alpha) = D^5$, donc $[D]$ est d'ordre divisant 5 ! Il est donc d'ordre 1 ou 5, mais il n'est pas principal car 2 n'est pas une norme. On a donc démontré donc que

$$\mathrm{Cl}(\mathbb{Z}[\frac{1+\sqrt{-47}}{2}]) \simeq \mathbb{Z}/5\mathbb{Z},$$

et qu'il est par exemple engendré par $[D]$ (et donc aussi par $[T] = [D]^{-2}$...).

6. Exercices

EXERCICE 7.1. *(i) Trouver tous les idéaux de $\mathbb{Z}[\sqrt{6}]$ contenant 15.*

(ii) Factoriser en produit d'idéaux premiers l'idéal $(1+2\sqrt{-5})$ de $\mathbb{Z}[\sqrt{-5}]$.

EXERCICE 7.2. *On se place dans l'anneau $A = \mathbb{Z}[\sqrt{-5}]$.*

(i) Factoriser en produit d'idéaux premiers les idéaux principaux (2), (3), $(1+\sqrt{-5})$ et $(1-\sqrt{-5})$.

(ii) Expliquer pourquoi la relation $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ n'est pas en contradiction avec la propriété de Dedekind, bien qu'elle entraîne comme on l'a vu au chapitre 5 que A n'est pas factoriel.

EXERCICE 7.3. *On se propose de déterminer $\mathrm{Cl}(\mathbb{Z}[\sqrt{-14}])$.*

(i) Montrer que tout idéal non nul de $A = \mathbb{Z}[\sqrt{-14}]$ est équivalent à un idéal contenant un entier $1 \leq N \leq 4$.

(ii) Déterminer tout les idéaux de A contenant $1, 2, 3$ et 4.

(iii) En considérant des petits nombres bien choisis représentés par la forme $x^2 + 14y^2$, montrer que $\mathrm{Cl}(A)$ est cyclique d'ordre 4.

EXERCICE 7.4. *Montrer de même que $\mathrm{Cl}(\mathbb{Z}[\sqrt{-13}]) \simeq \mathbb{Z}/2\mathbb{Z}$ et que $\mathrm{Cl}(\mathbb{Z}[\sqrt{-26}]) \simeq \mathbb{Z}/6\mathbb{Z}$.*

EXERCICE 7.5. (Principal équivaut à factoriel pour les ordres d'un corps de nombres) *Soit K un corps de nombres.*

(i) Montrer qu'un idéal premier non nul de $\mathcal{O}_K$ est principal si et seulement si il contient un élément premier de $\mathcal{O}_K$.

(ii) En déduire que $\mathcal{O}_K$ est factoriel si, et seulement si, il est principal.

(iii) Montrer que si un ordre A de K est factoriel, alors $A = \mathcal{O}_K$, puis que A est principal.

PROBLÈME 7.1. (Arithmétique de[1] $\mathbb{Z}[\alpha]$) *Soit $A = \mathbb{Z}[\alpha]$ où $\alpha \in \overline{\mathbb{Z}}$. Si $p \in \mathbb{Z}$ est un nombre premier, et si $Q \in (\mathbb{Z}/p\mathbb{Z})[X]$ est un facteur de $\Pi_{\alpha,\mathbb{Q}}$ dans $(\mathbb{Z}/p\mathbb{Z})[X]$, on notera $I(Q)$ l'idéal $pA + \widetilde{Q}(\alpha)$ défini dans la proposition 6.10.*

(i) Montrer que si Q et Q' sont premiers entre eux dans $(\mathbb{Z}/p\mathbb{Z})[X]$ alors $\mathrm{I}(Q)\mathrm{I}(Q') = \mathrm{I}(QQ')$. On pourra partir d'une relation de Bézout dans $(\mathbb{Z}/p\mathbb{Z})[X]$ entre Q et Q'.

(ii) En déduire que si $\overline{\Pi}_{\alpha,\mathbb{Q}} = Q_1 \cdots Q_g$ où les Q_i sont irréductibles unitaires deux à deux distincts, alors on a la décomposition $pA = \prod_{i=1}^{g}(pA + \widetilde{Q}_i(\alpha)A)$.

(iii) En déduire que si p ne divise pas l'entier $D = \mathrm{disc}(\Pi_{\alpha,\mathbb{Q}}) = \mathrm{disc}(A)$, tous les idéaux premiers de A contenant p sont inversibles.

(iv) (Factorisation conditionnelle) *Montrer que tout idéal de A de norme première à $\mathrm{disc}(A)$ se factorise de manière unique comme produit d'idéaux premiers de A.*

(v) Montrer que si I et J sont des idéaux non nuls de A de norme première à $\mathrm{disc}(A)$, alors $\mathrm{N}(IJ) = \mathrm{N}(I)\mathrm{N}(J)$.

1. On prendra garde que l'on ne suppose pas dans cet exercice que $\mathbb{Z}[\alpha]$ est l'anneau des entiers de $\mathbb{Q}(\alpha)$.

Chapitre 8

Formes binaires II : composition et genres

Ce chapitre est un retour sur la théorie des formes binaires étudiée au chapitre 3, en se focalisant pour simplifier sur le cas des discriminants $D < 0$. Nous y avions notamment démontré la finitude de l'ensemble $\mathrm{Cl}(D)$ des classes d'équivalence propre de formes positives de discriminant D, et nous avions même donné une recette, la théorie des formes réduites de Gauss, pour en trouver des représentants canoniques. Le premier objectif de ce chapitre est de démontrer, suivant Dedekind, que $\mathrm{Cl}(D)$ s'identifie naturellement à l'ensemble des classes $\mathrm{Cl}(A_D)$ de l'anneau d'entiers quadratiques imaginaires A_D de discriminant D. Dans cette bijection, le sous-ensemble $\mathrm{P}(D)$ des classes primitives correspond alors aux classes inversibles $\mathrm{Pic}(A_D)$.

Nous appliquerons ce résultat dans les deux directions. D'une part, cela fournit une méthode de calcul de $\mathrm{Cl}(A_D)$ plus directe que les méthodes utilisées précédemment. D'autre part, la structure de groupe de $\mathrm{Pic}(A_D)$ fournit une loi de groupe sur $\mathrm{P}(D)$: c'est le point de vue de Dedekind sur la composition de Gauss des formes. Suivant Gauss, cette loi de groupe a des conséquences fabuleuses sur le problème de la représentation des entiers par des formes de discriminant D. Nous discuterons notamment le cas où $|\mathrm{P}(D)|$ est impair, ainsi que la partition en genres de $\mathrm{P}(D)$.

1. Idéaux des entiers quadratiques imaginaires et formes binaires

Soit $D < 0$ un entier tel que $D \equiv 0, 1 \bmod 4$. On reconsidère le sous-anneau

$$A_D = \mathbb{Z}[\alpha] \subset \mathbb{C}$$

avec $\alpha = \frac{1}{2}\sqrt{D}$ si $D \equiv 0 \bmod 4$, et $\alpha = \frac{1+\sqrt{D}}{2}$ sinon. On peut supposer, pour fixer les idées, que $\sqrt{D}$ désigne la racine carré de partie imaginaire > 0 de D.

Dans tous les cas, $\mathrm{disc}(A_D) = D$. Si $\mathrm{N}(z) = z\overline{z}$, qui est aussi la norme de $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$, on a déjà constaté que $(x, y) \mapsto \mathrm{N}(x + y\alpha)$ est la forme principale de discriminant D. On se propose, suivant Dedekind, de généraliser cette observation à toutes les formes de discriminant D.

Une $\mathbb{R}$-base de $\mathbb{C}$ sera dite directe si son déterminant dans la base $1, \alpha$ est positif. Soit I un idéal non nul de A_D. Nous avons vu que I est un réseau de $\mathbb{C}$, il admet donc une $\mathbb{Z}$-base à deux éléments, disons u, v, qui est aussi une $\mathbb{R}$-base de $\mathbb{C}$. Quitte à remplacer v par $-v$ on peut supposer que u, v est directe. On considère alors l'application $q_{u,v} : \mathbb{Z}^2 \to \mathbb{Q}$ définie par $q_{u,v}(x, y) = \frac{1}{\mathrm{N}(I)}\mathrm{N}(xu + yv)$.

Proposition 8.1. *(i) $q_{u,v}$ est une forme quadratique binaire entière positive de discriminant D.*

(ii) La classe d'équivalence propre de $q_{u,v}$ ne dépend pas du choix de la base directe u, v de I. Mieux, elle dépend seulement de la classe de I dans $\mathrm{Cl}(A_D)$.

Démonstration — Tout d'abord, $q_{u,v}$ ne prend que des valeurs entières. En effet, si $z \in I$, alors $(z) \subset I$ et donc $\mathrm{N}(I)$ divise $\mathrm{N}((z)) = \mathrm{N}(z)$ (Lemme 7.15). De plus, $q_{u,v}$ est bien une forme quadratique : on constate en développant que $q_{u,v}(x,y) = ax^2 + bxy + cy^2$ avec $a = \frac{\mathrm{N}(u)}{\mathrm{N}(I)}$, $b = \frac{1}{\mathrm{N}(I)}\mathrm{Tr}_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}(u\overline{v})$ et $c = \frac{\mathrm{N}(v)}{\mathrm{N}(I)}$. Il est également clair que $q_{u,v}$ est positive.

Vérifions $\mathrm{disc}(q_{u,v}) = D$. Identifions le $\mathbb{R}$-espace vectoriel $\mathbb{C}$ à $\mathbb{R}^2$ au moyen de l'application $\beta : (x,y) \mapsto x+y\alpha$, de sorte que $\beta(\mathbb{Z}^2) = A_D$. On a déjà dit que $\mathrm{N}\circ\beta$ est la forme principale q_0 de discriminant D sur $\mathbb{Z}^2$. Soit $P \in \mathrm{M}_2(\mathbb{Z})$ la matrice de u, v dans la base $1, \alpha$, alors par définition on a $q_{u,v} = \frac{1}{\mathrm{N}(I)} q_0 \cdot P$. D'après la proposition 3.9 on a donc $\mathrm{disc}\, q_{u,v} = \frac{1}{\mathrm{N}(I)^2} \det P \,\mathrm{disc}\, q_0$. Comme on a $\mathrm{disc}\, q_0 = D$, il suffit de vérifier $|\det P| = \mathrm{N}(I)$. Mais par définition, on a aussi $\beta(P\mathbb{Z}^2) = I$. On conclut car l'indice du réseau $P\mathbb{Z}^2$ de $\mathbb{Z}^2$ vaut $|\det P|$ d'après la proposition 2.17.

Si u', v' est une autre $\mathbb{Z}$-base directe de I, alors par définition $\frac{1}{\mathrm{N}(I)}\mathrm{N}(xu' + yv')$ est proprement équivalente à la forme q. Enfin, si $z \in A_D \backslash \{0\}$, alors zI admet pour $\mathbb{Z}$-base directe zu, zv. On conclut car

$$\frac{1}{\mathrm{N}(zI)}\mathrm{N}(xzu + yzv) = \frac{\mathrm{N}(z)}{\mathrm{N}(zI)}\mathrm{N}(xu + yv) = \frac{1}{\mathrm{N}(I)}\mathrm{N}(xu + yv).$$

On a utilisé l'identité $\mathrm{N}(zI) = \mathrm{N}(z)\mathrm{N}(I)$ (Proposition 6.17). □

Considérons par exemple $D = -20$, i.e. $\alpha = \sqrt{-5}$. Calculons la forme associée à l'unique idéal premier contenant 2. C'est l'idéal $I = (2, \alpha+1)$, qui est de norme 2 et non principal comme on l'a déjà vu. Il faut déjà en déterminer une $\mathbb{Z}$-base directe. Vérifions que $2, 1+\alpha$ convient (ce n'est pas évident !). Il suffit de voir [1] qu'elle est $\mathbb{Z}$-génératrice de I car c'est une $\mathbb{R}$-base directe de $\mathbb{C}$. Par définition, $2, 2\alpha, 1+\alpha, \alpha(1+\alpha)$ engendrent I comme groupe abélien. On conclut car $2\alpha = 2(1+\alpha) - 2$ et $\alpha(1+\alpha) = \alpha - 5 = \alpha + 1 - 2.3$. La forme $q(x,y) = \frac{1}{\mathrm{N}(I)}\mathrm{N}(2x + (1+\alpha)y)$ est $2x^2 + 2xy + 3y^2$, qui est bien de discriminant -20. On a d'ailleurs vu qu'elle n'est pas équivalente à la forme principale. C'est un fait général comme nous allons le voir.

Rappelons que $\mathrm{Cl}(D)$ désigne l'ensemble des classes d'équivalence propre de formes positives de discriminant D. Si I est un idéal non nul de A_D on désigne par $q_I \in \mathrm{Cl}(D)$ la classe de la forme $q_{u,v}$ définie à partir d'une $\mathbb{Z}$-base directe u, v de I comme ci-dessus. La proposition montre qu'elle ne dépend que de la classe de I dans $\mathrm{Cl}(A_D)$. Le résultat principal de cette partie est le suivant.

Théorème 8.2. (Dedekind) $[I] \mapsto q_I$ *définit une bijection de* $\mathrm{Cl}(A_D)$ *sur* $\mathrm{Cl}(D)$.

Pour le démontrer, nous allons définir une application dans l'autre sens et vérifier que c'est un inverse de l'application ci-dessus. Soit $q(x,y) = ax^2 + bxy + cy^2$ une forme positive de discriminant D. En particulier, $a > 0$. Elle s'écrit aussi

$$q(x,y) = a\left((x + \frac{b}{2a}y)^2 - \frac{D}{4a^2}y^2\right) = a\mathrm{N}(x + \tau y), \text{ avec } \tau = \frac{b + \sqrt{D}}{2a}.$$

1. On peut également procéder ainsi. On a évidemment $2\mathbb{Z} + (\alpha+1)\mathbb{Z} \subset I$. Mais $1, \alpha+1$ est une $\mathbb{Z}$-base de $\mathbb{Z}[\alpha]$, donc $2\mathbb{Z} + (\alpha+1)\mathbb{Z}$ est un sous-groupe d'indice 2 de $\mathbb{Z}[\alpha]$. Comme d'autre part $\mathrm{N}(I) = 2$, on a bien $2\mathbb{Z} + (\alpha+1)\mathbb{Z} = I$.

Notons que le choix de τ (plutôt que $\overline{\tau}$) est uniquement déterminé par la propriété que $\mathrm{Im}(\tau) > 0$, i.e. que $1, \tau$ est directe. Comme $b \equiv D \bmod 2$, on constate que $a\tau = \frac{b+\sqrt{D}}{2} \in \alpha + \mathbb{Z}$. En particulier, $a\tau \in A_D$. On pose alors $I(q) = a\mathbb{Z} + a\tau\mathbb{Z} \subset A_D$.

PROPOSITION 8.3. *(i) $I(q)$ est un idéal de A_D de norme a.*

(ii) On a $q = q_{a,a\tau}$.

(iii) Si $q' \overset{+}{\sim} q$ alors $I(q') \sim I(q)$.

DÉMONSTRATION — Remarquons l'égalité $A_D = \mathbb{Z} + a\tau\mathbb{Z}$. En effet, comme A_D admet pour $\mathbb{Z}$-base $1, \alpha$, et comme $a\tau - \alpha \in \mathbb{Z}$, le groupe A_D admet aussi pour $\mathbb{Z}$-base $1, a\tau$. Il en résulte un isomorphisme de groupes additifs $A_D/I \simeq \mathbb{Z}/a\mathbb{Z}$, soit encore $\mathrm{N}(I) = a$.

Vérifions que $I(q)$ est un idéal de A_D. Par la description ci-dessus de A_D, ll faut voir que $a^2\tau$ et $(a\tau)^2$ sont dans $I(q)$. C'est évident pour $a^2\tau$. Mais on a $a\tau^2 - b\tau + c = 0$, et donc $a^2\tau^2 = ba\tau - ac \in I(q)$.

Calculons enfin la forme associée à la base $a, a\tau$ (directe) de l'idéal $I(q)$. Par définition, c'est donc

$$\frac{1}{a}\mathrm{N}(ax + a\tau y) = a\mathrm{N}(x + \tau y) = q(x, y).$$

Vérifions maintenant que si $q \overset{+}{\sim} q'$ alors $I(q) \sim I(q')$. Une manière serait de se ramener aux équivalences élémentaires. On peut aussi considérer $q'(x, y) = q(ex + fy, gx + hy)$ avec $eh - fg = 1$. On constate que l'on a

$$q'(x, y) = a\,\mathrm{N}(ex + fy + \tau(gx + hy)) = a\,\mathrm{N}((e + \tau g)x + (f + \tau h)y)$$

$$= a'\,\mathrm{N}(x + \tau' y) \text{ avec } \quad a' = a\,\mathrm{N}(e + \tau g),\ \tau' = \frac{f + \tau h}{e + \tau g}.$$

On a $\mathrm{Im}(\tau') = \frac{1}{\mathrm{N}(e+\tau g)}\mathrm{Im}((f + \tau h)(e + \overline{\tau} g)) = \frac{\mathrm{Im}(\tau)}{\mathrm{N}(e+\tau g)} > 0$. Par définition, on a aussi $I(q') = a'\mathbb{Z} + a'\tau'\mathbb{Z}$. Observons que $\mathbb{Z}(e + g\tau) + \mathbb{Z}(f + \tau h) = \mathbb{Z} + \tau\mathbb{Z}$ car $eh - fg = 1$ (Proposition 2.10). Ainsi, on a les égalités

$$(e + \tau g)I(q') = a'(\mathbb{Z}(f + \tau h) + \mathbb{Z}(e + \tau g)) = a'(\mathbb{Z} + \tau\mathbb{Z}) = \mathrm{N}(e + \tau g)I(q),$$

et donc $[I(q')] = [I(q)]$.

□

Démontrons maintenant le théorème. D'après la proposition ci-dessus, l'application $q \mapsto [I(q)]$ se factorise par $\mathrm{Cl}(D)$ et on a $q_{I(q)} = [q]$ pour tout q. Il ne reste qu'à voir que si $q_I = [q]$ alors on a $[I(q)] = [I]$ pour tout idéal non nul I. Soit I un tel idéal, et soit u, v une $\mathbb{Z}$-base directe de I. On a

$$q_{u,v}(x, y) = \frac{1}{\mathrm{N}(I)}\mathrm{N}(ux + vy) = a\mathrm{N}(x + \tau y)$$

avec $a = \frac{\mathrm{N}(u)}{\mathrm{N}(I)} \in \mathbb{Z}$ et $\tau = \frac{v}{u}$. Notons que $1, \tau$ est directe car u, v l'est. L'idéal $I(q_{u,v})$ est donc $a\mathbb{Z} + a\tau\mathbb{Z}$. On constate que $\mathrm{N}(I)I(q) = \overline{u}I$. En particulier, $[I(q_I)] = [I(q)] = [I]$, ce que l'on voulait. □

REMARQUE 8.4. Il découle de cette démonstration que la classe d'idéaux $[I]$ de A_D correspondant à la classe d'équivalence propre de la forme $q = (a, b, c)$ par le théorème de Dedekind contient l'idéal $I(q) = a\mathbb{Z} + \frac{b+\sqrt{D}}{2}\mathbb{Z}$, qui est de norme a. En particulier, $[I]$ contient un idéal de norme a pour tout entier a primitivement représenté par q.

Le théorème ci-dessus a de nombreuses applications. Par exemple, pour vérifier que deux idéaux non nuls I et J de A_D sont équivalents, il suffit de vérifier que les classes q_I et q_J sont les mêmes. Il suffit alors de vérifier que leurs formes réduites (au sens de Gauss) sont les mêmes, par l'algorithme que nous avons décrit au chapitre 3. Nous renvoyons à l'exercice 8.2 pour un exemple. Voici d'autres conséquences importantes.

COROLLAIRE 8.5. *(i)* $|\mathrm{Cl}(A_D)|$ *est le nombre de classes d'équivalence propre de formes positives de discriminant* D.

(ii) En particulier, A_D *est principal si, et seulement si, il n'y a qu'une telle classe.*

(iii) Les idéaux $a\mathbb{Z} + \frac{b+\sqrt{D}}{2}\mathbb{Z}$, *avec* (a, b, c) *parcourant les formes (positives) réduites de discriminant* D, *forment un système de représentants de* $\mathrm{Cl}(A_D)$.

Le (ii) avait été annoncé au théorème 4.18 du chapitre 5. Il découle du (i) qui est une conséquence immédiate du théorème de Dedekind. Le (iii) se déduit du (i), de la remarque 8.4, et du fait que les formes réduites de Gauss fournissent un ensemble de représentants de $\mathrm{Cl}(D)$ (Théorème 3.22).

REMARQUE 8.6. Le théorème de Dedekind fournit en particulier une nouvelle démonstration de la finitude du nombre de classes d'idéaux de A_D, à partir de celle de $\mathrm{Cl}(D)$ (Lagrange, Théorème 3.16). La méthode de calcul de $\mathrm{Cl}(A_D)$ fournie par le (iii) est en fait sensiblement plus efficace que celle utilisée précédemment (par la théorie de Minkowski). Par exemple, la remarque 8.4 appliquée à une forme réduite au sens de Lagrange (Théorème 3.17) assure que tout idéal de A_D est équivalent à un idéal de norme inférieure ou égale à $\sqrt{\frac{|D|}{3}}$, alors que la théorie de Minkowski fournirait au mieux la constante $\frac{2}{\pi}\sqrt{|D|}$, moins bonne car $\frac{\pi}{2} < \sqrt{3}$.

2. Supplément : identification des classes primitives et des classes opposées

Le théorème de Dedekind met en évidence l'intérêt de la notion d'équivalence propre. On peut se demander comment lire l'équivalence tout court, i.e. l'application $C \mapsto C^{\mathrm{opp}}$ sur $\mathrm{Cl}(D)$ en terme des classes d'idéaux associées. On rappelle que la conjugaison complexe $z \mapsto \overline{z}$ définit un automorphisme de A_D. En particulier, si I est un idéal de A_D, alors $\overline{I} = \{\overline{z}, z \in I\}$ en est un autre. De plus $\overline{\overline{I}} = I$. Il est clair enfin que si $I \sim J$ alors $\overline{I} \sim \overline{J}$: la conjugaison complexe induit une involution de $\mathrm{Cl}(A_D)$.

PROPOSITION 8.7. *Si* I *est un idéal non nul de* A_D *alors* $q_{\overline{I}} = q_I^{\mathrm{opp}}$.

Démonstration — En effet, soit u, v une $\mathbb{Z}$-base directe de I, et soit $q(x,y) = \frac{1}{\mathrm{N}(I)}\mathrm{N}(xu+yv)$ la forme associée. On constate que $q(x,-y) = \frac{1}{\mathrm{N}(I)}\mathrm{N}(xu-yv) = \frac{1}{\mathrm{N}(I)}\mathrm{N}(x\overline{u}-y\overline{v})$. Cela conclut car $\overline{u}, -\overline{v}$ est une $\mathbb{Z}$-base directe de $\overline{I}$, et car $z \mapsto \overline{z}$ induit un isomorphisme $A_D/I \to A_D/\overline{I}$, de sorte que $\mathrm{N}(I) = \mathrm{N}(\overline{I})$. □

On peut aussi déterminer les idéaux inversibles de A_D en terme de leur forme associée.

Proposition 8.8. *Si I est un idéal non nul de A_D, alors I est inversible si, et seulement si, q_I est primitive, auquel cas $\overline{I}$ en est un inverse. En particulier, $[I] \mapsto q_I$ induit une bijection*

$$\mathrm{Pic}(A_D) \xrightarrow{\sim} \mathrm{P}(D).$$

Démonstration — On peut supposer que $I = a\mathbb{Z} + a\tau\mathbb{Z}$ et que q_I est la classe de la forme (a,b,c) avec $\tau = \frac{b+\sqrt{D}}{2a}$ (Remarque 8.4). Calculons l'idéal $J = I\overline{I}$. C'est le groupe abélien engendré par a^2, $a^2\overline{\tau}$, $a^2\tau$ et $a^2\tau\overline{\tau}$. Comme $a\tau + a\overline{\tau} = b$ et $a^2\tau\overline{\tau} = \frac{b^2-D}{4} = ac$, on a $J = a(d\mathbb{Z} + a\tau\mathbb{Z})$ où d est le pgcd de a, b et c. En particulier, si q_I est primitive alors $J = (a)$ et donc $[I][\overline{I}] = [A_D]$.

Pour prouver la réciproque, considérons l'idéal $J\overline{J}$. C'est aussi le groupe abélien engendré par a^2d^2, $a^3d\tau$, $a^3d\overline{\tau}$ et $a^4\tau\overline{\tau} = a^3c$. Le même argument que ci-dessus montre que c'est $a^2d(\mathbb{Z}d + a\tau\mathbb{Z}) = adJ$. Si I est inversible, il en va de même de $\overline{I}$ et de J, et la relation $J\overline{J} = adJ$ entraîne $\overline{J} = (ad)$, puis $J = (ad)$. Comme d'autre part $J = a(d\mathbb{Z} + a\tau\mathbb{Z})$ on constate que $d = 1$: q_I est primitive. □

On rappelle que l'entier $D \equiv 0, 1 \bmod 4$ est un *discriminant fondamental* si toutes les formes de discriminant D sont primitives (voir l'exercice 3.2). D'après ce même exercice, il est équivalent de demander que D n'est pas de la forme m^2D' avec $m \in \mathbb{Z}$ et $D' \equiv 0, 1 \bmod 4$. Autrement dit, il est encore équivalent de demander que : soit $D \equiv 1 \bmod 4$ et D est sans facteur carré, soit $D \equiv 0 \bmod 4$ et $D/4$ est sans facteur carré et congru à $2, 3 \bmod 4$: c'est la condition pour que A_D soit l'anneau des entiers de $\mathbb{Q}(\sqrt{D})$.

Corollaire 8.9. *Il y a équivalence entre :*

(i) D est fondamental,

(ii) A_D est l'anneau des entiers de $\mathbb{Q}(\sqrt{D})$,

(iii) tout idéal non nul de A_D est inversible.

3. Composition de Gauss des formes

Définition 8.10. *Soient q et q' deux formes positives primitives de discriminant D. Une composée de q et q' est une forme primitive q'' de discriminant D telle qu'il existe deux applications $\mathbb{Z}$-bilinéaires $f, g : \mathbb{Z}^2 \times \mathbb{Z}^2 \to \mathbb{Z}$ satisfaisant l'identité remarquable*

$$q(x,y)q'(x',y') = q''(f((x,y),(x',y')), g((x,y),(x',y'))) \ \forall x, y, x', y' \in \mathbb{Z}.$$

Un premier intêret de cette notion est que si q et q' representent respectivement n et n', et si q'' est une composée de q et q', alors q'' représente nn'. Par exemple, la multiplicativité de la norme entraîne

$$\mathrm{N}(x+\alpha y)\mathrm{N}(x'+\alpha y') = \mathrm{N}((xx'+Dyy'+\alpha(xy'+yx))$$

si $D \equiv 0 \bmod 4$, ce qui montre que la forme principale est une composée de la forme principale et d'elle-même : on prend pour formes bilinéaires $f((x,y),(x',y')) = xx'+Dyy'$ et $g((x,y),(x',y')) = xy'+x'y$. Nous laissons au lecteur le soin de vérifier qu'une formule similaire vaut pour $D \equiv 1 \bmod 4$. Plus généralement, toute forme est une composée d'elle-même et de la forme principale, comme le montre l'identité (en discriminant pair) :

$$(x^2-(b^2-ac)y^2)(ax'^2+2bx'y'+cy'^2) = aX'^2+2bX'Y'+cY'^2$$

où $X = xx'-byx'-cyy'$ et $Y = xy'+yx'a+byy'$. En guise de dernier exemple, la forme principale est toujours composée d'une forme et d'elle-même, come le montre l'identité chère à Gauss :

$$(ax^2+2bxy+cy^2)(ax'^2+2bx'y'+cy'^2) = (axx'+b(xy'+x'y)+cyy')^2-(b^2-ac)(xy'-yx')^2.$$

Depuis Lagrange (et peut-être Euler), on sait en fait que deux formes primitives q et q' de même discriminant admettent toujours une composée, nous le verrons ci-dessous. Elles en admettent même une infinité, car toute forme équivalente à q'' est aussi une composée de q et q'. On vérifierait aussi aisément que si q'' est une composée de q et q' alors c'est aussi une composée de toute forme équivalente à q et de toute forme équivalente à q'. Un fait qui a beaucoup perturbé Lagrange et ses contemporains est que deux formes puissent avoir des composées non équivalentes. Par exemple, à équivalence près il y a deux formes primitives de discriminant -44, à savoir $(1,0,11)$ et $(3,2,4)$. Les identités remarquables de l'exercice 2.10 démontrent que $(3,2,4)$ et $(1,0,11)$ sont toutes les deux des composées de $(3,2,4)$ par elle-même.

On doit à Gauss d'avoir compris dans ses Disquisitiones Arithmeticae qu'étant données deux formes il en existe une composée qui est canonique à équivalence propre près, et que cette loi de composition muni $\mathrm{P}(D)$ d'une loi de groupe ! La construction originale de cette loi par Gauss et la vérification des axiomes de groupes, bien que directe chez lui, est très technique. Le lecteur assez curieux pour lire le livre de Gauss le verra notamment jongler avec 37 équations pour vérifier que sa composition est associative (Thm. 240 loc. cit.). Faut-il rappeler cependant que le concept de groupe n'existait pas à l'époque ? La démarche que nous allons suivre, qui est heureusement différente, est due à Dedekind.

Théorème 8.11. *(Gauss, Dedekind) Il existe une unique loi de groupe abélien sur* $\mathrm{P}(D)$ *telle que* $[I] \mapsto q_I$ *soit un isomorphisme de groupes* $\mathrm{Pic}(A_D) \xrightarrow{\sim} \mathrm{P}(D)$.

Elle a la propriété que pour toutes formes q, q' *positives et primitives de discriminant* D*, la classe d'équivalence propre* $[q]\cdot[q']$ *est constituée de composées de* q *et* q'.

Démonstration — L'application $[I] \mapsto q_I$ définit une bijection $\mathrm{Pic}(A_D) \xrightarrow{\sim} \mathrm{P}(D)$, et $\mathrm{Pic}(A_D)$ est un groupe pour la multiplication des idéaux (§ 1.1). Il existe donc une

seule structure de groupe sur $\mathrm{P}(D)$ qui fait de cette bijection un isomorphisme de groupes, à savoir

$$q_I \cdot q_J = q_{IJ}.$$

(on dit parfois que l'on a raisonné par "transport de structure"). Il reste à vérifier que q_{IJ} est bien une composée au sens plus haut de q_I et q_J. Fixons pour cela deux idéaux non nuls I et J, et considérons des $\mathbb{Z}$-bases directes respectives u, v, u', v', et u'', v'' de I, J et IJ. La multiplication de l'anneau A_D définit une application $\mathbb{Z}$-bilinéaire $I \times J \to IJ$. On en déduit en décomposant dans la base u'', v'' de IJ que les applications $f, g : \mathbb{Z}^2 \times \mathbb{Z}^2 \to \mathbb{Z}$ définies par

$$(xu + yv)(x'u' + y'v') = f((x,y),(x',y'))u'' + g((x,y),(x',y'))v'' \tag{5}$$

sont $\mathbb{Z}$-bilinéaires. Soient q, q' et q'' les trois formes positives primitives de discriminant D respectivement associées aux bases précédentes de I, J et IJ. La multiplicativité de la norme, appliquée à la relation (5), ainsi que la relation $\mathrm{N}(IJ) = \mathrm{N}(I)\mathrm{N}(J)$ (Lemme 8.15), entraîne

$$q(x,y)q'(x',y') = q''(f((x,y),(x',y')), g((x,y),(x',y'))).$$

Autrement dit, q'' est une composée de q et q'. On conclut car $[q] = q_I$, $[q'] = q_J$ et $[q''] = q_{IJ}$. □

Définition 8.12. *Si q et q' sont deux formes primitives de discriminant D, on appelle composée de Gauss de q et q' n'importe quelle forme q'' de discriminant D telle que $[q''] = [q] \cdot [q']$, pour le produit dans $\mathrm{P}(D)$ défini par le théorème ci-dessus. En particulier, une composée de Gauss est une composée.*

L'élément neutre de $\mathrm{P}(D)$ est par définition la classe de la forme associée aux idéaux principaux, c'est donc la classe de la forme principale de discriminant D, encore appelée *classe principale*. De plus, l'inverse d'une classe est simplement la classe opposé :

Proposition 8.13. *Si q est primitive, $[q^{\mathrm{opp}}] = [q]^{-1}$ dans $\mathrm{Cl}(D)$.*

Démonstration — En effet, une conséquence des propositions 8.7 et 8.8 est que si I est inversible on a $q_I^{\mathrm{opp}} = q_{\overline{I}} = q_I^{-1}$. □

Il résulte de ceci que les trois identités plus haut sont alors simplement conséquence des relations évidente $1.1 = 1$, $[q].1 = [q]$ et $[q][q]^{\mathrm{opp}} = 1$ dans $\mathrm{P}(D)$! La démonstration du théorème ci-dessus permet en pratique de calculer effectivement la composée de Gauss de deux formes, et donc de retrouver sans astuce les identités remarquables discutées plus haut (voir les exercices).

Exemple 8.14. Si l'on reprend l'exemple de $D = -44$, on comprend maintenant pourquoi $(3,2,4)$ et $(1,0,11)$ sont toutes les deux des composées de $(3,2,4)$ par elle-même. En effet, $\mathrm{P}(-44) \simeq \mathbb{Z}/3\mathbb{Z}$ est constitué de $[(1,0,11)]$ (classes principale), et des deux classes $[(3,\pm 2,4)]$ nécéssairement inverses et carré l'une de l'autre. La composée de Gauss de $[(3,2,4)]$ avec $[(3,2,4)]$ est donc $[(3,-2,4)]$, et la composée de Gauss de $[(3,-2,4)]$ avec $[(3,2,4)]$ est $[(1,0,11)]$. Comme $(3,2,4)$ et $(3,-2,4)$ sont équivalentes (bien que non proprement équivalentes), on obtient les deux composées recherchées de $(3,2,4)$ par elle-même !

Le reste de ce paragrphe est consacré à la démonstration du lemme suivant que nous avons admis dans la démonstration du théorème ci-dessus.

LEMME 8.15. *Si I, J sont des idéaux non nuls de A_D avec I inversible, alors* $\mathrm{N}(IJ) = \mathrm{N}(I)\mathrm{N}(J)$.

DÉMONSTRATION — Remarquons que nous avons déjà démontré ce résultat quand A_D est l'anneau des entiers de $\mathbb{Q}(\sqrt{D})$, i.e. quand D est fondamental (Théorème 7.17). De plus, quand A_D est général nous l'avons aussi démontré si I est principal (Proposition 6.17). Remarquons enfin que si I et J sont des idéaux non nuls quelconques de $A = A_D$ tels que $I + J = A$, alors $\mathrm{N}(IJ) = \mathrm{N}(I)\mathrm{N}(J)$. En effet, une généralisation classique du théorème chinois des restes assure que le morphisme naturel d'anneaux

$$A \to A/I \times A/J$$

est surjectif, de noyau $I \cap J = IJ$. Cette situation se produit notamment si $\mathrm{N}(I)$ et $\mathrm{N}(J)$ sont premiers entre eux. En effet, $\mathrm{N}(I + J)$ divise $\mathrm{N}(I)$ et $\mathrm{N}(J)$, donc $\mathrm{N}(I + J) = 1$ dans ce cas, i.e. $I + J = A$. Nous allons nous ramener à ces cas grâce au lemme qui suit.

On suppose donc I inversible et J non nul comme dans l'énoncé. Soit $M = \mathrm{N}(J)$. Soit I' un idéal de A équivalent à I et de norme première à M : cela existe par le lemme 8.16 (ii). En particulier, il existe $x, y \in A$ non nuls tels que $xI = yI'$. En mettant bout à bout les observations qui précèdent on justifie la suite d'égalités

$$\mathrm{N}(x)\mathrm{N}(IJ) = \mathrm{N}(xIJ) = \mathrm{N}(yI'J) = \mathrm{N}(y)\mathrm{N}(I'J) =$$

$$= \mathrm{N}(y)\mathrm{N}(I')\mathrm{N}(J) = \mathrm{N}(yI')\mathrm{N}(J) = \mathrm{N}(xI)\mathrm{N}(J) = \mathrm{N}(x)\mathrm{N}(I)\mathrm{N}(J),$$

et donc $\mathrm{N}(IJ) = \mathrm{N}(I)\mathrm{N}(J)$. □

LEMME 8.16. *Soit $M \geq 1$ un entier.*

(i) Une forme primitive représente au moins un entier premier à M.

(ii) Tout idéal inversible de A_D est équivalent à un idéal de norme première à M.

DÉMONSTRATION — Démontrons d'abord le (i). Il suffit de voir que pour tout nombre premier p, la forme q représente au moins un entier premier à p. En effet, soient $p_1, \ldots, p_r$ les diviseurs premiers distincts de M, ainsi que pour chaque i un élément $(x_i, y_i) \in \mathbb{Z}^2$ est que $n_i = q(x_i, y_i)$ est premier à p_i. D'après le théorème chinois des restes, on peut trouver $x \in \mathbb{Z}$ (resp. $y \in \mathbb{Z}$) tel que pour tout i on ait $x \equiv x_i \bmod p_i$ (resp. $y \equiv y_i \bmod p_i$). On constate alors que $q(x, y) \equiv n_i \bmod p_i$ pour chaque i, en particulier $q(x, y)$ est premier au produit $p_1 \cdots p_r$ et donc à M. Suppons donc p premier et écrivons $q = (a, b, c)$. Si $ax^2 + bxy + cy^2 \equiv 0 \bmod p$ pour tout $x, y \in \mathbb{Z}/p\mathbb{Z}$, on constate que alors $a \equiv b \equiv c \equiv 0$ (prendre $(1, 0)$, $(0, 1)$ et $(1, 1)$), ce qui est faux car q est primitive, ce qui conclut la première affirmation.

Le (ii) résulte du (i) et de la remarque 8.4. □

4. Application : cas des nombres de classes impairs

Nous donnons dans ce paragraphe deux belles applications dues à Gauss de sa structure de groupe sur $\mathrm{P}(D)$.

THÉORÈME 8.17. (Gauss) *Supposons que $h = |\mathrm{P}(D)|$ soit impair. Soit p un nombre premier ne divisant pas D et tel que D est un carré modulo $4p$, alors :*

(i) p^h est représenté par la forme principale de discriminant D,

(ii) Il existe $x, y \in \mathbb{Q}$ tels que $p = q(x, y)$, où q est la forme principale de discriminant D.

DÉMONSTRATION — Sous l'hypothèse sur p, le théorème de Lagrange 3.10 assure que p est représenté par une forme q de discriminant D, nécessairement positive, et primitive car p ne divise pas D. Un autre théorème de Lagrange, assure que $[q]^h = 1$ dans le groupe $\mathrm{P}(D)$, car ce dernier est d'ordre h. Ainsi, "la" composée de Gauss de q prise h fois avec elle-même est dans la classe principale. Mais cette composée représente p^h car q représente p, cela prouve le (i). Le (ii) se déduit du (i) en divisant par p^{h-1}, qui est un carré car h est impair. □

La seconde application est une condition nécessaire et suffisante sur D pour que $|\mathrm{P}(D)|$ soit impair.

THÉORÈME 8.18. (Gauss) $|\mathrm{P}(D)|$ *est impair si, et seulement si, l'une des conditions suivantes est satisfaite :*

(i) $-D$ est une puissance d'un nombre premier impair,

(ii) $D = -4, -8$, ou -16,

(iii) $D \equiv 4 \bmod 16$ et $-D/4$ est une puissance d'un nombre premier impair.

On commence par observer le lemme suivant, qui découle immédiatement de la proposition 8.13.

LEMME 8.19. *Les classes ambiguës de $\mathrm{P}(D)$ sont exactement les classes C telles que $C^2 = 1$. Elles forment en particulier un sous-groupe de $\mathrm{P}(D)$.*

Comme tout groupe abélien fini G tel que $x^2 = 1$ pour tout $x \in G$ est nécessairement isomorphe à $(\mathbb{Z}/2\mathbb{Z})^s$ pour un certain entier s, on comprend mieux pourquoi nous avions trouvé précédemment (Théorème 3.30) que le nombre des classes ambiguës est toujours une puissance de 2 !

Retournons à la démonstration du théorème 8.18. D'après Lagrange et Cauchy, un groupe fini est de cardinal impair si, et seulement si, il n'a pas d'élément d'ordre 2. D'après le lemme ci-dessus, il faut donc déterminer une condition nécessaire et suffisante sur D pour que la seule forme primitive ambiguë de discriminant D soit la forme principale. Mais le nombre exact de ces formes a été déterminé dans le théorème 3.30 (Gauss), en fonction du nombre de diviseurs premiers de D. Le théorème ci-dessus en est alors un cas particulier. □

5. Genre d'une forme binaire

On rappelle que $D \equiv 0, 1 \bmod 4$ est un entier < 0 fixé. Nous avons vu que si p est un nombre premier tel que D est un carré modulo $4p$, alors p est représenté par une forme q de discriminant D unique à équivalence près. Il n'y a pas de critère simple général sur p permettant de déterminer la classe de q. Cependant, nous allons voir que la congruence de p modulo D délimite un ensemble fini de classes de formes possibles, appelé genre, qui permet de réduire le problème de manière intéressante. Pour simplifier, nous supposerons de plus que $D \not\equiv 0 \bmod 16$.

Nous allons nous intéresser aux valeurs prises dans $(\mathbb{Z}/D\mathbb{Z})^\times$ par une forme primitive de discriminant D. On rappelle que pour tout entier N, la forme q représente des entiers premiers à N d'après le lemme 8.15. Pour chaque forme primitive q de discriminant D, et chaque nombre premier p divisant D, nous allons définir un invariant

$$\varepsilon_p(q) \in \{\pm 1\}$$

de la manière suivante. Soit p un tel nombre premier et $m \in \mathbb{Z}$ un entier premier à p représenté par q. Si p est impair, on pose $\varepsilon_p(q) = \left(\frac{m}{p}\right)$. Si $p = 2$, la définition de $\varepsilon_2(q)$ est un peu plus subtile. Soit H_D le sous-ensemble de $(\mathbb{Z}/8\mathbb{Z})^\times$ des éléments de la forme $u^2 - \frac{D}{4}v^2$, avec $u, v \in \mathbb{Z}/8\mathbb{Z}$. C'est un exercice de vérifier que c'est un sous-groupe, qu'il est aisé de déterminer en fonction de $D \bmod 4$. Il est toujours d'indice 1 ou 2 (voir l'exercice 8.3). On pose alors $\varepsilon_2(q) = 1$ si $m \bmod 8$ est dans H_D, $\varepsilon_2(q) = -1$ sinon.

LEMME 8.20. *Le signe $\varepsilon_p(q)$ ne dépend pas de l'entier m premier à p représenté par q.*

DÉMONSTRATION — Soit p un nombre premier divisant D. La forme $q = (a, b, c)$ étant primitive, on constate que soit a soit c est premier à p. Supposons que c'est a, l'autre cas étant similaire. Si $p \neq 2$, on peut alors écrire pour tout $x, y \in \mathbb{Z}$:

$$ax^2 + bxy + xy^2 \equiv a((x + \frac{b}{2a}y)^2 - D(\frac{y}{2a})^2) \equiv a(x + \frac{b}{2a}y)^2 \bmod p.$$

Si m et n sont premiers à p et représentés par q, on constate bien que $\left(\frac{n}{p}\right) = \left(\frac{a}{p}\right) = \left(\frac{m}{p}\right)$. Si $p = 2$, alors $D = b^2 - 4ac$ est pair, ainsi donc que b. Si on pose $b = 2b'$ on a alors pour tout $x, y \in \mathbb{Z}$,

$$ax^2 + bxy + xy^2 \equiv a((x + b'y)^2 - \frac{D}{4}(ya^{-1})^2) \bmod 8,$$

et on conclut encore car $H_D \subset (\mathbb{Z}/8\mathbb{Z})^\times$ est un sous-groupe. □

On désignera par $\Pi(D)$ l'ensemble des nombres premiers divisant D, privé du nombre premier 2 si $D \equiv 4 \bmod 16$. On exclut 2 dans ce cas car alors $H_D = (\mathbb{Z}/8\mathbb{Z})^\times$ et donc $\varepsilon_2(q)$ vaut toujours 1 : ce qui ne s'avèrerait pas très intéressant. Dans les autres cas, H_D a deux éléments car $D \not\equiv 0 \bmod 16$ par hypothèse.

DÉFINITION 8.21. *On dit que deux formes primitives q et q' de même discriminant D sont dans le même genre, et on note $q \overset{\text{g}}{\sim} q'$, si $\varepsilon_p(q) = \varepsilon_p(q')$ pour tout premier p divisant D.*

La relation $\overset{g}{\sim}$ est une relation d'équivalence sur les formes primitives de discriminant D. Observons que deux formes équivalentes sont dans le même genre car elles prennent les même valeurs, Autrement dit, $\varepsilon_p(q) = \varepsilon_p(q')$ si $q \sim q'$, et chaque genre est une réunion disjointe de classes d'équivalences.

La proposition suivante met en valeur la notion de genre. On dira qu'une forme q représente $a \in \mathbb{Z}/N\mathbb{Z}$ s'il existe $(x, y) \in \mathbb{Z}^2$ tel que $q(x, y) \equiv a \bmod N$.

PROPOSITION 8.22. *Soient q et q' deux formes primitives de discriminant D. Alors $q \overset{g}{\sim} q'$ si, et seulement si, pour tout entier $N \geq 1$, q et q' représentent les mêmes éléments de $\mathbb{Z}/N\mathbb{Z}$.*

Cette proposition ne serait pas très difficile à démontrer, nous l'admettrons cependant car nous ne l'utliserons pas pour démontrer les résultats qui suivent.

Donnons quelques exemples simples de calculs de genres. Considérons d'abord le discriminant $D = -20$. Dans ce cas $\Pi(D) = \{2, 5\}$, et comme $\frac{D}{4} \equiv 3 \bmod 4$ on constate que $H_D = \langle 5 \rangle$. À équivalence près, nous avons vu qu'il n'existe que deux formes de discriminant -20, à savoir $x^2 + 5y^2$ et $2x^2 + 2xy + 3y^2$. Ces formes ne sont pas dans le même genre. En effet, elles représentent respectivement 1 et 3, qui sont premiers à 10, et le premier est un carré modulo 5 et pas le second. On aurait aussi pu arguer en le nombre premier 2, car 3 qui n'est pas $\equiv 1, 5 \bmod 8$.

Discutons l'exemple $D = -44$. Dans ce cas $D \equiv 4 \bmod 16$, de sorte que $\Pi(-44) = \{11\}$. Á équivalence près, il y a exactement deux formes primitives de discriminant -44, à savoir $(1, 0, 11)$ et $(3, 2, 4)$. Ces formes sont dans le même genre, car $\left(\frac{4}{11}\right) = \left(\frac{3}{11}\right) = 1$. On retrouve le fait vu en exercices que $(1, 0, 11)$ et $(3, 2, 4)$ ne sont pas distinguables par des congruences.

Considérons maintenant le cas $D = -56 = -8.7$. On a $\Pi(-14) = \{2, 7\}$ et $H_D = \langle 5 \rangle$. Les formes réduites de ce discriminant sont $(1, 0, 14)$, $(2, 0, 7)$ et $(3, \pm 2, 5)$ (ces deux-là étant équivalentes), et donc $\mathrm{h}(-56) = 4$. On constate qu'il y a deux genres, l'un contenant les deux premières, l'autre contenant les deux secondes. En effet, $(1, 0, 14)$ et $(2, 0, 7)$ représentent respectivement 1 et 9, qui sont dans H_D, alors que 3 n'y est pas. De même, $\left(\frac{2}{7}\right) = \left(\frac{1}{7}\right) = 1$, et $\left(\frac{3}{7}\right) = -1$.

Reprenons l'étude générale des genres. Considérons l'application $\varepsilon : \mathrm{P}(D) \to \{\pm 1\}^{\Pi(D)}$ définie par $\varepsilon([q]) = (\varepsilon_p(q))$. On munit $\{\pm 1\}^{\Pi(D)}$ de sa structure de groupe évidente pour la multiplication coordonnée par coordonnée. Il est donc isomorphe à $(\mathbb{Z}/2\mathbb{Z})^{|\Pi(D)|}$.

THÉORÈME 8.23. (Gauss) *L'application ε est un morphisme de groupes. En particulier, tous les genres ont même cardinal.*

DÉMONSTRATION — Supposons que q'' est une composée de Gauss des deux formes primitives q et q'. Soit n, m des entiers premiers à D, représentés respectivement par q et q'. Alors mn est représenté par q''. Pour tout nombre premier p impair dans $\mathcal{P}(D)$ on a donc

$$\varepsilon_p(q'') = \left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right) = \varepsilon_p(q)\varepsilon_p(q').$$

Si $2 \in \Pi(D)$ cela vaut encore pour $p = 2$ car H_D est un sous-groupe d'indice 2 de $(\mathbb{Z}/8\mathbb{Z})^\times$. Cela montre que ε est un morphisme de groupes. En particulier, tous les genres sont de cardinal $|\mathrm{Ker}(\varepsilon)|$ (Lagrange). □

Le genre $\mathrm{Ker}(\varepsilon)$, qui est le genre de la classe principale, ou encore le genre dont tous les invariants ε_p sont 1, est parfois appelé *genre principal*. La détermination exacte du nombre des genres est le point culminant des Disquisitiones Arithmeticae de Gauss.

THÉORÈME 8.24. (Gauss)
(i) Le nombre total de genres est égal au nombre des classes ambiguës de $\mathrm{P}(D)$.
(ii) Une classe $C \in \mathrm{P}(D)$ *est dans le genre principal si et seulement si* $C = D^2$ *où* $D \in \mathrm{P}(D)$.
(ii)' Une forme primitive q *de discriminant* D *est dans le genre principal si, et seulement si,* q *représente un carré.*
(iii) L'image du morphisme ε *est un sous-groupe d'indice* 2 *dans* $\{\pm 1\}^{\Pi(D)}$.

Le reste de ce cours est consacré à la démonstration de ce théorème. Rappelons que Gauss a déterminé le nombre des classes ambiguës (Théorème 3.30). On constate que c'est 2^{t-1} où $t = |\Pi(D)|$. Comme le nombre de genres est le cardinal de l'image de ε, on constate que (i) est équivalent à (iii).

Vérifions maintenant que (ii) et (iii) sont également équivalents. Commençons par une observation générale. Soit G un groupe abélien fini. Soient $G[2] = \{g \in G, g^2 = 1\}$ et $C(G) = \{g^2, g \in G\}$ (les "carrés de G"), ce sont deux sous-groupes de G qui satisfont

$$|G[2]| = |G/C(G)|.$$

En effet, la multiplication par 2 définit un morphisme de groupes $G \to G$ de noyau $G[2]$ et d'image $C(G)$, et donc $|G[2]| = \frac{|G|}{|C(G)|}$. Soit maintenant $\varepsilon : G \to \{\pm 1\}^r$ un morphisme de groupes surjectif. Comme tout élément de $\{\pm 1\}^r$ est de carré 1, on constate que $C(G) \subset \mathrm{Ker}(\varepsilon)$. Comme $|G[2]| = |G/C(G)|$, l'inclusion $C(G) \subset \mathrm{Ker}(\varepsilon)$ est une égalité si, et seulement si, $|G[2]| = 2^r$. On conclut en posant $G = \mathrm{Cl}(D)$ car $|G[2]| = 2^{|\Pi(D)|-1}$ d'après le théorème 3.30 et le lemme 8.19.

Enfin, les propriétés (ii) et (ii)' sont également équivalentes. En effet il est clair que (ii) entraîne (ii)' : on écrit $[q] = [q']^2$ et on considère n'importe quel entier représenté par q'. Nous omettons la démonstration de l'assertion réciproque.

La démonstration originale de Gauss du théorème 8.24 consistait à démontrer directement la propriété (ii)'. Il utilise pour cela une théorie des formes quadratiques entières ternaires (i.e. à trois variables). Il n'est pas trop difficile en effet de le déduire du résultat suivant (attribué de nos jours en général à Legendre) : Si a, b, c sont des entiers premiers entre eux, l'équation $aX^2 + bY^2 + cZ^2 = 0$ a une solution entière (X, Y, Z) non triviale si et seulement si elle a une solution non triviale dans $\mathbb{R}$ et dans tous les $\mathbb{Z}/N\mathbb{Z}$, où $N \geq 1$. Comme nous n'avons pas parlé de formes ternaires dans ce cours, nous n'exposerons pas cette démonstration. Nous allons plutôt donner une démonstration directe de (iii) qui est basée sur le théorème de la progression arithmétique de Dirichlet : pour tous $a, b \geq 1$ premiers entre eux, il existe une infinité de nombres premiers $\equiv a \bmod b$. Nous renvoyons au *Cours d'arithmétique* de Serre

pour une démonstration. Ce résultat était conjecturé des comtemporains de Gauss mais non encore démontré à cette époque. Nous en démontrerons des cas particuliers dans le cours suivant.

Il sera commode d'introduire l'application $\chi : (\mathbb{Z}/8\mathbb{Z})^\times \to \{\pm 1\}$ telle que $\chi(x) = 1$ si, et seulement si, $x \in H_D$. C'est un morphisme de groupes car H_D est un sous-groupe d'indice 2 de $(\mathbb{Z}/8\mathbb{Z})^\times$. Le lemme suivant exprime χ au moyen du symbole de Jacobi, il est laissé en exercice au lecteur.

LEMME 8.25. *Supposons $D \equiv 0 \bmod 4$ et $n \in \mathbb{Z}$ impair. Alors $\chi(n) = \left(\frac{-1}{n}\right)$ (resp. $\left(\frac{2}{n}\right)$, resp. $\left(\frac{-2}{n}\right)$), si $\frac{D}{4} \equiv 3 \bmod 4$ (resp. $\frac{D}{4} \equiv 2 \bmod 8$, resp. $\frac{D}{4} \equiv 6 \bmod 8$).*

On commence par vérifier que $\mathrm{Im}(\varepsilon)$ tombe dans un sous-groupe d'indice 2 de $\{\pm 1\}^{\Pi(D)}$. Ce la découlera comme on le verra de la loi de réciprocité quadratique.

LEMME 8.26. (Gauss) *Il existe une partie $X \subset \Pi(D)$ non vide telle que pour toute forme primitive q de discriminant D,*

$$\prod_{p \in X} \varepsilon_p(q) = 1.$$

DÉMONSTRATION — Soit q une telle forme et soit n un entier impair positif et premier à D représenté par q. Quitte à diviser n par un carré on peut supposer que n est primitivement représenté par q, auquel cas D est un carré modulo n d'après le théorème 3.10. En particulier, $\left(\frac{D}{n}\right) = 1$ (symbole de Jacobi). Écrivons D sous la forme $D = uD'C$ où C est un carré, $u \in \{\pm 1, \pm 2\}$, et où D' est impair sans facteur carré de signe choisi tel que $D' \equiv 1 \bmod 4$. Il vient que

$$\left(\frac{u}{n}\right) = \left(\frac{D'}{n}\right).$$

D'autre part, la loi de réciprocité quadratique étendue au symbole de Jacobi assure que

$$\prod_{p | D'} \left(\frac{n}{p}\right) = \left(\frac{n}{|D'|}\right) = \left(\frac{D'}{n}\right)$$

car $D' \equiv 1 \bmod 4$. Les deux relations ci-dessus concluent lorsque $u = 1$, car alors $\left(\frac{u}{n}\right) = 1$. C'est notamment le cas si D est impair car dans ce cas $D, D', C \equiv 1 \bmod 4$ et donc $u = 1$. Si D est pair, on constate que $\frac{D}{4u} = D'\frac{C}{4} \equiv 1 \bmod 4$ car $D \not\equiv 0 \bmod 16$, donc $\frac{D}{4} \equiv u \bmod 4u$, de sorte que dans tous les cas

$$\chi(n) = \left(\frac{u}{n}\right),$$

ce qui fournit la relation cherchée. Au final, on peut prendre pour X l'ensemble des premiers divisant D' auxquels on rajoute 2 si D est pair non congru à 4 modulo 16 (auquel cas $u = 1$). Cet ensemble n'est en particulier pas vide. □

Pour finir la démonstration du théorème, fixons des $(\varepsilon_p) \in \{\pm 1\}^{\Pi(D)}$ quelconques tels que

$$\prod_{p \in X} \varepsilon_p = 1 \tag{6}$$

où X est l'ensemble décrit ci-dessus. Choisissons pour chaque nombre premier p impair dans $\Pi(D)$, un élément $a_p \in (\mathbb{Z}/p\mathbb{Z})^\times$ tel que $\left(\frac{a_p}{p}\right) = \varepsilon_p$. Si $2 \in \Pi(D)$, choisissons aussi un $a_2 \in (\mathbb{Z}/8\mathbb{Z})^\times$ tel que $\chi(a_2) = \varepsilon_2$. Par le théorème chinois des restes il existe un entier $a \in \mathbb{Z}$ tel que $a \equiv a_p \bmod p$ pour tout p impair dans $\Pi(D)$, et tel que $a \equiv a_2 \bmod 8$ si $2 \in \Pi(D)$.

Soit b le produit des éléments de $\Pi(D)$. Tous les a_p étant inversibles, les entiers a et b sont premiers entre eux. D'après le théorème de la progression arithmétique, il existe donc un nombre premier $\ell \neq 2$ tel que $\ell \equiv a \bmod b$. Par construction, $\left(\frac{\ell}{p}\right) = \varepsilon_p$ pour tout p impair et $\chi(\ell) = \varepsilon_2$ si $2 \in X$. Il ne reste qu'à voir qu'il existe une forme de discriminant D qui représente ℓ : le genre d'une telle forme q satisfait $\varepsilon_p(q) = \varepsilon_p$ pour tout $p \in \Pi(D)$ par définition.

D'après le théorème de Lagrange il est nécessaire et suffisant pour cela que

$$\left(\frac{D}{\ell}\right) = 1.$$

On développe ce symbole en utilisant la décomposition $D = uD'C$ du lemme précédent et à l'aide des propriétés du symbole de Jacobi. L'argument a déjà été donné dans le lemme et se réécrit

$$\left(\frac{D}{\ell}\right) = \left(\frac{u}{\ell}\right)\left(\frac{D'}{\ell}\right) = \left(\frac{u}{\ell}\right)\prod_{p|D'}\left(\frac{\ell}{p}\right)$$

$$= \left(\frac{u}{\ell}\right)\prod_{p\in X\text{impair}} \varepsilon_p.$$

Lorsque $u = 1$ alors X ne contient pas 2 : le produit ci-dessus vaut 1 par la formule (6). Sinon on a vu dans le lemme que $2 \in X$ et que $\left(\frac{u}{\ell}\right) = \chi(\ell)$, de sorte que l'on conclut encore par la formule (6). □

6. Exercices

Dans tous ces exercices, D désignera toujours un entier < 0 et congru à 0 ou 1 modulo 4.

EXERCICE 8.1. *Démontrer que $\mathbb{Z}[\frac{1+\sqrt{-163}}{2}]$ est principal.*

EXERCICE 8.2. *Soit $A = \mathbb{Z}[\alpha]$ avec $\alpha = \sqrt{-11}$. On considère les idéaux $I = (3, \alpha + 1)$ et $J = (23, \alpha + 9)$.*

(i) Montrer que ce sont des idéaux premiers et déterminer leur norme.

(ii) Déterminer un représentant de q_I et de q_J.

(iii) En déduire que I et J sont équivalents.

EXERCICE 8.3. *Soit $D \equiv 0 \bmod 4$ et $H_D \subset (\mathbb{Z}/8\mathbb{Z})^\times$ le sous-ensemble des éléments de la forme $u^2 - \frac{D}{4}v^2$ avec $u, v \in \mathbb{Z}/8\mathbb{Z}$. Montrer que H_D est un sous-groupe et le déterminer en fonction de D.*

EXERCICE 8.4. *(Composées élémentaires) On suppose* $D \equiv 0 \bmod 4$. *Soit* $\alpha = \frac{\sqrt{D}}{2}$, *ainsi que* $(a, 2b, c)$ *une forme de discriminant* $D \equiv 0 \bmod 4$, *et* $\tau = b + \alpha$. *Soit* $I = a\mathbb{Z} + a\tau\mathbb{Z} \subset A_D$.

(i) Rappeler pourquoi I *est un idéal de* A_D.

(ii) Déterminer les formes bilinéaires $f, g : \mathbb{Z}^2 \times \mathbb{Z}^2 \to \mathbb{Z}$ *telles que pour tout* $x, y, x', y' \in \mathbb{Z}$,

$$(x + \alpha y)(x'a + y'a\tau) = f((x, y), (x', y))a + g((x, y), (x', y'))a\tau.$$

(iii) En déduire une identité remarquable exprimant le fait que q *est composée de Gauss de* q *et de la forme principale de discriminant* D.

(iv) On suppose $(a, 2b, c)$ *primitive. Déterminer les formes bilinéaires* $f, g : \mathbb{Z}^2 \times \mathbb{Z}^2 \to \mathbb{Z}$ *telles que pour tout* $x, y, x', y' \in \mathbb{Z}$,

$$(ax + a\tau y)(ax' + a\overline{\tau}y') = f((x, y), (x', y'))a + g((x, y), (x', y'))a\alpha.$$

(v) En déduire une identité remarquable exprimant le fait que la forme principale est composée de Gauss de q *et de* q^{opp}.

EXERCICE 8.5. *(i) Trouver une identité remarquable exprimant le fait que* $(3, -2, 4)$ *est une composée de Gauss de* $(3, 2, 4)$ *et* $(3, 2, 4)$.

(ii) En utilisant cette identité et celles de l'exercice précédent, retrouver les quatres identités de l'exercice 2.10.

EXERCICE 8.6. *(i) Déterminer le groupe* $\mathrm{Cl}(-132)$ *ainsi que sa partition en genres.*

(ii) En déduire une caractérisation des nombres premiers représentés par chacune de ses classes.

(iii) Pour chaque paire de classes $\{[q], [q']\}$, *de composée de Gauss* $[q'']$, *expliciter une identité remarquable correspondant à la relation* $[q''] = [q] \cdot [q']$.

EXERCICE 8.7. *(i) Déterminer le groupe* $\mathrm{Cl}(-68)$ *ainsi que sa partition en genres.*

(ii) En déduire une caractérisation des nombres premiers de la forme $3a^2 + 2ab + 6b^2$.

(iii) Pour chaque paire de classes $\{[q], [q']\}$, *de composée de Gauss* $[q'']$, *expliciter une identité remarquable correspondant à la relation* $[q''] = [q] \cdot [q']$.

EXERCICE 8.8. *Soit* q *un nombre premier* $\equiv 3 \bmod 4$. *Soit* p *un nombre premier impair différent de* q *tel que* $\left(\frac{-q}{p}\right) = 1$. *Montrer sans utiliser la loi de réciprocité quadratique, mais à l'aide des théorèmes 8.17 et 8.18, que* $\left(\frac{p}{q}\right) = 1$.

EXERCICE 8.9. *Vérifier la table 2 du chapitre 7.*

EXERCICE 8.10. *On suppose que* D *est un discriminant fondamental. Montrer que les ordres de* $\mathbb{Q}(\sqrt{D})$ *sont les* $A_{m^2 D}$ *avec* $m \geq 1$ *entier.*

Chapitre 9

Formule du nombre de classes de Dirichlet

Dans ce dernier chapitre, nous exposons la démonstration par Dirichlet (1830) d'une formule obtenue par voie analytique pour h_K quand K est un corps quadratique imaginaire. Décrivons cette formule lorsque $K = \mathbb{Q}(\sqrt{-p})$ et $p \equiv 3 \bmod 4$ est un nombre premier.

Considérons la question, qui a priori n'a rien à voir, de savoir si [1] l'intervalle $\{1, \ldots, \frac{p-1}{2}\}$ contient plus de carrés ou de non-carrés modulo p. Désignons respectivement par C et N les nombres de carrés et non-carrés modulo p de cet intervalle, et intéressons-nous à l'écart $C - N \in \mathbb{Z}$. Comme $C + N = \frac{p-1}{2}$, notons que $C - N$ est impair.

p	3	7	11	19	23	31	43	47	59	67	71	79	83	103	107	127	131	139	151	163
$C - N$	1	1	3	3	3	3	3	5	9	3	7	5	9	5	9	5	15	9	7	3

TABLE 1. Valeurs de $C - N$ lorsque $p \equiv 3 \bmod 4$ et $p \leq 163$.

La première chose que l'on remarque est que l'on a $C > N$ dans tous les cas. Il semblerait aussi que si $p > 3$ et $p \equiv 3 \bmod 8$ alors $C \equiv N \bmod 3$. Comme nous le verrons, il y a en effet une raison élémentaire pour ceci. Ré-écrivons au final cette table en considérant plutôt la quantité renormalisée $(C - N)/\delta$ où δ vaut 3 si $p \equiv 3 \bmod 8$ et $p \neq 3$, 1 sinon.

p	3	7	11	19	23	31	43	47	59	67	71	79	83	103	107	127	131	139	151	163
$\frac{C-N}{\delta}$	1	1	1	1	3	3	1	5	3	1	7	5	3	5	3	5	5	3	7	1

TABLE 2. Valeurs de $(C - N)/\delta$ lorsque $p \equiv 3 \bmod 4$ et $p \leq 163$.

À ce point du cours, il est tentant de conjecturer l'énoncé suivant :

THÉORÈME 9.1. *(Dirichlet) Si* $p \equiv 3 \bmod 4$, *alors* $\mathrm{h}(-p) = \frac{C-N}{\delta}$.

On a vu au chapitre précédent que $\mathrm{h}(-p) = \mathrm{h}_{\mathbb{Q}(\sqrt{-p})}$: cela nous fournit donc une troisième interprétation de ce nombre ! La formule de Dirichlet est en fait plus générale et fournit une expression pour $\mathrm{h}(D)$ quand $D < 0$. Nous nous bornerons pour simpifier au cas (le plus intéressant) où D est un discriminant fondamental, auquel cas $\mathrm{h}(D) = \mathrm{h}_{\mathbb{Q}(\sqrt{D})}$. Cette nouvelle formule, bien que peu recommandable

1. Lorsque $p \equiv 1 \bmod 4$, -1 est un carré modulo p et donc cet intervalle contient exactement $\frac{p-1}{4}$ carrés modulo p : il y a donc toujours autant de carrés que de non carrés, et la question n'est pas intéressante.

pour calculer $\mathrm{h}(D)$ en pratique, est la clé de plusieurs développements, comme la preuve de la congruence de Kummer

$$\mathrm{h}(-p) \equiv -2\mathrm{B}_{\frac{p+1}{2}} \bmod p,$$

ou encore la preuve de ce que $\mathrm{h}(D) \to \infty$ quand $D \to -\infty$ (Hecke, Deuring, Heilbronn, Siegel). Elle intervient aussi de manière cruciale dans la preuve par Dirichlet du théorème de la progression arithmétique ! Un ingrédient fondamental dans la démonstration de Dirichlet est l'introduction de certains produits Euleriens généralisant la fonction ζ de Riemann : les fonctions L de Dirichlet, que nous commençerons par introduire.

Références : Les chapitres 6 et 7 du livre de Marcus *Number fields*, le chapitre 16 du livre de Ireland et Rosen, et la partie III du livre de Hilbert *The theory of algebraic number fields* (ou *Zahlbericht*). On pourra aussi consulter le livre de H. Cartan *Théorie élémentaire des fonctions analytiques d'une ou plusieurs variables complexes* pour les rudiments sur les fonctions d'une variable complexe.

1. Fonctions L de Dirichlet

1.1. Séries de Dirichlet. Une série de Dirichlet est une série à paramètre de la forme

$$L(s) := \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

où les a_n sont des nombres complexes fixés, et où s est une variable complexe. On rappelle que si t est un réel > 0, on pose $t^s = \mathrm{e}^{s\log(t)}$, où log désigne le logarithme népérien : c'est une fonction entière de la variable s (*i.e.* holomorphe sur $\mathbb{C}$ tout entier) qui ne s'annule pas.

Lemme 9.2. *Si la suite $(a_n)_{n\geq 1}$ est bornée, la série définissant $L(s)$ converge normalement sur tout demi-plan de la forme $\mathrm{Re}(s) > s_0$ avec s_0 réel > 1. En particulier, elle définit une fonction holomorphe sur le demi-plan $\mathrm{Re}(s) > 1$.*

Démonstration — On a $|n^s| = n^{\mathrm{Re}(s)}$ pour tout $n \geq 1$ et tout $s \in \mathbb{C}$. Le lemme découle alors de la convergence bien connue de la série à termes positifs $\sum_{n\geq 1} n^{-s}$ si s est réel > 1, qui est inférieure à $1 + \int_1^{\infty} t^{-s}dt = 1 + \frac{1}{s-1}$. □

1.2. La fonction ζ. L'exemple le plus simple de série de Dirichlet est la fonction ζ de Riemann

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

à laquelle le lemme ci-dessus s'applique, et qui est donc absolument convergente et holomorphe sur le demi-plan $\mathrm{Re}(s) > 1$. On sait depuis Riemann que ζ admet en fait un prolongement méromorphe à $\mathbb{C}$ tout entier, avec $s = 1$ pour unique pôle. Nous nous contenterons ici du résultat suivant.

Proposition 9.3. *La fonction ζ de Riemann admet un (unique) prolongement méromorphe sur le demi-plan $\mathrm{Re}(s) > 0$ ayant pour unique pôle $s = 1$. De plus, on a $\mathrm{Res}_{s=1}\ \zeta(s) = 1$.*

Démonstration — Soit $s \in \mathbb{C}$ tel que $\mathrm{Re}(s) > 1$. L'identité $\frac{1}{s-1} = \int_1^\infty t^{-s} dt$ permet d'écrire

$$\zeta(s) = \frac{1}{s-1} + \sum_{n\geq 1} \int_n^{n+1} (n^{-s} - t^{-s}) dt$$

Il suffit pour conclure de voir que la série de fonctions holomorphes ci-dessus converge normalement sur tout compact de $\{s \in \mathbb{C}, \mathrm{Re}(s) > 0\}$. La dérivée de $t \mapsto t^{-s}$ étant $-st^{-s-1}$, on a donc par accroissements finis

$$|\int_n^{n+1} (n^{-s} - t^{-s}) dt| \leq \operatorname*{Sup}_{n\leq t\leq n+1} |n^{-s} - t^{-s}| \leq \frac{|s|}{n^{\mathrm{Re}(s)+1}},$$

ce qui conclut. □

1.3. Fonctions L de Dirichlet. Soit D un entier ≥ 1. Un *caractère de Dirichlet modulo D* est un morphisme de groupes

$$\chi : (\mathbb{Z}/D\mathbb{Z})^\times \to \mathbb{C}^\times.$$

On associe à un tel χ une application $\chi' : \mathbb{Z} \to \mathbb{C}$ en posant $\chi'(n) = \chi(n \bmod D)$ si n est pas premier à D, et $\chi'(n) = 0$ sinon. On a alors $\chi'(mn) = \chi'(m)\chi'(n)$ pour tout $m, n \in \mathbb{Z}$. La construction $\chi \mapsto \chi'$ est bijective en un sens évident, et par la suite nous noterons toujours χ et χ' de la même manière. Dirichlet associe à un caractère χ modulo D la série

$$L(s, \chi) = \sum_{n\geq 1} \frac{\chi(n)}{n^s}.$$

On a $|\chi(n)| \leq 1$ pour tout $n \geq 1$, donc le lemme 9.2 s'applique et montre que $L(s, \chi)$ est absolument convergente et holomorphe sur $\mathrm{Re}(s) > 1$.

Donnons quelques exemples. Le *caractère trivial modulo D* est par définition celui valant identiquement 1 sur $(\mathbb{Z}/D\mathbb{Z})^*$. Dans le cas particulier $D = 1$, on constate $L(s, 1) = \zeta(s)$: la fonction zêta de Riemann est un cas particulier de fonction L de Dirichlet. Plus généralement, si χ est le caractère trivial modulo n'importe quel entier $D \geq 1$, la fonction $L(s, \chi)$ est très proche de ζ de Riemann (voir les exercices).

Soit $\chi : (\mathbb{Z}/3\mathbb{Z})^\times = \{\pm 1\} \to \mathbb{C}^\times$ le caractère de Dirichlet modulo 3 défini par $\chi(1) = 1$ et $\chi(-1) = -1$. On a donc

$$L(s, \chi) = \sum_{n\geq 1} \frac{1}{(3n+1)^s} - \frac{1}{(3n+2)^s}, \quad \mathrm{Re}(s) > 1.$$

On constate ici l'égalité $\chi(-) = \left(\frac{-}{3}\right)$. Plus généralement, le symbole de Legendre $\chi(-) = \left(\frac{-}{p}\right)$ modulo un nombre premier $p > 2$ est un exemple de caractère de Dirichlet modulo p. Sa fonction L jouera un grand rôle dans ce chapitre. On a alors pour $\mathrm{Re}(s) > 1$

$$L(s, \left(\frac{-}{p}\right)) = \sum_{\left(\frac{n}{p}\right)=1} \frac{1}{n^s} - \sum_{\left(\frac{n}{p}\right)=-1} \frac{1}{n^s}.$$

Quand χ est non trivial, on constate que $L(s, \chi)$ est une série de type alternée et donc que sa convergence doit être meilleure que pour ζ de Riemann.

PROPOSITION 9.4. *Si χ est un caractère de Dirichlet non trivial, alors la série définissant $L(s,\chi)$ converge uniformément sur tout compact du demi-plan* $\mathrm{Re}(s) > 0$. *En particulier,* $\mathrm{L}(s,\chi)$ *est une fonction holomorphe de s sur ce demi-plan.*

Nous aurons besoin pour vérifier cela du lemme classique suivant ("transformation d'Abel"), que l'on énonce dans une généralité un peu plus grande pour une ré-utilisation future.

LEMME 9.5. *Soit $(a_n)_{n\geq 1}$ une suite de nombres complexes. On suppose qu'il existe un nombre réel r tel que $\sum_{n\leq N} a_n = O(N^r)$ quand $N \to \infty$. Alors la série de fonctions $\sum_{n\geq 1} \frac{a_n}{n^s}$ converge uniformément sur tout compact du demi-plan* $\mathrm{Re}(s) > r$. *En particulier, sa somme est une fonction holomorphe sur ce demi-plan.*

DÉMONSTRATION — On pose $A_n = \sum_{k\leq n} a_k$. Si $1 < N \leq M$ on a par "transformation d'Abel"

$$\sum_{n=N}^{M} \frac{a_n}{n^s} = \sum_{n=N}^{M} \frac{A_n - A_{n-1}}{n^s} = \frac{A_M}{M^s} - \frac{A_{N-1}}{N^s} + \sum_{n=N}^{M-1} A_n\left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right).$$

De plus, $\frac{1}{n^s} - \frac{1}{(n+1)^s} = s\int_n^{n+1} t^{-s-1}dt$, de sorte que

$$\left|\frac{1}{n^s} - \frac{1}{(n+1)^s}\right| \leq \frac{|s|}{n^{\mathrm{Re}(s)+1}}.$$

Par hypothèse, il existe $C > 0$ tel que $|A_n| \leq Cn^r$ pour tout $n \geq 1$. Le lemme se déduit alors de l'estimée

$$\left|\sum_{n=N}^{M-1} A_n\left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right)\right| \leq C|s| \sum_{n=N}^{M-1} \frac{1}{n^{\mathrm{Re}(s)-r+1}} \leq \frac{C|s|}{\mathrm{Re}(s)-r} \ \frac{1}{(N-1)^{\mathrm{Re}(s)-r}}$$

et des inégalités $\left|\frac{A_M}{M^s}\right| \leq \frac{C}{M^{\mathrm{Re}(s)-r}}$ et $\left|\frac{A_{N-1}}{N^s}\right| \leq \frac{C}{N^{\mathrm{Re}(s)-r}}$ (critère de Cauchy). □

Démontrons maintenant la proposition 9.4. Soit χ un caractère de Dirichlet modulo D. Nous allons voir que $|\sum_{n\leq N} \chi(n)| \leq \varphi(D)$ pour tout $N \geq 1$ si χ est non trivial. Observons que si $n \geq 1$, alors

$$\sum_{i=n}^{n+D-1} \chi(i) = \sum_{i\in(\mathbb{Z}/D\mathbb{Z})^\times} \chi(i)$$

Cette dernière somme S est nulle. En effet, on peut le voir soit comme une relation d'orthogonalité entre le caractère trivial 1_D et le caractère $\chi \neq 1_D$ de $(\mathbb{Z}/D\mathbb{Z})^\times$, soit élémentairement comme suit. Pour tout $x \in (\mathbb{Z}/D\mathbb{Z})^\times$, on constate par changement de variable $i \mapsto xi$ que $\chi(x)S = S$. Si χ est non trivial il existe x tel que $\chi(x) \neq 1$, et donc $S = 0$. □

En fait, il est également connu depuis Dirichlet et Riemann que $L(s,\chi)$ admet un prolongement holomorphe à $\mathbb{C}$ tout entier quand χ est non trivial.

2. La fonction zêta des corps quadratiques imaginaires

2.1. La fonction zêta de Dedekind. La fonction ζ de Dedekind du corps de nombres K est

$$\zeta_K(s) = \sum_I \frac{1}{\mathrm{N}(I)^s},$$

où I parcourt les idéaux non nuls de $\mathcal{O}_K$. Nous verrons plus loin que cette série converge absolument si $\mathrm{Re}(s) > 1$, et coïncide donc avec la série de Dirichlet

$$\zeta_K(s) = \sum_{n\geq 1} \frac{a_n}{n^s},$$

où a_n est le nombre d'idéaux non nuls de $\mathcal{O}_K$ de norme n. C'est cette seconde définition de ζ_K que nous adopterons temporairement dans cette partie. Remarquons que tout idéal de $\mathcal{O}_K$ de norme n contient l'entier n (Lagrange !), et qu'il n'y a qu'un nombre fini d'idéaux de $\mathcal{O}_K$ contenant un entier n donné d'après le lemme 6.8.

La fonction ζ de Dedekind est aussi une généralisation de la fonction ζ de Riemann : $\zeta_{\mathbb{Q}}(s) = \zeta(s)$. Le but de cette partie est d'étudier $\zeta_K(s)$ lorsque K est un corps quadratique imaginaire. En guise d'exemple considérons le cas de $K = \mathbb{Q}(i)$. On rappelle que tout idéal de $\mathcal{O}_K = \mathbb{Z}[i]$ est principal et possède exactement $4 = |\mathbb{Z}[i]^\times|$ générateurs distincts. De plus $\mathrm{N}((a+bi)) = a^2 + b^2$. On en déduit

$$\zeta_{\mathbb{Q}(i)}(s) = \sum_{n\geq 1} \frac{a_n}{n^s}$$

où $4a_n$ est le nombre de façons d'écrire l'entier n comme somme de deux carrés.

2.2. Le cas des corps quadratiques imaginaires. Soit K un corps quadratique imaginaire ($r_2 = 1$) et soit $D = \mathrm{disc}(\mathcal{O}_K)$, de sorte que $\mathcal{O}_K = A_D$. On rappelle que h_K désigne le nombre de classes d'idéaux de $\mathcal{O}_K$, et que le théorème 8.2 du chapitre précédent assure que $\mathrm{h}_K = \mathrm{h}(D)$ (cela ne servira cependant pas ici). On note enfin $w_K = |\mathcal{O}_K^\times|$. Le théorème suivant est dû à Dirichlet (1831).

THÉORÈME 9.6. *(Formule analytique du nombre de classes) Si K est quadratique imaginaire, $\zeta_K(s)$ admet un (unique) prolongement méromorphe au demi-plan $\mathrm{Re}(s) > \frac{1}{2}$. Il a pour unique pôle $s = 1$, qui est simple, et de résidu*

$$\mathrm{Res}_{s=1}\ \zeta_K(s) = \frac{2\pi\ \mathrm{h}_K}{w_K\ |\mathrm{disc}(\mathcal{O}_K)|^{\frac{1}{2}}}.$$

2.3. Démonstration de la formule de Dirichlet. Cette partie est consacrée à la démonstration du théorème 9.6. On note a_n le nombre d'idéaux de $\mathcal{O}_K$ de norme n. Nous allons dénombrer ces derniers classe par classe : si $C \in \mathrm{Cl}(\mathcal{O}_K)$ est une classe d'idéaux on pose

$$a_{n,C} = |\{I \in C, \mathrm{N}(I) = n\}|,$$

de sorte que $a_n = \sum_{C\in\mathrm{Cl}(\mathcal{O}_K)} a_{n,C}$.

LEMME 9.7. *Pour toute classe $C \in \mathrm{Cl}(\mathcal{O}_K)$, on a $\sum_{k=1}^n a_{k,C} = \frac{2\pi\, n}{w_K\, |D|^{\frac{1}{2}}} + O(n^{\frac{1}{2}})$ quand $n \to \infty$.*

Cette proposition entraîne le théorème. En effet, on obtient d'une part que $\sum_{n\leq N} a_n = O(N)$, donc le lemme 9.7 entraîne comme promis que $\zeta_K(s)$ est absolument convergente si $\mathrm{Re}(s) > 1$ (elle est à termes positifs), et donc holomorphe dans cette région. Mieux, si l'on pose pour $\mathrm{Re}(s) > 1$

$$\zeta_K(s) - \frac{2\pi\, \mathrm{h}_K}{w_K |D|^{\frac{1}{2}}}\zeta(s) = \sum_{n\geq 1} \frac{b_n}{n^s}$$

alors le lemme 9.7 entraîne $\sum_{k\leq n} b_k = O(n^{\frac{1}{2}})$. Le lemme 9.5 assure que la série de Dirichlet de droite est convergente et holomorphe sur $\mathrm{Re}(s) > \frac{1}{2}$. L'identité ci-dessus est donc une égalité entre fonctions méromorphes sur $\mathrm{Re}(s) > 1/2$ par prolongement analytique (=zéros isolés). La formule analytique du nombre de classes se déduit alors de ce que ζ a pour résidu 1 en son pôle simple $s = 1$ (Proposition 9.3). □

Pour démontrer le lemme 9.7 il sera plus pratique de se ramener à dénombrer des idéaux principaux. C'est permis par l'énoncé suivant qui vaut pour tout corps de nombres K.

Lemme 9.8. *Soit C une classe d'idéaux de $\mathcal{O}_K$, J un idéal de $\mathcal{O}_K$ qui est dans la classe C^{-1}, et soit $n \geq 1$ un entier. L'application $I \mapsto IJ$ est une bijection entre l'ensemble des idéaux de norme n dans la classe C et celui des idéaux principaux inclus dans J et de norme $n\mathrm{N}(J)$.*

Démonstration — Si $I \in C$ alors $[I][J] = 1$ donc IJ est principal, de norme $\mathrm{N}(I)\mathrm{N}(J)$ par multiplicativité de la norme. L'application $I \mapsto IJ$ de l'énoncé est injective car J est inversible. Enfin, si $I' \subset J$ est principal de norme $n\mathrm{N}(J)$, il existe un unique I tel que $J = II'$ et on constate que $\mathrm{N}(I) = n$ (multiplicativité de la norme) et $[J] = [I]$: l'application est aussi surjective. □

Fixons J un idéal dans la classe C^{-1}. Il reste à dénombrer les idéaux principaux de J de norme $\leq n\mathrm{N}(J)$. Chaque tel idéal ayant exactement w_K générateurs, et comme $\mathrm{N}(z) = \mathrm{N}((z))$, il revient au même de dénombrer les éléments z du réseau $J \subset \mathbb{C}$ tels que $|z| \leq \sqrt{n\mathrm{N}(J)}$. On rappelle que J est de covolume $\frac{1}{2}\mathrm{N}(J)|D|^{\frac{1}{2}}$ (Thm. 6.15). On conclut alors par le lemme suivant, dans lequel $\mathbb{C}$ est identifié à $\mathbb{R}^2$ au moyen de la base $1, i$.

Lemme 9.9. *Soit $L \subset \mathbb{C}$ un réseau. Si $f(r) = |\{z \in L, |z| \leq r\}|$ alors*

$$f(r) = \frac{\pi\, r^2}{\mathrm{covol}(L)} + O(r), \;\; r \longrightarrow \infty.$$

Démonstration — Pour tout réel $r > 0$ on pose $B(r) = \{z \in \mathbb{C}, |z| \leq r\}$. Fixons Π un pavé fondamental de L ; il est d'aire $\mathrm{covol}(L)$. Fixons $\delta > 0$ vérifiant $\Pi \subset B(\delta)$. On a une réunion disjointe $\mathbb{C} = \coprod_{v\in L}(v + \Pi)$. Soit $n(r)$ le nombre des translatés $v + \Pi$, avec $v \in L$, vérifiant $v + \Pi \subset B(r)$. Si $(v + \Pi) \cap B(r) \neq \emptyset$, observons que $v + \Pi$ est strictement inclus dans $B(r + \delta)$. En particulier, on a les inégalités $n(r) \leq f(r) \leq n(r + \delta)$ et $\mathrm{covol}(L)\, n(r) \leq \pi r^2 \leq \mathrm{covol}(L)\, n(r + 2\delta)$. Cela conclut car pour $r > 2\delta$ ces deux encadrements entraînent

$$\pi(r - 2\delta)^2 \leq \mathrm{covol}(L) f(r) \leq \pi(r + \delta)^2.$$

□

3. Produits eulériens

3.1. Rappels sur les produits infinis. Soit b_n une suite de nombres réels positifs (ou ∞). La suite $\prod_{i=1}^{n}(1+b_i)$ croît avec l'entier n, et on note

$$\prod_n (1+b_n) \in \mathbb{R}_{>0} \cup \{\infty\}$$

sa limite. On dit que le produit des $1+b_n$ est convergent si $\prod_n(1+b_n) < \infty$. Il est clair que $\prod_n(1+b_n) \geq \sum_n b_n$, et l'inégalité $1+x \leq e^x$ pour $x \geq 0$ assure même que $\sum_n b_n < \infty$ si, et seulement si, $\prod_n(1+b_n) < \infty$.

Si b_n est une suite de nombres complexes, on dit que le produit des $1+b_n$ est absolument convergent si $\prod_n(1+|b_n|) < \infty$. Dans ce cas, la finitude de $\sum_n |b_n|$ montre par critère de Cauchy que la suite $\prod_{i=1}^{n}(1+b_i)$ converge quand $n \to \infty$ vers un nombre complexe noté $\prod_i(1+b_i)$. Elle entraîne de plus que pour toute bijection σ de $\mathbb{N}$, on a l'égalité $\prod_i(1+b_{\sigma(i)}) = \prod_i(1+b_i)$. Ces propriétés ne sont pas sans rappeler celles des familles sommables.

3.2. Produits eulériens. Un produit eulérien est un produit infini absolument convergent indexé par les nombres premiers. Dans ce chapitre, ils auront la forme particulière qui suit. Soit $(a_n)_{n\geq 1}$ une suite de nombres complexes. On suppose que $a_1 = 1$ et que $a_{nm} = a_n a_m$ si n et m sont premiers entre eux ("multiplicativité").

LEMME 9.10. (Euler) *Soient $s \in \mathbb{C}$ et $\sigma = \mathrm{Re}(s)$. Les conditions suivantes sont équivalentes :*

(i) $\prod_p(\sum_{i\geq 0} \frac{|a_{p^i}|}{p^{i\sigma}}) < \infty$, le produit étant pris sur tous les nombres premiers p,

(ii) $\sum_{n\geq 1} \frac{|a_n|}{n^\sigma} < \infty$.

Si elles sont satisfaites alors

$$\prod_p (\sum_{i\geq 0} \frac{a_{p^i}}{p^{is}}) = \sum_{n\geq 1} \frac{a_n}{n^s}.$$

le produit infini de gauche étant absolument convergent.

DÉMONSTRATION — On a l'inégalité dans $\mathbb{R}^+ \cup \{\infty\}$

$$\sum_{n\geq 1} \frac{|a_n|}{n^\sigma} \leq \prod_p (\sum_{i\geq 0} \frac{|a_{p^i}|}{p^{i\sigma}}) \leq e^{\sum_{n\geq 1} \frac{|a_n|}{n^\sigma}}.$$

En effet, cela découle de la factorialité de $\mathbb{Z}$ combinée à la multiplicativité de (a_n), ainsi que de l'inégalité $1+x \leq e^x$ pour $x \geq 0$. L'équivalence de (i) et (ii) en découle. Supposons maintenant que ces assertions sont satisfaites. Le (i) entraîne que le produit de gauche est absolument convergent. Soit N un entier et soit S_N l'ensemble des entiers n'ayant que des diviseurs premiers $\leq N$. Par factorialité de $\mathbb{Z}$ et multiplicativité de (a_n) on a l'égalité

$$\prod_{p\leq N} (\sum_{i\geq 0} \frac{a_{p^i}}{p^{is}}) = \sum_{n\in S_N} \frac{a_n}{n^s}.$$

On conclut la dernière assertion en faisant tendre $N \to \infty$, le terme de gauche convergent vers le produit infini indiqué par le (i) et celui de droite vers $\sum_{n\geq 1} \frac{a_n}{n^s}$ par le (ii). □

THÉORÈME 9.11. *Si χ est un caractère de Dirichlet, alors pour $\mathrm{Re}(s) > 1$ on a*

$$L(s,\chi) = \prod_p \frac{1}{1-\chi(p)p^{-s}},$$

le produit étant absolument convergent et indexé par tous les nombres premiers.

DÉMONSTRATION — En effet, on applique le lemme précédent à $a_n = \chi(n)$. La propriété (ii) est satisfaite si $\mathrm{Re}(s) > 1$. De plus, pour tout $i \geq 1$ et p premier on a $\chi(p^i) = \chi(p)^i$, d'où la série géométrique

$$\sum_{i\geq 1} \frac{\chi(p^i)}{p^{is}} = \frac{1}{1-\chi(p)p^{-s}}.$$

□

Quand $L(s,\chi) = \zeta(s)$, ce développement est bien connu et dû à Euler. C'est le point de départ de l'approche par la fonction ζ des propriétés de répartition des nombres premiers. Il admet un analogue pour tous les corps de nombres.

THÉORÈME 9.12. *ζ_K converge absolument sur $\mathrm{Re}(s) > 1$ et définit en particulier une fonction holomorphe sur ce demi-plan. De plus, si $\mathrm{Re}(s) > 1$ alors*

$$\zeta_K(s) = \prod_P \frac{1}{1-\mathrm{N}(P)^{-s}},$$

le produit étant absolument convergent et portant sur tous les idéaux premiers P de K.

DÉMONSTRATION — Soit a_n le nombre d'idéaux de $\mathcal{O}_K$ de norme n. On a $a_1 = 1$. Le fait que $\mathcal{O}_K$ est un anneau de Dedekind, ainsi que la multiplicativité de la norme, entraînent de plus que $a_{nm} = a_n a_m$ si m et n sont premiers entre eux, et aussi que pour tout nombre premier p et pour $\mathrm{Re}(s) > 0$:

$$\prod_{P|p} \frac{1}{1-\mathrm{N}(P)^{-s}} = \sum_{i\geq 0} \frac{a_{p^i}}{p^{is}}, \tag{7}$$

le produit étant indexé par l'ensemble fini des idéaux premiers P de $\mathcal{O}_K$ contenant p.

Vérifions que le produit de l'énoncé est absolument convergent. On rappelle que le nombre premier p étant donné, il y a au plus $[K:\mathbb{Q}]$ idéaux premiers P de $\mathcal{O}_K$ contenant p et que pour chaque tel P on a $\mathrm{N}(P) = p^f$ avec $f \geq 1$. En particulier, $|(1-\mathrm{N}(P)^{-s})^{-1} - 1| \leq 2p^{-\sigma}$ si $\sigma = \mathrm{Re}(s) > 0$. Ainsi, pour $\sigma = \mathrm{Re}(s) > 1$ on a

$$\sum_p \sum_{P|p} |(1-\mathrm{N}(P)^{-s})^{-1} - 1| \leq 2[K:\mathbb{Q}] \sum_p p^{-\sigma} < 2[K:\mathbb{Q}]\zeta(\sigma) < \infty$$

d'où la convergence absolue du produit de l'énoncé. L'identité (7) et la positivité des a_n montrent que la condition (i) du lemme 9.10 est satisfaite, et donc sa conclusion qui est le théorème. □

4. Factorisation de la fonction ζ d'un corps quadratique imaginaire

Considérons à nouveau le cas d'un corps quadratique imaginaire K. On écrit encore $K = \mathbb{Q}(\sqrt{D})$ avec D tel que $\mathcal{O}_K = A_D$. Bien que nous énoncerons les résultats pour un discriminant fondamental $D < 0$ quelconque, nous ne donnerons de démonstration complète que dans le cas particulier $D = -\ell$ avec ℓ un nombre premier $\equiv 3 \bmod 4$, en renvoyant aux exercices pour le cas général.

PROPOSITION 9.13. (Le caractère de Kronecker) *Il existe un unique caractère de Dirichlet*

$$\chi_D : (\mathbb{Z}/D\mathbb{Z})^\times \to \{\pm 1\}$$

tel que pour tout nombre premier $p \nmid D$, $\chi_D(p) = 1$ si, et seulement si, D est un carré modulo $4p$. Il est impair : $\chi(-1) = -1$.

DÉMONSTRATION — L'unicité est évidente. En ce qui concerne l'existence, supposons pour simplifier que $D = -\ell$ comme ci-dessus. Vérifions que

$$\chi_{-\ell}(-) = \left(\frac{-}{\ell}\right)$$

convient. En effet, l'assertion sur les premiers impairs s'écrit $\left(\frac{p}{\ell}\right) = \left(\frac{-\ell}{p}\right)$, qui découle de la loi de réciprocité quadratique car $\ell \equiv 3 \bmod 4$. D'autre part, $-\ell$ est un carré modulo 8 si, et seulement si, $\ell \equiv 7 \bmod 8$, l'assertion sur le nombre premier 2 découle alors de la loi complémentaire $\left(\frac{2}{\ell}\right) = (-1)^{\frac{\ell^2-1}{8}}$. Enfin, $\left(\frac{-1}{\ell}\right) = -1$ car $\ell \equiv 3 \bmod 4$. Nous renvoyons à l'exercice 9.7 pour le cas général. On verrait par exemple que si D est impair alors $\chi_D(-) = \left(\frac{-}{|D|}\right)$ (symbole de Jacobi). □

THÉORÈME 9.14. *Si* $\mathrm{Re}(s) > 1/2$ *et* $s \neq 1$, *alors* $\zeta_K(s) = \zeta(s)L(s, \chi_D)$.

DÉMONSTRATION — On a vu que les fonctions ζ_K, ζ et $L(s, \chi_D)$ sont méromorphes sur $\mathrm{Re}(s) > 1/2$ et holomorphes hors de $s = 1$. Il suffit donc de vérifier le théorème quand $\mathrm{Re}(s) > 1$ (principe des zéros isolés). Dans cette région, on a vu qu'elles possèdent un produit eulérien. D'après la proposition précédente et le Corollaire 7.19, la décomposition de $p\mathcal{O}_K$ en produit idéaux premiers quand p est premier se lit sur $\chi_D(p)$. En réordonnant les termes de l'écriture du produit eulérien (absolument convergent) de ζ_K en regroupant les premiers p ramifiés, puis décomposés, puis inertes, on constate que pour $\mathrm{Re}(s) > 1$

$$\zeta_K(s) = \prod_{p|D} \frac{1}{1-p^{-s}} \prod_{\chi_D(p)=1} \frac{1}{(1-p^{-s})^2} \prod_{\chi_D(p)=-1} \frac{1}{1-p^{-2s}}.$$

On conclut par le théorème 9.11 et la relation $1 - p^{-2s} = (1 - p^{-s})(1 + p^{-s})$. □

THÉORÈME 9.15. (Dirichlet) $\frac{2\pi\, \mathrm{h}(D)}{w_K |D|^{1/2}} = L(1, \chi_D)$. *En particulier,* $L(1, \chi_D) \neq 0$.

DÉMONSTRATION — Cela résulte du théorème précédent en écrivant de deux manières le résidu du pole simple de ζ_K en $s = 1$ (Thm. 9.6, Prop. 9.3). □

Le dernier miracle est qu'il existe une formule close simple pour $L(1,\chi_D)$.

THÉORÈME 9.16. (Dirichlet) *Soit* $\chi : (\mathbb{Z}/D\mathbb{Z})^\times \to \{\pm 1\}$ *tel que* $\chi(-1) = -1$. *Alors*

$$L(1,\chi) = \frac{\pi}{|D|^{1/2}(2-\chi(2))} \sum_{1\leq k<\frac{-D}{2}} \chi(k).$$

Combinée au théorème précédent, on en déduit la formule annoncée dans l'introduction pour $\mathrm{h}(D)$!

THÉORÈME 9.17. (Formule du nombre de classes de Dirichlet) *Si* $D<0$ *est un discriminant fondamental alors*

$$\mathrm{h}(D) = \frac{w_K}{2(2-\chi_D(2))} \sum_{1\leq k<\frac{-D}{2}} \chi_D(k).$$

4.1. Démonstration du théorème 9.16. La fin de cette partie est consacrée à établir la formule plus haut pour $L(1,\chi)$ dans le cas particulier où $\chi(-) = \left(\frac{-}{\ell}\right)$ avec ℓ premier $\equiv 3 \bmod 4$. Nous indiquerons à la fin les modifications nécessaires pour traiter le cas général.

Soit $\zeta = e^{\frac{2i\pi}{\ell}}$ et $G = \sum_{a=1}^{\ell-1} \chi(a)\zeta^a$ la somme de Gauss relative à ℓ. Un changement de variables $a \mapsto na$ assure que pour tout $n \in (\mathbb{Z}/\ell\mathbb{Z})^\times$ on a

$$\chi(n) = \frac{1}{G} \sum_{a\in(\mathbb{Z}/\ell\mathbb{Z})^\times} \chi(a)\zeta^{na}.$$

C'est encore vrai si $n \equiv 0 \bmod \ell$ car les deux membres sont égaux à 0 cela vaut donc pour tout $n \in \mathbb{Z}$.

LEMME 9.18. $L(1,\chi) = \frac{1}{G}\sum_{a\in(\mathbb{Z}/\ell\mathbb{Z})^\times} \chi(a)(\sum_{n\geq 1} \frac{\zeta^{na}}{n})$.

En effet, la proposition 9.4 permet d'écrire $L(1,\chi)$ comme limite quand N tend vers $+\infty$ des sommes partielles $\sum_{n=1}^{N\ell} \frac{\chi(n)}{n}$, et on utilise l'identité ci-dessus et l'assertion de convergence du lemme qui suit.

LEMME 9.19. *Si* $1 \leq a \leq \ell-1$, *la série* $\sum_{n\geq 1} \frac{\zeta^{an}}{n}$ *est convergente de somme* $-\log(2\sin(\frac{a\pi}{\ell})) - i\pi(\frac{a}{\ell} - \frac{1}{2})$.

DÉMONSTRATION — Dans ce lemme, ℓ est un entier ≥ 1 quelconque et $\zeta = e^{\frac{2i\pi}{\ell}}$. La série $\sum_{n\geq 1} \frac{\zeta^{na}}{n}$ est convergente (bien que non absolument convergente) d'après le lemme 9.5 car $|\sum_{n=p}^{q} \zeta^{an}|$ est bornée indépendamment de p, q, puisque ℓ ne divise pas a.

Considérons le logarithme principal sur $\mathbb{C} - \mathbb{R}_{\geq 0}$, qui est défini par $\log(re^{i\theta}) = \log(r) + i\theta$ si $r > 0$ et $\theta \in]-\pi, \pi[$. Il est bien connu que c'est une fonction holomorphe sur cet ouvert dont le développement en série entière autour de 1 s'écrit

$$-\log(1-z) = \sum_{n\geq 1} \frac{z^n}{n}, \quad |z| < 1.$$

Le lemme de convergence radiale d'Abel (voir les exercices) assure que cette identité vaut aussi sur $|z| = 1$ et $z \neq 1$. Mais $1 - \zeta^a = -2i\zeta^{a/2}\sin(\frac{a\pi}{\ell})$ où $\sin(\frac{a\pi}{\ell}) > 0$ et $\frac{a\pi}{\ell} - \frac{\pi}{2} \in]-\frac{\pi}{2}, \frac{\pi}{2}[$. □

Observons que $\sum_{a\in(\mathbb{Z}/\ell\mathbb{Z})^\times}\chi(a)=0$ et que $\chi(a)\log(\sin(\frac{a\pi}{\ell}))$ est changé en son opposé par le changement de variables $a\mapsto\ell-a$ car $\chi(-1)=-1$. On a démontré le

LEMME 9.20. $L(1,\chi)=\frac{-i\pi}{\ell G}\sum_{a=1}^{\ell-1}\chi(a)a$.

Il est possible de simplifier encore un peu la somme de droite.

LEMME 9.21. $\sum_{a=1}^{\ell-1}\chi(a)a=\frac{-\ell}{2-\chi(2)}\sum_{a=1}^{\frac{\ell-1}{2}}\chi(a)$.

DÉMONSTRATION — Posons $A=\sum_{a=1}^{\ell-1}\chi(a)a$, $A'=\sum_{a=1}^{\frac{\ell-1}{2}}\chi(a)a$ et $B=\sum_{a=1}^{\frac{\ell-1}{2}}\chi(a)$. On constate que

$$A=A'+\sum_{a=1}^{\frac{\ell-1}{2}}\chi(\ell-a)(\ell-a)=2A'-\ell B,$$

car $\chi(\ell-a)=\chi(-a)=-\chi(a)$. On conclut par la seconde relation

$$A=\sum_{a=1}^{\frac{\ell-1}{2}}\chi(2a)2a+\sum_{a=1}^{\frac{\ell-1}{2}}\chi(\ell-2a)(\ell-2a)=4\chi(2)A'-\ell\chi(2)B.$$

□

Notons que si $\chi(2)=-1$, i.e. $\ell\equiv 3 \bmod 8$, et si $\ell\neq 3$, il résulte de ce lemme que $\sum_{a=1}^{\frac{\ell-1}{2}}\chi(a)\in 3\mathbb{Z}$, fait que nous avions observé dans l'introduction. Jusqu'ici nous avons donc montré l'identité suivante.

COROLLAIRE 9.22. $L(1,\chi)=\frac{i\pi}{G(2-\chi(2))}\sum_{a=1}^{\frac{\ell-1}{2}}\chi(a)$.

On rappelle que $G^2=-\ell$ car $\ell\equiv 3 \bmod 4$, i.e. $G=\pm i\ell^{1/2}$. On constate que le théorème 9.16 découle du calcul par Gauss du signe de iG :

THÉORÈME 9.23. (Gauss) $G=i\sqrt{\ell}$.

Nous renvoyons à l'exercice 1.14 pour la démonstration par Dirichlet de ce théorème. Avec les notations de l'énoncé il est donc équivalent au fait que $C\geq N$! Observons que sans cette détermination du signe de la somme de Gauss, on peut simplement conclure que pour $\ell>3$,

$$\mathrm{h}(-\ell)=\frac{|C-N|}{2-(-1)^{\frac{\ell^2-1}{8}}},$$

ce qui est déjà fort intéressant. Pour traiter le cas d'un caractère $\chi:(\mathbb{Z}/\ell\mathbb{Z})^\times\to\{\pm 1\}$ modulo un entier $\ell\geq 1$ quelconque et tel que $\chi(-1)=-1$, on procède de manière tout à fait similaire en introduisant la somme de Gauss relative à χ définie par

$$G(\chi)=\sum_{a\in(\mathbb{Z}/\ell\mathbb{Z})^\times}\chi(a)\zeta^a,$$

où l'on a encore $\zeta=e^{\frac{2i\pi}{\ell}}$. Tous les lemmes ci-dessus s'appliquent verbatim, jusqu'à le dernière étape qui consiste à determiner $G(\chi)$, et on a encore $G(\chi)=i\ell^{1/2}$ (Dirichlet, comparer avec l'exercice 1.14).

5. La formule analytique du nombres de classes de Dedekind

La formule analytique du nombre de classes admet une généralisation à tous les corps de nombres.

THÉORÈME 9.24. (Dedekind) *$\zeta_K(s)$ est holomorphe sur* $\mathrm{Re}(s) > 1$ *et admet un prolongement méromorphe sur* $\mathrm{Re}(s) > 1 - \frac{1}{[K:\mathbb{Q}]}$ *avec pour unique pôle simple* $s = 1$. *De plus,*

$$\mathrm{Res}_{s=1}\zeta_K(s) = \frac{2^{r_1+r_2}\pi^{r_2}\mathrm{h}_K R_K}{w_K|\mathrm{disc}(K)|^{\frac{1}{2}}}.$$

Quand K est quadratique réel il est aussi dû à Dirichlet. Le nombre w_K est le nombre (fini) de racines de l'unité dans $\mathcal{O}_K$. La quantité R_K, appelée régulateur de K, n'a pas été définie dans ce cours : on la définit quand on démontre le théorème des unités de Dirichlet, nous renvoyons par exemple à ce sujet au livre de Marcus *Number fields*. Notons que $R_K = 1$ quand $K = \mathbb{Q}$ où K est un corps quadratique imaginaire. C'est bien le théorème 9.6 quand K est quadratique imaginaire. Quand $K = \mathbb{Q}$, on a $w_{\mathbb{Q}} = 2$, $r_1 = 1$, $r_2 = 0$, on trouve que le résidu vaut 1 : c'est en accord avec la proposition 9.3.

Mentionnons pour conclure le résultat fameux suivant :

THÉORÈME 9.25. (Hecke) *Pour tout corps de nombres K, $\zeta_K(s)$ admet un prolongement méromorphe à $\mathbb{C}$ tout entier qui admet $s = 1$ pour unique pôle.*

6. Exercices

EXERCICE 9.1. (Théorème de la convergence radiale d'Abel) *Soit $f(z) = \sum_{n\geq 0} a_n z^n$ une série entière de rayon de convergence ≥ 1 et telle que $\sum_n a_n$ converge. Montrer que $f(r) \to \sum_n a_n$ si $r \underset{r \text{ reel}}{\longrightarrow} 1^-$.*

EXERCICE 9.2. *Montrer* $1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} + \cdots = \frac{\pi}{4}$.

EXERCICE 9.3. *Montrer* $\sum_{n\geq 0} \frac{1}{7n+1} + \frac{1}{7n+2} - \frac{1}{7n+3} + \frac{1}{7n+4} - \frac{1}{7n+5} - \frac{1}{7n+6} = \frac{\pi}{\sqrt{7}}$.

EXERCICE 9.4. *(i) Décrire l'unique caractère χ de Dirichlet modulo 4 qui est non trivial.*

(ii) Montrer $\zeta_{\mathbb{Q}(i)}(s) = \zeta(s)L(s,\chi)$.

(iii) En déduire que le nombre de façons d'écrire un entier n comme somme de deux carrés est $4(d_1(n) - d_3(n))$ où $d_i(n)$ est le nombre de diviseurs de n congrus à i modulo 4.

(iv) Vérifier la formule analytique du nombre de classes sur cet exemple.

EXERCICE 9.5. *Soit K un corps quadratique imaginaire et soit $D = \mathrm{disc}(K)$.*

(i) Soit $C \in \mathrm{Cl}(O_K)$ une classe d'idéaux et q une forme binaire positive de discriminant D telle que $[q] = q_{C^{-1}}$. Montrer que pour $\mathrm{Re}(s) > 1$ on a l'égalité de séries absolument convergentes

$$w_K \sum_{I \in C} \frac{1}{\mathrm{N}(I)^s} = \sum_{n \geq 1} \frac{r_q(n)}{n^s} = \sum_{(x,y) \in \mathbb{Z}^2 \setminus (0,0)} \frac{1}{q(x,y)^s}.$$

où $r_C(n) = |\{(x,y) \in \mathbb{Z}^2, q(x,y) = n\}|$ (il ne dépend pas du choix de q tel que $[q] = q_{C^{-1}}$).

(ii) En déduire pour tout entier $n \geq 1$ la relation $\sum_C r_C(n) = w_K \sum_{d|n} \chi_D(d)$.

Exercice 9.6. *Soit 1_N le caractère de Dirichlet modulo N trivial. Montrer que pour $\mathrm{Re}(s) > 1$ on a*

$$L(s, 1_N) = \prod_{p|N} (1 - p^{-s})\ \zeta(s) = \prod_{p \nmid N} \frac{1}{1 - p^{-s}}.$$

Exercice 9.7. (Le caractère de Kronecker) *Soit $D \in \mathbb{Z}$ non carré tel que $D \equiv 0, 1 \bmod 4$. Soit $\chi_D : \mathbb{Z} \to \{0, \pm 1\}$ l'unique fonction telle que :*

(a) $\chi_D(mn) = \chi_D(n)\chi_D(m)$ pour tout $m, n \in \mathbb{Z}$,

(b) $\chi_D(-1) \in \{\pm 1\}$ est du signe de D, $\chi_D(n) = 0$ si, et seulement si, n n'est pas premier à D,

(c) pour tout nombre premier $p \nmid D$, on a $\chi_D(p) = 1$ si, et seulement si, D est un carré modulo $4p$.

On se propose de montrer que χ_D est D-périodique : $\chi_D(n + D) = \chi_D(n)$ pour tout $n \in \mathbb{Z}$.

(i) On suppose D non fondamental, i.e. $D = D'C^2$ avec $C \in \mathbb{Z}$ et $D' \equiv 0, 1 \bmod 4$. Montrer que $\chi_D(n) = \chi_{D'}(n)$ pour tout n premier à D.

(ii) On suppose D fondamental impair. Montrer que $\chi_D(n) = \left(\frac{n}{|D|}\right)$ (symbole de Jacobi) pour tout entier $n \in \mathbb{Z}$.

(iii) On suppose D fondamental pair, et on écrit $D = 4D'u$ avec $D' \equiv 1 \bmod 4$ et $u = \{-2, -1, 2\}$. Montrer que $\chi_D(n) = \left(\frac{n}{|D'|}\right) \chi(n)$ pour tout $n \in 2\mathbb{Z} + 1$, où $\chi(n) = (-1)^{\frac{n-1}{2}}$, $(-1)^{\frac{n^2-1}{8}}$ ou $(-1)^{\frac{n-1}{2} + \frac{n^2-1}{8}}$ selon que $u = -1, 2$ ou -2 respectivement.

(iv) Conclure.

Exercice 9.8. (Densité de Dirichlet)

(i) Montrer que si s est réel > 1, on a

$$\sum \frac{1}{np^{ns}} \leq 2\zeta(2s),$$

la somme de gauche portant sur les entiers $n \geq 2$ et les nombres premiers p.

(ii) En déduire $\sum_p \frac{1}{p^s} = -\log(s-1) + O(1)$ *quand* $s \to 1^+$.

Soit $\mathcal{P}$ *l'ensemble des nombres premiers. On dit que* $A \subset \mathcal{P}$ *admet une densité de Dirichlet si il existe* $\mathrm{d}(A) \in \mathbb{R}_{\geq 0}$ *tel que* $\sum_{p \in A} p^{-s} \underset{s \to 1^+}{\sim} -d(A)\log(s-1)$. *On appelle alors* $\mathrm{d}(A)$ *la densité (de Dirichlet) de* A. *D'après (ii),* $\mathcal{P}$ *admet pour densité* 1.

(iii) Montrer que si $A \subset \mathcal{P}$ *admet une densité de Dirichlet, il en va de même de* $\mathcal{P}\backslash A$, *ainsi que l'égalité*

$$\mathrm{d}(A) + \mathrm{d}(\mathcal{P}\backslash A) = 1.$$

(iv) Montrer que si A *est fini alors* $\mathrm{d}(A) = 0$. *Donner un exemple de partie* $A \subset \mathcal{P}$ *infinie admettant* 0 *pour densité.*

Exercice 9.9. (Densité des premiers $p \equiv 1 \bmod 4$, d'après Dirichlet)

(i) Montrer $\sum_{p \equiv 1 \bmod 4} \frac{1}{p^s} + \sum_{p \equiv 3 \bmod 4} \frac{1}{p^s} = -\log(s-1) + O(1)$ *quand* $s \to 1^+$.

(ii) En considérant $\log L(s, \chi_{-4})$, *montrer aussi que quand* $s \to 1^+$ *alors*

$$\sum_{p \equiv 1 \bmod 4} \frac{1}{p^s} - \sum_{p \equiv 3 \bmod 4} \frac{1}{p^s} = O(1).$$

(iii) En déduire que pour $i = 1, 3$, *l'ensemble des premiers* $p \equiv i \bmod 4$ *admet la densité de Dirichlet* $\frac{1}{2}$. *En particulier, ces ensembles sont infinis.*

Exercice 9.10. *Supposons* $D < 0$ *et* $D \equiv 0, 1 \bmod 4$. *Montrer que l'ensemble des nombres premiers* $p > 2$ *tels que* $\chi_D(p) = 1$ *est de densité* $\frac{1}{2}$. *En particulier, il est infini.*

Soit $N \geq 1$ un entier. Il n'est pas difficile de voir par des arguments similaires que la non-nullité de $L(1, \chi)$ pour tous les caractères de Dirichlet non triviaux modulo N entraîne que pour tout entier a premier à N, l'ensemble des nombres premiers $p \equiv a \bmod N$ admet pour densité $\frac{1}{\varphi(N)}$ (Dirichlet). Ceci peut se déduire soit par la formule analytique du nombre de classes pour le corps cyclotomique $\mathbb{Q}(e^{2i\pi/N})$ (voir par exemple le livre de Marcus), soit élémentairement. On pourra consulter par exemple le chapitre VI du *Cours d'arithmétique* de J.-P. Serre, ou le chapitre 2 du livre *Multiplicative number theory* de H. Davenport. Un bon exercice pour comprendre le cas général est le suivant.

Problème 9.1. *Soit* $1 \leq a \leq 4$. *Montrer que la densité des nombres premiers* $\equiv a \bmod 5$ *est* $\frac{1}{4}$.

Annexe A

Problèmes de révisions et examens

1. Problèmes de révisions

Problème 1. (Théorème de Rabinowitz) *Soit k un entier ≥ 2. On se propose de démontrer l'équivalence entre les propriétés suivantes :*

(a) *x^2+x+k est un nombre premier pour tout entier $0 \leq x < k-1$,*

(b) *x^2+x+k est un nombre premier pour tout entier $0 \leq x < \sqrt{k/3} - 1/2$,*

(c) $|\mathrm{Cl}(1-4k)| = 1$.

(i) Montrer (b) $\Rightarrow$ (c) *(penser aux formes réduites).*

(ii) Soit $n \in \mathbb{Z}$ non carré et représenté par la forme $(1,1,k)$. Montrer $n \geq k$.

(iii) Montrer que si une forme q représente primitivement l'entier n, et si m est un diviseur de n, alors il existe une forme q' de même discriminant que q et qui représente primitivement l'entier m.

(iv) En déduire (c) $\Rightarrow$ (a).

(v) Conclure, puis expliquer l'observation d'Euler : les 40 premières valeurs du polynôme X^2+X+41 sont des nombres premiers.

Problème 2. *Soit x un entier algébrique de polynôme minimal P. Montrer que si $|P(0)|$ est un nombre premier (au sens usuel) alors x est un élément premier de l'anneau $\mathbb{Z}[x]$.*

Problème 3. *(i) Déterminer des représentants de $\mathrm{Cl}(-132)$ ainsi que ses classes ambiguës.*

(ii) Déterminer l'ensemble C des carrés de $\mathbb{Z}/11\mathbb{Z}$.

(iii) Soit n un entier. Montrer que si $n \equiv 2 \bmod 3$, alors n n'est pas représenté par les formes x^2+33y^2 et $6x^2+6xy+7y^2$. Montrer de même que si $\left(\frac{n}{11}\right) = -1$ alors n n'est pas représenté par $3x^2+11y^2$.

(iv) En déduire que tout nombre premier $p \equiv 5 \bmod 12$ tel que $p \bmod 11 \notin C$ est de la forme $2x^2+2xy+17y^2$. Vérifier ce résultat sur quelques exemples.

Problème 4. *(i) Soit $u : \mathbb{Z}^n \to \mathbb{Z}^n$ une application $\mathbb{Z}$-linéaire vérifiant $\det(u) \neq 0$. Montrer que $u(\mathbb{Z}^n) = \{u(x) \mid x \in \mathbb{Z}^n\}$ est un sous-groupe de $\mathbb{Z}^n$ d'indice fini égal à $|\det(u)|$.*

(ii) (Application) *Soient $\alpha \in \overline{\mathbb{Z}}$, $K = \mathbb{Q}(\alpha)$ et $A = \mathbb{Z}[\alpha]$. Montrer que si $x \in A \backslash \{0\}$, alors l'idéal principal xA de A est d'indice fini égal à $|\mathrm{N}_{K/\mathbb{Q}}(z)|$.*

L'exercice qui suit concerne les corps cyclotomiques $\mathbb{Q}(\zeta)$ où $\zeta = e^{\frac{2i\pi}{p}}$ et p est un nombre premier. On rappelle que $\Pi_{\zeta,\mathbb{Q}}$ est le polynôme cyclotomique $\varphi_p = 1 + X + \cdots + X^{p-1}$. Dans le chapitre 4, on trouvera une démonstration du fait que l'anneau des entiers de $\mathbb{Q}(\zeta)$ est $\mathbb{Z}[\zeta]$. Cette information ne sera cependant pas nécessaire dans cet exercice.

PROBLÈME 5. (Un critère de non principalité de $\mathbb{Z}[e^{\frac{2i\pi}{p}}]$) *On suppose $p \equiv 3 \bmod 4$. On se propose de montrer que si $\mathbb{Z}[e^{\frac{2i\pi}{p}}]$ est principal, alors tout nombre premier $\ell \equiv 1 \bmod p$ est représenté par la forme $x^2 + xy + \frac{1+p}{4}y^2$.*

(i) Montrer $\sqrt{-p} \in \mathbb{Q}(\zeta)$.

(ii) Montrer que si L/K est une extension de corps de nombres, on a $\mathrm{N}_{L/\mathbb{Q}} = \mathrm{N}_{K/\mathbb{Q}} \circ \mathrm{N}_{L/K}$.

> *Indication : on pourra introduire un corps de nombres M contenant tous les $\sigma(L)$ avec $\sigma \in \Sigma(L)$, choisir pour chaque $\sigma \in \Sigma(K)$ un élément $\sigma' \in \Sigma(M)$ prolongeant σ, et vérifier que tout élément de $\Sigma(L)$ s'écrit de manière unique sous la forme $\sigma' \circ \tau$ où $\tau \in \Sigma(L/K)$ et $\sigma \in \Sigma(K)$.*

(iii) En déduire que si un entier n est de la forme $\mathrm{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(x)$ avec $x \in \mathbb{Z}[\zeta]$, alors on a $n = z\overline{z}$ où $z \in \mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$.

(iv) Soit ℓ un nombre premier tel que $\ell \equiv 1 \bmod p$. Montrer que φ_p est scindé dans $(\mathbb{Z}/\ell\mathbb{Z})[X]$.

(v) (suite) En déduire que $\mathbb{Z}[\zeta]$ contient un idéal Q de norme ℓ.

(vi) (suite) Montrer que si Q est principal alors ℓ est représenté par la forme $x^2 + xy + \frac{1+p}{4}y^2$.

(vii) Conclure.

(viii) En déduire que pour $p = 23$ l'anneau $\mathbb{Z}[\zeta]$ n'est pas principal (Kummer).

PROBLÈME 6. *Soient P le polynôme $X^4 - X + 1$, $\alpha \in \mathbb{C}$ une racine de P, et $A = \mathbb{Z}[\alpha]$.*

(i) Montrer $\alpha \notin \mathbb{R}$.

(ii) Montrer que α est une unité de l'anneau A, et que l'on a $\alpha^4 \neq 1$ et $\alpha^3 \neq \pm 1$.

(iii) En déduire que P est irréductible dans $\mathbb{Q}[X]$.

(iv) Montrer que tout idéal non nul de A est équivalent à un idéal contenant 1 ou 2.

(v) Montrer que X^2+X+1 est l'unique polynôme irréductible de degré 2 dans $(\mathbb{Z}/2\mathbb{Z})[X]$.

(vi) Montrer que l'anneau A est principal.

(vii) (Bonus) En déduire que A est l'anneau des entiers de $\mathbb{Q}(\alpha)$.

Données : on a $\operatorname{disc} P = -229$ et $\frac{3\sqrt{229}}{2\pi^2} \simeq 2.30$ à 10^{-2} près.

2. Examen 2011-2012

PROBLÈME 1. *On s'intéresse aux formes positives de discriminant* -136.

(i) Déterminer des représentants de $\mathrm{Cl}(-136)$.

(ii) Déterminer les classes ambiguës et les classes d'équivalence de formes de ce discriminant.

(iii) Soit p *un nombre premier tel que* $p \equiv 5, 7 \bmod 8$ *et* $\left(\frac{p}{17}\right) = -1$. *Montrer que* p *est de la forme* $5x^2 + 2xy + 7y^2$ *avec* $x, y \in \mathbb{Z}$.

On considère l'anneau $A = \mathbb{Z}[\alpha]$ *avec* $\alpha = \sqrt{-34}$.

(iv) Montrer que A *est un anneau de Dedekind.*

(v) Factoriser en produits d'idéaux premiers dans A *les idéaux* (2), (3), (5), (7) *et* $(1+\alpha)$.

(vi) Déduire de la théorie de Minkowski que $\mathrm{Cl}(A)$ *est engendré par les classes des idéaux*

$$D = 2A + (\alpha + 1)A \quad \text{et} \quad C = 5A + (\alpha + 1)A.$$

(vii) Vérifier que D *n'est pas principal.*

(viii) Montrer que DC^2 *est principal.*

(ix) En déduire $\mathrm{Cl}(A) \simeq \mathbb{Z}/4\mathbb{Z}$ *et que* $\mathrm{Cl}(A)$ *est engendré par* $[C]$.

(x) Pour chaque classe dans $\mathrm{Cl}(A)$ *déterminer la classe dans* $\mathrm{Cl}(-136)$ *qui lui est associée par le théorème de Dedekind.*

(xi) En déduire la table de multiplication de $\mathrm{Cl}(-136)$ *pour la loi de composition de Gauss.*

(xii) Supposons que p *et* q *sont deux nombres premiers (non nécessairement distincts) satisfaisant les conditions du (iii). Montrer que* pq *est de la forme* $2x^2 + 17y^2$, *ainsi que de la forme* $x^2 + 34y^2$.

(xiii) Vérifier ceci sur quelques exemples.

PROBLÈME 2. *Soit* $\zeta = e^{\frac{2i\pi}{8}}$. *On rappelle que l'on a* $\Pi_{\zeta,\mathbb{Q}} = X^4 + 1$.

(i) Soit $\iota : \mathbb{Q}(\zeta) \to \mathbb{C}^2$ *le plongement canonique (justifier), montrer* $\mathrm{covol}(\iota(\mathbb{Z}[\zeta])) = 4$.

(ii) En déduire que tout idéal non nul de $\mathbb{Z}[\zeta]$ *est équivalent à un idéal contenant* 1 *ou* 2.

(iii) (suite) Montrer qu'il existe cinq tels idéaux et les déterminer.

(iv) Montrer l'égalité $2 = \prod_{i \in (\mathbb{Z}/8\mathbb{Z})^\times} (1 - \zeta^i)$.

(v) Montrer que $\mathbb{Z}[\zeta]$ *est principal.*

(vi) En déduire que $\mathbb{Z}[\zeta]$ *est l'anneau des entiers de* $\mathbb{Q}(\zeta)$.

PROBLÈME 3. *Soit* $k > 0$ *un entier pair sans facteur carré. On suppose que l'équation* $y^2 = x^5 - k$ *admet une solution* $x, y \in \mathbb{Z}$, *on se propose de montrer que* $\mathrm{h}(-4k)$ *est divisible par* 5. *On pose* $A = \mathbb{Z}[\alpha]$ *avec* $\alpha = \sqrt{-k}$.

(i) Montrer que x *et* y *sont impairs et premiers entre eux.*

(ii) En déduire $(y + \alpha)A + (y - \alpha)A = A$.

(iii) Montrer qu'il existe un idéal I de A tel que $(y+\alpha) = I^5$.

(iv) On suppose $5 \nmid \mathrm{h}(-4k)$, montrer que I est principal.

(v) (suite) En déduire qu'il existe $a, b \in \mathbb{Z}$ vérifiant

$$y + \alpha = a^5 - 10ka^3b^2 + 5k^2ab^4 + (5a^4b - 10a^2b^3k + b^5k^2)\alpha.$$

(vi) (suite) En déduire $5a^4 - 10a^2k + k^2 = \pm 1$, puis conclure en raisonnant modulo 8.

(vii) Montrer que $\mathrm{h}(-296)$, $\mathrm{h}(-488)$, $\mathrm{h}(-776)$ et $\mathrm{h}(-872)$ sont multiples de 5 (noter que $3^5 = 243$).

3. Examen 2012-2013

PROBLÈME 1. *On s'intéresse aux formes positives de discriminant -104.*

(i) Déterminer l'ensemble des carrés de $(\mathbb{Z}/13\mathbb{Z})^\times$.

(ii) Soit p un nombre premier impair. Donner une condition nécessaire et suffisante sur $p \bmod 8$ et $p \bmod 13$ pour que -104 soit un carré modulo p.

(iii) Déterminer des représentants de $\mathrm{Cl}(-104)$.

(iv) Déterminer les classes ambiguës et les classes d'équivalence de formes de ce discriminant.

(v) On suppose que p est un nombre premier tel que $p \equiv 1, 3 \bmod 8$ et tel que p est un carré modulo 13. Montrer que p est, exclusivement, soit de la forme $x^2 + 26y^2$, soit de la forme $3x^2 + 2xy + 9y^2$.

(vi) Vérifier par des exemples que les deux cas se produisent.

On considère l'anneau $A = \mathbb{Z}[\alpha]$ avec $\alpha = \sqrt{-26}$.

(vii) Vérifier que A est l'anneau des entiers de $\mathbb{Q}(\alpha)$ et déterminer $\mathrm{disc}(A)$.

(viii) Déterminer les idéaux premiers de A contenant respectivement 2, 3 et 5.

(ix) (suite) Montrer qu'aucun de ces idéaux n'est principal.

(x) Factoriser en produits d'idéaux premiers dans A les idéaux (2), (3), (5), $(\alpha+2)$ et $(\alpha-2)$.

(xi) Déduire de la théorie de Minkowski que le groupe $\mathrm{Cl}(A)$ est engendré par les classes des idéaux trouvés au (viii).

(xii) Montrer que $\mathrm{Cl}(A)$ est engendré par les classes de $D = 2A + \alpha A$ et $T = 3A + (\alpha+1)A$.

(xiii) Montrer que T^3 est principal.

(xiv) En déduire $\mathrm{Cl}(A) \simeq \mathbb{Z}/6\mathbb{Z}$ et que $\mathrm{Cl}(A)$ est engendré par $[DT]$.

(xv) Montrer que les idéaux trouvés à la question (viii) forment un système de représentants des classes non triviales de $\mathrm{Cl}(A)$.

(xvi) Pour chaque classe $[I]$ dans $\mathrm{Cl}(A)$ déterminer la classe q_I de $\mathrm{Cl}(-104)$ qui lui est associée par Dedekind, et vérifier que $[I] \mapsto q_I$ induit bien une bijection $\mathrm{Cl}(A) \xrightarrow{\sim} \mathrm{Cl}(-104)$.

(xvii) En déduire l'ordre de $[(3,2,9)]$ dans le groupe $\mathrm{P}(-104) = \mathrm{Cl}(-104)$, ainsi qu'une composée de Gauss de $(2,0,13)$ et $(3,2,9)$.

(xviii) (Application) Montrer que si p est un nombre premier tel que $p \equiv 1, 3 \bmod 8$ et tel que p est un carré modulo 13, alors p^3 est de la forme $x^2 + 26y^2$ avec $x, y \in \mathbb{Z}$.

Problème 2. *(Un théorème de Gross-Rohrlich) Soit $A \subset \overline{\mathbb{Z}}$ un sous-anneau tel que $A^\times = \{1, -1\}$. Soit p un nombre premier impair et soient $x, y \in A$ tels que $x^p + y^p = 1$. On se propose de montrer, en préliminaire, que l'on a soit $(x, y) = (1, 0)$, soit $(x, y) = (0, 1)$.*

(i) Montrer $x + y \in A^\times$.

(ii) En considérant une congruence adéquate, montrer $x + y = 1$.

(iii) En déduire qu'il existe $P \in \mathbb{Z}[X]$ vérifiant $x(xP(x) - 1) = 0$.

(iv) Conclure.

Soient p un nombre premier, $K = \mathbb{Q}(\sqrt{1 - 2^{p+2}})$ et $\mathrm{h}_K := |\mathrm{Cl}(\mathcal{O}_K)|$. On se propose de démontrer que p divise h_K (théorème de Gross-Rohrlich).

(v) On écrit $1 - 2^{p+2} = DN^2$ où $D, N \in \mathbb{Z}$ et D est sans facteur carré. Montrer la congruence $D \equiv 1 \bmod 8$.

(vi) En déduire $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ et déterminer $\mathcal{O}_K^\times$.

(vii) Rappeler pourquoi $\mathrm{h}_K = |\mathrm{Cl}(D)|$ et conclure si $p = 2$.

(viii) Expliciter un élément $z \in \mathcal{O}_K$ tel que $2^p = z(1 - z)$.

(ix) Montrer qu'il existe des idéaux I et J de $\mathcal{O}_K$ tels que $(z) = I^p$ et $(1 - z) = J^p$.

(x) Supposons que p ne divise pas h_K. Montrer que I et J sont principaux.

(xi) En déduire que si $p \neq 2$ et p ne divise pas h_K, il existe $x, y \in \mathcal{O}_K$ tels que $z = x^p$ et $1 - z = y^p$.

(xii) Conclure.

(xiii) (Application) Montrer que $|\mathrm{Cl}(-511)|$ est multiple de 14.

4. Examen 2013-2014

Problème 1. *(i) Déterminer des représentants de $\mathrm{Cl}(-55)$ ainsi que ses classes ambiguës.*

(ii) En déduire que le groupe $\mathrm{P}(-55)$ est cyclique d'ordre 4 et donner sa table de multiplication.

(iii) Donner deux composées non équivalentes de la forme $(2, 1, 7)$ par elle-même.

(iv) Soit p un nombre premier tel que $p \neq 5, 11$. Montrer que p est représenté par une forme de discriminant -55 si, et seulement si, on a $\left(\frac{p}{5}\right) = \left(\frac{p}{11}\right)$. On traitera à part le cas $p = 2$.

(v) (suite) Supposons $\left(\frac{p}{5}\right) = \left(\frac{p}{11}\right) = -1$. Montrer que p est de la forme $2x^2 + xy + 7y^2$. Le vérifier sur deux exemples.

Problème 2. *Les deux parties de ce problème sont indépendantes.*

I. *Dans la question préliminaire suivante, A est un anneau intègre et $\pi \in A$ est irréductible.*

(i) Vérifier que si $(\pi) \subset I$ où I est un idéal principal de A, alors $I = (\pi)$ ou $I = A$. Rappeler aussi pourquoi l'idéal (π) est premier si et seulement si π est un élément premier.

Soit K un corps de nombres vérifiant $|\mathrm{Cl}(\mathcal{O}_K)| = 2$. On se propose de démontrer que pour tout $x \in \mathcal{O}_K$ qui n'est pas nul ou une unité, il existe un unique entier $n \geq 1$ tel que x soit produit de n éléments irréductibles de $\mathcal{O}_K$ (théorème de L. Carlitz).

(ii) Soit $\pi \in \mathcal{O}_K$ un élément irréductible non premier. Montrer que l'on a $(\pi) = PQ$, où P et Q sont des idéaux premiers non principaux de $\mathcal{O}_K$.

(iii) Soit $\mathcal{I}$ l'ensemble des idéaux non nuls de $\mathcal{O}_K$. Montrer qu'il existe $f : \mathcal{I} \to \mathbb{N}$ telle que :

- *pour tout $I, J \in \mathcal{I}$, $f(IJ) = f(I) + f(J)$,*
- *pour tout $P \in \mathcal{I}$ premier, $f(P) = 2$ si P est principal, $f(P) = 1$ sinon.*

(iv) Soient $\pi_1, \ldots, \pi_n$ et $\pi'_1, \ldots, \pi'_m$ des irréductibles de $\mathcal{O}_K$, où n et m sont des entiers ≥ 1. Montrer que l'égalité $\prod_{i=1}^{n} \pi_i = \prod_{j=1}^{m} \pi'_j$ entraîne $n = m$.

II. *On s'intéresse au corps de nombres $K = \mathbb{Q}(\sqrt{-31}) \subset \mathbb{C}$.*

(v) Vérifier que l'on a $\mathcal{O}_K = \mathbb{Z}[\alpha]$ avec $\alpha = \frac{1+\sqrt{-31}}{2}$, et déterminer $\mathrm{disc}(\mathcal{O}_K)$.

(vi) Déterminer les idéaux de $\mathcal{O}_K$ contenant 2 ou 3. Lesquels d'entre eux sont principaux ? (resp. premiers ?)

(vii) Décomposer en produit d'idéaux premiers les idéaux (2), (3) et (α).

(viii) Déduire de la théorie de Minkowski que l'on a $\mathrm{Cl}(\mathcal{O}_K) \simeq \mathbb{Z}/3\mathbb{Z}$.

(ix) Déterminer la classe de formes de discriminant -31 associée par Dedekind à l'idéal $(2, \alpha)$, puis expliciter la bijection de Dedekind $\mathrm{Cl}(\mathcal{O}_K) \xrightarrow{\sim} \mathrm{Cl}(-31)$.

(x) Soit p un nombre premier de la forme $2x^2+xy+4y^2$. Montrer que p est irréductible dans $\mathcal{O}_K$, et qu'il existe un irréductible $\pi \in \mathcal{O}_K$ tel que $p^3 = \pi\overline{\pi}$. Expliciter le cas $p = 2$.

(xi) Comparer les questions (x) et (iv).

Problème 3. *(Formes qui représentent un carré, d'après Gauss) Soit $K = \mathbb{Q}(\sqrt{d})$ où $d \in \mathbb{Z}$ n'est pas un carré. Soit I un idéal non nul de $\mathcal{O}_K$. On se propose de démontrer, en préliminaire, que l'entier $\mathrm{N}(I)$ est un carré si, et seulement si, il existe $m \in \mathbb{Z}$ et un idéal J de $\mathcal{O}_K$ tels que $I = mJ^2$.*

(i) Vérifier que si $I = mJ^2$, où m et J sont comme ci-dessus, alors $\mathrm{N}(I)$ est un carré.

(ii) Soit p un nombre premier. Rappeler pourquoi une et une seule des propriétés suivantes est satisfaite :

1. *$(p) = P^2$ où P est un idéal premier de $\mathcal{O}_K$,*
2. *$(p) = PQ$ où P et Q sont des idéaux premiers distincts de $\mathcal{O}_K$,*
3. *l'idéal (p) est premier.*

Déterminer, dans chacun des cas, les idéaux premiers de $\mathcal{O}_K$ contenant p, ainsi que leurs normes.

(iii) Conclure si $\mathrm{N}(I) = p^{2n}$ avec $n \geq 1$ et p premier.

(iv) Conclure dans tous les cas.

(v) (Application) Soit $x \in I$ non nul. Montrer que si $\frac{|\mathrm{N}_{K/\mathbb{Q}}(x)|}{\mathrm{N}(I)}$ est un carré alors $[I]$ est un carré dans le groupe $\mathrm{Cl}(\mathcal{O}_K)$. (On pourra introduire un idéal J tel que $(x) = IJ$.)

Soit $D \in \mathbb{Z}$ tel que $D \equiv 0, 1 \bmod 4$ et $D < 0$. On suppose que D est un discriminant fondamental, c'est-à-dire $\mathrm{Cl}(D) = \mathrm{P}(D)$.

(vi) Vérifier que l'anneau A_D introduit en cours est l'anneau des entiers de $\mathbb{Q}(\sqrt{D})$.

(vii) Soit q une forme de discriminant D. Montrer que q représente un carré si, et seulement si, $[q]$ est un carré dans $\mathrm{P}(D)$ (théorème de Gauss).

5. Examen 2014-2015

Problème 1. *Soient p un nombre premier $\equiv 1 \bmod 4$ et $A = \mathbb{Z}[\sqrt{-p}]$. On se propose de démontrer que $|\mathrm{Cl}(A)|$ est multiple de 4 si, et seulement si, on a $p \equiv 1 \bmod 8$.*

(i) Justifier l'égalité $\mathrm{Pic}(A) = \mathrm{Cl}(A)$.

(ii) Considérons l'idéal $D = (2, 1 + \sqrt{-p})$ de A. Montrer $D^2 = (2)$ et $\mathrm{N}(D) = 2$.

(iii) Montrer que D n'est pas principal.

(iv) En déduire $|\mathrm{Cl}(A)| \equiv 0 \bmod 2$.

(v) Déterminer la forme réduite de Gauss dans la classe q_D de $\mathrm{Cl}(-4p)$ qui est associée à l'idéal D par la construction de Dedekind.

(vi) Montrer que les formes réduites et ambiguës de discriminant $-4p$ sont $(1, 0, p)$ et $(2, 2, \frac{p+1}{2})$.

(vii) En déduire que $[D]$ est l'unique élément d'ordre 2 du groupe $\mathrm{Cl}(A)$.

Si G est un groupe abélien, on note $\mathrm{C}(G) = \{g^2,\ g \in G\}$ le sous-groupe des carrés de G.

(viii) Soit G un groupe abélien fini possédant un unique élément d'ordre 2, noté z. Montrer $|\mathrm{C}(G)| = |G|/2$. En déduire que $z \in C$ si, et seulement si, on a la congruence $|G| \equiv 0 \bmod 4$.

On rappelle que l'on a défini dans le cours un morphisme de groupes $\varepsilon_p : \mathrm{P}(-4p) \to \{\pm 1\}$.

(ix) Déterminer $\varepsilon_p((2, 2, \frac{p+1}{2}))$.

(x) En déduire que si $|\mathrm{Cl}(A)| \equiv 0 \bmod 4$ alors $p \equiv 1 \bmod 8$.

Afin de prouver la réciproque, on se propose de démontrer que $\mathrm{C}(\mathrm{P}(-4p)) = \ker \varepsilon_p$ (Gauss).

(xi) Montrer qu'il existe un nombre premier $\ell \equiv 3 \bmod 4$ qui n'est pas un carré modulo p. (On admettra que si $a, b \in \mathbb{Z}$ sont premiers entre eux, il existe un nombre premier ℓ tel que $\ell \equiv a \bmod b$ (Dirichlet)).

(xii) En déduire qu'il existe une forme binaire q de discriminant $-4p$ telle que $\varepsilon_p(q) = -1$.

(xiii) En déduire l'égalité $\mathrm{C}(\mathrm{P}(-4p)) = \ker \varepsilon_p$.

(xiv) Montrer que $\mathrm{Cl}(A) \equiv 0 \bmod 4$ si, et seulement si, $p \equiv 1 \bmod 8$.

Les parties II et III du problème suivant sont indépendantes.

PROBLÈME 2. *Soient $d \in \mathbb{Z}$ tel que $d > 0$ et $P(X) = X^3 + dX + 1$.*

Partie I. Questions préliminaires

(i) Montrer que P admet une unique racine $\alpha \in \mathbb{R}$, et vérifier que α est dans l'intervalle $]-\frac{1}{d},\ -\frac{1}{d}+\frac{1}{d^2}\ [$.

(ii) Montrer que P est irréductible dans $\mathbb{Q}[X]$, et de discriminant $-4d^3-27$.

On considère le corps de nombres $K = \mathbb{Q}(\alpha) \subset \mathbb{R}$, où α est la racine réelle de P.

(iii) Déterminer les entiers $[K : \mathbb{Q}]$, r_1 et r_2 relatifs au corps de nombres K.

On fixe un plongement $\sigma : K \to \mathbb{C}$ tel que $\sigma(\alpha) \neq \alpha$ (justifier). On note $|z|$ le module de $z \in \mathbb{C}$.

(iv) Montrer que pour tout $x \in \mathcal{O}_K$, on a $|\sigma(x)|^2 \in \mathbb{Z}[x]$.

Partie II. On se propose de déterminer le groupe des unités $A^\times$ de l'anneau $A = \mathbb{Z}[\alpha] \subset \mathbb{R}$. On pose $A^1 = \{x \in A^\times,\ x > 0\}$.

(v) Montrer que A^1 est un sous-groupe de $A^\times$ contenant $-\alpha$, et $A = \{\pm x, x \in A^1\}$.

(vi) Montrer $A^1 = \{x \in A,\ x\,|\sigma(x)|^2 = 1\}$.

(vii) Montrer que pour tout réel $\rho > 1$, l'ensemble des $x \in \mathcal{O}_K^\times$ vérifiant $\frac{1}{\rho} \leq |x| \leq \rho$ est fini. En déduire que $\{\log x,\ x \in A^1\}$ est un réseau de $\mathbb{R}$.

(viii) Montrer qu'il existe un unique $\varepsilon \in A^1$ tel que $\varepsilon > 1$ et $A^1 = \langle\varepsilon\rangle$, puis que l'on a un isomorphisme $A^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.

(ix) (suite) Montrer $\mathbb{Z}[\varepsilon] = \mathbb{Z}[\alpha]$ et qu'il existe un unique entier $n \geq 1$ tel que $-\alpha^{-1} = \varepsilon^n$.

Dans la question suivante, on admettra que si $Q \in \mathbb{R}[X]$ est un polynôme unitaire de degré 3 possédant une unique racine réelle β, et si on a $Q(0) = 1$ et $\beta > 1$, alors $|\mathrm{disc}\, Q| < 4\beta^3 + 24$ (inégalité d'Artin).

(x) (suite) Montrer $(-\alpha^{-1})^{1/n} > d$, puis $n < \frac{\log(\frac{d^2}{d-1})}{\log d}$ si $d > 1$.

(xi) En déduire que si $d > 1$ on a $A^1 = \langle -\alpha\rangle$, puis $A^\times = \langle\alpha, -1\rangle$.

Partie III. On suppose désormais $d = 4$ et l'on se propose de déterminer $\mathrm{Cl}(\mathcal{O}_K)$.

(xii) Justifier la relation $\mathrm{disc}\,\mathbb{Z}[\alpha] = |\mathcal{O}_K/\mathbb{Z}[\alpha]|^2\,\mathrm{disc}\,\mathcal{O}_K$. En déduire $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

(xiii) Montrer que tout idéal non nul de $\mathbb{Z}[\alpha]$ est équivalent à un idéal divisant l'idéal (n) où $n \in \{1, 2, 3, 4\}$. (Indication : on a l'inégalité $\frac{8}{9}\sqrt{283} < 5\pi$).

(xiv) Montrer les décompositions $(2) = D_1D_2$ et $(3) = T_1T_2$ où D_1, D_2, T_1 et T_2 sont des idéaux premiers de $\mathbb{Z}[\alpha]$ de normes respectives $2, 4, 3$ et 9.

(xv) Montrer $(1-\alpha) = D_1T_1$ et $(1+\alpha) = D_1^2$. On pourra utiliser l'identité :

$$\det\begin{bmatrix} a & 0 & -b \\ b & a & -4\,b \\ 0 & b & a \end{bmatrix} = a^3 - b^3 + 4ab^2.$$

(xvi) En déduire $\mathrm{Cl}(\mathcal{O}_K) = \langle\,[D_1]\,\rangle$ et $[D_1]^2 = 1$.

(xvii) Montrer qu'il existe un morphisme surjectif d'anneaux $\varphi : \mathbb{Z}[\alpha] \to \mathbb{Z}/17\mathbb{Z}$ envoyant α sur 2.

(xviii) En utilisant le résultat de la question (xi), montrer que si $x \in A^\times$ *alors* $\varphi((1+\alpha)x)$ *n'est pas un carré dans* $\mathbb{Z}/17\,\mathbb{Z}$.

(xix) En déduire que D_1 *n'est pas principal. Conclure.*

6. Examen 2015-2016

Problème 1. *On pose* $\alpha = \frac{1+\sqrt{-127}}{2}$ *et* $A = \mathbb{Z}[\alpha]$.

(i) Déterminer des représentants de $\mathrm{Cl}(-127)$.

(ii) Déduire du théorème de Dedekind que $\mathrm{Cl}(A)$ *est isomorphe au groupe* $\mathbb{Z}/5\mathbb{Z}$.

On se propose de redémontrer le (ii) sans utiliser le théorème de Dedekind.

(iii) Montrer que tout idéal non nul de A *est équivalent à un idéal contenant un entier* N *avec* $1 \leq N \leq 7$.

(iv) Montrer que $\mathrm{Cl}(A)$ *est un groupe, et qu'il est engendré par les classes des idéaux premiers de* A *contenant* $2, 3, 5$ *ou* 7.

(v) Montrer qu'il existe exactement deux idéaux premiers de A *contenant* 2, *disons* I *et* J, *et que l'on a* $(2) = IJ$. *Montrer de plus que* I *et* J *ne sont pas principaux.*

(vi) Montrer que les idéaux (3), (5) *et* (7) *sont premiers.*

(vii) En déduire que $\mathrm{Cl}(A)$ *est engendré par la classe de* I.

(viii) Vérifier que la norme de α (*resp.* $1-\alpha$) *vaut* 2^5, *et en déduire que* $[I]$ *est d'ordre* 5 *dans* $\mathrm{Cl}(A)$. *Conclure.*

Problème 2. *Un théorème d'Ankeny et Chowla.*

Soient n et g deux entiers > 1. On suppose que l'entier $D = 1 - 4n^g$ est sans facteur carré. On se propose de montrer que si $K = \mathbb{Q}(\sqrt{D})$, alors le groupe $\mathrm{Cl}(\mathcal{O}_K)$ possède un élément d'ordre g. On pose $\alpha = \frac{1+\sqrt{D}}{2}$ et on note I l'idéal (α) de $\mathcal{O}_K$. On rappelle que si J est un idéal de $\mathcal{O}_K$, alors $\overline{J} = \{\overline{z}, z \in J\}$ est encore un idéal de $\mathcal{O}_K$ (où $\overline{z}$ désigne le conjugué du nombre complexe z).

(i) Montrer $\mathcal{O}_K = A_D = \mathbb{Z}[\alpha]$.

(ii) Montrer que I *et* $\overline{I}$ *sont "premiers entre eux", c'est-à-dire que l'on a* $I + \overline{I} = \mathcal{O}_K$.

(iii) Montrer $I\,\overline{I} = (n)^g$, *puis qu'il existe un idéal* J *de* $\mathcal{O}_K$ *tel que* $I = J^g$.

(iv) Soit $m \geq 1$ *un entier. Montrer* $J^m \neq \overline{J}^m$, *puis* $J^m \neq (x)$ *pour tout* $x \in \mathbb{Z}$.

(v) Soient q *la forme principale de discriminant* D *et* $(x, y) \in \mathbb{Z}^2$. *Montrer que si on a* $q(x, y) = n^m$ *avec* $1 \leq m < g$, *alors* $y = 0$.

(vi) Démontrer que $[J]$ *est d'ordre* g *dans* $\mathrm{Cl}(\mathcal{O}_K)$ *(théorème d'Ankeny-Chowla).*

(vii) Montrer $J = \mathbb{Z}n + \mathbb{Z}\alpha$.

(viii) En déduire l'ordre de la classe de la forme $(n, 1, n^{g-1})$ *dans le groupe* $\mathrm{P}(D)$.

(ix) (Application) *Montrer que le groupe* $\mathrm{P}(-2047)$ *contient un élément d'ordre* 18. *Question bonus : expliciter une forme de discriminant* -2047 *dont la classe est d'ordre* 18.

Données : $-2047 = -23 \cdot 89 = 23 \cdot (23 - 4 \cdot 28)$.

Problème 3. *Soient* K *un corps de nombres et* A *un ordre de* K. *On se propose, suivant Dirichlet, d'étudier la structure du groupe des unités* $A^\times$ *de l'anneau* A.

(i) Montrer l'égalité $A^\times = \{x \in A, |\mathrm{N}_{K/\mathbb{Q}}(x)| = 1\}$. *(On pourra utiliser la notion de polynôme caractéristique d'un élément de* K*.)*

(ii) Montrer que pour tout réel C*, il n'existe qu'un nombre fini d'idéaux de* A *de norme* $< C$.

(iii) En déduire que si $(x_m)_{m\geq 1}$ *est une suite d'éléments de* $A - \{0\}$ *telle que la suite* $(|\mathrm{N}_{K/\mathbb{Q}}(x_m)|)_{m\geq 1}$ *est majorée, il existe* $x \in A - \{0\}$ *tel que pour une infinité d'entiers* $m \geq 1$*, on a* $x_m/x \in A^\times$.

Pour simplifier, nous supposerons désormais que K est *totalement réel*, c'est-à-dire que tout plongement de K est à valeurs dans $\mathbb{R}$. En particulier, on a $K \subset \mathbb{R}$. On pose $n = [K : \mathbb{Q}]$ et on note Σ l'ensemble des plongements de K. On munit l'espace vectoriel réel $\mathbb{R}^\Sigma$ (de dimension n) de la mesure de Lebesgue pour laquelle le réseau $\mathbb{Z}^\Sigma$ est de covolume 1. Enfin, on note $\iota : K \to \mathbb{R}^\Sigma$ le plongement canonique, $x \mapsto (\sigma(x))_\sigma$.

(iv) Rappeler pourquoi $\iota(A)$ *est un réseau de covolume* $|\mathrm{disc}\, A|^{1/2}$.

(v) Soient σ *et* σ' *deux éléments distincts de* Σ*. Montrer que pour tout réel* $\epsilon > 0$*, il existe* $x \in A - \{0\}$ *tel que* $|\sigma(x)| \leq \epsilon$*,* $|\sigma'(x)| \leq \frac{1}{\epsilon}\,|\mathrm{disc}\, A|^{1/2}$*, et* $|\tau(x)| \leq 1$ *pour tout* $\tau \in \Sigma - \{\sigma, \sigma'\}$.

(vi) (suite) En déduire qu'il existe une suite $(u_m)_{m\geq 1}$ *d'unités de* A*, et un réel* $C > 0$*, tels que :*

(a) la suite des réels $\sigma(u_m)$ *tend vers* 0 *quand* m *tend vers l'infini,*

(b) pour tout $m \geq 1$*, on a* $|\sigma(u_m)\sigma'(u_m)| \leq C$ *et* $|\tau(u_m)| \leq C$ *pour tout* $\tau \in \Sigma - \{\sigma, \sigma'\}$.

(vii) (suite) Vérifier qu'il existe un réel $c > 0$ *tel que pour tout entier* $m \geq 1$*, on a les inégalités* $|\sigma(u_m)\sigma'(u_m)| \geq c$ *et* $|\tau(u_m)| \geq c$ *pour tout* $\tau \in \Sigma - \{\sigma, \sigma'\}$.

(viii) En déduire que si $(a_\sigma) \in \mathbb{R}^\Sigma$ *est tel que* $\sum_{\sigma\in\Sigma} a_\sigma \log|\sigma(u)| = 0$ *pour tout* $u \in A^\times$*, alors on a* $a_\sigma = a_{\sigma'}$ *pour tous* $\sigma, \sigma' \in \Sigma$.

On considère l'application $\lambda : A^\times \to \mathbb{R}^\Sigma$, $x \mapsto (\log|\sigma(x)|)_\sigma$, et on pose $H = \{(x_\sigma) \in \mathbb{R}^\Sigma,\ \sum_\sigma x_\sigma = 0\}$.

(ix) Vérifier que λ *est un morphisme de groupes, dont l'image est incluse dans l'hyperplan* $H \subset \mathbb{R}^\Sigma$.

(x) Soient r *un nombre réel* ≥ 0 *et* E_r *l'ensemble des* $x \in A^\times$ *tels que* $|\log|\sigma(x)|| \leq r$ *pour tout* $\sigma \in \Sigma$*. Montrer que l'ensemble* E_r *est fini.*

(xi) En déduire que $\mathrm{Im}\,\lambda$ *est discret dans* H*, et que* $\ker\lambda$ *est un sous-groupe fini de* $\mathbb{R}^\times$.

(xii) Montrer que $\mathrm{Im}\,\lambda$ *est un réseau de* H.

(xiii) Montrer $\ker\lambda = \{\pm 1\}$.

(xiv) En déduire l'existence d'un isomorphisme de groupes $A^\times \simeq \{\pm 1\} \times \mathbb{Z}^{n-1}$ (théorème de Dirichlet)*. Pour cela, on pourra choisir* $u_1, \ldots, u_{n-1} \in A^\times$ *tels que* $(\lambda(u_i))_{1\leq i\leq n-1}$ *est une* $\mathbb{Z}$*-base de* $\mathrm{Im}\,\lambda$*, et considérer l'application* $\{\pm 1\}\times\mathbb{Z}^{n-1} \to A^\times, (e, (m_1, \ldots, m_{n-1})) \mapsto e\prod_{i=1}^{n-1} u_i^{m_i}$.

(xv) (Application à l'équation de Pell-Fermat) Soit d *un entier* > 0 *qui n'est pas un carré. Montrer qu'il existe une infinité de couples* $(x, y) \in \mathbb{Z}^2$ *tels que* $x^2 - dy^2 = 1$.

7. Examen 2016-2017

PROBLÈME 1. (*Formes de discriminant* -95) *On pose* $\alpha = \frac{1+\sqrt{-95}}{2}$ *et* $A = \mathbb{Z}[\alpha]$ $(= \mathrm{A}_{-95})$.

(i) Déterminer des représentants de $\mathrm{Cl}(-95)$*, ainsi que ses classes primitives.*

(ii) Déterminer l'ensemble des éléments d'ordre 2 *du groupe* $\mathrm{P}(-95)$.

(iii) Justifier que A *est un anneau de Dedekind et donner* $\Pi_{\alpha,\mathbb{Q}}$.

On considère les idéaux $D = 2A + \alpha A$, $\overline{D} = 2A + (\alpha - 1)A$ *et* $C = 5A + (\alpha + 2)A$.

(iv) Montrer que ces idéaux sont premiers et déterminer leur norme.

(v) Montrer que C *n'est pas principal, ainsi que les relations* $(5) = C^2$ *et* $(2) = D\overline{D}$.

(vi) En déduire la classe $\mathrm{q}_C \in \mathrm{P}(-95)$ *associée à* C *par la bijection de Dedekind.*

(vii) En déduire aussi l'égalité $(7 + \alpha) = \overline{D}^4 C$.

(viii) Montrer que $\mathrm{Cl}(A)$ *est un groupe cyclique d'ordre* 8*, engendré par la classe de* D.

(ix) Montrer que $2, \alpha$ *est une* $\mathbb{Z}$*-base de* D*, puis déterminer la classe* $\mathrm{q}_D \in \mathrm{P}(-95)$.

(x) Déterminer le carré et le cube de la classe de $(2, 1, 12)$ *dans* $\mathrm{P}(-95)$.

(xi) En déduire la table de multiplication du groupe $\mathrm{P}(-95)$.

(xii) (Application) Supposons que l'entier n *est représenté par la forme* $(2, 1, 12)$*. Montrer que* n^2, n^3 *et* n^4 *sont respectivement représentés par les formes* $(4, 1, 6)$*,* $(3, 1, 8)$ *et* $(5, 5, 6)$.

PROBLÈME 2. *Soient* K *un corps de nombres et* A *un ordre de* K*. On se propose d'abord de démontrer l'équivalence des propriétés suivantes :*

(a) $A = \mathcal{O}_K$*,*

(b) tout idéal maximal de A *est inversible,*

(c) tout idéal non nul de A *est inversible.*

Si $x \in K$ et $E \subset K$, on pose $xE = \{xe,\ e \in E\}$ et $A[x] = \{P(x),\ P \in A[X]\}$.

(i) Soient $a, b \in A$ *avec* $b \neq 0$*, et soit* I *un idéal inversible de* A*, tels que* $aI \subset bI$*. Montrer que* b *divise* a *dans* A.

(ii) Montrer que tout élément de K *s'écrit sous la forme* a/m *avec* $a \in A$ *et* $m \in \mathbb{Z}$ *non nul. En déduire que pour tout sous-ensemble fini* E *de* K *il existe* $m \in \mathbb{Z}$ *non nul tel que* $mE \subset A$.

(iii) Soit $x \in \mathcal{O}_K$*. Montrer qu'il existe* $m \in \mathbb{Z}$ *non nul tel que* $mA[x] \subset A$.

(iv) (suite) En déduire qu'il existe un idéal I *non nul de* A *vérifiant* $xI \subset I$.

(v) Montrer (c) $\Rightarrow$ *(a).*

(vi) Soient I, J *des idéaux non nuls de* A *avec* $IJ = I$*. Montrer* $J = A$*. (On pourra se contenter de pointer l'endroit du cours où cet énoncé est démontré !)*

(vii) Montrer (b) $\Rightarrow$ *(c). Conclure.*

On s'intéresse maintenant au cas $A = \mathbb{Z}[\alpha]$ avec $\alpha \in \overline{\mathbb{Z}}$. Soient $\Pi_{\alpha,\mathbb{Q}} \in \mathbb{Z}[X]$ le polynôme minimal de α sur $\mathbb{Q}$, p un nombre premier fixé et $P \in (\mathbb{Z}/p\mathbb{Z})[X]$ la réduction modulo p de $\Pi_{\alpha,\mathbb{Q}}$. On rappelle que pour tout diviseur Q de P dans $(\mathbb{Z}/p\mathbb{Z})[X]$, on dispose de l'idéal de A noté $\mathrm{I}(Q)$ dans le cours.

(viii) Que vaut $\mathrm{I}(P)$ *?*

(ix) Soient $Q, Q' \in (\mathbb{Z}/p\mathbb{Z})[X]$*. On suppose que* Q *et* Q' *sont des diviseurs de* P *dans* $(\mathbb{Z}/p\mathbb{Z})[X]$*, et qu'ils sont premiers entre eux. Soient* $\widetilde{Q}, \widetilde{Q'} \in \mathbb{Z}[X]$ *vérifiant* $\widetilde{Q} \equiv Q \bmod p$ *et* $\widetilde{Q'} \equiv Q' \bmod p$*. Montrer qu'il existe* $U, U' \in \mathbb{Z}[X]$ *tels que* $U(\alpha)\widetilde{Q}(\alpha) + U'(\alpha)\widetilde{Q'}(\alpha) \in 1 + pA$*.*

(x) (suite) En déduire $\mathrm{I}(QQ') = \mathrm{I}(Q)\mathrm{I}(Q')$*.*

(xi) Montrer que si P *est sans facteur carré, tout idéal premier de* A *contenant* p *est inversible.*

Problème 3. *Soit* ℓ *un nombre premier impair, on considère l'anneau* $A = \mathbb{Z}[\zeta]$ *avec* $\zeta = e^{2i\pi/\ell}$*. On se propose d'abord de redémontrer que* A *est l'anneau des entiers du corps de nombres* $K = \mathbb{Q}(\zeta)$*. On pose* $\Phi_\ell(X) = \frac{X^\ell - 1}{X - 1} = 1 + X + \cdots + X^{\ell-1}$ *; on rappelle que* $\Phi_\ell(X)$ *est irréductible dans* $\mathbb{Q}[X]$*.*

(i) Donner les entiers $[K : \mathbb{Q}]$*,* r_1 *et* r_2 *associés au corps de nombres* K*. Montrer que l'application* $\sigma \mapsto \sigma(\zeta)$ *induit une bijection entre* $\Sigma(K)$ *et* $\{\zeta^i,\ i = 1, \ldots, \ell - 1\}$*.*

(ii) Montrer $\mathrm{N}_{K/\mathbb{Q}}(1 - \zeta) = \ell$*.*

(iii) En déduire que $(1 - \zeta)$ *est un idéal maximal de* A *contenant* ℓ*.*

(iv) En déduire également $|\mathrm{disc}\, \mathbb{Z}[\zeta]| = \ell^{\ell-2}$*.*

(v) Montrer que $(1 - \zeta)$ *est l'unique idéal premier de* A *contenant* ℓ*.*

(vi) Montrer que si p *est un nombre premier* $\neq \ell$*, alors la réduction modulo* p *de* $\Phi_\ell(X)$ *est sans facteur carré dans* $(\mathbb{Z}/p\mathbb{Z})[X]$*.*

(vii) Conclure (on utilisera les résultats du problème 2).

On considère désormais le cas particulier $\ell = 7$. On se propose de démontrer que l'anneau $A = \mathbb{Z}[e^{2i\pi/7}]$ est principal. On utilisera librement les données et informations situées plus bas.

(viii) Montrer que tout idéal non nul de A *est équivalent à un idéal de* A *contenant un entier* N *avec* $1 \leq N \leq 4$*.*

(ix) Montrer que le groupe $\mathrm{Cl}(A)$ *est engendré par la classe de l'idéal* $(2, \zeta^3 + \zeta + 1)$*.*

(x) Montrer $\mathrm{N}_{K/\mathbb{Q}}(\zeta^3 + \zeta + 1) = 8$*, puis conclure.*

Données : (a) on a $\frac{\sqrt{7}}{\pi^3} \cdot 2^4 \cdot 3^{-4} \cdot 5 \cdot 7^2 = 4.13$ *à* 10^{-2} *près, (b) la réduction modulo* 3 *de* $\Phi_7(X)$ *est irréductible dans* $(\mathbb{Z}/3\mathbb{Z})[X]$*, (c) on a* $\Phi_7(X) \equiv (X^3 + X + 1)(X^3 + X^2 + 1) \bmod 2$*, (d) on a l'égalité*

$$\det \begin{bmatrix} 1 & 0 & 0 & -1 & 1 & -1 \\ 1 & 1 & 0 & -1 & 0 & 0 \\ 0 & 1 & 1 & -1 & 0 & -1 \\ 1 & 0 & 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & -1 & 1 & 0 \end{bmatrix} = 8.$$

8. Examen 2017-2018

Problème 1. (*Formes de discriminant* -87)

(i) Déterminer des représentants de $\mathrm{Cl}(-87)$ *et* $\mathrm{P}(-87)$.

(ii) Donner des représentants des classes d'ordre 1 *et* 2 *du groupe* $\mathrm{P}(-87)$.

(iii) En utilisant l'homomorphisme $\varepsilon_3 : \mathrm{P}(-87) \to \{\pm 1\}$ *de la théorie du genre, déterminer un sous-groupe d'ordre* 3 *de* $\mathrm{P}(-87)$.

(iv) En déduire que le groupe $\mathrm{P}(-87)$ *est isomorphe à* $\mathbb{Z}/6\mathbb{Z}$.

(v) Déterminer l'ordre de chacun des éléments de $\mathrm{P}(-87)$.

(vi) Soit $p \neq 2$ *un nombre premier* $\equiv -1 \bmod 3$. *Déterminer* $\left(\frac{-3}{p}\right)$ *puis l'équivalence entre :*

(a) -87 *est un carré modulo* p,

(b) p *n'est pas un carré modulo* 29, *ou* $p = 29$,

(c) p *est représenté par la forme* $(3, 3, 8)$ *ou par la forme* $(2, 1, 11)$.

(vii) En déduire que si le nombre premier p *n'est ni un carré modulo* 3, *ni un carré mod* 29, *alors* p^3 *est de la forme* $3x^2 + 3xy + 8y^2$ *avec* $x, y \in \mathbb{Z}$.

On pose $\alpha = \frac{1+\sqrt{-87}}{2}$ *et* $A = \mathbb{Z}[\alpha]$ $(= \mathrm{A}_{-87})$.

(viii) Rappeler pourquoi A *est l'anneau des entiers de* $\mathbb{Q}(\sqrt{-87})$.

On considère $D = 2A + \alpha A$, $S = 7A + (2 + \alpha)A$, *et leurs conjugués complexes* $\overline{D}$ *et* $\overline{S}$.

(ix) Montrer que D *et* $\overline{D}$ *(resp.* S *et* $\overline{S}$*) sont les idéaux premiers de* A *contenant* 2 *(resp.* 7*) et donner leur norme. Montrer de plus les relations* $2A = D\overline{D}$ *et* $7A = S\overline{S}$.

(x) Décomposer en produit d'idéaux premiers l'idéal $(2 + \alpha)A$.

(xi) Déterminer des représentants des classes q_D *et* q_S *dans* $\mathrm{P}(-87)$ *qui sont associées par Dedekind aux idéaux* D *et* S *respectivement.*

(xii) En déduire que $\mathrm{Cl}(A)$ *est un groupe cylique d'ordre* 6, *engendré par* $[D]$.

(xiii) Montrer $[D]^2 = [S]^{\mathrm{opp}}$ *et en déduire la table de multiplication de* $\mathrm{P}(-87)$.

Problème 2. *Soient* $\alpha = 2\cos\frac{2\pi}{7}$ *et* $K = \mathbb{Q}(\alpha)$.

(i) Montrer l'égalité $\alpha^3 + \alpha^2 - 2\,\alpha - 1 = 0$. *En déduire* $[K : \mathbb{Q}] = 3$.

(ii) Déterminer les entiers r_1 *et* r_2 *associés à* K.

(iii) Montrer que l'anneau $\mathbb{Z}[\alpha]$ *est principal.*

(iv) En déduire $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

Donnée : le discriminant du polynôme $X^3 + X^2 - 2\,X - 1$ *est* 49.

Dans l'exercice suivant, nous dirons par abus de langage que *la classe* $C \in \mathrm{Cl}(D)$ *représente l'entier* n si les formes dans la classe C ont cette propriété. On rappelle qu'à tout idéal non nul I de A_D, la construction de Dedekind associe une classe $\mathrm{q}_I \in \mathrm{Cl}(D)$.

PROBLÈME 3. *Soit $D < 0$ un discriminant*[1] *fondamental. On se propose de démontrer le théorème suivant connu de Gauss : "Soient q une forme de discriminant D et p un nombre premier représenté par q et premier à D, alors l'ordre de $[q]$ dans $\mathrm{P}(D)$ est le plus petit entier $m \geq 1$ tel que p^m est primitivement représenté par la forme principale de discriminant D".*

(i) Rappeler pourquoi A_D est l'anneau des entiers de $\mathbb{Q}(\sqrt{D})$.

Un idéal I de A_D sera dit primitif, *s'il n'est pas de la forme mI' avec $m \in \mathbb{Z}$, $m \geq 2$, et I' un idéal de A_D. Dans les questions (ii) à (v) suivantes, on fixe un idéal non nul I de A_D et on choisit un idéal non nul J tel que IJ est principal* (justifier l'existence de J).

(ii) Montrer que les entiers représentés par q_J sont les $\frac{\mathrm{N}(z)}{\mathrm{N}(J)}$ avec $z \in J$.

(iii) Soit $n \geq 1$ un entier. Montrer que q_J représente n si, et seulement si, il existe un idéal de A_D qui est équivalent à I et de norme n.

(iv) Soit $n \geq 1$ un entier. Montrer que q_J représente primitivement n si, et seulement si, il existe un idéal primitif de A_D qui est équivalent à I et de norme n.

(v) Montrer que q_I et q_J sont équivalentes. En déduire que les énoncés (iii) et (iv) sont encore vrais si l'on remplace q_J par q_I.

On fixe désormais un nombre premier p ne divisant pas D, et tel que D est un carré modulo $4p$.

(vi) Montrer qu'il existe exactement deux idéaux premiers de A_D contenant p, disons P et P', et que l'on a $p\mathrm{A}_D = PP'$ et $\mathrm{N}(P) = \mathrm{N}(P') = p$.

(vii) Montrer que p est représenté par les classes q_P et $\mathrm{q}_{P'}$, et seulement par ces classes.

(viii) Montrer que pour tout entier $m \geq 1$, les seuls idéaux primitifs de A_D de norme p^m sont P^m et $(P')^m$.

(ix) En déduire que pour tout entier $m \geq 1$, l'entier p^m est primitivement representé par $(\mathrm{q}_P)^m$, par $(\mathrm{q}_{P'})^m$, et par aucune autre classe de $\mathrm{P}(D)$.

(x) Montrer que l'ordre de q_P dans le groupe $\mathrm{P}(D)$ est le plus petit entier $m \geq 1$ tel que p^m est primitivement représenté par la forme principale de discriminant D. Conclure.

(xi) (Application) On suppose que l'entier $n \geq 2$ est tel que $9 - 2^{n+3}$ est sans facteur carré. Montrer que la classe de la forme $(2, 1, 2^n - 1)$ est d'ordre $n + 1$ dans $\mathrm{P}(9 - 2^{n+3})$.

(xii) Montrer que p^2 est primitivement représenté par la forme principale de discriminant D si, et seulement si, q_P est ambiguë.

1. On rappelle qu'un discriminant fondamental est un entier $D \in \mathbb{Z}$ vérifiant $D \equiv 0, 1 \bmod 4$ et tel que toute forme de discriminant D est primitive. Autrement dit, D n'est pas de la forme $n^2 D'$ avec $n \geq 2$ et $D' \equiv 0, 1 \bmod 4$.

9. Examen 2018-2019

PROBLÈME 1. *On pose* $\alpha = \frac{1+\sqrt{-155}}{2}$ *et* $A = \mathbb{Z}[\alpha]$.

(i) Déterminer des représentants de $\mathrm{Cl}(-155)$ *et ses classes ambiguës.*

(ii) En déduire la structure du groupe $\mathrm{P}(-155)$.

(iii) En utilisant le théorème de Dedekind, déterminer la structure du groupe $\mathrm{Pic}(A)$.

On se propose de redémontrer le (iii) sans utiliser le théorème de Dedekind.

(iv) Montrer que tout idéal non nul de A *est équivalent à un idéal contenant un entier* N *avec* $1 \leq N \leq 7$.

(v) Montrer que $\mathrm{Cl}(A)$ *est un groupe, et qu'il est engendré par les classes des idéaux premiers de* A *contenant* $2, 3, 5$ *ou* 7.

(vi) Montrer qu'il existe exactement deux idéaux premiers de A *contenant* 3*, à savoir* $T = (3, \alpha)$ *et* $T' = (3, \alpha - 1)$*, et que l'on a* $(3) = TT'$.

(vii) Montrer que les idéaux (2) *et* (7) *sont premiers, et que l'on a* $(5) = C^2$ *avec* C *l'unique idéal premier de* A *contenant* 5.

(viii) Montrer $(\alpha - 3) = CT^2$ *et que* C *n'est pas principal.*

(ix) En déduire que $\mathrm{Cl}(A)$ *est engendré par la classe de* T*, et conclure.*

Si K est un corps de nombres, on rappelle que $\Sigma(K)$ désigne l'ensemble de ses plongements. On dira que K est *totalement réel* si pour tout σ dans $\Sigma(K)$ on a $\sigma(K) \subset \mathbb{R}$.

PROBLÈME 2. (Un théorème de Hermite) *On fixe un entier* $n \geq 1$*. On se propose de démontrer que pour tout entier* d *il n'existe qu'un nombre fini de corps de nombres totalement réels, de degré* n*, et de discriminant* d.

(i) (Question préliminaire) Soient K *un corps de nombres et* $x \in K$ *avec* $\mathbb{Q}(x) \neq K$*. Montrer que pour tout* σ *dans* $\Sigma(K)$*, il existe* τ *dans* $\Sigma(K) - \{\sigma\}$ *vérifiant* $\tau(x) = \sigma(x)$.

Dans les questions suivantes, K est un corps de nombres totalement réel fixé de degré n, et on pose $\Sigma(K) = \{\sigma_1, \ldots, \sigma_n\}$ (justifier) et $d = |\mathrm{disc}\, K|$.

(ii) Montrer qu'il existe un élément $x \in \mathcal{O}_K$ *non nul vérifiant* $|\sigma_1(x)| \leq 2^{n-1}\sqrt{d}$ *et* $|\sigma_i(x)| \leq 1/2$ *pour tout* $i \neq 1$.

(iii) Montrer $|\sigma_1(x)| \geq 2^{n-1}$.

(iv) En déduire $K = \mathbb{Q}(x)$.

(v) Conclure en examinant le polynôme caractéristique de x *dans l'extension* $K/\mathbb{Q}$.

PROBLÈME 3. (Un anneau d'entiers non monogène)

Partie I. Soit p un nombre premier. Pour tout anneau A on note $\mathrm{Hom}(A, \mathbb{Z}/p\mathbb{Z})$ l'ensemble des morphismes d'anneaux de A dans $\mathbb{Z}/p\mathbb{Z}$.

(i) Montrer que si x *est dans* $\overline{\mathbb{Z}}$*, et si* R *est le polynôme minimal de* x *sur* $\mathbb{Q}$*, alors* $\mathrm{Hom}(\mathbb{Z}[x], \mathbb{Z}/p\mathbb{Z})$ *est en bijection avec l'ensemble des racines dans* $\mathbb{Z}/p\mathbb{Z}$ *de la réduction modulo* p *de* R.

(ii) Montrer que si K est un corps de nombres, et si $P_1, \dots, P_r$ désignent les idéaux premiers distincts de $\mathcal{O}_K$ de norme p, alors $\mathrm{Hom}(\mathcal{O}_K, \mathbb{Z}/p\mathbb{Z})$ a au moins r éléments.

(iii) (suite) En déduire que si $\mathcal{O}_K$ est de la forme $\mathbb{Z}[x]$ avec x dans $\mathcal{O}_K$, on a $r \leq p$.

Partie II. Soient α dans $\overline{\mathbb{Q}}$, $K = \mathbb{Q}(\alpha)$ et R le polynôme minimal de α sur $\mathbb{Q}$.

(iv) Montrer que pour tout $t \in \mathbb{Q}$ on a $\mathrm{N}_{K/\mathbb{Q}}(t - \alpha) = R(t)$.

(v) On suppose $\alpha \neq 1$. Montrer $\mathrm{Tr}_{K/\mathbb{Q}} \frac{1}{1-\alpha} = \frac{R'(1)}{R(1)}$.

Partie III. Soient $\alpha \in \mathbb{C}$ vérifiant $\alpha^3 - \alpha - 8 = 0$ et $K = \mathbb{Q}(\alpha)$. On se propose de démontrer que $\mathcal{O}_K$ n'est pas de la forme $\mathbb{Z}[x]$ avec $x \in \mathcal{O}_K$.

(vi) Montrer que $t^3 - t - 8$ est irréductible dans $\mathbb{Q}[t]$. En déduire $[K : \mathbb{Q}]$.

(vii) En contemplant l'égalité $8 = \alpha(\alpha - 1)(\alpha + 1)$, montrer que tout idéal premier de $\mathcal{O}_K$ contenant 2 contient soit α, soit $\alpha + 1$ (exclusivement).

(viii) Montrer que l'idéal principal $P = (\alpha - 2)\mathcal{O}_K$ est de norme 2.

(ix) En déduire que P est l'unique idéal premier de $\mathcal{O}_K$ contenant 2 et α.

(x) On suppose qu'il existe un unique idéal premier Q de $\mathcal{O}_K$ contenant 2 et $\alpha + 1$. Montrer qu'il existe un entier $m \geq 1$ vérifiant $(\alpha - 1)\mathcal{O}_K = Q^m = (\alpha + 1)\mathcal{O}_K$.
Indication : on pourra observer $\mathrm{N}_{K/\mathbb{Q}}(\alpha \pm 1) = 8$.

(xi) (suite) En déduire que l'élément $\beta = \frac{1+\alpha}{1-\alpha}$ est dans $\mathcal{O}_K$.

(xii) Montrer $\mathrm{Tr}_{K/\mathbb{Q}} \beta = -7/2$.

(xiii) En déduire qu'il existe au moins 2 idéaux premiers de $\mathcal{O}_K$ contenant 2 et $\alpha + 1$, disons Q_1 et Q_2.

(xiv) Montrer $2\mathcal{O}_K = PQ_1Q_2$ et $\mathrm{N}(Q_1) = \mathrm{N}(Q_2) = 2$.

(xv) Conclure.

Partie IV. (Bonus)

(xvi) Montrer $(\alpha) = P^3$.

(xvii) Quitte à échanger les rôles de Q_1 et Q_2, montrer $(\alpha + 1)\mathcal{O}_K = Q_1^2Q_2$ et $(\alpha - 1)\mathcal{O}_K = Q_1Q_2^2$.

(xviii) En déduire $\frac{\alpha(\alpha+1)}{2} \in \mathcal{O}_K$.

(xix) Montrer $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\frac{\alpha(\alpha+1)}{2}$. (Observer que le discriminant de $t^3 - t - 8$ est $-4 \cdot 431$.)

(xx) Retrouver que l'anneau $\mathcal{O}_K/2\mathcal{O}_K$ est isomorphe à l'anneau produit $(\mathbb{Z}/2\mathbb{Z})^3$.

Annexe B

Solutions, indications et corrigés

1. Exercices du chapitre 1

Exercice 1.1. Les nombres 47 et 79 sont premiers $\equiv 3 \bmod 4$, d'où les égalités

$$\left(\frac{47}{79}\right) = -\left(\frac{79}{47}\right) = -\left(\frac{32}{47}\right) = -\left(\frac{2}{47}\right) = -1$$

et donc 49 n'est pas un carré modulo 79.

Exercice 1.3. On a $4(X^2+aX+b) = (2X+a)^2 - D$. Observer aussi que X^2+X+1 est le seul polynôme irréductible de degré 2 dans $\mathbb{Z}/2\mathbb{Z}[X]$.

Exercice 1.5. Observer que l'on a $\prod_{a=1}^{\frac{p-1}{2}}(p-a) \equiv (-1)^{\frac{p-1}{2}}(\frac{p-1}{2})! \bmod p$.

Exercice 1.6. Pour le (ii), on pourra imiter les décompositions dans $\mathbb{C}[X]$

$$X^4+1 = (X^2+i)(X^2-i) = (X^2+\sqrt{2}X+1)(X^2-\sqrt{2}X+1) = (X^2+i\sqrt{2}X-1)(X^2-i\sqrt{2}-1).$$

Exercice 1.7. Observer que -1 est une puissance 4ème si et seulement si $(\mathbb{Z}/p\mathbb{Z})^\times$ admet un élément d'ordre 8. Conclure par la cyclicité de ce dernier.

Exercice 1.8. (i) Observer que $x \mapsto p-x$ échange les carrés de $\{1,\dots,\frac{p-1}{2}\}$ et ceux de $\{\frac{p+1}{2},\cdots,p-1\}$. Le (ii) découle du (i) car $C+N \equiv 1 \bmod 2$ si $p \equiv 3 \bmod 4$. Pour les (iii) et (iv), écrire

$$A = \sum_{a=1}^{\frac{p-1}{2}} \left[a\left(\frac{a}{p}\right) + (p-a)\left(\frac{p-a}{p}\right)\right] \quad \text{et} \quad A = \sum_{a=1}^{\frac{p-1}{2}} \left[2a\left(\frac{2a}{p}\right) + (p-2a)\left(\frac{p-2a}{p}\right)\right].$$

Exercice 1.9.(i) $\mathrm{N}(x^2=a)$ vaut 1 si $a=0$, 2 si a est un carré, 0 sinon, ce qui coïncide dans tous les cas avec $1+\left(\frac{a}{p}\right)$. Pour le (ii), observer que si $a \neq 0$ on a

$$\left(\frac{a(1-\alpha a)}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{(1-\alpha a)}{p}\right) = \left(\frac{a}{p}\right)^{-1}\left(\frac{(1-\alpha a)}{p}\right) = \left(\frac{a^{-1}-\alpha}{p}\right),$$

puis que $a \mapsto a^{-1}-\alpha$ est une bijection de $(\mathbb{Z}/p\mathbb{Z})^\times$ sur $\mathbb{Z}/p\mathbb{Z}-\{-\alpha\}$. Au (v) on trouve $1+(p-1)(1+\left(\frac{-\alpha\beta}{p}\right))$ solutions.

Exercice 1.10. Si m est un carré modulo n, il l'est aussi modulo tous les premiers divisant n, et donc $\left(\frac{m}{n}\right) = 1$ par définition.

Exercice 1.11. Supposons $x^{\frac{n-1}{2}} = \left(\frac{x}{n}\right)$ pour tout $x \in (\mathbb{Z}/n\mathbb{Z})^\times$. Si n n'est pas premier, on pourra écrire $n = p^\alpha m$ avec $(m,p)=1$ et considérer un x tel que $x \equiv 1 \bmod m$ et $x \bmod p^\alpha$ est un générateur de $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$. Pour le (ii), observer que $x \mapsto x^{\frac{n-1}{2}}\left(\frac{x}{n}\right)^{-1}$ est un morphisme de groupes non trivial $(\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times$, son noyau est donc de cardinal $\leq \frac{\varphi(n)}{2}$.

Exercice 1.12. Soit $S = \sum_{a=1}^{p-1} a^j$, où $j \geq 1$ est un entier. Observer que $x^j S \equiv S \bmod p$ pour tout $x \in \mathbb{Z}$ premier à p. En considérant une racine primitive modulo p, en déduire $S \equiv 0 \bmod p$ si $j \neq 0 \bmod p-1$.

Exercice 1.13. On a $\sum_{a=0}^{p-1}\zeta^{a^2} = 1 + 2\sum_{a\in C(p)}\zeta^a = 2\sum_{a\in C(p)}\zeta^a - \sum_{a=1}^{p-1}\zeta^a = G$.

Exercice 1.14. Soit $a \leq k \leq b-1$ un entier. On applique le théorème de convergence de Dirichlet (en analyse de Fourier) à la fonction 1-périodique nulle aux entiers et coïncidant avec f sur $]k, k+1[$. On en déduit

$$\frac{f(k)+f(k+1)}{2} = \lim_{A\to\infty} \sum_{n=-A}^{A} \int_k^{k+1} f(t)e^{2i\pi nt}dt.$$

Le (i) en découle en sommant sur $k = a, \ldots, b-1$, la sommation dans l'énoncé étant à prendre au sens ci-dessus. Pour le (ii), on applique le (i) à la fonction $f(t) = e^{2i\pi t^2/N}$ sur le segment $[0, N]$. Un changement de variables $u = t + \frac{nN}{2}$ montre

$$\int_0^N f(t)e^{2i\pi nt}dt = i^{-n^2}N \int_{\frac{nN}{2}}^{\frac{(n+2)N}{2}} e^{\frac{2i\pi u^2}{N}}du,$$

le (ii) s'en déduit en séparant les n pairs et impairs. On en déduit enfin $I = (1-i)^{-1} = \frac{1+i}{2}$ en prenant $N = 1$, car dans ce cas on a $G_1 = 1$.

Exercice 1.15. Pour le (ii), observer que si $p-1 = 2\ell$ avec $\ell = \frac{p-1}{2}$ premier, un élément x de $(\mathbb{Z}/p\mathbb{Z})^\times$ est une racine primitive si et seulement si son ordre n'est pas $1, 2$ ou $\ell = \frac{p-1}{2}$.

Exercice 1.16. Un élément du groupe additif $\mathbb{Z}/2^n\mathbb{Z}$ est générateur si et seulement si il n'est pas congru à 0 modulo 2, le (i) s'ensuit en considérant une racine primitive modulo p. Pour le (ii), observer que si $p > 3$ alors $p \equiv 1 \bmod 4$ et $p \equiv 2 \bmod 3$, donc $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1$.

Exercice 1.17. En utilisant l'exercice précédent, vérifier que 10 est une racine primitive modulo 65537. Le résultat est donc 65536.

Exercice 1.18. Considérons la $\mathbb{R}$-algèbre $\mathbb{H} = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$ des quaternions de Hamilton. Le sous-groupe fini $\{\pm 1, \pm i, \pm j, \pm k\} \subset \mathbb{H}^\times$ n'est pas cyclique (ni même commutatif).

Exercice 1.19. Remarquer que $(\mathbb{Z}/2\mathbb{Z})^r$ n'est pas cyclique si $r > 1$. Si p est premier et $n \geq 1$, observer que $(\mathbb{Z}/p^n\mathbb{Z})^\times$ admet un sous-groupe isomorphe à $\mathbb{Z}/2\mathbb{Z}$, même à $(\mathbb{Z}/2\mathbb{Z})^2$ si $p = 2$ et $n \geq 3$. La condition nécessaire du (ii) se déduit alors du (i) et de l'isomorphisme chinois des restes.

Exercice 1.21. Considérer par exemple les $\sqrt[2^i]{N}$ pour $i \geq 1$.

Exercice 1.22. Si p et q sont premiers impairs, la relation d'Eisenstein montre $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^s$ où s est le nombre de points à coordonnées entières à l'intérieur du rectangle OP'S'Q'. En effet, les seuls points à coordonnées entières sur la diagonale $y = qx/p$ du rectangle OPSQ sont O et S car p et q sont premiers entre eux. On conclut le (i) car on a $s = \frac{p-1}{2}\frac{q-1}{2}$.

Montrons la relation d'Eisenstein. Comme q est premier à p, la multiplication par q est injective dans $\mathbb{Z}/p\mathbb{Z}$; on a donc $|R| = |X| = \frac{p-1}{2}$. Pour montrer le (ii) il suffit alors de voir que l'application de l'énoncé est injective. Soient $r, r' \in R$ de parités différentes et tels que $r + r' = p$. On écrit $r \equiv qx \bmod p$ et $r' \equiv qx' \bmod p$ pour $x, x' \in X$. Il vient $x + x' \equiv 0 \bmod p$ car q est premier à p, puis $x + x' = p$, ce qui est absurde modulo 2.

Le (ii) entraîne $\prod_{x\in X} x \equiv \prod_{r\in R}(-1)^r r \bmod p$. Le (iii) s'en déduit car on a $\prod_{r\in R} r \equiv q^{\frac{p-1}{2}} \prod_{x\in X} x \bmod p$ (le produit sur X est non nul car p est premier).

Le (iv) est immédiat car x est pair et p est impair. On a déjà observé que la droite $y = qx/p$ ne contient aucun point (x, y) avec $y \in \mathbb{Z}$ et $x \in X$ car q est premier à p, on a donc $f = \sum_{x\in X}[qx/p]$ en dénombrant abscisse par abscisse, ce qui prouve le (v) d'après le (iv).

Pour le (vi), on raisonne abscisse par abscisse en observant qu'il y a $q-1$ entiers compris strictement entre 0 et q, et $q - 1 \equiv 0 \bmod 2$. La symétrie $(x, y) \mapsto (p - x, q - y)$ identifie les points à coordonnées entières et d'abscisse paire intérieurs au triangle S'SQ", aux points à coordonnées entières et d'abscisse impaire intérieurs au triangle OP'S'. Le (vii) se déduit alors de (v) et (vi).

Le premier point du (viii) découle du (v) pour $q = 2$. Si $n \in \mathbb{Z}$ est un entier impair, notons $f(n)$ le nombre d'entiers pairs compris entre $n/2$ et n. On a $f(1) = 0$, $f(3) = 1$, $f(5) = 1$ et $f(7) = 2$. On observe de plus $f(n + 8) = f(n) + 2$. Ainsi, on a $f(n) \equiv \frac{n^2-1}{8} \bmod 2$.

2. Exercices du chapitre 2

Exercice 2.1. $(a,b) = b\,(m,1) + \frac{a-mb}{n}\,(n,0)$.

Exercice 2.2. Ce groupe abélien L est un réseau car il est compris entre $\mathbb{Z}^3$ et $10\mathbb{Z}^3$. C'est le noyau du morphisme de groupes $\mathbb{Z}^3 \to \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $(a,b,c) \mapsto (a-b \bmod 5, b-a-c \bmod 2)$. Ce morphisme est surjectif, comme on le voit en considérant les éléments $(0,0,1)$ et $(1,0,1)$. Le réseau L est donc de covolume 10. Une base est donnée par les éléments $(1,1,0)$, $(0,5,1)$ et $(0,0,2)$. En effet, on a $(a,b,c) = a\,(1,1,0) + \frac{b-a}{5}\,(0,5,1) + \frac{5c-(b-a)}{10}\,(0,0,2)$.

Exercice 2.5. D'après le cours, le covolume de $L(e)$ est $|\det(e_1,\dots,e_n)|$. De plus, l'indice de $L(e)$ dans L est l'entier $\mathrm{covol}(L)/|\det(e_1,\cdots,e_n)|$. Ainsi, on a $L = L(e)$ si et seulement si cet indice est 1, i.e. $\mathrm{covol}(L) = |\det(e_1,\cdots,e_n)|$.

Exercice 2.6. Pour le (i), notons (e_i) la $\mathbb{Z}$-base canonique de $\mathbb{Z}^n$. On constate que pour tout (x_i) élément de $\mathbb{Z}^n$, il existe une unique partie $I \subset \{1,\dots,n\}$, et un unique $y \in 2\mathbb{Z}^n$, vérifiant $x - y = \sum_{i\in I} e_i$. L'indice en question est donc $|\mathcal{P}(I)| = 2^n$.

Exercice 2.7. Si $e_1,\dots,e_m$ engendre A comme groupe abélien, alors $\mathrm{Vect}_{\mathbb{Q}}(A) = \mathrm{Vect}_{\mathbb{Q}}(e_1,\dots,e_m)$ est de dimension finie $\leq m$. Pour le (ii), extraire de $\{e_i\}$ une $\mathbb{Q}$-base de $\mathrm{Vect}_{\mathbb{Q}}(A)$, disons $e_1,\dots,e_n$ quitte à renuméroter les e_i. Décomposer les e_j dans la $\mathbb{Q}$-base des e_i avec $i \leq n$ et prendre pour N le ppcm des dénominateurs des $n \cdot m$ coordonnées obtenues. Considérer enfin les inclusions $\mathbb{Z}^n \subset f^{-1}(A) \subset \frac{1}{N}\mathbb{Z}^n$ (injectivité de f).

Exercice 2.8. Soit p un nombre premier impair tel que $\left(\frac{-6}{p}\right) = 1$. Comme $\frac{4\sqrt{6}}{\pi} < \frac{10}{\pi} < 4$ au moins l'un de p, $2p$ ou $3p$ est de la forme a^2+6b^2. Si p est de la forme a^2+6b^2 on constate que a est impair, puis $p \equiv \pm 1 \bmod 8$. Si $2p$ est de la forme a^2+6b^2 alors $a = 2c$ est pair et on a donc $p = 2c^2+3b^2$. De même si $3p = a^2+6b^2$ alors $a = 3c$ est multiple de 3 et $p = 3c^2+2b^2$. Pour conclure, il suffit de remarquer que si p est de la forme $2a^2+3b^2$ alors b est impair, puis $p \equiv \pm 3 \bmod 8$.

Exercice 2.9. Pour le (i), observer que si $3n = a^2+11b^2$ alors $\pm a \equiv b \bmod 3$. Se ramener au cas $a \equiv b \bmod 3$ et poser $a = b+3u$. Pour l'assertion concernant $4n$ raisonner modulo 2. Pour le (ii), distinguer selon que a est pair, b est pair, ou a et b sont impairs, et utiliser les secondes identités remarquables. Le (iii) se déduit de $4\frac{\sqrt{11}}{\pi} < \frac{14}{\pi} < 5$ et de (i) et (ii). Pour le (iv), appliquer le (i) à $3p$ ou $4p$.

Exercice 2.10. Les ensembles $P(N)$ et $Q(N)$ sont non vides. En effet, le premier contient 1, et pour le second on peut par exemple invoquer le lemme 8.16. Donnons une autre méthode, basée sur l'observation que 3 et 4 sont de la forme $3a^2+2ab+4b^2$, mais ne sont pas toujours inversibles modulo N. Soient M et N des entiers premiers entre eux. On observe que l'isomorphisme chinois $\mathbb{Z}/MN\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ induit une bijection $Q(MN) \xrightarrow{\sim} Q(M) \times Q(N)$. En particulier, il suffit de montrer que $Q(N)$ est non vide lorsque N est impair, et lorsque N est une puissance de 2. Mais si N est impair (resp. non divisible par 3), la classe de 4 (resp. 3) est dans $Q(N)$.

Montrons $P(N) = Q(N)$. Les premières et dernières identités remarquables montrent respectivement que $P(N)$ et $Q(N)$ sont stables par multiplication, ce sont donc des sous-groupes du groupe $(\mathbb{Z}/N\mathbb{Z})^\times$ car ce dernier est fini. En particulier, 1 est dans $P(N)$ et $Q(N)$. Les secondes et troisièmes identités montrent respectivement $P(N)\cdot Q(N) \subset P(N)$ et $P(N)\cdot Q(N) \subset Q(N)$. Comme $1 \in P(N), Q(N)$, on en tire $Q(N) \subset P(N)$ et $P(N) \subset Q(N)$, *i.e.* $P(N) = Q(N)$. Le (ii) découle des identités remarquables données et du corollaire 2.37.

Exercice 2.12. Pour le (i), la considération de l'homothétie de rapport r montre $\mu(C_n(r)) = r^n c_n$. Si $n \geq 2$ on calcule c_n par tranches selon la coordonnée $t = x_n$:

$$c_n = \int_{-1}^{1} \mu(C_{n-1}(\sqrt{1-t^2}))dt.$$

Pour le (ii), on intègre deux fois par parties.

Exercice 2.13. Pour le (i), on constate sur la table 3 que si $n \leq 4$ alors $\sqrt{2}^n c_n > 2^n$. Ainsi, pour un $0 < r < \sqrt{2}$ assez proche de $\sqrt{2}$, on a $\mu(C_n(r)) > 2^n \mathrm{covol}(L)$. Le lemme du corps convexe de Minkowski assure donc que L contient un élément v non nul tel que $v\cdot v < 2$, on conclut car $v\cdot v$ est entier par hypothèse. Pour le (ii), on pose $u = x - (x\cdot v)v$. Pour le (iii) on observe que si l'espace euclidien $\mathbb{R}^n$ est somme directe orthogonale de deux sous-espaces U_1 et U_2, et si L_i est un réseau de U_i, alors $\mathrm{covol}(L_1 \oplus L_2) =$

covol(L_1)covol(L_2), où tous ces covolumes sont calculés de sorte que le pavé fondamental d'une base orthonormée soit de volume 1.

Exercice 2.14. Pour le (i), observer que D_8 est d'indice 2 dans $\mathbb{Z}^8$, donc de covolume 2. Pour le (ii), observer que tout élément de E_8 est soit dans D_8, soit de la forme $u+e$ avec $u \in \mathrm{D}_8$. Autrement dit, D_8 est d'indice 2 dans E_8, qui est donc de covolume 1. Pour le (iii), observer que $e \cdot e = 2$ et que $e \cdot u \in \mathbb{Z}$ si $u \in \mathrm{D}_8$. Pour le (iv), remarquer que 1 n'est pas pair, donc ne peut pas être de la forme $v \cdot v$.

3. Exercices du chapitre 3

Exercice 3.1. La forme $(5, 16, 13)$ est de discriminant -4. D'après le cours il n'y a qu'une telle forme de ce discriminant à équivalence près (équivalente à $(1, 0, 1)$). Si $p \equiv 1 \bmod 4$ alors -4 est un carré modulo p, et donc $(5, 16, 13)$ représente p par Lagrange.

Exercice 3.4. (vu en cours) On a $\sqrt{44/3} < 4$. Les formes réduites de discriminant -20 sont les trois formes $(1, 0, 11)$ et $(3, \pm 2, 4)$. Seule la première est ambiguë, les deux autres étant opposées. À équivalence près, les deux formes de discriminant -44 sont donc $(1, 0, 11)$ et $(3, 2, 4)$.

Exercice 3.5. On a $\sqrt{84/3} < 6$. Les formes réduites de discriminant $-84 = -3 \cdot 4 \cdot 7$ sont les formes $(1, 0, 21)$, $(3, 0, 7)$, $(2, 2, 11)$ et $(5, 4, 5)$, qui sont toutes ambiguës.

Exercice 3.6. On a $\sqrt{56/3} < 5$. Les formes réduites de discriminant $-56 = -8 \cdot 7$ sont donc $(1, 0, 14)$, $(2, 0, 7)$ et $(3, \pm 2, 5)$.

Exercice 3.7. Si $D \equiv 0 \bmod 4$, les couples $(x, y) \in \mathbb{Z}^2$ tels que $x^2 - \frac{D}{4}y^2 = 1$ sont $(\pm 1, 0)$, sauf si $D = -4$ auquel cas il y a aussi $(0, \pm 1$. Si $D \equiv 1 \bmod 4$. Les couples $(x, y) \in \mathbb{Z}^2$ tels que $x^2 + xy + \frac{1-D}{4}y^2 = 1$, soit encore tels que $(2x + y)^2 - Dy^2 = 4$, sont $(\pm 1, 0)$, sauf si $D = -3$ auquel cas il y a aussi $\pm(1, -1)$. Pour le (ii), observer que $(1 + \sqrt{2})(1 - \sqrt{2}) = -1$ puis que $a_n^2 - 2b_n^2 = (-1)^n$ pour tout entier $n \in \mathbb{Z}$.

Exercice 3.9 Le (i) est immédiat. Observer que si $c, d \in \mathbb{R}$ et $\tau \in \mathbb{H}$, alors $c\tau + d \neq 0$. L'action naturelle de $\mathrm{GL}_2(\mathbb{C})$ sur $\mathbb{C}^2$ définit par restriction une action de $\mathrm{GL}(2, \mathbb{R})$ sur $\mathbb{C}^2$. Si $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, et si $\tau \in \mathbb{H}$, on constate que

$$g \begin{pmatrix} \tau \\ 1 \end{pmatrix} = (c\tau + d) \begin{pmatrix} g \cdot \tau \\ 1 \end{pmatrix}.$$

Le (ii) s'ensuit (sans calcul !). Pour le (iii) considérer les éléments $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ de $\mathrm{SL}_2(\mathbb{Z})$.

Vérifions le (iv). Fixons $\tau_0 \in \mathbb{H}$ et considérons son orbite $O = \mathrm{SL}_2(\mathbb{Z}) \cdot \tau_0 \subset \mathbb{H}$. Montrons que $\tau \mapsto \mathrm{Im}(\tau)$ atteint son maximum sur O en un élément de $O \cap D$. Observons que $\mathbb{Z} + \tau_0\mathbb{Z}$ est un réseau de $\mathbb{C}$: il n'a donc qu'un nombre fini d'éléments dans le disque unité. Il résulte de ceci et du (i) que l'ensemble des $\mathrm{Im}(\tau)$ avec $\tau \in O$ admet un plus grand élément, disons $\mathrm{Im}(\tau)$. Quitte à user des translations (inverses l'une de l'autre et préservant O), $\tau \mapsto \tau \pm 1$, on peut supposer sans changer $\mathrm{Im}(\tau)$ que $-\frac{1}{2} < \mathrm{Re}(\tau) \leq \frac{1}{2}$. Par maximalité on a encore, $|c\tau + d| \geq 1$ pour tout $(c, d) \in \mathbb{Z}^2$ premiers entre eux. Pour $(c, d) = (1, 0)$ on obtient $|\tau| \geq 1$. Si $|\tau| > 1$ alors $\tau \in D$. Si $|\tau| = 1$, alors quitte à remplacer τ par $-1/\tau \in O$, ce qui ne change pas $\mathrm{Im}(\tau)$, on peut encore supposer que $\tau \in D$, ce que l'on voulait.

Assertion (v) (d'où l'on déduit (vi) immédiatement). Observons que si on a $z \in D$ et $|cz + d| \leq 1$ avec $c, d \in \mathbb{Z}$ premiers entre eux, alors soit $(c, d) = (0, \pm 1)$, soit $(c, d) = (\pm 1, 0)$ et $|z| = 1$, soit $(c, d) = \pm(1, -1)$ et $z = \rho := e^{i\pi/3}$ (observer que $|c| \geq 2$ est impossible car $\mathrm{Im}(z) \geq \frac{\sqrt{3}}{2} > \frac{1}{2}$). Supposons maintenant que l'on a $\tau, \tau' \in D$ avec $\mathrm{Im}\,\tau \geq \mathrm{Im}\,\tau'$ et $\tau' = g\tau$ pour un certain élément $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. On a alors $|c\,\tau + d| \leq 1$. On applique l'observation à $z = \tau$. Si $c = 0$ et $d = \pm 1 = a$, alors g est la translation $\tau \mapsto \tau + ab$, et donc $b = 0$ et $\tau' = \tau$ à cause des conditions sur la partie réelle. Si $c = \pm 1$, $d = 0$, et $|\tau| = 1$, alors $b = -c$ et donc $\tau' = g.\tau = a/c - \frac{1}{\tau} \in D$. Par définition de D cela entraîne $\tau = \rho$ et $a/c = 1$. Enfin, si $c = -d = \pm 1$, donc $(a + b)d = 1$, alors $\tau' = \frac{a\tau+b}{c\tau+d} = \frac{a/d\,(\tau-1)+1}{1-\tau} = -a/d + \frac{1}{1-\tau}$. Dans ce cas on a vu que $\tau = \rho$, de sorte que $1/(1 - \tau) = \tau$, d'où l'on tire que $a = 0$ et encore $\tau' = \tau$.

Pour le (vii), on a $\tau(q) = -\frac{b}{2a} + \frac{\sqrt{D}}{2a}$ où $D < 0$ est le discriminant de (a, b, c) et $\sqrt{D} \in \mathbb{H}$. (viii) est un calcul sans difficulté. Pour le (ix), on observe d'abord que q est réduite au sens de Gauss si et seulement si $\tau(q) \in D$, et on conclut par le (iv).

4. Exercices du chapitre 4

Exercice 4.1. Comme $\mathrm{N}(1+i)=2$ est premier, $1+i$ est irréductible. Si p est premier et $p=a^2+b^2$ avec $a,b\in\mathbb{Z}$, alors $p=\mathrm{N}(a+bi)=\pi\overline{\pi}$ où $\pi=a+bi$ est irréductible car de norme première. Les unités de $\mathbb{Z}[i]$ sont $\pm1,\pm i$, donc les associés de $a+bi$ sont $a+bi,-a-bi,-b+ai,b-ai$. Cette liste ne contient pas $a-bi$ sauf si $b=0$ ou $a=\pm b$. Le premier cas ne se produit jamais, et le second uniquement si $p=a^2+b^2=2$. Pour le (ii), observer que si p est un nombre premier et si π est un facteur irréductible de p dans $\mathbb{Z}[i]$, alors $\mathrm{N}(\pi)$ est un diviseur propre de $\mathrm{N}(p)=p^2$, donc $\mathrm{N}(\pi)=p$, et p est somme de deux carrés. Si π est irréductible dans $\mathbb{Z}[i]$, alors $(\pi)\cap\mathbb{Z}$ est un idéal de $\mathbb{Z}$ dont le générateur est par définition le plus petit nombre entier N divisible par π dans $\mathbb{Z}[i]$. Mais π est premier dans $\mathbb{Z}[i]$ car ce dernier est factoriel, donc N est nécessairement premier. Ainsi, chaque irréductible de π divise un unique nombre premier de $\mathbb{Z}$, et sont donc dans la liste (i), (ii) et (iii).

Exercice 4.2 Les éléments $z=a+bi\in\mathbb{Z}^2$ tels que $\mathrm{N}(z)=p$ sont exactement les diviseurs de p qui ne sont pas des unités. Si $p=\pi\overline{\pi}$ avec $\pi\in\mathbb{Z}[i]$ fixé, on a vu que π et $\overline{\pi}$ sont deux irréducibles non associés. La factorisation unique dans $\mathbb{Z}[i]$ donne donc exactement 8 solutions, à savoir les 4 associés de π et les 4 de $\overline{\pi}$. Autrement dit, si $p=a^2+b^2$, les seules autres écritures de p comme somme de deux carrés sont celles obtenues en remplaçant (a,b) par $(\pm a,\pm b)$ et $(\pm b,\pm a)$.

Exercice 4.3 On a $-3+15i=3(-1+5i)$ et le nombre 3 est premier dans $\mathbb{Z}[i]$. De plus, $\mathrm{N}(-1+5i)=26=2\cdot13$, on s'attend donc (étant donnée la propriété de factorisation unique et la classification des irréductibles) que $-1+5i$ soit de la forme $(1+i)\pi$ où $\mathrm{N}(\pi)=13$ (premier congru à 1 modulo 4). On constate en effet que $(-1+5i)=(1+i)(2+3i)$.

Exercice 4.4 Pour le (i), observer que $4=-2i(1+i)^2$ est bien dans l'idéal en question, et que de plus $i\cdot2(1+i)=2(-1+i)=2(1+i)-4$. Pour le (ii), écrire $a+bi=a-b+b(1+i)$, de sorte que $a+bi\equiv3 \bmod 2(1+i)$ si et seulement si $b\equiv0 \bmod 2$ et $a-b\equiv3 \bmod 4$. Pour le (iii), observer que tout élément inversible de l'anneau $\mathbb{Z}[i]/2(1+i)\mathbb{Z}[i]$ s'écrit de manière unique sous la forme $3u$ où $u\in\mathbb{Z}[i]^\times$.

Exercice 4.5 On a $(a+b\alpha)(c+d\alpha)=ac-pbd+(ad+bc)\alpha$. Mais p divise $ac-pbd$ si et seulement si p divise a ou p divise c.

Exercice 4.6 Montrons le (i). $\mathrm{I}_{a,b}$ est un idéal de A si, et seulement si, on a $\sqrt{d}\,\mathrm{I}_{a,b}\subset\mathrm{I}_{a,b}$. Il est équivalent de demander que l'on a $a\sqrt{d}\in\mathrm{I}_{a,b}$ et $(b+\sqrt{d})\sqrt{d}=d+b\sqrt{d}\in\mathrm{I}_{a,b}$. La relation $a\sqrt{d}=a(\sqrt{d}-b)+ba$ montre que l'on a toujours $a\sqrt{d}\in\mathrm{I}_{a,b}$. L'identité $d+b\sqrt{d}=(d-b^2)+b(\sqrt{d}+b)$, et le fait que $1,\sqrt{d}$ est une $\mathbb{R}$-base de $\mathbb{C}$, montrent que l'on a $d+b\sqrt{d}\in\mathrm{I}_{a,b}$ si, et seulement si, $d-b^2\in a\mathbb{Z}$.

Pour le (ii), on constate que si $\beta:=b+\sqrt{d}$, alors $1,\beta$ est une $\mathbb{Z}$-base de A. En effet, on a $x+y\sqrt{d}=(x-by)\cdot1+y\beta$. De plus, $a\cdot1$ et β est une $\mathbb{Z}$-base de $\mathrm{I}_{a,b}$. On a donc $A/\mathrm{I}_{a,b}\simeq\mathbb{Z}/a\mathbb{Z}$ (considérer par exemple l'application $\mathbb{Z}$-linéaire $A\to\mathbb{Z}/a\mathbb{Z},x+y\beta\mapsto x \bmod a$.)

Montrons le (iii). Si I est un idéal principal de A, alors il existe z dans A avec $I=Az$. On a vu en cours $\mathrm{N}(I)=\mathrm{N}(zA)=\mathrm{N}(z)$. Mais $\mathrm{N}(x+y\sqrt{d})=x^2+dy^2$. Donc si $\mathrm{N}(I)$ n'est pas un carré alors $\mathrm{N}(I)\geq d$.

D'après le (i), (ii) et (iii), pour tout entier $b\in\mathbb{Z}$ et tout entier $a>0$ non carré tell que a divise b^2-d, on a $a\geq d$. Pour $b=0$, cela montre que soit $-d=1$ ou 2, soit $-d$ est premier impair. Dans ce dernier cas, on réapplique cette observation à $b=1$, de sorte que $1-d$ est pair, et $a=2$. On en déduit $|d|\leq2$.

Exercice 4.7 On raisonne dans l'anneau euclidien $\mathbb{Z}[\alpha]$ avec $\alpha=\frac{1+\sqrt{-7}}{2}$. On constate en effet que $y^2+y=x^3-2$ s'écrit aussi $\mathrm{N}(y+\alpha)=x^3$. Pour le (i), on pourra observer que $\pi=\sqrt{-7}$ est irréductible (car de norme7) et donc premier car $\mathbb{Z}[\alpha]$ est euclidien donc factoriel. On pourrait aussi raisonner comme dans l'Exercice 4.5. Pour le (ii), on observe que π et $\overline{\pi}=-\pi$ sont associés, de sorte que $v_\pi(y+\alpha)=v_\pi(y+\overline{\alpha})$. Comme $y+\alpha-(y+\overline{\alpha})=\sqrt{-7}=\pi$, on a de plus $v_\pi(y+\alpha)\leq1$. Mais on a aussi $2v_\pi(y+\alpha)=3v_\pi(x)$, de sorte que $v_\pi(y+\alpha)$ est multiple de 3, d'où $v_\pi(y+\alpha)=0$. On en déduit que $y+\alpha$ et $y+\overline{\alpha}$ sont premiers entre eux, et donc $y+\alpha=(a+b\alpha)^3$ pour certains $a,b\in\mathbb{Z}$. On conclut comme dans l'exemple du cours.

Exercice 4.9 Le (i) est tautologique. Pour le (ii), observer que si $x\in A$ est tel que $m=bx$ est multiple de a, alors $a|x$, puis ab divise m.

Exercice 4.10 (i) L'élément $\sqrt{-5}$ est premier et ne divise pas $1+\sqrt{-5}$, ils sont donc premiers entre eux, et on conclut donc par le (i) de l'Exercice 4.9.

(ii) Un ppcm m de 2 et $1+\sqrt{-5}$ serait de norme multiple de $\mathrm{N}(2)=4$ et $\mathrm{N}(1+\sqrt{-5})=6$, donc multiple de 12. D'autre part m diviserait $2(1+\sqrt{-5})$ dont la norme est 24, ainsi que $2\cdot 3=(1-\sqrt{-5})(1+\sqrt{-5})$, dont la norme est 36. Il vient que $\mathrm{N}(m)$ diviserait $\mathrm{pgcd}(24,36)=12$, puis $\mathrm{N}(m)=12$. Mais $(1,0,5)$ ne représente pas 12, et donc m n'existe pas.

(iii) Supposons que d est un pgcd des nombres de l'énoncé. Il est donc multiple des irréductibles non associés 3 et $1+\sqrt{-5}$. Écrivons $d=3a$. La relation $d|3(1\pm\sqrt{-5})$ équivaut à $a|(1\pm\sqrt{-5})$, et entraîne que $a=\pm 1$ car $1+\sqrt{-5}$ et $1-\sqrt{-5}$ sont premiers entre eux (irréductibles non associés !). Il reste $d=\pm 3$, également absurde car 3 n'est pas divisible par $1+\sqrt{-5}$.

(vii) Supposons que $(1+\sqrt{-5})a$ est divisible par 2 avec $a\in\mathbb{Z}[\sqrt{-5}]$. Si l'on écrit $a=u+v(1+\sqrt{-5})$ avec $u,v\in\mathbb{Z}$, on constate que $(1+\sqrt{-5})a=-6v+(1+\sqrt{-5})(u+2v)$. Mais ce nombre est multiple de 2 dans $\mathbb{Z}[\sqrt{-5}]$ si et seulement si ses deux coordonnées dans la $\mathbb{Z}$-base 1 et $1+\sqrt{-5}$ le sont (pourquoi ?), i.e. si et seulement si u est pair, i.e. $a\in I$.

Exercice 4.13 L'intégrité de A résulte du lemme des zéros isolés et de la connexité de $\mathbb{C}$. Si $f\in A$ ne s'annule pas, il est bien connu que $1/f$ est holomorphe, i.e. $f\in A^\times$. Le (ii) découle simplement du fait, également bien connu, que si $f\in A$ s'annule en $a\in\mathbb{C}$, alors $z\mapsto f(z)/(z-a)$ se prolonge en une fonction holomorphe sur $\mathbb{C}$, disons $g\in A$, de sorte que $f(z)=(z-a)g(z)$. Le (iii) découle de l'existence de $f\in A$ ayant une infinité de zéros, comme par exemple $z\mapsto\sin(z)$.

5. Exercices du chapitre 5

Exercice 5.1. Si $d\in\mathbb{Z}$ n'est pas un carré, alors X^2-d est irréductible dans $\mathbb{Q}[X]$ est donc $[\mathbb{Q}(\sqrt{d}):\mathbb{Q}]=2$. Si $d=d'u^2$ avec $u\in\mathbb{Z}$ alors $\mathbb{Q}(\sqrt{d})=\mathbb{Q}(\sqrt{d'})$.

Si d,d' sont sans facteur carré et distincts, alors $\mathbb{Q}(\sqrt{d})\cap\mathbb{Q}(\sqrt{d'})=\mathbb{Q}$. En effet, sinon $\mathbb{Q}(\sqrt{d})=\mathbb{Q}(\sqrt{d'})$ pour des raisons de dimension, et donc $\sqrt{d}=a+b\sqrt{d'}$ avec $a,b\in\mathbb{Q}$. Cela entraîne $d=a^2+d'b^2+2ab\sqrt{d'}$, puis $ab=0$ car $1,\sqrt{d'}$ est $\mathbb{Q}$-libre. Si $a=0$ alors $d=d'b^2$, si $b=0$ alors $d=a^2$: les deux cas sont absurdes.

Enfin, si $[K:\mathbb{Q}]=2$ et si $x\in K\backslash\mathbb{Q}$ alors $K=\mathbb{Q}(x)$ avec $\Pi_{x,\mathbb{Q}}=X^2+aX+b$ irréductible dans $\mathbb{Q}[X]$. En particulier, son discriminant $d:=a^2-4b$ n'est pas un carré dans $\mathbb{Q}$. Mais $(2x+a)^2=a^2-4b$ donc $2x+a=\pm\sqrt{d}\in K$, puis $\mathbb{Q}(\sqrt{d})=K$.

Exercice 5.2 D'après l'Exercice 5.1, il faut voir que pour tout entier d sans facteur carré, il existe une racine de l'unité ζ telle que $\sqrt{d}\in\mathbb{Q}(\zeta)$. Se ramener au cas où d est premier, et dans ce cas considérer la somme de Gauss.

Exercice 5.3 Si d n'est pas un cube dans $\mathbb{Q}$, et si $\alpha=\sqrt[3]{d}$, alors $[\mathbb{Q}(\alpha):\mathbb{Q}]=3$. Un calcul dans la base $1,\alpha,\alpha^2$ montre que $\mathrm{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(a+b\alpha+c\alpha^2)=a^3+db^3+d^2c^3-3abcd$. Conclure dans ce cas par multiplicativité de la norme. Dans le cas général, fixer $a,b,c,a',b',c'\in\mathbb{Z}$ et observer que l'identité cherchée équivaut à l'annulation d'un certain polynôme en d à coefficients dans $\mathbb{Z}$, qui s'annule sur l'infinité des non cubes.

Exercice 5.4 Observer que $\mathrm{disc}(P)\neq 0$ puis que $\frac{\mathrm{disc}(Q)}{\mathrm{disc}(P)}\in\mathbb{Q}\cap\overline{\mathbb{Z}}=\mathbb{Z}$.

Exercice 5.5 C'est un calcul direct dans la $\mathbb{Z}$-base $1,\sqrt{d}$ si $d\not\equiv 1 \bmod 4$, dans $1,\frac{1+\sqrt{d}}{2}$ sinon.

Exercice 5.6 Pour le (i), d'après le cours le carré de l'indice de $\sum_i\mathbb{Z}e_i$ dans $\mathcal{O}_K$ divise l'entier $\mathrm{disc}_{K/\mathbb{Q}}(e_1,\cdots,e_n)$. Cet indice est donc 1 par hypothèse. Pour le (ii), X^3-X+1 est irréductible dans $\mathbb{Q}[X]$ car sans racine rationnelle, donc $[K:\mathbb{Q}]=3$. Son discriminant est ± 23, sans facteur carré, d'où le (ii).

Exercice 5.7 Le (i) est immédiat en considérant la $\mathbb{Q}$-base $1,x,x^2$ de K. Le (ii) se déduit de $\mathrm{Tr}_{K/\mathbb{Q}}(x)=\mathrm{Tr}_{K/\mathbb{Q}}(x^2)=0$.Pour le (iii), l'indication montre d'abord que $4(3b)^3\in\mathbb{Z}$, ce qui entraîne $3b\in\mathbb{Z}$ car $3b\in\frac{1}{2}\mathbb{Z}$, puis on voit que $3c\in\mathbb{Z}$ de la même manière. Pour le (v), observer que la norme de l'élément $\pm\frac{1}{3}(1-x+x^2)$ vaut $\pm\frac{1}{27}(1-2+4-6)\notin\mathbb{Z}$.

Exercice 5.8 Comme m et n sont distincts et sans facteurs carré, on a $\mathbb{Q}(\sqrt{m})\cap\mathbb{Q}(\sqrt{n})=\mathbb{Q}$ (Exercice 5.1). On en déduit $[K:\mathbb{Q}(\sqrt{n})]=2$ puis $[K:\mathbb{Q}]=4$ par la base télescopique, ainsi que le fait que $1,\alpha,\beta,\alpha\beta$ est une $\mathbb{Q}$-base de K. Observons qu'un $\sigma\in\Sigma(K)$ est uniquement déterminé par ses valeurs $\sigma(\sqrt{n})$ et $\sigma(\sqrt{m})$. Mais $\sigma(\sqrt{n})=\pm\sqrt{n}$ et $\sigma(\sqrt{m})=\pm\sqrt{m}$, donc les 4 possibilités de signes sont atteintes car $|\Sigma(K)|=[K:\mathbb{Q}]=4$.

Soit $z = a + b\sqrt{n} + c\sqrt{m} + d\sqrt{mn} \in \mathcal{O}_K$ avec $a, b, c, d \in \mathbb{Q}$. Considérons l'unique $\sigma \in \Sigma(K)$ vérifiant $\sigma(\sqrt{n}) = -\sqrt{n}$ et $\sigma(\sqrt{m}) = \sqrt{m}$). On a alors $\sigma(z) \in \mathcal{O}_K$ et $\sigma(z) = a - b\sqrt{n} + c\sqrt{m} - d\sqrt{mn}$. On en déduit

$$z + \sigma(z) = 2a + 2c\sqrt{m} \in \mathcal{O}_{\mathbb{Q}(\sqrt{m})} = \mathbb{Z} + \mathbb{Z}\beta.$$

En particulier, on a $4a, 4c \in \mathbb{Z}$. On conclut le (ii) en considérant de même les deux autres plongements non triviaux.

Le (i) montre que $\mathrm{disc}(K)$ est un diviseur de m^2n^2. Le (ii) montre que

$$\mathrm{disc}(1, \sqrt{n}, \sqrt{m}, \sqrt{mn}) = 4^4 n^2 m^2$$

divise $16^4\mathrm{disc}(\mathcal{O}_K)$, il vient que $\mathrm{disc}(K) = m^2n^2$ car m et n sont impairs, et donc que $1, \alpha, \beta, \alpha\beta$ est une $\mathbb{Z}$-base de $\mathcal{O}_K$ par le (i).

Exercice 5.9 On considère le morphisme d'anneaux $\varphi : (\mathbb{Z}/2\mathbb{Z})[X, Y] \to \mathcal{O}_K/2\mathcal{O}_K$ envoyant X sur la classe de α et Y sur celle de β. Il est surjectif par l'exercice précédent. De plus $X^2 - X \in \mathrm{Ker}(\varphi)$. En effet, $\alpha^2 - \alpha = \frac{n-1}{4} \in 2\mathbb{Z}$ car $n \equiv 1 \bmod 8$. De même, $Y^2 - Y \in \mathrm{Ker}(\varphi)$, de sorte que φ induit par passage au quotient un morphisme surjectif d'anneaux $\varphi^* : A \to \mathcal{O}_K/2\mathcal{O}_K$. Mais $|\mathcal{O}_K/2\mathcal{O}_K| = 2^4$. De plus, on voit que A est engendré comme $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel par les classes de 1, X, Y et XY, il a donc au plus 2^4 éléments. Pour des raisons de cardinal il s'ensuit que φ^* est bijective.

Pour le (ii), observer que se donner un morphisme d'anneaux $\psi : A \to \mathbb{Z}/2\mathbb{Z}$ est équivalent par la propriété universelle d'un quotient à se donner deux éléments $x = \psi(X), y \in \psi(Y) \in \mathbb{Z}/2\mathbb{Z}$ tels que $x^2 = x$ et $y^2 = y$. Cette dernière condition est automatiquement satisfaite dans $\mathbb{Z}/2\mathbb{Z}$. Il y a donc exactement deux choix pour x et deux pour y. La seconde assertion du (iii) est la propriété universelle du quotient. La première s'en déduit car tout polynôme a évidemment au plus deux racines dans $\mathbb{Z}/2\mathbb{Z}$.

Enfin, si $\mathcal{O}_K$ est monogène, alors il existe un polynôme $P \in \mathbb{Z}[X]$ unitaire de degré 4 tel que $\mathcal{O}_K \simeq \mathbb{Z}[X]/(P)$, et donc $\mathcal{O}_K/2\mathcal{O}_K \simeq (\mathbb{Z}/2\mathbb{Z})[X]/(P \bmod 2)$, ce qui est absurde par (i) et (ii).

Exercice 5.10 Si $x \in \mathcal{O}_K$, il existe $y \in \mathcal{O}_K$ tel que $xy = 1$. La multiplicativité de $\mathrm{N} = \mathrm{N}_{K/\mathbb{Q}}$ entraîne $\mathrm{N}(xy) = 1 = \mathrm{N}(x)\mathrm{N}(y)$, puis $\mathrm{N}(x) = \pm 1$ car $\mathrm{N}(\mathcal{O}_K) \subset \mathbb{Z}$. Réciproquement, si $\mathrm{N}(x) = \pm 1$ et $x \in \mathcal{O}_K$, alors $\chi_{x,K/\mathbb{Q}}(X) \in \mathbb{Z}[X]$ et son coefficient constant vaut ± 1. Ainsi, $x^n + \sum_{i=1}^{n-1} a_i x^i \pm 1 = 0$ avec des $a_i \in \mathbb{Z}$. On conclut par l'identité $1 = \pm x(x^{n-1} + \sum_{i=1}^{n-1} a_i x^{i-1})$.

Exercice 5.11 Pour le (ii), observer que si $x \in U(K)$, et si $\chi_{x,K/\mathbb{Q}} = X^n + \sum_{i=0} a_i X^i$ alors $a_i \in \mathbb{Z}$ et $|a_i| \leq \binom{n}{i}$. Il n'y a donc qu'un nombre fini de polynômes caractéristiques possibles. Ces polynômes ont au total un nombre fini de racines, donc $U(K)$ est fini. Soient $n = |U(K)|$ et $\mu_n = \{\zeta \in \mathbb{C}, \zeta^n = 1\}$. Si $x \in U(K)$ alors $x^n = 1$ (Lagrange) donc $U(K) \subset \mu(K) \subset \mu_n$. Mais $|U(K)| = |\mu_n| = n$ donc $U(K) = \mu(K) = \mu_n$. Le (iv) se déduit du (iii) en considérant $K = \mathbb{Q}(x)$. Pour le (iv), on écrit $U(K) = \mu_n$, donc $\zeta = e^{2i\pi/n} \in K$, puis $\mathbb{Q}(\zeta) \subset K$. La base téléscopique entraîne que $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ divise $[K : \mathbb{Q}]$, mais $\varphi(n) = [\mathbb{Q}(\zeta) : \mathbb{Q}]$ (irréductibilité du polynôme cyclotomique).

Exercice 5.12 Soit $K = \mathbb{Q}(\alpha)$, c'est le corps de fractions de $\mathbb{Z}[\alpha]$. On sait que $\mathcal{O}_K$ est intégralement clos. Si $\mathbb{Z}[\alpha]$ l'est aussi, alors par définition il contient $\mathcal{O}_K$. Il est donc égal à $\mathcal{O}_K$ car $\alpha \in \mathcal{O}_K$ par hypothèse.

Exercice 5.13 Si $P = QR = \prod_i (X - x_i)$ alors $x_i \in \overline{\mathbb{Z}}$ car $P \in \mathbb{Z}[X]$ est unitaire. Les racines de Q et R dans $\mathbb{C}$ sont parmi les x_i, donc $P, Q \in \overline{\mathbb{Z}}[X]$ car ils sont unitaires à un signe près. On conclut car $\mathbb{Q} \cap \overline{\mathbb{Z}} = \mathbb{Z}$. Le (i) s'ensuit et le (ii) en est une conséquence immédiate.

Exercice 5.15 Écrivons $K = \mathbb{Q}(x)$ avec $x \in \overline{\mathbb{Z}}$. Si $P = \Pi_{x,\mathbb{Q}}$ alors $\mathrm{disc}(K)$ est le carré d'un entier non nul fois $\mathrm{disc}(P)$. Par définition, $\mathrm{disc}(P)$ est un produit de termes de la forme $(a-b)^2 = (b-a)^2$ où $\{a, b\}$ parcourt les parties à deux éléments de l'ensemble R des racines de P dans $\mathbb{C}$. La conjugaison complexe induit une involution de R, et donc de l'ensemble de ses parties, disons $I \mapsto \overline{I} = \{\overline{x}, x \in I\}$. Obervons que si $a \neq b$, alors $(a-b)^2(\overline{a} - \overline{b})^2 = |a-b|^4$ est réel strictement positif. De plus, $I = \overline{I}$ et $|I| = 2$ si et seulement si $I = \{a, \overline{a}\}$ avec $a \in R$ non réel, auquel cas $(a - \overline{a})^2 = -4\mathrm{Im}(a)^2$. On conclut car le nombre d'éléments non réels de R est $2s$ par définition.

Exercice 5.16 Pour le (i), observer que l'élément $S = \prod_{1 \leq i < j \leq n}(x_i + x_j)$ est un polynôme symétrique à coefficients entiers en les x_i. C'est donc un polynôme à coefficients entiers en les coefficients de P (qui est unitaire), donc $S \in \mathbb{Z}$. Pour le (ii), on remarque que si $a, b \in \overline{\mathbb{Z}}$ alors $(a-b)^2 = (a+b-2b)^2 \equiv (a+b)^2 \bmod 4$. On en déduit $\mathrm{disc}(P) \equiv S^2 \bmod 4$ et on conclut car $S \in \mathbb{Z}$ par le (i). Le (iii) s'en déduit car $\mathrm{disc}(K)$ est le carré d'un entier non nul fois $\mathrm{disc}(\Pi_{x,\mathbb{Q}})$ où $x \in \overline{\mathbb{Z}}$ est un élément primitif de K.

6. Exercices du chapitre 6

Exercice 6.2 On a $\Pi_{\alpha,\mathbb{Q}} = X^2 + X + 5$ donc $\mathrm{disc}(A) = -19$. D'après Minkowski tout idéal non nul de A est équivalent à un idéal contenant N avec $1 \leq N \leq C(A) = \frac{1}{2}\frac{4}{\pi}\sqrt{19} < 3$ (voir la table). Mais X^2+X+5 est irréductible dans $(\mathbb{Z}/2\mathbb{Z})[X]$ donc les seuls idéaux de A contenant 2 sont $2A$ et A. Ainsi, $\mathrm{Cl}(A) = 1$ et donc A est principal. On a vu au chapitre 4 qu'il n'est pas euclidien.

Exercice 6.3 On a $\Pi_{\alpha,\mathbb{Q}} = X^2 + 5$ donc $\mathrm{disc}(A) = -20$. D'après Minkowski, tout idéal non nul de A est équivalent à un idéal contenant N avec $1 \leq N \leq C(A) = \frac{1}{2}\frac{4}{\pi}\sqrt{20} < 3$ (voir la table). Comme $X^2 + 5 \equiv (X-1)^2 \bmod 2$, les idéaux contenant 2 sont $2A$, $2A + (\alpha - 1)A = I$ et A. Ainsi, tout idéal est équivalent à I ou bien principal.

Si $I = zA$ alors $\mathrm{N}(I) = |\mathrm{N}(z)|$. Mais $\mathrm{N}(I) = 2$ (pourquoi ?) et $x^2 + 5y^2$ ne représente pas 2, donc I n'est pas principal. Ainsi, $[I] \neq [A]$ et donc $|\mathrm{Cl}(A)| = 2$.

On a $I^2 = (4, (\alpha-1)^2, 2(\alpha-1))$. Mais $(\alpha-1)^2 = -4 - 2\alpha = -2(2+\alpha)$, donc

$$I^2 = (2)(2, 2+\alpha, \alpha - 1) = (2)$$

car $1 = (2+\alpha) - 2 - (\alpha - 1)$. Ainsi, $[I]^2 = 1 = [A]$ dans $\mathrm{Cl}(A)$, et donc $\mathrm{Cl}(A) \simeq \mathbb{Z}/2\mathbb{Z}$. Si J est un idéal non nul de A, alors J est principal si et seulement si $[J] = 1$ dans $\mathrm{Cl}(A)$. On conclut car $[J] \neq [IJ]$ dans le groupe $\mathrm{Cl}(A)$, car $[I] \neq [A]$.

Exercice 6.4 Le (i) et (ii) sont similaires à l'exercice précédent. Comme $(\alpha-1)^2 = -2(1+\alpha)$, on a $I^2 = (4, -2(1+\alpha), 2(\alpha-1)) = 2(2, \alpha+1, \alpha-1) = 2I$. La structure de $\mathrm{Cl}(A) = \{[A], [I]\}$ est donc telle que $[I]^2 = [I]$: ce n'est donc pas un groupe (c'est l'unique monoïde unitaire à deux éléments qui n'est pas un groupe !). Si J est un idéal non nul de A, alors on constate que $[JI] = [J][I] = [I]$ quel que soit $[J]$, donc IJ n'est jamais principal.

Exercice 6.7 On a $\mathrm{disc}(X^3 - d) = -27d^2$. Si $K = \mathbb{Q}(\sqrt[3]{d})$ alors $r_1 = 1$ et $r_2 = 1$. Quand $d = 2$, Minkowski nous dit que tout idéal non nul de A est équivalent à un idéal contenant un entier $\leq \frac{4}{\pi}\frac{3!}{3^3}6\sqrt{3} = \frac{16}{\pi\sqrt{3}} < 3$ (donnée). Les idéaux de A contenant 2 sont $A, 2A$, $I = 2A + \alpha A$ et $J = 2A + \alpha^2 A$, donc $\mathrm{Cl}(A) = \{[A], [I], [J]\}$. On a $\alpha^3 = 2$ donc $2 \in \alpha^2 A \subset \alpha A$, donc $I = (\alpha)$ et $J = (\alpha)^2$ sont principaux, puis $|\mathrm{Cl}(A)| = 1$. L'anneau A est un ordre de $\mathbb{Q}(\alpha)$. Il est principal, donc intégralement clos, et donc il contient $\mathcal{O}_{\mathbb{Q}(\alpha)}$: c'est donc exactement l'anneau des entiers de $\mathbb{Q}(\alpha)$.

Exercice 6.8 Soient $\zeta = e^{2i\pi/5}$, $K = \mathbb{Q}(\zeta)$ et $A = \mathbb{Z}[\zeta]$. On a $r_1 = 0$ et $r_2 = 2$. De plus $\mathrm{disc}(A) = \mathrm{disc}(X^4 + X^3 + X^2 + X + 1) = 5^3$ (exercice 5.14). On vérifie que

$$C(2,4) \cdot 5\sqrt{5} \simeq 1,7 < 2,$$

donc A est principal par Minkowski.

7. Exercices du chapitre 7

Exercice 7.1 (i) Soit $\alpha = \sqrt{6}$, alors $A = \mathbb{Z}[\alpha]$ est l'anneau des entiers de $\mathbb{Q}(\sqrt{6})$. Les idéaux contenant 15 sont donc les facteurs de (15). Comme $X^2 - 6 \equiv X^2 \bmod 3$, on a $(3) = T^2$ avec $T = (3, \alpha)$ premier. Comme $X^2 - 6 \equiv (X-1)(X+1) \bmod 5$ on a $(5) = C_+C_-$ avec $P_\pm = (5, \alpha \pm 1)$ premier. Ainsi, $(15) = T^2C_+C_-$. Les idéaux cherchés sont donc les 12 idéaux suivants :

$$A,\ T,\ C_+,\ C_-,\ T^2 = (3),\ TC_+,\ TC_-,\ C_+C_- = (5),\ T^2C_+,\ T^2C_-,\ TC_+C_-,\ T^2C_+C_- = (15).$$

(ii) Soit $\alpha = \sqrt{5}$, alors $A = \mathbb{Z}[\alpha]$ est l'anneau des entiers de $\mathbb{Q}(\alpha)$. L'idéal principal engendré par $\beta = 1 + 2\alpha$ est de norme $N(\beta) = 1 + 4.5 = 21 = 3 \cdot 7$. Il est donc produit d'un idéal premier de norme 3 par un autre de norme 7. Les idéaux premiers contenant 3 sont les deux idéaux $T_\pm = (3, \alpha \pm 1)$ et ceux contenant 7 sont $S_\pm = (7, \alpha \pm 3)$. Mais $\beta = 2\alpha + 1 = 2(\alpha - 1) + 3 \in T_-$ et $\beta = 2(\alpha - 3) + 7 \in S_-$, donc T_- et S_- divisent (β), puis $(\beta) = T_-S_-$ (identité pas très difficile à vérifier à posteriori !).

Exercice 7.4 Traitons d'abord le cas de $A = \mathbb{Z}[\alpha]$ avec $\alpha = \sqrt{-13}$. On a $\mathrm{disc}(A) = \mathrm{disc}(X^2 + 13) = -52$. Les estimées de Minkowski démontrent que tout idéal non nul de A est équivalent à un idéal contenant un entier N tel que $1 \leq N \leq \frac{2}{\pi}\sqrt{52} < 5$. Les idéaux de A contenant 2 sont $2A$, $D = (2, \alpha + 1)$ (premier) et A car $X^2 + 13 \equiv (X+1)^2 \bmod 2$. De plus, $X^2 + 13$ est irréductible modulo 3, donc les seuls idéaux de A contenant 3 sont $3A$ et A. De plus, A est l'anneau des entiers de $\mathbb{Q}(\sqrt{-13})$, car -13 est sans facteur carré et $\equiv 3 \bmod 4$. D'après le cours (ou par un calcul direct) on a $(2) = D^2$, donc $(4) = D^4$, de sorte que les idéaux contenant 4 sont les D^i par la propriété de Dedekind. Il s'ensuit qu'en tant que groupes

$\mathrm{Cl}(A) = \langle [D] \rangle$. Mais D n'est pas principal car 2 n'est pas représenté par $x^2 + 13\,y^2$, et $[D]^2 = [A]$, donc $\mathrm{Cl}(A) = \mathbb{Z}/2\mathbb{Z}$.

Supposons maintenant $A = \sqrt{26}$, donc $\mathrm{disc}(A) = -92$ et tout idéal non nul de A est équivalent à un idéal contenant un entier N tel que $1 \leq N \leq \frac{2}{\pi}\sqrt{92} < 7$(Minkowski). A est l'anneau des entiers de $\mathbb{Q}(\sqrt{-26})$ car -26 est sans facteur carré et $\equiv 2 \bmod 4$. Il s'ensuit que $\mathrm{Cl}(A)$ est engendré *comme groupe* par les idéaux premiers divisant $2, 3, 4, 5, 6$, i.e. par les idéaux premiers contenant $2, 3$ ou 5. Ce sont respectivement $D = (2, \alpha)$, $T_\pm = (3, \alpha \pm 1)$ et $C_\pm = (5, \alpha \pm 2)$ (de normes 2, 3 et 5). D'après le cours on a les relations $(2) = D^2$, $(3) = T_+T_-$ et $(5) = C_+C_-$. La forme $x^2 + 26\,y^2$ représente $27 = \mathrm{N}((1+\alpha)) = 3^3$ et $30 = \mathrm{N}((2+\alpha)) = 2 \cdot 3 \cdot 5$. Mais $1 + \alpha \in T_+$ et $1 + \alpha \notin T_-$ (sinon on aurait $3 - (1+\alpha) - (1-\alpha) = 1 \in T_-$ et donc $T_- = A$), et $2 + \alpha$ est manifestement dans D, T_- et C_+, donc

$$(1 + \alpha) = T_-^3 \ \text{ et } \ (2 + \alpha) = DT_-C_+$$

par multiplicativité de la norme et propriété de Dedekind. On en déduit les relations $[D]^2 = [A]$, $[T_+][T_-] = [A]$, $[T_-]^3 = [A]$, $[D][T_-][C_+] = [A]$ et $[C_-][C_+] = [A]$ donc $\mathrm{Cl}(A)$ est engendré par $[D]$ et $[T_-]$. Mais $[DT_-]^3 = [D]$ et $[DT_-]^2 = [T_-]^{-1}$ donc $\mathrm{Cl}(A)$ est engendré par l'élément $[DT_-]$ dont l'ordre divise 6. Comme ni 2 ni 3 n'est représenté par $x^2 + 26\,y^2$, ni D ni T_- n'est principal et donc $\mathrm{Cl}(A) \simeq \mathbb{Z}/6\mathbb{Z}$.

Exercice 7.5 (i) Il est évident qu'un idéal principal non nul (π) d'un anneau A quelconque est premier si et seulement π est un élément premier, comme on l'a déjà remarqué dans le cours. Il faut donc simplement que vérifier que si un idéal premier $P \subset \mathcal{O}_K$ contient un élément premier π, alors $P = (\pi)$. Mais l'idéal (non nul) (π) est premier par l'observation précédente, il est donc maximal par un résultat du cours, et donc $(\pi) = P$.

(ii) Supposons $\mathcal{O}_K$ factoriel. Nous allons montrer que tous les idéaux premiers de $\mathcal{O}_K$ sont principaux. Il en résultera que $\mathcal{O}_K$ est principal par la propriété de Dedekind. Soient P un idéal premier non nul de $\mathcal{O}_K$ et $z \in P$ un élément non nul. Comme $\mathcal{O}_K$ a la propriété de factorisation (par exemple car il est noethérien), z est produit fini d'irréductibles. Comme P est premier il contient au moins un des facteurs irréductibles π de z. Mais π étant irréductible et $\mathcal{O}_K$ étant factoriel, π est premier, et donc $P = (\pi)$ d'après le (i).

(iii) Supposons qu'un ordre $A \subset \mathcal{O}_K$ est factoriel. L'anneau A étant un ordre on a $\mathrm{Frax}(A) = K$. Comme il est factoriel il est intégralement clos, donc en particulier $\mathcal{O}_K = \overline{\mathbb{Z}} \cap K \subset A$, et donc $\mathcal{O}_K = A$.

Problème 7.1 (i) Soient Q et Q' sont deux diviseurs de $P = \overline{\Pi}_{\alpha,\mathbb{Q}} \in (\mathbb{Z}/p\mathbb{Z})[X]$. Supposons Q et Q' premiers entre eux. D'après Bezout il existe $U, V \in (\mathbb{Z}/p\mathbb{Z})[X]$ tels que $UQ + VQ' = 1$. Soient $\widetilde{U}, \widetilde{V}, \widetilde{Q}$ et $\widetilde{Q'} \in \mathbb{Z}[X]$ des relevés respectifs de U, V, Q et Q'. On a donc $\widetilde{U}\widetilde{Q} + \widetilde{V}\widetilde{Q'} - 1 \in p\mathbb{Z}[X]$. Évaluée en α cette relation montre que $(\widetilde{Q}(\alpha), \widetilde{Q'}(\alpha)) = A$. Mais

$$\mathrm{I}(Q)\mathrm{I}(Q') = (p, \widetilde{Q}(\alpha))(p, \widetilde{Q'}(\alpha)) = p^2A + p(\widetilde{Q}(\alpha), \widetilde{Q'}(\alpha)) + \widetilde{Q}(\alpha)\widetilde{Q'}(\alpha)A.$$

Ainsi, $\mathrm{I}(Q)\mathrm{I}(Q') = (p, \widetilde{Q}(\alpha)\widetilde{Q'}(\alpha)) = \mathrm{I}(QQ')$.

(ii) Le (i) s'applique récursivement et montre que $\prod_{i=1}^{g} \mathrm{I}(Q_i) = \mathrm{I}(\prod_{i=1}^{g} Q_i) = \mathrm{I}(P) = pA$.

8. Problèmes de révision

Problème 1. (i) Comme $D<0$ toute classe d'équivalence propre de formes de discriminant D contient une et une seule forme réduite au sens de Gauss.

Déterminons les formes réduites (a,b,c) telles que $D=b^2-4ac=-132=-4\cdot 3\cdot 11$ suivant la méthode du cours. On rappelle notamment que $|b|\leq a\leq c$, $a\leq\sqrt{\frac{|D|}{3}}$ et $b\equiv D \bmod 2$. Comme $132/3=44<7^2$ on a donc $a<7$, puis $b=\pm 6,\pm 4,\pm 2,0$.

On résoud alors $ac=\frac{b^2-D}{4}$. Si $b=0$ alors $ac=3\cdot 11$, ce qui donne les formes

$$(3,0,11) \text{ et } (1,0,33).$$

Si $b=\pm 2$ alors $a\geq 2$, puis $ac=33+1=34=2\cdot 17$, ce qui donne simplement

$$(2,2,17)$$

(car $(2,-2,17)$ n'est pas réduite). Si $b=\pm 4$ alors $a\geq 4$ et $ac=33+4=37$: il n'y a pas de telle forme réduite. Si $b=\pm 6$ alors $a\geq 6$ et $ac=33+9=42=6\cdot 7$, ce qui donne simplement la forme

$$(6,6,7)$$

(car $(6,-6,7)$ n'est pas réduite). On a donc pour formes réduites de discriminant -132 les formes $(1,0,33)$, $(2,2,17)$, $(3,0,11)$ et $(6,6,7)$, puis $\mathrm{h}(-132)=4$. On constate que toutes ces formes sont ambiguës (voir le premier point du théorème sur les formes ambiguës).

(ii) $C=\{0,1,3,4,5,9\}$.

(iii) Soit n un entier. Si $n=x^2+33y^2$ alors n est un carré modulo 3, donc $n\equiv 0,1 \bmod 3$. De même, si $n=6x^3+6xy+7y^2$ alors $n\equiv 7y^2\equiv y^2 \bmod 3$, et donc n est aussi un carré modulo 3. Enfin, si $n=3x^2+11y^2$ alors $n\equiv 3x^2 \bmod 11$ et donc n est un carré modulo 11 car $3\in C$.

(iv) Supposons que $p\equiv 5 \bmod 12$ et que $\left(\frac{p}{11}\right)=-1$. Vérifions d'abord que p est représenté par une forme de discriminant -132. Comme $p>2$ il faut vérifier que -132 est un carré modulo p. Par multiplicativité du symbole de Legendre on a

$$\left(\frac{-132}{p}\right)=(-1)^{\frac{p-1}{2}}\left(\frac{3}{p}\right)\left(\frac{11}{p}\right)$$

et par la loi de réciprocité quadratique $\left(\frac{3}{p}\right)=(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)$ et $\left(\frac{11}{p}\right)=(-1)^{\frac{p-1}{2}}\left(\frac{p}{11}\right)$ car $11\equiv 3 \bmod 4$. Si p est comme dans l'énoncé, alors $p\equiv 1 \bmod 4$, $\left(\frac{3}{p}\right)=\left(\frac{11}{p}\right)=-1$, puis $\left(\frac{-132}{p}\right)=1$.

Le théorème de Lagrange assure alors qu'un tel p est représenté par l'une des formes $(1,0,33)$, $(2,2,17)$, $(3,0,11)$ et $(6,6,7)$. D'après le (iii), le seul cas possible est d'être représenté par $(2,2,17)$.

Les trois premiers nombres premiers concernés sont $p=17,29$ et 41, qui sont bien de la forme $2x^2+2xy+17y^2$: prendre $y=1$ et respectivement $x=0,2,3$.

Problème 2. (i) Soit $e_1,\dots,e_n$ la $\mathbb{Z}$-base canonique de $\mathbb{Z}^n$. La famille

$$u(e_1),\dots,u(e_n)$$

est une $\mathbb{R}$-base de $\mathbb{R}^n$, car $\det(u)\neq 0$. Par $\mathbb{Z}$-linéarite de u, $u(\mathbb{Z}^n)$ est le réseau de $\mathbb{R}^n$ engendré par cette $\mathbb{R}$-base. Posons $L=u(\mathbb{Z}^n)$. On a donc $\mathrm{covol}(L)=|\det_{\{e_i\}}(u(e_1),\dots,u(e_n))|=|\det(u)|$. Le réseau L étant un sous-réseau de $\mathbb{Z}^n$, il est d'indice fini dans $\mathbb{Z}^n$, d'indice $\mathrm{covol}(L)/\mathrm{covol}(\mathbb{Z}^n)=\mathrm{covol}(L)$ car $\mathrm{covol}(\mathbb{Z}^n)=1$ (par convention), d'après la proposition 2.17.

(ii) Soit $n=[\mathbb{Q}(\alpha):\mathbb{Q}]$. D'après le cours, $1,\alpha,\dots,\alpha^{n-1}$ est une $\mathbb{Z}$-base de A et une $\mathbb{Q}$-base de $\mathbb{Q}(\alpha)$, de sorte que l'application $\mathbb{Q}$-linéaire $\psi:\mathbb{Q}^n\to\mathbb{Q}(\alpha)$, $(x_i)\mapsto\sum_{i=1}^n x_i\alpha^{i-1}$, est une bijection satisfaisant $\psi(\mathbb{Z}^n)=A$. Si $x\in\mathbb{Q}(\alpha)$, l'application $m'_x:=\psi^{-1}\circ m_x\circ\psi$ est un endomorphisme de $\mathbb{Q}^n$ de déterminant $\det(\psi^{-1}\circ m_x\circ\psi)=\det(m_x)=\mathrm{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(x)$. Mais si $x\in A$, $m_x(A)\subset A$, et donc $m'_x(\mathbb{Z}^n)\subset\mathbb{Z}^n$. Le (i) appliqué à m'_x montre que $|\mathbb{Z}^n/m'_x(\mathbb{Z}^n)|=|\mathrm{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(x)|$, et on conclut car ψ induit un isomorphisme de $\mathbb{Z}^n/m'_x(\mathbb{Z}^n)$ sur A/xA.

Problème 3. (i) Si $p\equiv 3 \bmod 4$ la somme de Gauss relative à p est de carré $-p$, et appartient à $\mathbb{Q}(\zeta)$.

(ii) Comme $\Sigma(L)$ est fini, les $\sigma(L)$ avec $\sigma \in \Sigma(L)$ forment un ensemble fini de corps de nombres, ils engendrent donc un corps de nombres que l'on note M. On rappelle que si L/K est une extension de corps de nombres, l'application de restriction $\Sigma(L) \to \Sigma(K)$ est surjective. Appliquant ceci à M/K, on peut donc trouver pour tout $\sigma \in \Sigma(K)$ un élément $\sigma' \in \Sigma(M)$ tel que $\sigma'_{|K} = \sigma$. Il y a en fait $[M : K]$ choix pour un tel σ' mais n'importe quel choix fixé conviendra dans l'argument qui suit.

Vérifions comme suggéré que les $[L : K] \cdot [K : \mathbb{Q}] = [L : \mathbb{Q}]$ éléments $\sigma' \circ \tau$ avec $\sigma \in \Sigma(K)$ et $\tau \in \Sigma(L/K)$ sont exactement les $[L : \mathbb{Q}]$ éléments de $\Sigma(L)$. Il suffit de vérifier qu'ils sont distincts. Supposons donc $\sigma'_1 \circ \tau_1 = \sigma'_2 \circ \tau_2$ avec les τ_i dans $\Sigma(L/K)$ et les σ_i dans $\Sigma(K)$. On a donc $(\tau_1)_{|K} = (\tau_2)_{|K} = \mathrm{Id}_K$ par l'hypothèse, et donc $\sigma'_1(x) = \sigma'_2(x)$ pour tout $x \in K$. Cela entraîne $\sigma_1 = \sigma_2$, et donc $\sigma'_1 = \sigma'_2$. Par injectivité des plongements, il reste alors $\tau_1 = \tau_2$, ce qui conclut.

Ceci étant dit, fixons $x \in L$. On a d'une part $\mathrm{N}_{L/K}(x) = \prod_{\tau \in \Sigma(L/K)} \tau(x)$ (prop 5.14). Comme cette norme est un élément de K, pour tout $\sigma \in \Sigma(K)$, on a $\sigma(\mathrm{N}_{L/K}(x)) = \sigma'(\mathrm{N}_{L/K}(x))$. Mais $\tau(x) \in M$ pour tout $\tau \in \Sigma(L/K)$ donc on peut écrire

$$\sigma(\mathrm{N}_{L/K}(x)) = \sigma'(\mathrm{N}_{L/K}(x)) = \prod_{\tau \in \Sigma(L/K)} \sigma' \circ \tau(x).$$

On conclut par la suite d'égalités

$$\mathrm{N}_{K/\mathbb{Q}} \circ \mathrm{N}_{L/K}(x) = \prod_{\sigma \in \Sigma(K), \tau \in \Sigma(L/K)} (\sigma' \circ \tau)(x) = \prod_{\sigma \in \Sigma(L)} \sigma(x) = \mathrm{N}_{L/\mathbb{Q}}(x).$$

On a utilisé la Proposition 5.14 pour $K/\mathbb{Q}$, L/K ainsi que l'indication démontrée au paragraphe précédent.

(iii) Soient $L = \mathbb{Q}(\zeta)$ et $K = \mathbb{Q}(\sqrt{-p})$. On a $K \subset L$ d'après le (i). Supposons $n = \mathrm{N}_{L/\mathbb{Q}}(x)$ avec $x \in \mathbb{Z}[\zeta]$. Alors $n = \mathrm{N}_{K/\mathbb{Q}}(z) = z\overline{z}$ avec $z = \mathrm{N}_{L/K}(x)$, d'après le (ii). Mais $\mathbb{Z}[\zeta] \subset \mathcal{O}_K$, $\mathrm{N}_{L/K}(\mathcal{O}_L) \subset \mathcal{O}_K$ et $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$.

(iv) Soit ℓ un nombre premier. Si $\ell \equiv 1 \bmod p$ alors le polynôme $X^p - 1 = (X-1)\varphi_p$ divise le polynôme $X^{\ell-1} - 1$ dans $\mathbb{Z}[X]$. Mais $X^{\ell-1} - 1$ est scindé à racines distinctes dans $(\mathbb{Z}/\ell\mathbb{Z})[X]$ (petit théorème de Fermat), il en va donc de même de φ_p.

(v) (suite) D'après le (iv), il existe au moins un $a \in \mathbb{Z}$ tel que $\varphi_p(a) \equiv 0 \bmod \ell$. Considérons le morphisme surjectif d'anneaux $\psi : \mathbb{Z}[X] \to \mathbb{Z}/\ell\mathbb{Z}, P \mapsto P(a) \bmod \ell$. Alors $\varphi_p = \Pi_{\zeta,\mathbb{Q}}$ est dans $\mathrm{Ker}(\psi)$, de sorte que ψ se factorise par $\mathbb{Z}[X]/(\Pi_{\zeta,\mathbb{Q}}) \simeq \mathbb{Z}[\zeta]$ (d'après le cours), et définit donc par passage au quotient un morphisme surjectif d'anneaux $\psi' : \mathbb{Z}[\zeta] \to \mathbb{Z}/\ell\mathbb{Z}$. Ainsi, $\mathbb{Z}[\zeta]/\ker(\psi') \simeq \mathbb{Z}/\ell\mathbb{Z}$ et $Q := \ker(\psi')$ est un idéal de $\mathbb{Z}[\zeta]$ de norme ℓ.

(vi) (suite) Supposons $Q = x\mathbb{Z}[\zeta]$ pour un certain $x \in \mathbb{Z}[\zeta]$. Le (ii) du problème 2 assure que $\ell = \mathrm{N}(Q) = |\mathrm{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(x)|$. D'après le (iii) ci-dessus, si $z = \mathrm{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}(\sqrt{-p})}(x) \in \mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$ on a

$$\ell = |\mathrm{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(x)| = |z\overline{z}| = z\overline{z}.$$

On conclut car si $\alpha = \frac{1+\sqrt{-p}}{2}$ et $x, y \in \mathbb{Z}$, alors

$$\mathrm{N}(x + y\sqrt{\alpha}) = x^2 + xy + \frac{1+p}{4}y^2.$$

(vii) Ainsi, si $\mathbb{Z}[\zeta]$ est principal, alors la forme $x^2 + xy + \frac{1+p}{4}y^2$ représente tous les nombres premiers $\ell \equiv 1 \bmod p$.

(viii) Si $p = 23$, le nombre premier $\ell = 47$ est congru à 1 modulo p. Mais la forme $x^2 + xy + 6y^2$ ne représente pas 47. En effet, c'est x^2 pour $y = 0$, $x^2 + x = x(x \pm 1)$ si $y = \pm 1$, $(x \pm 1)^2 + 23$ si $y = \pm 2$, et enfin

$$x^2 + xy + 6y^2 = \frac{1}{4}(2x + y)^2 + \frac{23}{4}y^2 \geq \lceil 9\frac{23}{4} \rceil = \lceil \frac{208}{4} \rceil = 52 > 47$$

si $|y| \geq 3$.

9. Corrigé de l'examen 2011-2012

Problème 1. (i) Il suffit de déterminer les formes réduites de Gauss (a,b,c) de discriminant -136. Elles satisfont en particulier $b \equiv 0 \bmod 2$ et $|b| \leq a \leq \sqrt{\frac{136}{3}} < 7$ car $136/3 < 49$. On trouve $(1,0,34)$, $(2,0,17)$ et $(5,\pm 2,7)$.

(ii) Les classes ambigües sont celles de $(1,0,34)$ et $(2,0,17)$. Il y a donc 3 formes à équivalence près : $(1,0,34)$, $(2,0,17)$ et $(5,2,7)$.

(iii) La loi de réciprocité quadratique assure que pour $p \neq 2, 17$

$$\left(\frac{-136}{p}\right) = \left(\frac{-2}{p}\right)\left(\frac{17}{p}\right) = (-1)^{\frac{p-1}{4}+\frac{p^2-1}{8}}\left(\frac{p}{17}\right)$$

car $17 \equiv 1 \bmod 4$. Si p est comme dans l'énoncé il vient que -136 est un carré modulo p, et donc modulo $4p$ car $-136 \equiv 0 \bmod 4$ et p est impair. Il est donc représenté par l'une des formes $(1,0,34)$, $(2,0,17)$ et $(5,2,7)$ (et même une seule) par le (ii) et le théorème de Lagrange.

Si p est représenté par l'une des deux premières alors soit $p \equiv 2x^2 \bmod 17$, soit $p \equiv x^2 \bmod 17$, ce qui est absurde car p n'est pas un carré modulo 17, alors que 2 l'est ($17 \equiv 1 \bmod 8$).

(iv) A est de Dedekind car -34 est sans facteur carré et $\equiv 2 \bmod 4$.

(v) On a les factorisations $X^2+34 \equiv X^2$ modulo 2, irréductible modulo 3, $\equiv X^2-1$ modulo 5 et 7. On en déduit que (3) est premier. De plus, si $D = 2A + \alpha A$, $C = 5A + (\alpha+1)A$, $C' = 5A + (\alpha-1)A$, $S = 7A + (\alpha+1)A$ et $S' = 7A + (\alpha-1)A$, alors ces idéaux sont premiers distincts et on a : $(2) = D^2$, $(5) = CC'$, $(7) = SS'$.

On a $\alpha+1 \in C, S$ donc les idéaux premiers distincts C et S divisent $(\alpha+1)$. Mais $\mathrm{N}(\alpha+1) = 35 = \mathrm{N}(C)\mathrm{N}(S)$ donc $(\alpha+1) = CS$.

(vi) Minkowski nous dit que toute classe d'idéaux non nuls contient un idéal contenant $1 \leq N \leq 7$, i.e. divisant (N) pour un tel N par la propriété de Dedekind. Ces idéaux sont donc produits d'idéaux premiers contenant $2, 3, 5$ ou 7. Ainsi, $\mathrm{Cl}(A)$ est engendré par tous les idéaux premiers ci-dessus. Les relations $[C][C'] = 1$, $[S][S'] = 1$ et $[C][S] = 1$ assure que $\mathrm{Cl}(A)$ est engendré par $[C]$ et $[D]$.

(vii) $\mathrm{N}(D) = 2$ et 2 n'est pas de la forme $x^2 + 34y^2$ donc D n'est pas principal. Par contre $\mathrm{N}(CD^2) = 2 \cdot 25 = 50$ est la norme des éléments $\pm(\alpha \pm 4)$. Comme $\alpha - 4$ n'est pas dans C' (sinon on aurait aussi $\alpha - 1 - (\alpha - 4) = 3 \in C'$ puis $5 - 2 \cdot 3 = -1 \in C'$ ce qui est absurde), la propriété de Dedekind entraîne $DC^2 = (\alpha - 4)$.

(viii) On a $[D]^2 = 1$ car $(2) = D^2$, et $[D] \neq 1$, donc $[D]$ est d'ordre 2. De plus, $[D][C]^2 = 1$, donc $[D] = [C]^2$ d'où l'on tire que $\mathrm{Cl}(A)$ est engendré par $[C]$ qui est d'ordre 4.

(ix) Le théorème de Dedekind définit un isomorphisme de groupes entre $\mathrm{Cl}(A)$ avec $\mathrm{Cl}(-136)$, ce dernier étant muni de la loi de composition de Gauss. On a donc $\mathrm{Cl}(-136) \simeq \mathbb{Z}/4\mathbb{Z}$. La classe principale est l'élément neutre, l'autre classe ambigüe $[(2,0,17)]$ est l'élément d'ordre 2, et les classes de $[(5,\pm 2,7)]$ sont donc des générateurs (inverses l'un de l'autre). Cela détermine uniquement la table de multiplication.

(x) En particulier, $[(5,2,7)]^2 = [(2,0,17)]$ et $[(5,2,7)][(5,-2,7)] = 1$. Le résultat s'en déduit car une composée de Gauss est une composée au sens du cours.

(xi) 5 et 7 ont les propriétés requises. On a $35 = 2 \cdot 9 + 17 = 1 + 34$.

Problème 2. (i) Les conjugués sur $\mathbb{Q}$ de ζ sont les racines de $\Pi_{\zeta,\mathbb{Q}} = X^4 + 1$, i.e. ζ, ζ^3, ζ^5 et ζ^7 qui sont tous complexes non réels, donc l'entier r_2 du corps de nombres $\mathbb{Q}(\zeta)$ est $\frac{4}{2} = 2$. Le discriminant de $X^4 + 1$ vaut 4^4 par une formule du cours, le covolume de $\iota(\mathbb{Z}[\zeta])$ vaut donc

$$\frac{1}{2^{r_2}}|4^4|^{1/2} = 4.$$

(ii) D'après Minkowski tout idéal non nul de $\mathbb{Z}[\zeta]$ est équivalent à un idéal contenant un entier N compris entre 1 et $\left(\frac{4}{\pi}\right)^2 \frac{4!}{4^4} \cdot 4 \cdot 4 = 3\frac{8}{\pi^2} < 3$.

(iii) Comme $X^4 + 1 \equiv (X-1)^4 \bmod 2$, on déduit du cours que les idéaux de $\mathbb{Z}[\zeta]$ contenant 2 sont les 5 idéaux $I_i = (2, (\zeta-1)^i)$ avec $i = 0, \ldots, 4$. On a $I_0 = \mathbb{Z}[\zeta]$ (l'anneau tout entier) qui est aussi l'unique idéal contenant 1.

(iv) La dérivée en 1 de $X^8 - 1 = \prod_{i=0}^{7}(X - \zeta^i)$ s'écrit de deux façons

$$8 = \prod_{i=1}^{7}(1 - \zeta^i).$$

Mais $\zeta^2 = i$, $\zeta^4 = -1$ et $\zeta^6 = -i$, donc $(1-\zeta^2)(1-\zeta^4)(1-\zeta^6) = (1-i)(1+i)2 = 4$, ce qui conclut la première formule. Pour la seconde on remarque que pour tout $i = 1, \ldots, 7$ on a

$$1 - \zeta^i = (1 - \zeta)(\sum_{k=0}^{i-1} \zeta^k) \in (1 - \zeta)\mathbb{Z}[\zeta].$$

(v) On déduit du (iv) que $2 \in (1 - \zeta^i)$ pour $i \leq 4$, donc $I_i = ((1 - \zeta)^i)$ est principal.

(vi) On en déduit que tout idéal de $\mathbb{Z}[\zeta]$ est équivalent à un idéal principal : $\mathbb{Z}[\zeta]$ est principal.

(vii) Principal implique factoriel implique intégralement clos, donc $\mathbb{Z}[\zeta]$ est intégralement clos. Il contient donc l'anneau des entiers de $\mathbb{Q}(\zeta)$, et donc il est égal à ce dernier.

Problème 3. (i) Soient $x, y \in \mathbb{Z}$ tels que $y^2 = x^5 - k$. On a $y \equiv x \bmod 2$ car $k \equiv 0 \bmod 2$. Il suffit donc de montrer que x et y sont premiers entre eux. Si $d > 1$ divse x et y alors d^2 divise k : absurde.

(ii) L'idéal $(y + \alpha, y - \alpha)$ contient $2y$ et $(y - \alpha)(y + \alpha) = x^5$. Mais $2y$ et x^5 sont premiers entre eux par le (i), il contient donc 1 par Bézout.

(iii) On a $(y - \alpha)(y + \alpha) = (x)^5$. Comme les idéaux $(y - \alpha)$ et $(y + \alpha)$ sont premiers entre eux dans l'anneau de Dedekind $\mathbb{Z}[\alpha]$ (car $k \equiv 2 \bmod 4$ est sans facteur carré), on déduit de l'unicité de la décomposition en produit d'idéaux premiers que $(y + \alpha)$ est de la forme I^5 pour un certain idéal I de $\mathbb{Z}[\alpha]$.

(iv) On sait que $\mathrm{h}(-4k)$ est le cardinal du groupe $\mathrm{Cl}(A)$. Si il est premier à 5, ce groupe n'a pas d'élément d'ordre 5. Comme $[I]^5 = [I^5] = 1$, il vient que $[I] = 1$.

(v) Ainsi, I est principal, disons engendré par $z \in \mathbb{Z}[\alpha]$. On a donc $(y+\alpha) = (z^5)$ puis $y+\alpha = uz^5$ où u est une unité de A, i.e. $u = \pm 1$ par un résultat du cours. Mais alors $u = u^5$ et donc $y+\alpha = (uz)^5$. Soient $a, b \in \mathbb{Z}$ des entiers tels que $uz = a + b\alpha$. On conclut par la formule du binôme.

(vi) On rappelle que $1, \alpha$ est une $\mathbb{Z}$-base de A. En égalisant le coefficient en α on obtient

$$1 = b(5a^4 + 10a^2b^2k + b^4k^2).$$

Donc $b = \pm 1$ (tous les termes sont entiers), puis $b^2 = b^4 = 1$, d'où la première assertion. En égalisant le coefficient en 1 on constate aussi que $y \equiv a \bmod 2$, donc a est impair. En particulier $a^2 \equiv 1 \bmod 8$. Il vient $5 + k(k + 2) \equiv \pm 1 \bmod 8$. Comme k est pair, $k(k + 2) \equiv 0 \bmod 8$, puis $5 \equiv \pm 1 \bmod 8$: c'est absurde.

(vii) On regarde les entiers $3^5 - y^2 > 0$ avec y impair, i.e. $y \in \{1, 3, 5, 7, 9, 11, 13, 15\}$. On trouve respectivement $242, 234, 218, 194, 122, 74, 18$. Mais 9 divise 18 et 234, et $11^2 \cdot 2 = 242$. Par contre, $218 = 2 \cdot 109$, $194 = 2 \cdot 97$, $122 = 2 \cdot 67$ et $74 = 2 \cdot 37$ sont sans facteur carré : ces valeurs de k conviennent donc et on en déduit le résultat.

10. Corrigé de l'examen 2012-2013

Problème 1. (i) Les carrés de $(\mathbb{Z}/13\mathbb{Z})^\times$ sont $\pm 1, \pm 3$ et ± 4.

(ii) On a $-104 = -8 \cdot 13$. En particulier -104 est un carré modulo 13. Si $p \neq 2, 13$, on a

$$\left(\frac{-104}{p}\right) = \left(\frac{-2}{p}\right)\left(\frac{13}{p}\right) = \left(\frac{-2}{p}\right)\left(\frac{p}{13}\right)$$

Ainsi -104 est un carré modulo p si et seulement si $\left(\frac{-2}{p}\right) = \left(\frac{p}{13}\right)$. Mais $\left(\frac{-2}{p}\right) = (-1)^{\frac{p-1}{4}+\frac{p^2-1}{8}}$ vaut 1 si et seulement si $p \equiv 1, 3 \bmod 8$. On conclut par le (i).

(iii) Il suffit de déterminer les formes réduites de Gauss (a, b, c) de discriminant -104. Elles satisfont en particulier $b \equiv 0 \bmod 2$ et $|b| \leq a \leq \sqrt{\frac{104}{3}} < 6$ car $104/3 < 35 < 6^2$. On trouve $(1, 0, 26)$ et $(2, 0, 13)$ pour $b = 0$, $(3, \pm 2, 9)$ pour $b = \pm 2$, et $(5, \pm 4, 6)$ pour $b = \pm 4$.

(iv) Les classes ambiguës sont celles de $(1, 0, 26)$ et $(2, 0, 13)$. Il y a donc 4 formes à équivalence (non nécessairement propre) près : $(1, 0, 34)$, $(2, 0, 13)$, $(3, 2, 9)$ et $(5, 4, 6)$.

(v) Si $p \equiv 1, 3 \bmod 8$ et p est un carré modulo 13, alors -104 est un carré modulo p d'après le (ii). Il l'est donc également modulo $4p$ car $-104 \equiv 0 \bmod 4$ et p est impair. Il est donc représenté par l'une des 4 formes précédentes, et même par une seule, d'après un résultat du cours dû à Lagrange. Si p est de la forme $2x^2 + 13y^2$ alors $p \equiv 2x^2$ modulo 13, ce qui est absurde car 2 n'est pas un carré modulo 13 (observer que $p \neq 13$). Si p est de la forme $5x^2 + 4xy + 6y^2$, alors x est impair et donc $p \equiv 5, -1 \bmod 8$ (selon que y est pair ou impair). C'est encore absurde.

(vi) La forme $(3, 2, 9)$ représente 3 et la forme $(1, 0, 26)$ représente le nombre premier $107 = 9^2 + 26$.

(vii) A est l'anneau des entiers de $\mathbb{Q}(\alpha)$ car -26 est sans facteur carré et $\equiv 2 \bmod 4$.

(viii) On a les factorisations $X^2 + 26 \equiv X^2$ modulo 2, $X^2 + 26 \equiv X^2 - 1 = (X - 1)(X + 1)$ modulo 3, et $X^2 + 26 \equiv X^2 - 4 = (X - 2)(X + 2)$ mod 5. D'après le cours, les idéaux premiers cherchés sont donc $D = (2, \alpha)$, $T_\pm = (3, \alpha \pm 1)$ et $C_\pm = (5, \alpha \pm 2)$.

(ix) Si un idéal I de A est principal engendré par $z \in A$, on sait que $\mathrm{N}(z) = \mathrm{N}(I)$. En particulier, $\mathrm{N}(I)$ est de la forme $x^2 + 26y^2$. D'après le cours, les idéaux premiers précédents sont de norme respective $2, 3, 3, 5, 5$. Mais aucun de ces entiers n'est représenté par $x^2 + 26y^2$.

(x) D'après le cours, (vii) et (viii), on a $(2) = D^2$, $(3) = T_+T_-$ et $(5) = C_+C_-$. Le nombre $\alpha + 2$ est de norme $4 + 26 = 30 = 2 \cdot 3 \cdot 5$. De plus, $\alpha + 2$ est dans les trois idéaux premiers distincts D, T_- et C_+. La propriété de Dedekind montre alors que $(\alpha + 2)$ est divisible par DT_-C+. Ce dernier étant également de norme 30, on a l'égalité $(\alpha + 2) = DT_-C_+$. De même, $(\alpha - 2) = DT_+C_-$.

(xi) Minkowski nous dit que toute classe d'idéaux non nuls de A contient un idéal contenant un entier $1 \leq n \leq \frac{2}{\pi}\sqrt{104} < 2\sqrt{104/9} < 2\sqrt{12} = \sqrt{48} < 7$. Par la propriété de Dedekind, un tel idéal est un diviseur de (2), (3), (4) = (2)(2), (5) ou (6) = (2)(3), ses facteurs premiers étant donc parmi ceux du (viii). On en déduit que $\mathrm{Cl}(A)$ est engendré comme groupe par les classes de D, $T_\pm$ et $C_\pm$.

(xii) On a $[T_+][T_-] = 1$, $[C_+][C_-] = 1$, et $[D][T_-][C_+] = 1$ par le (x). Ainsi, $\mathrm{Cl}(A) = \langle [D], [T] \rangle$ où $T = T_+$.

(xiii) L'énoncé suggère que T^3 est principal, auquel cas il doit être engendré par un élément $z \in A$ tel que $N(z) = 3^3 = 27$. Il n'y a que deux tels éléments, à savoir $\pm\alpha + 1$. Les diviseurs premiers de $(\pm\alpha + 1)$ sont ceux contenant 3, donc T_- et $T = T_+$. Mais comme $\alpha + 1 \in T$ mais $\alpha + 1$ n'est pas dans T^-, car sinon $-1 = \alpha + 1 - (\alpha - 1) - 3$ serait dans T^-, il vient que $(\alpha + 1) = T^a$ puis $a = 3$ en prenant la norme.

On aurait aussi pu calculer directement. Comme $(\alpha + 1)^2 = 2(\alpha + 1) - 27$, on a $T^2 = (9, 3(\alpha + 1), 2(\alpha + 1)) = (9, \alpha + 1)$ et puis $T^3 = (27, 18(\alpha + 1), 2(\alpha + 1)) = (27, \alpha + 1) = (\alpha + 1)$.

(xiv) On a vu que $\mathrm{Cl}(A) = \langle [D], [T] \rangle$ avec $[D]^2 = 1$ et $[T]^3 = 1$. Ainsi, $[DT]^3 = [D]$ et $[DT]^4 = [T]$, donc $\mathrm{Cl}(A)$ est engendré par $[DT]$. On a $[DT]^6 = 1$, donc $[DT]$ est d'ordre divisant 6. Comme ni T, ni D ne sont principaux, les relations $[DT]^3 = [D]$ et $[DT]^2 = [T]^{-1}$ montrent $[DT]$ est d'ordre 6, ce qui conclut.

(xv) D'après la question précédente, un système de représentants des classes non triviales est donné par les $[DT]^i$ avec $i = 1, \ldots, 5$. Mais on constate que $[DT] = [C_-]^{-1} = [C_+]$, $[DT]^2 = [T]^2 = [T_-]$, $[DT]^3 = [D]$, $[DT]^4 = [T]$, $[DT]^5 = [DT]^{-1} = [C_-]$.

(xvi) Par un argument vu en classe, $2, \alpha$ est une $\mathbb{Z}$-base de D. De même, $3, \alpha \pm 1$ en est une de $T_\pm$, et $5, \alpha \pm 2$ en est une de $C_\pm$. Un calcul direct de la forme associée à ces $\mathbb{Z}$-base, montre que si $I = D$, $T_\pm$, $C_\pm$, alors la classe q_I est respectivement celle de $(2, 0, 13)$, $(3, \pm 2, 9)$ et $(5, \pm 4, 6)$. On conclut par (xv) et (iii).

(xvii) On a $q_T = [(3, 2, 9)]$, donc l'ordre de $[(3, 2, 9)]$ dans $\mathrm{Cl}(-104)$ est celui de $[T]$ dans $\mathrm{Cl}(A)$, i.e. 3. De même, $q_D = [(2, 0, 13)]$ donc $q_{DT} = q_D q_T = q_{C_+} = [(5, 4, 6)]$.

(xviii) Sous l'hypothèse sur p, on a vu au (v) que p est représenté par une forme q qui est soit la forme principale soit $(3, 2, 9)$. Dans tous les cas, $[q]^3$ est la classe de la forme principale par le (xvii), donc p^3 est représenté par la forme principale.

Problème 2. (i) La relation $x^p + y^p = 1$ s'écrit aussi $(x+y)(\sum_{i=0}^{p-1} x^i(-y)^{p-1-i}) = 1$, la somme entre parenthèse étant dans A, donc $x + y \in A^\times$.

(ii) Si $x + y = -1$, on a la congruence $(-1)^p \equiv x^p + y^p = 1$ modulo $p\overline{\mathbb{Z}}$. On en tire la congruence traditionnelle $(-1)^p \equiv 1 \bmod p$, ce qui est absurde car $p \neq 2$.

(iii) On part de $x^p + (1 - x)^p = 1$, l'énoncé s'en déduit pour $P = \frac{1}{p} \sum_{i=1}^{p-2} (-X)^{i-1} \binom{p}{i+1} \in \mathbb{Z}[X]$.

(iv) De $x(xP(x) - 1) = 0$ on tire que soit $x = 0$, soit $xP(x) = 1$ et donc $x \in A^\times = \{\pm 1\}$. Si $x = 0$ alors $y = 1 - x = 1$, si $x = 1$ alors $y = 1 - x = 0$, si $x = -1$ alors $y = 1 - x = 2$, ce qui est absurde car alors $x^p + y^p = -1 + 2^p \neq 1$ (car $p \neq 1$).

(v) On a $DN^2 \equiv 1 \bmod 8$. En particulier, N est impair, et donc $N^2 \equiv 1 \bmod 8$, puis $D \equiv 1 \bmod 8$.

(vi) On a $K = \mathbb{Q}(\sqrt{D})$, et comme D est sans facteur carré et $D \equiv 1 \bmod 4$, le cours assure que $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$, et $\mathcal{O}_K^\times = \{\pm 1\}$ car $D \equiv 1 \bmod 4$ est sans facteur carré, $D < 0$, et $D \neq -3$.

(vii) Le théorème de Dedekind assure que $h_K = |\mathrm{P}(D)|$ car $\mathcal{O}_K = A_D$. Mais $D \equiv 1 \bmod 4$ est sans facteur carré, donc $\mathrm{Cl}(D) = \mathrm{P}(D)$.

Si $p = 2$ alors $D = 1 - 2^4 = -15$. Les réduites de Gauss (a, b, c) de ce discriminant satisfont $b \equiv 1 \bmod 2$ et $b^2 \leq 15/3 < 3^2$, donc $b = \pm 1$. On trouve $(1, 1, 4)$ et $(2, 1, 2)$. Ainsi, $|\mathrm{Cl}(-15) = 2|$, ce qui conclut si $p = 2$.

(viii) On a $2^p = \frac{1-N^2D}{4} = \frac{1-N\sqrt{D}}{2} \frac{1+N\sqrt{D}}{2} = z(1 - z)$ si $z = \frac{1-N\sqrt{D}}{2}$. Comme N est impair (cf. (v)), $z \in \mathcal{O}_K$.

(ix) Les idéaux (z) et $(1 - z)$ sont premiers entre eux. En effet, s'ils possèdent un facteur commun Q, alors $z, 1 - z \in Q$, et donc $1 \in Q = \mathcal{O}_K$. La relation $(z)(1 - z) = (2)^p$, ainsi que la propriété de Dedekind, entraîne alors que (z) et $(1 - z)$ dont des puissances p-èmes d'idéaux de $\mathcal{O}_K$.

(x) Si $I^p = (z)$, alors $[I]^p = 1$ dans $\mathrm{Cl}(\mathcal{O}_K)$. En particulier, l'ordre de $[I]$ divise p, c'est donc 1 ou p car p est premier. Si p ne divise pas h_K, cet ordre est 1, i.e. I est principal. Le raisonnement est le même pour J.

(xi) Si p ne divise pas h_K on peut trouver $x \in \mathcal{O}_K$ tels que $I = (x)$ d'après le (x). En particulier, $(x^p) = (z)$ et donc x^p et z sont associés dans $\mathcal{O}_K$. Ainsi, $x^p = \pm z$ car $\mathcal{O}_K^\times = \{\pm 1\}$ par le (vi). Il vient que $z = (\pm x)^p$ car $p \neq 2$. Quitte à remplacer x en $-x$ on peut donc supposer que $z = x^p$. De même, on peut trouver y tel que $1 - z = y^p$.

(xii) Pour conclure, on peut supposer $p > 2$ d'après le (vi). Si p ne divise pas h_K, alors on peut trouver $x, y \in \mathcal{O}_K$ tels que $x^p + y^p = 1$ et $2^p = x^p(1 - x^p)$ d'après les questions précédentes. Le (iv) s'applique à $A = \mathcal{O}_K$ car on a vu au (vi) que $\mathcal{O}_K^\times = \{\pm 1\}$. Il montre que $x = 0$ ou $x = 1$, ce qui est absurde car cela conduit à $2^p = 0$.

(xiii) Pour $p = 7$, on a $1 - 2^9 = -511 = -7 \cdot 73$ (sans facteur carré..). En particulier, $|\mathrm{Cl}(-511)| = h_K$ est multiple de 7. Mais d'autre part, on sait que $|\mathrm{Cl}(-511)|$ est pair d'après Gauss, car le nombre impair -511 n'est pas puissance d'un nombre premier. Ainsi, $|\mathrm{Cl}(-511)|$ est multiple de 14. Si l'on ne veut pas invoquer le théorème de Gauss, on peut aussi vérifier qu'il y a un élément d'ordre 2 dans $\mathrm{P}(-511) = \mathrm{Cl}(-511)$, i.e. une forme ambiguë réduite non triviale. Comme -511 est impair, une telle forme est nécessairement de la forme (a, a, c) avec $1 < a < c$ et satisfait $a^2 - 4ac = -511$. La seule solution est $a = 7$, $a - 4c = -73$, i.e. $(7, 7, 20)$. Avec un peu d'acharnement, on pourrait en fait voir que $|\mathrm{Cl}(-511)| = 14$.

11. Corrigé de l'examen 2013-2014

Problème 1. (i) On détermine les réduites de Gauss (a,b,c) de discriminant -55 par l'algorithme du cours. En particulier b est impair et $|b| \leq [\sqrt{55/3}] = 4$. On a $(55+1)/4 = 14 = 1*14 = 2*7$ d'où $(1,1,14)$ et $(2,\pm 1,7)$, puis $(55+9)/4 = 16 = 4*4$ d'où $(4,3,4)$ (car $(4,-3,4)$ n'est pas réduite). Sont ambigües $(1,1,14)$ et $(4,3,4)$ par la caractérisation de Gauss.

(ii) $\mathrm{P}(-55) = \mathrm{Cl}(-55)$ car toutes les formes de discriminant -55 sont primitives (d'après le (i), ou plus généralement car -55 est fondamental). C'est donc un groupe d'ordre 4 pour la loi de Gauss. On sait que le neutre correspond à la classe de la forme principale et que les éléments de carré 1 correspondent aux classes ambiguës. Ainsi, la classe x de la forme non ambiguë $(2,1,7)$, dont l'ordre divise 4, est nécessairement d'ordre exactement 4. De plus, $x^2 = [(4,3,4)]$ (car d'ordre 2), $x^4 = [(1,1,14)]$ (élément neutre), et $x^3 = x^{-1} = x^{\mathrm{opp}} = [(2,-1,7)]$. La table de multiplication de $\mathrm{P}(-55) = \langle x \rangle$ s'en déduit.

(iii) On a vu que le carré de $[(2,1,7)]$ est $[(4,3,4)]$, donc $(4,3,4)$ est une composée de Gauss de $(2,1,7)$ par elle-même. On a aussi vu que $[(2,-1,7)]$ est l'inverse de $[(2,1,7)]$, de sorte que $[(2,1,7)][(2,-1,7)] = [(1,1,14)]$. Mais $(2,-1,7)$ est (non proprement) équivalente à $(2,1,7)$, de sorte que $(1,1,14)$ est également une composée (qui n'est pas de Gauss !) de $(2,1,7)$ par lui-même. On conclut car $(4,3,4)$ et $(1,1,14)$ sont non équivalentes, étant toutes deux ambiguës et non proprement équivalentes.

(iv) D'après Lagrange p est représenté par une forme q de discriminant -55 si et seulement si -55 est un carré modulo $4p$. Vérifions que c'est équivalent à la condition de l'énoncé. C'est vrai si $p = 2$ car $-55 \equiv 1 \bmod 8$ est un carré modulo 8, et 2 n'est ni un carré modul 5, ni modulo 11. Supposons $p > 2$, -55 est donc un carré mod. $4p$ ssi $\left(\frac{-55}{p}\right) = \left(\frac{5}{p}\right)\left(\frac{-11}{p}\right) = 1$, ou ce qui revient au même ssi $\left(\frac{5}{p}\right) = \left(\frac{-11}{p}\right)$. Par hypothèse $p \neq 5, 11$. La loi de réciprocité quadratique montre que $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$ (car 5 est premier $\equiv 1 \bmod 4$) et $\left(\frac{-11}{p}\right) = \left(\frac{p}{11}\right)$ (car 11 est premier $\equiv 3 \bmod 4$).

(v) Le (i) montre que q est équivalente à $(1,1,14)$, $(2,1,7)$ ou $(4,3,4)$. Mais q représente $p \neq 5$ donc $\varepsilon_5(q) = \left(\frac{p}{5}\right) = -1$. Comme $(1,1,16)$ et $(4,3,4)$ représentent respectivement 1 et 4, qui sont des carrés premiers à 5, on a $\varepsilon_5(1,1,14) = \varepsilon_5(4,3,4) = 1$. La seule possibilité est donc que q est équivalente à $(2,1,7)$. Exemples : $p = 2, 7, 13, 17, \ldots$.

Problème 2. (i) Si $(\pi) \subset (x)$ alors $x | \pi$, donc x est soit une unité, soit associé à π, i.e $(x) = A$ ou $(x) = (\pi)$. Le second point est du cours.

(ii) L'idéal (π) n'est pas premier par π n'est pas premier. Il est non nul et strict car $\pi \neq 0$ et π n'est pas une unité par définition. Par la propriété de Dedekind, il est donc divisible par un produit de deux idéaux premiers P et Q de $\mathcal{O}_K$. En particulier, (π) est inclus dans P, Q et PQ, ces trois idéaux étant distincts de $\mathcal{O}_K$. Comme π n'est pas premier, P et Q ne sont pas principaux d'après le (i). Comme $|\mathrm{Cl}(\mathcal{O}_K)| = 2$, il vient que $[P] = [Q]$ (classe non principale). Mais alors PQ est principal car $[PQ] = [P][Q] = [P]^2 = 1$ dans le groupe $\mathrm{Cl}(\mathcal{O}_K) \simeq \mathbb{Z}/2\mathbb{Z}$. Donc PQ et principal, puis $PQ = (\pi)$ par le (i).

(iii) Il existe une et une seule telle fonction f car tout idéal est produit unique d'idéaux premiers. On peut la définir ainsi. Si $P \in \mathcal{I}$ est premier, posons $e_P = 2$ si P est principal, $e_P = 1$ sinon. Pour $I \in \mathcal{I}$, on pose alors $f(I) = \sum_P v_P(I) e_P$ (où $v_P(I)$, introduit en cours, est la plus grande puissance de P divisant I).

(iv) Soit $\pi \in \mathcal{O}_K$ irréductible. Si π est premier alors $f((\pi)) = 2$ par définition. Sinon, $(\pi) = PQ$ où P et Q sont premiers non principaux d'après le (ii). On a donc encore $f((\pi)) = 1 + 1 = 2$. Ainsi, $f((\pi)) = 2$ pour tout irréductible π de $\mathcal{O}_K$. Il s'ensuit que $f((\pi_1 \cdots \pi_n) = f(\prod_{i=1}^n (\pi_i)) = \sum_{i=1}^n f((\pi_i)) = 2n$ et de même $f((\pi'_1 \cdots \pi'_m)) = 2m$, d'où $2n = 2m$ puis $n = m$.

(v) -31 est sans facteur carré et $\equiv 1 \bmod 4$, donc $\mathcal{O}_K = \mathbb{Z}[\alpha]$ où α est comme dans l'énoncé. Comme $\Pi_{\alpha,\mathbb{Q}} = X^2 + X + 8$, il vient que $\mathrm{disc}(\mathcal{O}_K) = \mathrm{disc}(\Pi_{\alpha,\mathbb{Q}}) = 1 - 32 = -31$.

(vi) $X^2-X+8 \equiv X(X-1) \bmod 2$ (produit de deux polynômes irréductibles unitaires distincts), donc les idéaux de $\mathcal{O}_K$ contenant 2 sont, d'après le cours, les 4 idéaux distincts $(2), D_1 := (2,\alpha), D_2 = (2,\alpha+1)$ et $\mathbb{Z}[\alpha]$. Parmi-ceux là, les idéaux premiers sont ceux correspondants aux facteurs irréductibles, i.e. D_1 et D_2 (qui sont de norme $2^1=2$). De plus, X^2-X+8 est irréductible modulo 3, car on constate par évaluation en 0, 1 et -1 qu'il n'a pas de racine dans $\mathbb{Z}/3\mathbb{Z}$, donc les idéaux de $\mathbb{Z}[\alpha]$ contenant 3 sont $(3) = (3, \Pi_{\alpha,\mathbb{Q}}(\alpha))$ et $\mathbb{Z}[\alpha]$ d'après le cours, seul (3) étant premier. Les idéaux premiers trouvés sont donc exactement D_1, D_2 et (3). De plus, (2), (3) et $\mathbb{Z}[\alpha]$ sont tautologiquement principaux. Mais 2 n'est pas de la forme $x^2+xy+8y^2$ (forme principale de discriminant -31), car 8 n'est pas de la forme $4*(x^2+xy+8y^2) = (2x+y)^2+31y^2$, donc ni D_1 ni D_2 n'est principal (on utilise $\mathrm{N}((z)) = |\mathrm{N}_{K/\mathbb{Q}}(z)| = z\overline{z}$).

(vii) D'après le cours (ou par une vérification directe), $(2) = D_1D_2$. De plus (3) étant premier, sa décomposition est simplement ... $(3) = (3)$! Enfin, $\mathrm{N}(\alpha) = 8$, dont 2 est l'unique facteur premier, donc les seuls facteurs premiers de (α) sont parmi D_1 et D_2. Le premier est effectivement un facteur car $\alpha \in D_1 = (2,\alpha)$ (contenir = diviser). Ce n'est pas le cas du second car $\alpha \in (2, 1+\alpha)$ entraînerait $1 = (1+\alpha)-\alpha \in (2,\alpha+1)$ ce qui est absurde (on sait que $(2,\alpha+1) \neq \mathbb{Z}[\alpha]$, cf. (vi)). Ainsi $(\alpha) = D_1^m$ puis $m=3$ en prenant la norme.

(viii) D'apŗes Minkowski, tout idéal non nul de $\mathcal{O}_K$ est équivalent à un idéal contenant un entier $1 \leq m \leq \frac{2}{\pi}\sqrt{31} < 4$ (par exemple, par la table du cours). D'après le (vi), ces idéaux sont soit principaux, soit équivalents à D_1 ou D_2, ces deux derniers étant non principaux. Comme $D_1D_2 = (2)$, il s'ensuit que $\mathrm{Cl}(\mathcal{O}_K)$ est engendré par $[D_1]$. Comme $D_1^3 = (\alpha)$ est principal d'après (vii), et D_1 n'est pas principal, la classe $[D_1]$ est d'ordre 3.

(ix) Vérifions que $2, \alpha$ est une $\mathbb{Z}$-base (clairement directe) de D_1. Soit $J = 2\mathbb{Z}+\alpha\mathbb{Z}$. On a $J \subset D_1$. De plus, $2\alpha \in J$ et $\alpha^2 = \alpha - 8 \in J$, donc $\alpha J \subset J$. Cela montre que J est un idéal de $\mathcal{O}_K$, puis que $D_1 \subset J$ et $D_1 = J$. Comme D_1 est de norme 2, on a $q_{2,\alpha} = \frac{1}{2}(\mathrm{N}(2)x^2 + \mathrm{Tr}(2\overline{\alpha})xy + \mathrm{N}(\alpha)y^2) = 2x^2+xy+4y^2$. La bijection de Dedekind est donc $[\mathcal{O}_K] \mapsto [(1,1,8)]$, $[D_1] \mapsto [(2,1,4)]$ et $[D_1]^{-1} \mapsto [(2,1,4)]^{\mathrm{opp}} = [(2,-1,4)]$. (Il serait aisé de vérifier que $(1,1,8)$, $(2,1,4)$ et $(2,-1,4)$ sont bien les seules réduites de Gauss de discriminant -31).

(x) Si p est réductible alors $p = uv$ avec $u, v \in \mathcal{O}_K$ non unités, i.e. de norme > 1 d'après le cours, et donc $\mathrm{N}(u) = \mathrm{N}(v) = p$. Vérifions que p n'est pas une norme de $\mathcal{O}_K$. En effet, cela signifie que p est représenté par la forme principale de discriminant -31 (en particulier, -31 est un carré modulo $4p$). Mais ceci est absurde d'après le théorème de Lagrange car p est déjà représenté par la forme $(2,1,4)$, qui n'est pas équivalente à la forme principale (c'est une réduite de Gauss distincte de la forme principale). En revanche, comme $[(2,1,4)]^3 = [(1,1,8)]$ d'après le (ix), donc p^3 est représenté par la forme principale, i.e. $p^3 = \mathrm{N}(\pi) = \pi\overline{\pi}$ pour un certain $\pi \in \mathcal{O}_K$. Un tel π est nécessairement irréductible, car si $\pi = uv$ où u et v ne sont pas des unités, alors soit $\mathrm{N}(u) = p$ soit $\mathrm{N}(v) = p$, qui sont impossible comme on l'a déjà vu. Exemple : $8 = \mathrm{N}(\alpha)$.

(xi) Le (x) montre que l'hypothèse $|\mathrm{Cl}(\mathcal{O}_K)| = 2$ est nécessaire dans le (iv).

Problème 3. (i) Si $I = mJ^2$ alors $\mathrm{N}(I) = \mathrm{N}((m))\mathrm{N}(J)^2 = m^2\mathrm{N}(J)^2$.

(ii) Écrivons $\mathcal{O}_K = \mathbb{Z}[\alpha]$; on dispose d'un α explicite en fonction de d d'après le cours mais ce ne sera pas utile, en revanche on va utiliser que $R := \Pi_{\alpha,\mathbb{Q}}$ est de la forme $X^2+aX+b \in \mathbb{Z}[X]$. Si $\overline{R} = R \bmod p$ admet une racine double dans $\mathbb{Z}/p\mathbb{Z}$, i.e. $\overline{R} = (X-t)^2$ avec $t \in \mathbb{Z}/p\mathbb{Z}$, alors $\mathcal{O}_K$ admet un unique idéal premier P contenant p, à savoir $(p, \alpha - t)$, tel que $\mathrm{N}(P) = p$, et donc $(p) = P^2$ par la propriété de Dedekind. Si $\overline{R}$ admet deux racines distinctes, i.e. $\overline{R} = (X-t)(X-t')$ avec $t \neq t' \in \mathbb{Z}/p\mathbb{Z}$, alors $\mathcal{O}_K$ admet exactement deux idéaux premiers distincts contenant p, à savoir $P = (p, \alpha - t)$ et $Q = (p, \alpha - t')$, tous deux de norme $p^1 = p$, et donc $(p) = PQ$. Dans le dernier cas, $\overline{R}$ est irréductible donc (p) est premier dans $\mathcal{O}_K$ (de norme p^2).

(iii) Si $\mathrm{N}(I) = p^{2n}$, tout idéal premier divisant I est de norme une puissance de p, donc contient p. Si on est dans le cas 1., on a donc $I = P^a$, puis $p^{2n} = \mathrm{N}(P)^a = p^a$ et donc $a = 2n$. Dans ce cas I est le carré de P^n. Dans le cas 2., on a donc $I = P^aQ^b$ pour $a, b \geq 0$. Quitte a échanger les rôles de P et Q supposons $a \leq b$. Comme $(p) = PQ$, on peut aussi écrire $I = (p^a)Q^{b-a}$, puis en prenant les normes $p^{2n} = p^{2a+b-a}$. Il s'ensuit que $b-a$ est pair, et donc $I = (p^a)(Q^{(b-a)/2})^2$. Enfin dans le cas 3., $I = (p)^n = (p^n)$.

(iv) Supposons que $\mathrm{N}(I)$ est un carré. Écrivons $\mathrm{N}(I) = \prod_{i=1}^n p_i^{\alpha_i}$ où les p_i sont premiers et distincts. Par multiplicativité de la norme et le fait que les idéaux premiers sont de norme une puissance d'un nombre premier, la propriété de Dedekind permet d'écrire $I = I_1I_2\cdots I_n$ où $\mathrm{N}(I_i) = p_i^{\alpha_i}$. Si

$\mathrm{N}(I)$ est un carré, alors α_i est pair pour tout i, donc I_i est de la forme $m_i J_i^2$ pour tout i par le (iii), et donc $I = (\prod_i m_i)(\prod_i J_i)^2$.

(v) Si $x \in I$ est non nul alors I divise (x) (contenir = diviser), i.e. il existe un idéal J tel que $(x) = IJ$. En prenant la norme il vient que $\mathrm{N}(J) = |\mathrm{N}_{K/\mathbb{Q}}(x)|/\mathrm{N}(I)$ est un entier. Si c'est un carré, alors $\mathrm{N}(J)$ est un carré, et en particulier $[J]$ un carré dans $\mathrm{Cl}(\mathcal{O}_K)$ d'après le (iv). On conclut car $[I] = [J]^{-1}$.

(vi) C'est la caractérisation du cours des discriminants fondamentaux combinée à la description de l'anneau des entiers de $\mathbb{Q}(\sqrt{D})$.

(vii) (3) Si $[q]$ est un carré dans $\mathrm{P}(D)$, disons $[q] = [q']^2$, alors q représente le carré de tout entier représenté par q', car q est une composée de q' par elle-même. Réciproquement, si q représente un carré m^2, et si $I \in \mathrm{Pic}(A_D) = \mathrm{Cl}(A_D)$ est un idéal dont la classe correspond à $[q]$ par le théorème de Dedekind, alors il existe $x \in I$ tel que $m^2 = \frac{\mathrm{N}(x)}{\mathrm{N}(I)}$ par définition. Le (v) assure que $[I]$ est un carré dans $\mathrm{Pic}(A_D)$ et donc $[q]$ est un carré dans $\mathrm{P}(D)$.

12. Corrigé de l'examen 2014-2015

Problème 1. (i) $-p$ est sans facteur carré et $\equiv 3 \bmod 4$, on conclut par la proposition 5.22.

(ii) Si $P = \Pi_{\sqrt{-p},\mathbb{Q}}$ alors $P = X^2 + p$. De plus $P \equiv (X+1)^2 \bmod 2$; la proposition 6.11 montre que Q est de norme 2. Le théorème 7.17, qui s'applique par le (i), montre que $(2) = Q^2$.

(iii) Supposons $D = (z)$ avec $z \in A$. Alors $\mathrm{N}(D) = z\overline{z}$ (proposition 4.12.3). Écrivons $z = a + b\sqrt{-p}$ avec $a, b \in \mathbb{Z}$. Le (ii) entraîne $2 = a^2 + pb^2$, puis $b = 0$ (car $p > 2$) : absurde.

(iv) D'après le (i), $\mathrm{Cl}(A)$ est un groupe. D'après (ii) et (iii), $[D]$ est d'ordre 2 dans $\mathrm{Cl}(A)$. On conclut par Lagrange.

(v) Soit $J \subset D$ le sous-groupe engendré par 2 et $\alpha = 1 + \sqrt{-p}$. Comme $1, \alpha - 1$ est une $\mathbb{Z}$-base de A, il en va de même de $1, \alpha$, ce qui montre que $|A/J| = 2$. Comme d'autre part $|A/D| = 2$ d'après le (ii), on a $J = D$. On constate que $1, \alpha$ est une $\mathbb{R}$-base directe de $\mathbb{C}$ (comme dans le cours, on prend la convention que $\sqrt{-p} = i\sqrt{p}$). Ainsi,

$$\mathrm{q}_{1,\alpha}(x,y) := \frac{1}{2}\mathrm{N}(2x + \alpha y) = \frac{1}{2}((2x+y)^2 + py^2) = 2x^2 + 2xy + \frac{p+1}{2}y^2.$$

La forme $(2, 2, \frac{p+1}{2})$ est réduite au sens de Gauss car $\frac{p+1}{2} > 2$ si $p \equiv 1 \bmod 4$.

(vi) Soit (a,b,c) une réduite de Gauss de discriminant $-4p$, i.e. $b^2 - 4ac = -4p$. En particulier, $b = 2b'$ est pair et $b'^2 - ac = -p$. D'après le théorème 3.29 (i), (a,b,c) est ambiguë si et seulement si on a $b = 0$, ou $a = b$, ou $a = c$.

Si $b = 0$, alors $ac = p$. Comme p est premier, le seul cas possible est $(1, 0, p)$ (forme principale). Si $b = a$ $(= 2b')$, alors $b'(2c - b') = p$, les deux cas $b' = 1, p$ conduisent aux deux possibilités $(2, 2, \frac{p+1}{2})$, $(2p, 2p, \frac{p+1}{2})$, seule la première étant réduite. Si $a = c$, alors $(a - b')(a + b') = p$ (avec $a - b' \geq 0$). La seule possibilité est $a - b' = 1$ et $a + b' = p$, i.e. $(a,b,c) = (\frac{p+1}{2}, p-1, \frac{p+1}{2})$, qui n'est pas réduite car $p > 3$.

(vii) On a $A = A_{-4p}$ avec la notation du cours. La bijection de Dedekind $\mathrm{Cl}(A) \xrightarrow{\sim} \mathrm{Cl}(-4p) = \mathrm{P}(-4p)$ (la denière égalité vient du (i)) fait correspondre éléments de carré 1 et classes ambiguës (Lemme 8.19), et envoie $[A]$ et $[D]$ sur $[(1,0,p)]$ et $[(2, 2, \frac{p+1}{2})]$ (cours + question (v)). On conclut par le (vi).

(viii) G étant abélien, l'application $g \mapsto g^2$ est un morphisme de groupes $G \to G$ de noyau $\langle z \rangle$ et d'image $\mathcal{C}(G)$. Ainsi $|\mathcal{C}(G)| = |G|/|\langle z \rangle| = |G|/2$. Si $z = g^2$ alors g est d'ordre 4 et donc $|G| \equiv 0 \bmod 4$ (Lagrange). Réciproquement, si $|G| \equiv 0 \bmod 4$ alors $|\mathcal{C}(G)| = |G|/2$ est pair et donc $\mathcal{C}(G)$ possède un élément d'ordre 2 (Cauchy), nécessairement égal à z.

(ix) $(2, 2, \frac{p+1}{2})$ représente 2 qui est premier à p, donc $\varepsilon_p((2, 2, \frac{p+1}{2})) = \left(\frac{2}{p}\right)$.

(x) Si $|\mathrm{Cl}(A)| \equiv 0 \bmod 4$, alors $[D]$ est un carré dans $\mathrm{Cl}(A)$ (question (viii), ou ce qui revient au même $[(2, 2, \frac{p+1}{2})]$ est un carré dans $\mathrm{P}(-4p)$. Comme ε_p est un morphisme de groupes, cela entraîne $\varepsilon_p(2, 2, \frac{p+1}{2}) = 1$. I.e. $p \equiv \pm 1 \bmod 8$ d'après le (ix) et la loi supplémentaire. Comme $p \equiv 1 \bmod 4$, on a même $p \equiv 1 \bmod 8$.

(xi) Comme $p > 2$ il existe au moins un entier $m \in \mathbb{Z}$ tel que m n'est pas un carré modulo p (en particulier m est premier à p). Par le lemme chinois des restes, il existe un entier a tel que $a \equiv 3 \bmod 4$ et $a \equiv m \bmod p$. En particulier, a est premier à $b := 4p$. Par le théorème de la progression arithmétique de Dirichlet, il existe un premier ℓ tel que $\ell \equiv a \bmod b$, il convient.

(xii) Soit ℓ comme au (xii). Montrons qu'il existe une forme de discriminant $-4p$ qui représente ℓ. Par Lagrange, il faut voir que $-4p$ est un carré modulo 4ℓ, i.e. modulo 4 et modulo ℓ car ℓ est impair. Il est évident que $-4p$ est un carré mod 4 (c'est 0). De plus, en utilisant la loi quadratique et le symbole de -1 (ℓ et p sont impairs) on a

$$\left(\frac{-4p}{\ell}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{\ell}\right) = (-1) \times (-1) = 1$$

la seconde égalité découlant du (xi). D'après Lagrange, il existe une forme q de discriminant $-4p$ qui représente ℓ. En particulier, $\varepsilon_p(q) = \left(\frac{\ell}{p}\right) = -1$.

(xiii) Le (xii) montre que le morphisme ε_p est surjectif. Son noyau est donc de cardinal $|\mathrm{P}(-4p)|/2$, et contient évidemment $\mathcal{C}(\mathrm{P}(-4p))$. On conclut car ce dernier est de cardinal $|\mathrm{P}(-4p)|/2$ d'après le (vii) et le (viii).

(xiv) On a déjà vu que $\mathrm{Cl}(A) \equiv 0 \bmod 4$ si et seulement si $(2,2,\frac{p+1}{2})$ est un carré dans $\mathrm{P}(-4p)$. D'après le (xiii), il est équivalent de demander $\varepsilon_p(2,2,\frac{p+1}{2}) = 1$, i.e. $p \equiv 1 \bmod 8$ d'après le (ix).

PROBLÈME 2. (i) $x \mapsto P(x)$ est strictement croissante sur $\mathbb{R}$ car $P'(X) = 3X^2 + d$ ne s'annule pas ($d > 0$). On a $P(-1/d) = (-1/d)^3 < 0$ et $P(-1/d + 1/d^2) = \frac{(1-d)^3+d^5}{d^6} > 0$. Le (i) se déduit du théorème des valeurs intermédiaires.

(ii) L'assertion $-\mathrm{disc}\, P = 4d^3 + 27$ suit du formulaire du Chap. 5 §2. Comme P est de degré 3, il est irréductible dans $\mathbb{Q}[X]$ si et seulement si il admet une racine rationelle. Comme il est unitaire à coefficients entiers, une telle racine serait nécessairement dans $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$. Cela contredit le (i) car $-1 < \alpha < 0$.

(iii) D'après (ii), $\Pi_{\alpha,\mathbb{Q}} = P$ et donc $[K : \mathbb{Q}] = \deg P = 3$. D'après le cours, $\sigma \mapsto \sigma(\alpha)$ induit une bijection entre $\Sigma(K)$ et les plongements de K, de sorte que r_1 est le nombre de racines réelles de P, i.e. 1, et $r_2 = ([K : \mathbb{Q}] - r_1)/2 = 1$ également.

L'existence de σ suit de l'explication précédente : soit $\beta \neq \alpha$ une racine de P, non dans $\mathbb{R}$ d'après (i), l'unique $\sigma \in \Sigma(K)$ tel que $\sigma(\alpha) = \beta$ convient. La racine restante de P est $\overline{\beta}$. Ainsi, $\Sigma(K) = \{\mathrm{id}, \sigma, \overline{\sigma}\}$.

(iv) La question (iii) montre que $\mathrm{N}_{K/\mathbb{Q}}(x) = x\sigma(x)\overline{\sigma(x)} = x|\sigma(x)|^2$. Si x est dans $\mathcal{O}_K$, alors $\chi_{x,K/\mathbb{Q}} = X^3 + aX^2 + bX + c$ avec $c = -\mathrm{N}_{K/\mathbb{Q}}(x)$ et $a, b, c \in \mathbb{Z}$ (théorème 5.20). L'équation $\chi_{x,K/\mathbb{Q}}(x) = 0$ s'écrit donc aussi

$$x(x^2 + ax + b - |\sigma(x)|^2) = 0.$$

Si $x = 0$ il n'y a rien à démontrer, et sinon on en tire $|\sigma(x)|^2 = x^2 + ax + b \in \mathbb{Z}[x]$.

(v) A^1 est un sous-groupe de $A^\times$ car $\mathbb{R}_{>0}$ est un sous-groupe de $\mathbb{R}^\times$. On a $\alpha(\alpha^2 + d) = -1 \in A^\times$, et $\alpha^2 + d \in A$, donc $\alpha \in A^\times$. On conclut car $\alpha < 0$ par le (i).

(vi) Si $x \in A$ satisfait $x|\sigma(x)|^2 = 1$ alors $x > 0$ et $x \in A^*$ car $|\sigma(x)|^2 \in A$ (question (v)), donc $x \in A^1$. Réciproquement, si $x \in A^1$ alors il existe $y \in A$ tel que $xy = 1$. En appliquant la multiplicativité de la norme de $K/\mathbb{Q}$, et le fait que $\mathrm{N}_{K/\mathbb{Q}}(A) \subset \mathbb{Z}$, il vient que $\mathrm{N}_{K/\mathbb{Q}}(x) \in \mathbb{Z}^\times = \{\pm 1\}$. On conclut car $\mathrm{N}_{K/\mathbb{Q}}(x) = x|\sigma(x)|^2 > 0$.

(vii) Soit $x \in A^1$. Si $\frac{1}{\rho} \leq x \leq \rho$ alors $|\sigma(x)| = 1/\sqrt{x}$ d'après le (vi), il vérifie donc $\frac{1}{\sqrt{\rho}} \leq |\sigma(x)| \leq \sqrt{\rho}$. D'après le (iii), on constate donc que $|\tau(x)| \leq \rho$ pour tout $\tau \in \Sigma(K)$. On applique la prop. 5.14.(iii) : les relations coefficients racines montrent que les coefficients du polynôme $\chi_{x,K/\mathbb{Q}}$ sont tous $\leq$ à un réel $\mathrm{C}(\rho)$ qui ne dépend que de ρ (et non de x) ; on peut prendre $\mathrm{C}(\rho) = 3\rho^3$. Ces coefficients sont de plus entiers car $x \in \mathcal{O}_K$. Ainsi, à $\rho > 1$ fixé l'ensemble des $\chi_{x,K/\mathbb{Q}}$, avec $x \in A^1$ tel que $\frac{1}{\rho} \leq x \leq \rho$, est fini, ainsi donc que l'ensemble des tels x car un polynôme n'a qu'un nombre fini de racines.

(viii) Le logarithme $\log : \mathbb{R}_{>0} \to \mathbb{R}$ est un isomorphisme de groupes, donc $\log A^1$ est un sous-groupe de $\mathbb{R}$. Soit $r > 0$, l'ensemble $\{x \in A^1, |\log x| < r\} = \{x \in A^1, e^{-r} < x < e^r\}$ est fini par le (vii), donc $\log A^1$ est discret dans $\mathbb{R}$. Enfin, $-\alpha \in A^1$ d'après (v) et $-\alpha < 1$ d'après le (i), donc $\log A^1$ est non réduit à 0 : c'est un réseau.

(ix) Le (viii) montre que $\log A^1 = \mathbb{Z}\log\varepsilon$ pour un unique $\varepsilon \in A^1$ tel que $\varepsilon > 1$. En prenant l'exponentielle, on en déduit que A^1 est le groupe monogène infini engendré par ε (isomorphe à $\mathbb{Z}$). On conclut car l'application $\{\pm 1\} \times A^1 \to A^\times, (u, x) \mapsto ux$, est un isomorphisme de groupes.

(x) Comme $-\alpha^{-1} \in A^1$ il existe un unique entier $n \in \mathbb{Z}$ tel que $-\alpha^{-1} = \varepsilon^n$, d'après le (ix). Mais $-\alpha < 1$, donc $-1/\alpha > 1$, et donc $n > 1$. Il est évident que $\mathbb{Z}[\varepsilon] \subset \mathbb{Z}[\alpha]$. Comme $\varepsilon^{-1} = |\sigma(\varepsilon)|^2 \in \mathbb{Z}[\varepsilon]$ (question (iv)), on a aussi $\mathbb{Z}[\alpha] \subset \mathbb{Z}[\varepsilon]$.

(xi) De même (c'est seulement plus simple), $\mathbb{Q}(\alpha) = \mathbb{Q}(\varepsilon)$. Soit $Q = \chi_{\varepsilon,K/\mathbb{Q}}$. Alors $Q \in \mathbb{R}[X]$ est unitaire. Il vérifie $Q(0) = -\varepsilon|\sigma(\varepsilon)|^2 = -1$ (question (vi)). Comme $K = \mathbb{Q}(\varepsilon)$ le fait que $r_1 = 1$ (prouvé au (iii)) montre que ε a un $\mathbb{Q}$-conjugué réel (lui-même) et deux autres non réels : $\sigma(\varepsilon)$ et $\overline{\sigma(\varepsilon)}$. Comme $K = \mathbb{Q}(\varepsilon)$ on a aussi $Q = \Pi_{\varepsilon,\mathbb{Q}}$. Ainsi, $\mathrm{disc}\, Q = \mathrm{disc}\, \mathbb{Z}[\varepsilon] = \mathrm{disc}\, A = \mathrm{disc} P$.

(xii) L'inégalité d'Artin montre que $4d^3+27 = |\mathrm{disc}P| = |\mathrm{disc}Q| < 4(-\alpha^{-3})^{1/n}+24$. En particulier, $(-\alpha^{-1})^{1/n} > d$. Mais $\alpha < (1-d)/d^2$ d'après le (i), donc $-1/\alpha < \frac{d^2}{d-1}$ si $d>1$. On conclut par passage aux log. Pour une démonstration de l'inégalité d'Artin, voir par exemple le livre *Algebraic number theory*, A. Fröhlich & M. J. Taylor, Cambridge adv. math. studies 27, Chap. V, §3, fomrule (3.2).

(xiii) Il suffit de voir que $\log(\frac{d^2}{d-1}) < 2\log(d)$, soit encore $\frac{d^2}{d-1} < d^2$ pour $d>1$, ce qui est évident. Cela montre $n=1$, puis que $\varepsilon = -\alpha^{-1}$. On conclut par (ix) et (v).

Observer que si $d=1$ alors $P(-2/3) = 1-\frac{26}{27} > 0$ donc $\alpha < -2/3$, puis $-\alpha^{-1} < 3/2$. L'inégalité d'Artin montre plus précisément que $4\,(-\alpha^{-1})^{3/n}+24 > |\mathrm{disc}(P)| = 31$, i.e. $(-\alpha^{-3})^{1/n} > 7/4$. Ainsi, $n < 3\frac{\log 3/2}{\log 7/4}$. Un petit calcul montre alors que $n=1$ ou 2. Cependant, on peut montrer que dans ce cas par un argument de congruences modulo 13 que $-\alpha$ n'est pas un carré dans $\mathbb{Z}[\alpha]$, et conclure également $n=1$ dans ce cas.

(xiv) C'est la proposition-définition 6.15 : pour tout $x \in \overline{\mathbb{Z}}$, $\mathbb{Z}[x]$ contient une $\mathbb{Q}$-base de $L=\mathbb{Q}(x)$ et donc $\mathrm{disc}\ \mathbb{Z}[x] = |\mathcal{O}_K/\mathbb{Z}[x]|\mathrm{disc}\ \mathbb{Z}[x]$. On a $\mathrm{disc}\ A = \mathrm{disc}\ P = -4^4-27 = -283$. Mais 283 est sans facteur carré (c'est un nombre premier, cf l'annexe). Comme $|\mathcal{O}_K/A|$ est un entier ≥ 1, c'est 1, i.e. $\mathcal{O}_K = A$.

(xv) On rappelle que $r_2=1$ et $\mathrm{disc}\ A = -283$. D'après Minkowski, tout idéal non nul de A est équivalent à un idéal de A contenant un entier n tel que $1 \leq n \leq (4/\pi)3!/3^2\sqrt{283} < 5$ d'après l'énoncé. On conclut car "contenir c'est diviser", puisque A est égal à $\mathcal{O}_K$ par le (xiv).

(xvi) On applique le théorème 7.17 (car $A=\mathcal{O}_K$) et la prop. 6.11. On conclut car $X^3+4X+1 \equiv (X-1)(X^2+X+1) \bmod 2$ (décomposition en irréductibles dans $\mathbb{Z}/2[X]$) et $X^3+4X+1 \equiv (X-1)(X^2+X-1) \bmod 3$ (idem). Ainsi, $D_1=(2,\alpha-1)$, $D_2=(2,\alpha^2+\alpha+1)$, $T_1=(3,\alpha-1)$ et $T_2=(3,\alpha^2+2\alpha-1)$.

(xvii) On rappelle que si Q est un idéal premier de $\mathcal{O}_K$ alors $\mathrm{N}(Q)$ est une puissance de l'unique nombre premier p appartenant à Q (thm. 7.16 (ii)). Comme contenir = diviser, on a de plus $p \in Q$ si et seulement si Q divise (p). On conclut par le (xvi).

(xviii) Si $m \in \mathbb{Q}$, alors

$$\mathrm{N}_{K/\mathbb{Q}}(m-\alpha) = (m-\alpha)(m-\sigma(\alpha))(m-\overline{\sigma(\alpha)}) = P(m).$$

On a donc $\mathrm{N}_{K/\mathbb{Q}}(1+\alpha) = -P(-1) = 4$ et $\mathrm{N}_{K/\mathbb{Q}}(1-\alpha) = P(1) = 6$. En particulier, les facteurs premiers de $(1+\alpha)$ et $(1-\alpha)$ sont parmi $\{D_1, D_2, T_1, T_2\}$. Par multiplicativité de la norme, la seule possibilité pour $(1-\alpha)$ est donc $(1-\alpha) = D_1T_1$. De même, les deux possibilités pour $(1+\alpha)$ sont D_1^2 et D_2. Mais $1+\alpha = 1-\alpha+2 \in D_1$, donc D_1 divise $(1+\alpha)$. Ainsi, $(1+\alpha) = D_1^2$.

(xix) D'après la question (xv), tout idéal non nul de A est équivalent à un idéal divisant (1), (2), (3) ou $(2)^2$. Comme $A=\mathcal{O}_K$, un tel idéal est donc un produit (éventuellement vide) d'idéaux parmi $\{D_1, D_2, T_1, T_2\}$. Ainsi, le groupe $\mathrm{Cl}(A)$ est engendré par les classes de ces 4 idéaux premiers. Mais $[D_1][D_2] = [T_1][T_2] = 1$ d'après le (xvi), et $[D_1][T_1] = 1$ d'après le (xviii). Donc le groupe $\mathrm{Cl}(A)$ est engendré par $[D_1]$, qui est de carré 1 par la relation $D_1^2 = (1+\alpha)$.

(xx) On observe que 2 est une racine de $P = X^3+4X+1$ modulo 17. Ainsi, le morphisme d'anneaux $\mathbb{Z}[X] \to \mathbb{Z}/17$, $P(X) \mapsto P(2) \bmod 17$, est nul sur l'élément X^3+4X+1, il se factorise donc en un morphisme d'anneaux $\mathbb{Z}[X]/(P) \to \mathbb{Z}/17$. Mais P est le polynôme minimal de α (question (ii)) et donc $\mathbb{Z}[X]/(P)$ est naturellement isomorphe à $\mathbb{Z}[\alpha]$ d'après le cours.

(xix) $\varphi(-1) = -1$ est un carré non nul dans $\mathbb{Z}/17\mathbb{Z}$ car $17 \equiv 1 \bmod 4$. $\varphi(\alpha) = 2$ est également un carré non nul modulo 17 car $17 \equiv 1 \bmod 8$. Comme $A^\times = \langle -1, \alpha\rangle$, $\varphi(A^\times)$ est inclus dans le groupe des carrés de $(\mathbb{Z}/17)^\times$. Mais $\varphi(1+\alpha) = 3$ et $\left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = \left(\frac{-1}{3}\right) = -1$, ce qui conclut.

(xxii) Si $D_1 = (z)$ avec $z \in A$ alors $D_1^2 = (z^2) = (1+\alpha)$, donc $z^2 = (1+\alpha)x$ avec $x \in A^\times$. En particulier, $\varphi((1+\alpha)x) = \varphi(z)^2$ est un carré : absurde. Ainsi, D_1 n'est pas principal, et $\mathrm{Cl}(A) \simeq \mathbb{Z}/2\mathbb{Z}$.

13. Corrigé de l'examen 2015-2016

Problème 1. (i) D'après Gauss, il suffit de déterminer les formes réduites (a,b,c) de discriminant $D=-127$. On a $|b|\leq a\leq \sqrt{127/3}<7$ et $b\equiv 1 \bmod 2$, donc b vaut $\pm 1,\pm 3,\pm 5$. On applique l'algorithme du cours : $(b^2-D)/4=ac$ vaut respectivement $32,34,38$. Les deux derniers cas ne conduisent à aucune forme réduite ($|b|\leq a\leq c$), et le cas $b=\pm 1$ donne les formes $(1,1,32)$, $(2,\pm 1,16)$, $(4,\pm 1,8)$. Ainsi, $\mathrm{Cl}(-127)$ a exactement 5 éléments, représentés par ces 5 formes.

(ii) L'anneau A est l'anneau A_{-127} du cours car $-127\equiv 1 \bmod 4$. Comme 127 est premier (Annexe B !), donc sans facteur carré, c'est aussi l'anneau des entiers de $\mathbb{Q}(\sqrt{-127})$. Ainsi, on sait que $\mathrm{Cl}(A)$ est un groupe. D'après Dedekind, on a $|\mathrm{Cl}(A)|=|\mathrm{Cl}(-127)|$, qui vaut 5 par le (i). Mais un groupe d'ordre premier p est isomorphe à $\mathbb{Z}/p\mathbb{Z}$, car un élément distinct de 1 est nécessairement d'ordre p d'après Lagrange.

(iii) On a $\Pi_{\alpha,\mathbb{Q}}=X^2-X+32$, donc $\mathrm{disc}A=\mathrm{disc}\,(X^2-X+32)=-127$ (et en général, $\mathrm{disc}\,A_D=D$). D'après Minkowski, tout idéal non nul de A est équivalent à un idéal contenant un entier $N\leq 1$ tel que $N\leq \frac{4}{\pi}\cdot\frac{1}{2}\cdot\sqrt{127}<8$. En effet, le corps $K=\mathbb{Q}(\alpha)$ et de degré 2 et n'a pas de plongement réel.

(iv) On a déjà justifié au (ii) le fait que A est l'anneau des entiers de $\mathbb{Q}(\alpha)$, et donc que $\mathrm{Cl}(A)$ est un groupe. D'après le (iii), tout idéal de A est équivalent à un idéal contenant, un idéal (N) avec $1\leq N\leq 7$. Comme un tel idéal est produit d'idéaux premiers ayant la même propriété (par la propriété de Dedekind de $A=\mathcal{O}_{\mathbb{Q}(\alpha)}$), le groupe $\mathrm{Cl}(A)$ est a fortiori engendré par les classes des idéaux premiers P de A contenant un entier ≤ 7, et donc un nombre premier $p\leq 7$.

(v) Le polynôme X^2-X+32 est congru à $X(X-1)$ modulo 2. D'après le cours (Prop. 6.11), les idéaux de $A=\mathbb{Z}[\alpha]$ contenant 2 sont donc les quatre idéaux $A, 2A, (2,\alpha)$ et $(2,\alpha-1)$. Parmi ceux-là, les idéaux premiers sont (disons) $I:=(2,\alpha)$ et $J:=(2,\alpha-1)$ (les $\mathrm{I}(Q)$ avec Q facteur irréductible unitaire de $X(X-1)$, cf l'exemple suivant la définition 7.7) et sont de norme $2^1=2$. Comme A est l'anneau des entiers de $\mathbb{Q}(\alpha)$ (cf (ii)), un théorème du cours montre que l'on a $(2)=IJ$ (Thm. 7.17). Pour voir que ni I, ni J, n'est principal, il suffit de voir que A n'admet aucun idéal principal de norme 2, i.e. aucun élément de norme 2 (car $\mathrm{N}(z)=\mathrm{N}((z))$. Mais si $x,y\in\mathbb{Z}$ on a $\mathrm{N}(x+y\alpha)=x^2+xy+32y^2$ (forme principale de discriminant -127). Elle ne représente pas 2, car $4(x^2+xy+32y^2)=(2x+y)^2+127y^2$ ne représente pas 8.

(vi) Observons que la réduction modulo p du polynôme $\Pi_{\alpha,\mathbb{Q}}=X^2-X+32$ est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$ pour $p=3,5,7$. Il suffit de voir que dans chacun des cas, il n'a pas de racine dans $\mathbb{Z}/p\mathbb{Z}$. D'après la relation $4(X^2-X+32)=(2X-1)^2+127$, et $p>2$, il est équivalent de voir que -127 n'est pas un carré modulo p. Mais $-127=2 \bmod 3$ (non carré), $-127\equiv -2 \bmod 5$ (non carré), et $-127\equiv -1 \bmod 7$ (non carré car $7\equiv 3 \bmod 4$). Ainsi, pour ces 3 valeurs de p, l'idéal $(p)=\mathrm{I}(X^2-X+32)$ est premier d'après la proposition 6.11 (et l'exemple suivant la définition 7.7).

(vii) Soit P un idéal premier de A contenant un nombre premier p, ou ce qui revient au même divisant (p), avec $p\leq 7$. Si $p\neq 2$, alors $P=(p)$ d'après le (v). Un tel P est donc principal. D'autre part, si $p=2$ on a $P=I$ ou $P=J$ d'après le (v), ainsi que $IJ=(2)$. Cette dernière relation montrer que $[I]=[J]^{-1}$ dans $\mathrm{Cl}(A)$. D'après la question (iv), $\mathrm{Cl}(A)$ est donc engendré par $[I]$ (et aussi par $[J]$).

(viii) L'équation $\alpha(1-\alpha)=\mathrm{N}(\alpha)=2^5$ montre que l'idéal (α) est de norme 2^5. En particulier, d'après la propriété de Dedekind et le (iv), ses facteurs premiers sont parmi $\{I,J\}$. On a clairement $\alpha\in I$. Si $\alpha\in J$, alors $1=\alpha-(\alpha-1)\in J$, ce qui est absurde car $J\neq A$ (il est de norme 2). Donc $\alpha\notin J$, i.e. J ne divise pas (α). La seule possibilité est donc $(\alpha)=I^5$. En particulier, $[I]^5=1$ dans $\mathrm{Cl}(A)$. L'ordre de $[I]$ est donc 1 ou 5. Ce n'est pas 1 car I est non principal (question (iv)).

Problème 2. (i) Par hypothèses, D est sans facteur carré et $\equiv 1 \bmod 4$, donc $\mathcal{O}_K=A_D$ d'après le cours (Prop. 5.22).

(ii) On a $\overline{\alpha}=1-\alpha$, et donc $\overline{I}=(\overline{\alpha})=(1-\alpha)$. Ainsi, $1=\alpha+1-\alpha\in I+\overline{I}$, d'où l'énoncé.

(iii) On a $\alpha\overline{\alpha}=\alpha(1-\alpha)=n^g$, et donc $I\overline{I}=(\alpha)(1-\alpha)=(\alpha(1-\alpha))=(n^g)=(n)^g$. Comme les idéaux I et $\overline{I}$ n'ont pas de facteurs premier commun (ou ce qui revient au même, ne sont pas inclus dans un même idéal premier) d'après le (x), la propriété de factorisation unique des idéaux montre que I (et $\overline{I}$) est la puissance g-ème d'un (unique) idéal, on le note J.

(iv) Si $\overline{J}^m = \overline{\mathrm{J}^m}$, alors en élevant à la puissance g on a $I^m = \overline{I}^m$, ce qui est absurde car I et $\overline{I}$ sont premiers entre eux par le (ii). Si $J^m = (x)$ avec $x \in \mathbb{Z}$, alors $\overline{x} = x$ et donc on a les égalités $\overline{J}^m = \overline{J^m} = \overline{(x)} = (x) = J^m$: on est ramené au cas précédent.

(v) La forme principale de discriminant D est $q(x,y) = x^2 + xy + n^g y^2$. En particulier on a $4\,q(x,y) = (2x+y)^2 + (4\,n^g - 1)y^2$. Ainsi, si on a $(x,y) \in \mathbb{Z}^2$ et $q(x,y) = n^m$ avec $y \neq 0$, on a l'inégalité $4n^g - 1 \leq 4n^m$, i.e. $n^g \leq n^m$ car $n, g \geq 1$, et donc $m \geq g$.

(vi) Soit $m \geq 1$ l'ordre de $[J]$ dans $\mathrm{Cl}(A)$. La relation $J^g = I = (\alpha)$, i.e. $[J]^g = 1$, montre m divise g. De plus, il existe $z \in A$ tel que $J^m = (z)$. En particulier, on a $\mathrm{N}(J)^m = \mathrm{N}(z)$. La relation $J^g = (\alpha)$ montre que $\mathrm{N}(J)^g = n^g$, i.e. $\mathrm{N}(J) = n$. Écrivons $z = x + y\alpha$ avec $x, y \in \mathbb{Z}$. On a $\mathrm{N}(z) = n^m$, ou ce qui revient au même $q(x,y) = n^m$ (avec q principale de discriminant D). Le (v) montre que $y = 0$ ou $m \geq g$ (et donc $m = g$). Mais si $y = 0$ on a $J^m = (x)$, ce qui est absurde par le (iv).

(vii) On a déjà vu $\mathrm{N}(J) = n$, i.e. J est d'indice n dans A. Le théorème de Lagrange montre alors $n \in J$. Soit $J' \subset J$ le sous-groupe $\mathbb{Z}n + \mathbb{Z}\alpha$. Comme $1, \alpha$ est une $\mathbb{Z}$-base de A, J' est un sous-groupe d'indice n dans A, donc d'indice 1 dans J, i.e. $J = J'$.

(viii) n, α est une $\mathbb{Z}$-base de l'idéal J d'après la question précédente, manifestement directe relativement à la $\mathbb{R}$-base $1, \alpha$ de $\mathbb{C}$. Calculons la forme binaire associée à cette base par Dedekind. On a $q_{n,\alpha}(x,y) = \frac{1}{n}(n^2x^2 + nxy + n^g y^2) = nx^2 + xy + n^{g-1}y^2$. Ainsi, l'isomorphisme de groupes $\mathrm{P}(D) \xrightarrow{\sim} \mathrm{Cl}(A)$ fait correspondre la classe d'équivalence propre de $(n, 1, n^{g-1})$ avec la classe de l'idéal J. On conclut par la question (vi).

(ix) On a $-2047 = 1 - 2 \cdot 2^9 = -23 \cdot 89$ sans facteur carré, donc on est dans le cas particulier $n = 2$ et $g = 9$. Le groupe $\mathrm{P}(-2047)$ admet un élément d'ordre 9 d'après le (viii). La classe de la forme réduire ambiguë $(23, 23, 28)$ (non principale), qui est bien de discriminant -2047 par la donnée de l'énoncé, est d'ordre 2 d'après le cours. On conclut car si un groupe abélien G possède un élément a d'ordre m et un élément b d'ordre n premier à n, l'élément ab est d'ordre mn (Lemme 1.30).

Pour la question bonus, on observe que d'après le cours, le sous-groupe $V = 23\mathbb{Z} + \frac{23+\sqrt{D}}{2}\mathbb{Z} = 23\mathbb{Z} + (\alpha + 11)\mathbb{Z}$ est un idéal de A dont la classe correspond à la classe d'équivalence propre de $(23, 23, 28)$. Il s'agit de déterminer la classe de formes associées à l'idéal VJ (où $J = \mathbb{Z}2 + \mathbb{Z}\alpha$). Mais VJ est engendré $\mathbb{Z}$-linéairement par $46, 23\alpha, 2(\alpha+11), \alpha(\alpha+11) = 12\alpha - 512$. Une petite analyse montre que $VJ = \mathbb{Z}46 + \mathbb{Z}(\alpha - 12)$. La forme associée à la base $46, \alpha - 12$ convient : on trouve $(46, -23, 14)$. On a les équivalences propres $(46, -23, 14) \overset{+}{\sim} (14, 23, 46) \overset{+}{\sim} (14, -5, 37)$ (cette dernière est réduite).

Problème 3. (i) On rappelle que d'après le cours, si $x \in A$ alors $\mathrm{N}_{K/\mathbb{Q}}(x) \in \mathbb{Z}$. Si $x \in A^\times$ il existe $y \in A$ tel que $xy = 1$, puis par multiplicativité de $\mathrm{N}_{K/\mathbb{Q}}$: $1 = \mathrm{N}_{K/\mathbb{Q}}(1) = \mathrm{N}_{K/\mathbb{Q}}(xy) = \mathrm{N}_{K/\mathbb{Q}}(x)\mathrm{N}_{K/\mathbb{Q}}(y)$, et donc $\mathrm{N}_{K/\mathbb{Q}}(x) \in \mathbb{Z}^\times = \{\pm 1\}$. Réciproquement, si $x \in A$ vérifie $\mathrm{N}_{K/\mathbb{Q}}(x) = \pm 1$, on sait qu'il existe un polynôme unitaire P dans $\mathbb{Z}[X]$ tel que $P(x) = 0$ et $P(0) = \mathrm{N}_{K/\mathbb{Q}}(x)$: par exemple, $P = \chi_{x,K/\mathbb{Q}}$ convient d'après le cours. On écrit $P = QX \pm 1$. On en tire $\pm 1 = Q(x)x$, i.e. $\pm\mathrm{Q}(x) \in A$ est un inverse de x dans A.

(ii) La norme d'un idéal non nul est un entier ≥ 1, il suffit donc de voir qu'il n'y a qu'un nombre fini d'idéaux de A de norme $M \geq 1$ donnée. Par Lagrange, un idéal de norme $M \geq 1$ contient M. On conclut car on a vu que A/MA est fini (et n'a donc qu'un nombre fini d'idéaux) : Lemme 6.8.

(iii) On rappelle que si $x \in A$, on a $\mathrm{N}((x)) = |\mathrm{N}_{K/\mathbb{Q}}(x)|$. L'hypothèse et le (ii) montrent donc qu'il existe un idéal I et une infinité d'entiers $m \geq$ tels que l'on a $I = (x_m)$. L'idéal I est évidement non nul et principal, disons $I = (x)$ avec $x \in A - \{0\}$. De plus, si $y \in A$ on a $(y) = (x)$ si et seulement si y et x sont associés, i.e. $y/x \in A^\times$. Cela conclut.

(iv) Dans les notations du cours, on a $n = r_1$ et $r_2 = 0$ (et ι est bien le plongement canonique choisi dans le cours). On conclut car on sait que $\iota(A)$ est un réseau de covolume $2^{-r_2}|\mathrm{disc}(A)|^{1/2}$ (Prop.-Déf. 6.15).

(v) Soit $\epsilon > 0$. On onsidère le sous-ensemble B_ϵ de $\mathbb{R}^\Sigma$ constitué des n-uples (x_τ) tels que $|x_\tau| \leq 1$ pour $\tau \notin \{\sigma, \sigma'\}$, $|x_\sigma| \leq \epsilon$ et $|x_{\sigma'}| \leq |\mathrm{disc}A|^{1/2}/\epsilon$. C'est un convexe compact symétrique de mesure $2^n \cdot |\mathrm{disc}A|^{1/2} = 2^n \mathrm{covol}\iota(A)$. D'après le lemme du corps convexe de Minkowski, on peut donc trouver $x \in A - \{0\}$ tel que $\iota(x) \in B_\epsilon$.

(vi) On applique la question précédente à une suite de réels ϵ_m tendant vers 0. On en tire une suite x_m d'éléments de A tels que $|\tau(x_m)| \leq 1$ pour tout $m \geq 1$ et $\tau \notin \{\sigma, \sigma'\}$, $|\sigma(x_m)|$ tend vers 0 quand m tend vers l'infini, et $|\sigma(x_m)\sigma'(x_m)| \leq |\mathrm{disc}(A)|^{1/2}$. En particulier, on a

$$|\mathrm{N}_{K/\mathbb{Q}}(x_m)| \leq |\mathrm{disc}(A)|^{1/2}$$

pour tout m, à cause de la formule du cours $\mathrm{N}_{K/\mathbb{Q}}(x) = \prod_{\tau\in\Sigma} \tau(x)$ pour tout $x \in K$. On peut donc appliquer le (iii) à la suite (x_m). Il montre que quitte à la remplacer par une sous-suite, il existe $x \in A - \{0\}$ tel que $x_m/x \in A^\times$ pour tout $m \geq 1$. On pose $u_m = x_m/x$. Si $\tau \in \Sigma$ on a $|\tau(u_m)| = |\tau(x_m)|/|\tau(x)|$. On en déduit le (vi) avec pour constante C tout majorant de l'ensemble fini $\{\frac{1}{|\tau(x)|}, \tau \in \Sigma\} \cup \{\frac{|\mathrm{disc}\, A|^{1/2}}{|\tau(x)\tau'(x)|}, (\tau, \tau') \in \Sigma^2\}$.

(vii) Soit $y \in A^\times$ et $I \subset \Sigma$. D'après le (i) on a l'égalité

$$\prod_{\tau\in I} \tau(x) = \prod_{\tau\in\Sigma-I} \frac{1}{\tau(x)}.$$

En particulier $\frac{1}{|\tau(y)|} = \prod_{\tau'\in\Sigma\{\tau\}} |\tau'(y)|$. On en tire $1/|\tau(u_m)| \leq C^{n-2}$ pour tout $m \geq 1$ et $\tau \notin \{\sigma, \sigma'\}$. De même (pour $I = \{\sigma, \sigma'\}$), on a $1/|\sigma(u_m)\sigma'(u_m)| \leq C^{n-2}$. Autrement dit, la constante $c = C^{2-n}$ convient.

(viii) Supposons qu'il existe $(a_\sigma) \in \mathbb{R}^\Sigma$ tel que $\sum_{\sigma\in\Sigma} a_\sigma \log|\sigma(u)| = 0$ pour tout $u \in A^\times$. Soient σ, σ' deux éléments distincts de Σ. Il faut voir $a_\sigma = a'_\sigma$. D'après les questions (v)-(vii), il existe une suite d'unités $(u_m)_{m\geq 1}$ de A telle que, lorsque m tends vers l'infini on a :

(a) $\log|\tau(u_m)| = O(1)$ si $\tau \neq \sigma, \sigma'$,

(b) $\log|\sigma'(u_m)| = -\log|\sigma'(u_m)| + O(1)$,

(c) $\log|\sigma(u_m)|$ tends vers $-\infty$.

On a $\sum_{\sigma\in\Sigma} a_\sigma \log|\sigma(u_m)| = 0$ pour tout $m \geq 1$. En faisant tendre m vers l'infini, (a) et (b) montrent que l'on a la relation $(a_\sigma - a_{\sigma'})\log|\sigma(u_m)| = O(1)$. Enfin, (c) montre $a_\sigma = a'_\sigma$.

(ix) Le fait que λ est un morphisme de groupes est évident. Enfin, si $x \in A^\times$ la relation $1 = |\mathrm{N}_{K/\mathbb{Q}}(x)| = \prod_{\sigma\in\Sigma} |\sigma(x)|$ montre après passage au logarithme $0 = \sum_{\sigma\in\Sigma} \log|\sigma(x)|$.

(x) Si $x \in \mathrm{E}_r$, alors $x \in A$ et $e^{-r} \leq |\sigma(x)| \leq e^r$ pour tout $\sigma \in \Sigma$. L'ensemble E_r est donc fini car $\iota(A)$ est un réseau d'après le cours (question (iv)).

(xi) Soient $||.|| : \mathbb{R}^\Sigma \to \mathbb{R}_{\geq 0}$ la norme définie par $||(x_\sigma)|| = \mathrm{Sup}_\sigma |x_\sigma|$ et $\mathrm{D}_r = \{x \in \mathbb{R}^\Sigma, ||x|| \leq r\}$. On a $\mathrm{D}_r \cap \mathrm{Im}\,\lambda = \lambda(\mathrm{E}_r)$, qui est fini d'après le (x). De même, $\ker\lambda = \mathrm{E}_0$ est fini. C'est un sous-groupe de $A^\times \subset K^\times \subset \mathbb{R}^\times$.

(xii) On a déja vu que $\mathrm{Im}\,\lambda$ est un sous-groupe discret de $\mathbb{R}^\Sigma$, inclus dans H, c'est donc un sous-groupe discret de H (la restriction de $||.||$ à H est une norme...). D'autre part, la question (viii) montre que $\mathrm{Im}\,\lambda$ n'est inclus dans aucun hyperplan de $\mathbb{R}^\Sigma$ distinct de H, ainsi $\mathrm{Im}\,\lambda$ engendre $\mathbb{R}$-linéairement H : c'est un réseau de H.

(xiii) Il est clair que si $x \in \mathbb{R}^\times$ vérifie $x^m = 1$ avec $m \geq 1$, alors $x = \pm 1$. En particulier, tout sous-groupe fini de $\mathbb{R}^\times$ est inclus dans $\{\pm 1\}$. Comme on a évidemment $\{\pm 1\} \subset \ker\lambda$, le (xi) (et Lagrange !) montre $\ker\lambda = A^\times$.

(xiv) On note f l'application de l'énoncé. C'est clairement un morphisme de groupes. Vérifions qu'il est injectif. Soit $(e, (m_1, \ldots, m_{n-1})) \in \{\pm 1\} \times \mathbb{Z}^{n-1}$ tel que $eu_1^{m_1} \cdots u_{n-1}^{m_{n-1}} = 1$. En appliquant le morphisme λ à cette identité, on trouve $0 = \sum_{i=1}^{n-1} m_i \lambda(u_i)$. Comme les $\lambda(u_i)$ forment une $\mathbb{Z}$-base de $\mathrm{Im}\,\lambda$, on a donc $m_i = 0$ pour tout $i = 1, \ldots, n-1$. La relation de départ s'écrit donc $e = 1$: on a montré que f est injectif. Il ne reste qu'à voir que f est surjectif. Soit $x \in A^\times$. On regarde $\lambda(x) \in \mathrm{Im}\,\lambda = \sum_i \mathbb{Z}\lambda(u_i)$. On peut donc trouver $(m_1, \ldots, m_{n-1}) \in \mathbb{Z}^{n-1}$ tel que $\lambda(x) = \lambda(\prod_{i=1}^{n-1} u_i^{m_i})$, autrement dit $x \prod_{i=1}^{n-1} u_i^{-m_i} \in \ker\lambda$. On conclut car $\ker\lambda = \{\pm 1\}$.

(xv) Par hypothèse sur d, le corps $\mathbb{Q}(\sqrt{d})$ est de degré 2 sur $\mathbb{Q}$ et totalement réel : les deux racines de $X^2 - d$ sont dans $\mathbb{R} - \mathbb{Q}$. Soit $A = \mathbb{Z}[\sqrt{d}]$. Si $(x, y) \in \mathbb{Z}^2$, un exemple du cours montre $\mathrm{N}_{K/\mathbb{Q}}(x + y\sqrt{d}) = x^2 - dy^2$. D'après le (i), il s'agit de voir qu'il y a une infinité de $z \in A^\times$ tels que $\mathrm{N}_{K/\mathbb{Q}}(z) = 1$. Mais d'après le (xiv), on a $A^\times \simeq \{\pm 1\} \times \mathbb{Z}$. En particulier, $A^\times$ est infini. Il en va donc de même du noyau du morphisme $A^\times \to \{\pm 1\}$, $z \mapsto \mathrm{N}_{K/\mathbb{Q}}(z)$.

14. Corrigé de l'examen 2016-2017

Problème 1. (i) D'après un théorème de Gauss, toute forme est proprement équivalente à une et une seule forme réduite (nécessairement de même discriminant). Soit (a,b,c) une forme réduite de discriminant -95. On a $-a < |b| \leq a \leq c$, b impair, et $a \leq \sqrt{95/3} < \sqrt{32} < 6$, donc $b = \pm 1, \pm 2, \pm 3$ et $(b^2 - D)/4 = ac$. Pour $b^2 = 1$ on a $ac = 24$, et on trouve $(1,1,24)$, $(2,\pm 1,12)$, $(3,\pm 1,8)$ et $(4,\pm 1,6)$. Pour $b^2 = 3$ on a $ac = 26$, et aucune forme réduite. Pour $b^2 = 5$ on a $ac = 30$, qui conduit à $(5,5,6)$. Les 8 formes exhibées sont bien réduites, et conviennent donc. Elles sont primitives (conformément au fait que -95 est fondamental).

(ii) Les classes de carré 1 de $\mathrm{P}(D)$ sont les classes ambiguës, i.e. les classes de formes ambiguës. Les formes $(1,1,24)$ et $(5,5,6)$ sont ambiguës (car du type (a,a,c)), et les 6 autres ne le sont manifestement pas. La classe de $(1,1,24)$ est d'ordre 1. La seule classe d'ordre 2 est donc celle de $(5,5,6)$.

(iii) Comme -95 est non carré, sans facteur carré et congru à 1 modulo 4, un résultat du cours assure que A_{-95} est l'anneau des entiers de $\mathbb{Q}(\sqrt{-95})$. C'est donc un anneau de Dedekind, par un autre résultat du cours. Le polynôme minimal $\Pi_{\alpha,\mathbb{Z}}$ de α sur $\mathbb{Q}$ est $(X-\alpha)(X-\overline{\alpha}) = X^2 - X + 24$.

(iv) On a $\Pi_{\alpha,\mathbb{Q}} \equiv X(X-1) \bmod 2$, donc D et $\overline{D}$ sont des "I(Q)" du cours pour $p = 2$ et $Q = X$ et $X - 1$ respectivement. Comme un tel Q est irréductible de degré 1, D et $\overline{D}$ sont premiers de norme $2^1 = 2$. De même, C est premier de norme 5 à cause de la relation $\Pi_{\alpha,\mathbb{Q}} \equiv (X+2)^2 \bmod 5$.

(v) Si $C = (z)$ avec $z \in A$, alors on $\mathrm{N}(C) = \mathrm{N}(z)$ (cours) et donc 5 est représenté par $(1,1,24)$. Mais $5 = x^2 + xy + 24y^2$ avec $x, y \in \mathbb{Z}$ entraine $20 = (2x+y)^2 + 95 \cdot y^2$, puis $y = 0$, puis $5 = x^2$: absurde. Les décomposition cherchées découlent d'un théorème du cours, qui utilise le fait que $\mathbb{Z}[\alpha]$ est l'anneau des entiers de $\mathbb{Q}(\sqrt{-95})$ et les décompositions mod 2 et 5 de $\Pi_{\alpha,\mathbb{Q}}$ données au (iv).

(vi) La bijection de Dedekind est un isomorphisme de groupes $[I] \mapsto \mathrm{q}_I$, entre $\mathrm{Pic}(A) = \mathrm{Cl}(A)$ et $\mathrm{P}(-95)$. D'après le (v), on a $[C]^2 = 1$ et $[C] \neq 1$, donc $[C]$ est d'ordre 2. Il en résulte que q_C est d'ordre 2, c'est donc la classe de $(5,5,6)$ d'après le (ii).

(vii) On a $\mathrm{N}(7+\alpha) = 7^2 + 7 + 24 = 80$. Les idéaux premiers de A contenant $7+\alpha$, et donc $(7+\alpha)\overline{(7+\alpha)} = 80 = 2^4 \cdot 5$, contiennent donc 2 ou 5. Mais A étant Dedekind, les relations $(2) = D\overline{D}$ et $(5) = C^2$ montrent que ces idéaux sont parmi D, $\overline{D}$ et C, puis l'existence d'une décomposition $(7+\alpha) = D^a\overline{D}^bC^c$. Par multiplicativité de la norme dans $A = \mathcal{O}_{\mathbb{Q}(\sqrt{-95})}$, on a $80 = 2^{a+b}5^c$ donc $c = 1$ et $a+b = 4$. Si D divise $7+\alpha$, alors on a $7+\alpha = 1+2\cdot 3+2\alpha$ puis $1 \in D$ et $D = A$, ce qui est faux car $\mathrm{ND} = 2$. Donc $a = 0$ et $b = 4$.

(viii) Le (vii) entraîne $1 = [\overline{D}]^4[C]$ dans $\mathrm{Cl}(A)$. On a aussi $[D][\overline{D}] = 1$ car $(2) = D\overline{D}$, donc $[D]^4 = [C]$ dans $\mathrm{Cl}(A)$. Comme $[C]$ est d'ordre 2, l'ordre de $[D]$ est exactement 8 (il divise 8, mais pas 4). Ainsi, $[D]$ engendre un sous-groupe cyclique d'ordre 8 dans $\mathrm{Cl}(A)$. On a déjà justifié $\mathrm{Cl}(A) \simeq \mathrm{P}(-95)$, donc $|\mathrm{Cl}(A)| = 8$ par le (i), ce qui conclut.

(ix) Le groupe $2\mathbb{Z} + \alpha\mathbb{Z}$ est clairement d'indice 2 dans A, et inclus dans D, qui est aussi d'indice (=norme) 2 par le (iv), on a donc $D = 2\mathbb{Z}+\alpha\mathbb{Z}$. La base $2, \alpha$ est directe (on conserve les conventions du cours), donc q_D est la classe d'équivalence propre de la forme

$$\mathrm{q}_{2,\alpha}(x,y) = \frac{1}{2}\mathrm{N}(2x+y\alpha) = \frac{1}{2}(4x^2 + 2xy + 24y^2),$$

i.e. de $(2,1,12)$.

(x) On a $C^2 = \langle 2, \alpha\rangle^2 = \langle 4, 2\alpha, \alpha^2\rangle$. Les relations $\alpha^2 = \alpha - 24$ et $24 = 4 \cdot 6$ montrent successivement $C^2 = \langle 4, 2\alpha, \alpha\rangle = \langle 4, \alpha\rangle$. Ensuite, on constate de même les égalités

$$C^2C = \langle 4, \alpha\rangle\langle 2, \alpha\rangle = \langle 8, 2\alpha, \alpha^2\rangle = \langle 8, 2\alpha, \alpha\rangle = \langle 8, \alpha\rangle$$

(on a utilisé $8 \cdot 3 = 24$). On a $\mathrm{N}(C^n) = 2^n$ ($A = \mathcal{O}_{\mathbb{Q}(\sqrt{-95})}$ et $\mathrm{N}(C) = 2$). Un calcul immédiat montre $\mathrm{q}_{4,\alpha} = (4,1,6)$ et $\mathrm{q}_{8,\alpha} = (8,1,3)$. En utilisant que (a,b,c) est proprement équivalent à $(c,-b,a)$, on en déduit que q_{C^2} et q_{C^3} sont les classes respectives de $(4,1,6)$ et $(3,-1,8)$. On conclut car on a $\mathrm{q}_{C^n} = (\mathrm{q}_C)^n$ par définition de la loi de groupe sur $\mathrm{P}(D)$.

(xi) D'après (viii) et (ix), l'application $\mathbb{Z}/8\mathbb{Z} \to \mathrm{P}(-95)$, $i \mapsto (\mathrm{q}_C)^i$ est un isomorphisme de groupe. Il suffit donc de déterminer $(\mathrm{q}_C)^i$ pour tout entier $0 \leq i \leq 7$. Ces classes sont respectivement : celle de $(1,1,24)$ pour $i=0$ (forme principale, ordre 1), celle de $(4,1,6)$ pour $i=2$ et celle de $(3,-1,8)$ pour $i=3$ d'après (x), celle de $(5,5,6)$ pour $i=4$ d'après (vi). On conclut car $(\mathrm{q}_C)^5 = (\mathrm{q}_C)^{-3} = (\mathrm{q}_C^3)^{\mathrm{opp}}$ est donc la classe de $(3,1,8)$, et de même $(\mathrm{q}_C)^6 = (\mathrm{q}_C)^{-2}$ est celle de $(4,-1,6)$ et $(\mathrm{q}_C)^7 = (\mathrm{q}_C)^{\mathrm{opp}}$ est celle de $(2,-1,12)$.

(xii) Si n est représenté par $(2,1,12)$, dont la classe est q_C, alors n^i est représenté par toute forme dans la classe de q_C^i, ainsi que par toute forme équivalente à une telle forme. On conclut par le (xi). En guise d'exemple, l'assertion est manifestement satisfaite pour $n=2$ (noter $5+5+6=16$).

Problème 2. (i) Comme I est inversible, il existe un idéal J non nul de A tel que IJ est principal, disons $IJ=(z)$. L'inclusion $aI \subset bI$ entraine $aIJ \subset bIJ$, c'est-à-dire $(az) \subset (bz)$. En multipliant par $1/z$ (noter $z \neq 0$), il reste $(a) \subset (b)$: $a.1 \in bA$ et donc b divise a.

(ii) Comme A est un ordre de K, il contient une $\mathbb{Q}$-base de K. On en déduit $K = \bigcup_m \frac{1}{m}A$, la réunion portant sur les $m \in \mathbb{Z}$ avec $m \geq 1$. Écrivons $E = \{e_1, \ldots, e_n\}$ et choisissons $m_i \in \mathbb{Z} - \{0\}$ tel que $m_i e_i \in A$. Alors l'entier $m = m_1 m_2 \cdot m_n$ est non nul et vérifie $mE \subset A$.

(iii) Comme x est dans $\mathcal{O}_K$, il existe $m_0, m_1, \ldots, m_{n-1}$ dans $\mathbb{Z}$ tels que $x^n = \sum_{i=0}^{n-1} m_i x^i$. D'après un énoncé du cours (chapitre 1), tout élément de $A[x]$ s'écrit alors sous la forme $\sum_{i=0}^{n} a_i x^i$ avec $a_i \in A$. Il suffit donc de montrer qu'il existe $m \in \mathbb{Z} - \{0\}$ avec $mx^i \in A$ pour tout $i \in \{0,1,\ldots,n-1\}$. Cela résulte du (ii) appliqué à l'ensemble fini $E = \{x^i,\ 0 \leq i \leq n-1\}$.

(iv) $A[x]$ est un sous-anneau de K. En particulier, c'est un sous-groupe additif stable par multiplication par A et par x. Il en va donc de même de $aA[x]$ pour tout $a \in A$. Soit $m \in \mathbb{Z} - \{0\}$ tel que $mA[x] \subset A$, un tel $a = m$ existe par (iii). La remarque précédente assure que $mA[x]$ est un idéal de A. Il est non nul : il contient $m.1 = m \neq 0$.

(v) Supposons (c) vérifiée. Soit x dans $\mathcal{O}_K$ non nul. En particulier, x est dans K, donc s'écrit sous la forme a/b avec $b = m$ non nul dans $\mathbb{Z}$ (par le (ii)). Soit I comme au (iv). On a $a/bI \subset I$, donc $aI \subset bI$. D'après (c), I est inversible. Le (i) entraîne donc que b divise a dans A, i.e. $x \in A$. Ainsi, on a $\mathcal{O}_K \subset A$, puis $A = \mathcal{O}_K$.

(vi) C'est le cas $\alpha = 1$ du Lemme 7.4, dont la démonstration ne nécessite pas que A soit l'anneau des entiers de K, comme nous l'avions observé en cours.

(vii) Supposons (b) vérifié mais qu'il existe un idéal non nul de A non inversible. Considérons un tel idéal I de norme minimale. L'idéal I n'est pas maximal, d'après (b). Il est donc inclus dans un idéal maximal P de A. Mais P est premier donc inversible d'après (b), on a donc $I = JP$ pour un idéal J de A. On a $I = JP \subsetneq J$ d'après le (vi), donc $\mathrm{N}(J) < \mathrm{N}(I)$. Donc J est inversible. Mais alors $I = JP$ est inversible (produit de deux inversibles) : absurde. Il ne reste que (a) $\Rightarrow$ (b) (ou (c)), qui est un théorème du cours.

(viii) On a $\mathrm{I}(P) = pA + \Pi_{\alpha,\mathbb{Q}}(\alpha)A = pA$.

(ix) D'après Bézout, il existe V, V' dans $(\mathbb{Z}/p\mathbb{Z})[X]$ tels que $UQ + U'Q' = 1$. Soient $U, U' \in \mathbb{Z}[X]$ arbitraires tels que $U \equiv V \bmod p$ et $U' \equiv V' \bmod p$. On a $U\widetilde{Q} + U'\widetilde{Q} \equiv 1 \bmod p\mathbb{Z}[X]$, et conclut en évaluant en $X = \alpha$.

(x) On a $\mathrm{I}(Q) = (p, \widetilde{Q}(\alpha))$ et $\mathrm{I}(Q') = (p, \widetilde{Q'}(\alpha)$, donc $\mathrm{I}(Q)\mathrm{I}(Q')$ est l'idéal $p(p, \widetilde{Q}(\alpha), \widetilde{Q'}(\alpha)) + (\widetilde{Q}(\alpha)\widetilde{Q'}(\alpha))$. D'après le (ix) on a $1 \in (p, \widetilde{Q'}(\alpha), \widetilde{Q}(\alpha))$, donc l'idéal ci-dessus est $\mathrm{I}(QQ')$.

(xi) On écrit $P = \prod_i P_i$ avec les P_i irréductibles distincts. Le (x) montre par récurrence $\mathrm{I}(P) = \prod_i \mathrm{I}(P_i)$. Le $\mathrm{I}(P_i)$ sont les idéaux premiers de A contenant p par le cours, et leur produit est principal : ce sont des idéaux inversibles.

Problème 3. (i) On a $\Phi_\ell(\zeta) = 0$ et Φ_ℓ est irréductible dans $\mathbb{Q}[X]$, donc $\Phi_\ell = \Pi_{\zeta,\mathbb{Q}}$. En particulier, on a $\ell - 1 = \deg \Phi_\ell = [K : \mathbb{Q}]$. Les racines de Φ_ℓ sont les éléments de $\mu = \{\zeta^i, i = 1, \ldots, \ell-1\}$. On en déduit d'une part l'assertion sur $\Sigma(K)$ (cours), et d'autre part, comme ℓ est impair, que tous ces éléments sont complexes non réels. On a donc $r_1 = 0$ et $r_2 = (\ell-1)/2$.

(ii) On a $\Phi_\ell(X) = \prod_{i=1}^{\ell-1}(X - \zeta^i)$, puis $\ell = \Phi_\ell(1) = \prod_{i=1}^{\ell-1}(1-\zeta^i)$ en faisant $X = 1$. On conclut par la relation $\mathrm{N}_{K/\mathbb{Q}}(x) = \prod_{\sigma \in \Sigma(K)} \sigma(x)$ et la description de $\Sigma(K)$ en (i).

(iii) D'après le cours on a $\mathrm{N}((1-\zeta)) = |\mathrm{N}_{K/Q}(1-\zeta)|$. Donc l'idéal $(1-\zeta)$ de A est de norme ℓ, i.e. d'indice ℓ dans A. Un sous-groupe d'indice premier ℓ dans A est forcément maximal pour l'inclusion, car $A/\ell A \simeq \mathbb{Z}/\ell\mathbb{Z}$ n'a pas d'autres sous-groupes que 0 et $\mathbb{Z}/\ell\mathbb{Z}$. Ainsi, $(1-\zeta)$ est un sous-groupe maximal de A, donc un idéal maximal de A en particulier.

(iv) D'après le (i), on a la formule $\mathrm{disc}\Phi_\ell = \prod_{1\leq i<j\leq \ell-1}(\zeta^i-\zeta^j)^2$. En particulier, $\pm\mathrm{disc}\Phi_\ell$ est le produit sur tous les couples (i,j) avec $i\neq j$, des $(\zeta^i-\zeta^j)$. On a donc $\mathrm{disc}|\Phi_\ell| = \prod_{1\leq i\leq \ell-1} m_i$ avec

$$m_i = |\prod_{j\neq i}(\zeta^i-\zeta^j) = |\prod_{j\neq i}(1-\zeta^{j-i})| = \ell|1-\zeta^{-i}|^{-1},$$

(la seconde égalité utilise (ii)), ce qui conclut par (ii) encore.

(v) On a $\Phi_\ell \equiv (X-1)^{\ell-1} \bmod \ell$, donc d'après le cours il existe un et un seul idéal premier de A contenant ℓ, à savoir l'idéal $\mathrm{I}(X-1) = (\ell, \zeta-1)$. Mais on a vu que $(\zeta-1)$ est maximal, de sorte que l'inclusion évidente $(\zeta-1)\subset \mathrm{I}(X-1)$ entraîne $\mathrm{I}(X-1) = (\zeta-1)$.

(vi) Soit p premier $\neq \ell$. La réduction modulo p du polynôme $X^\ell-1$ est sans facteur carré. En effet, si $P\in\mathbb{Z}/p\mathbb{Z}[X]$ est tel que P^2 divise $X^\ell-1$, alors P divise le polynôme dérivé de $X^\ell-1$, qui vaut $\ell X^{\ell-1}$, et donc $X^\ell-1$ car ℓ est premier à p. C'est absurde, car X ne divise pas $X^\ell-1$. Ainsi, Φ_ℓ (qui divise $X^\ell-1$) est sans facteur carré également.

(vii) D'après le (vi) et le problème 2 (xi), les idéaux premiers de A contenant un premier $p\neq\ell$ sont inversibles. D'après le (v), l'unique idéal premier de A contenant ℓ est $(1-\zeta)$, qui est aussi inversible (car principal...). Mais d'après le cours, tout idéal premier de A contient un premier p de $\mathbb{Z}$. Ainsi, tous les idéaux premiers de A sont inversibles. Le (b) $\Rightarrow$ (a) du problème 2 entraîne donc $A = \mathcal{O}_K$.

(viii) D'après Minkowski, (i) et (iv), tout idéal de A est équivalent à un idéal contenant un entier N avec $1\leq N\leq C(3,6)\sqrt{7^5}\simeq 4.12$ d'après l'énoncé.

(ix) On a démontré que A est l'anneau des entiers de $\mathbb{Q}(\zeta)$ (donc de Dedekind). Le (viii) montre donc que $\mathrm{Cl}(A)$ est engendré par les classes des idéaux premiers de A contenant un entier $1\leq N\leq 4$, i.e. un entier $1\leq N\leq 3$. D'après les données, l'unique idéal premier contenant 3 est l'idéal principal (3). De plus, on constate que X^3+X+1 et X^3+X^2+1 n'ont pas de racine dans $\mathbb{Z}/2\mathbb{Z}$, ils sont donc irréductibles dans $\mathbb{Z}/2\mathbb{Z}[X]$. Les idéaux premiers contenant 2 sont donc $I = (2,\zeta^3+\zeta+1)$ et $J = (2,\zeta^3+\zeta^2+1)$, et on a $IJ = (2)$ car A est l'anneau des entiers de $\mathbb{Q}(\zeta)$. La relation $1 = [I][J]$ entraîne bien que $\mathrm{Cl}(A)$ est engendré par $[I]$.

(x) On constate que la multiplication par $1+\zeta+\zeta^3$ a pour matrice dans la base $1,\zeta,\cdots,\zeta^5$ la matrice indiquée dans les données. Le déterminant de cette matrice est 8, et aussi $\mathrm{N}_{K/\mathbb{Q}}(1+\zeta+\zeta^3)$ par définition. Mais la norme de I vaut $2^{\deg(X^3+X+1)} = 8$, et I contient $(1+\zeta+\zeta^3)$ qui est aussi de norme 8, on a donc $I = (1+\zeta+\zeta^3)$: c'est un idéal principal, et A est principal d'après le (ix).

15. Corrigé de l'examen 2017-2018

Problème 1. (i) (5) D'après Gauss, des représentants distincts de $\mathrm{Cl}(-87)$ sont donnés par les formes réduites de discriminant -87. Si (a,b,c) est une telle forme, on a b impair et $|b| \leq a \leq \sqrt{87/3} = \sqrt{29} < 6$, donc $b = \pm 1, \pm 3, \pm 5$. On écrit $\frac{87+b^2}{4} = ac$, on trouve respectivement 22, 24 et 28 pour $|b| = 1, 3, 5$. Cela conduit aux 6 formes réduites

$$(1,1,22), (2,\pm 1,11), \ (3,3,8) \text{ et } (4,\pm 3,6).$$

Elles sont toutes primitives, et forment donc des représentants de $\mathrm{P}(-87) = \mathrm{Cl}(-87)$.

(ii) (3) On sait que l'élément neutre est la classe de la forme principale, i.e. de $(1,1,22)$. De plus, les classes de carré 1 sont les classes ambiguës. D'après le cours et le (i), ce sont celles de $(1,1,2)$ et $(3,3,8)$ (cette dernière représente donc l'unique classe d'ordre 2).

(iii) (4) D'après le cours, $\varepsilon_3 : \mathrm{P}(-87) \to \{\pm 1\}$ est un morphisme de groupes. Il est surjectif car $\varepsilon_3((2,1,11)) = \left(\frac{2}{3}\right) = -1$ (noter que 2 est représenté par $(2,1,11)$ et premier à -87). Comme $\mathrm{P}(-87)$ a 6 éléments, son noyau est un sous-groupe d'ordre 3. Comme on a $\varepsilon_3((4,\pm 3,6)) = \left(\frac{4}{3}\right) = 1$, on a

$$\ker \varepsilon_3 = \{[(1,1,22)], [(4,3,6)], [(4,-3,6)]\}.$$

(iv) (2) Dans un groupe commutatif, le produit d'un élément d'ordre 2 par un élément d'ordre 3 est d'ordre 6. Comme $\mathrm{P}(-87)$ a six éléments par (i), on conclut par (ii) et (iii).

(v) (2) On a déjà vu que les classes de $(1,1,22)$, $(3,3,8)$, $(4,\pm 3,6)$ sont d'ordre respectifs $1,2,3$. Les deux dernières classes, $[(2,\pm 1,11)]$, sont inverses l'une de l'autre et d'ordre 6 par le (iv).

(vi) (6) On a $3^* = (-1)^{\frac{3-1}{2}} = -3$ puis d'après la loi de réciprocité quadratique

$$\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = -1.$$

Par multiplicativité du symbole de Legendre et la loi de réciprocité quadratique (noter que 29 est premier $\equiv 1 \bmod 4$) on a de plus

$$\left(\frac{-87}{p}\right) = \left(\frac{-3}{p}\right)\left(\frac{29}{p}\right) = -\left(\frac{p}{29}\right).$$

Cela démontre l'équivalence entre (a) et (b). Comme p est impair, (a) est équivalent au fait que p est représenté par une forme q de discriminant -87 par Lagrange. Cela montre (c) implique (a). Supposons (a) et soit q qui représente p on a $\epsilon_3(q) = \left(\frac{p}{3}\right) = -1$. D'après le (iii), q est donc proprement équivalente à $(2,\pm 1,11)$ ou $(3,3,8)$. Comme les formes $(2,\pm 1,11)$ sont équivalentes, on a montré (c).

(vii) (4) Si $p = 2$ alors 8 est bien représenté par $(3,3,8)$. On suppose $p \neq 2$; d'après (vi), p est représenté par q avec $q = (2,1,11)$ ou $q = (3,3,8)$. Remarquons que $[q]$ est d'ordre 6 dans le premier cas, $[2]$ dans le second. Dans tous les cas $[q]^3$ est d'ordre 2 : c'est $[(3,3,8)]$ par le (ii), et représente p^3 par Gauss.

(viii) (1) $D = -3 \cdot 29$ est sans facteur carré et $\equiv 1 \bmod 4$, et on applique le cours.

(ix) (4) On a $\alpha + \overline{\alpha} = 1$, donc on a concrètement

$$\overline{D} = 2A + (\alpha - 1)A, \quad \overline{S} = 7A + (\alpha - 3)A.$$

Le polynôme minimal de α est $P = X^2 - X + 22$. Modulo 2 il vaut $X(X+1)$, modulo 7 il vaut $(X-3)(X+2)$. On a donc $D = \mathrm{I}_2(X)$, $\overline{D} = \mathrm{I}_2(X-1)$, $S = \mathrm{I}_7(X+2)$ et $\overline{S} = \mathrm{I}_7(X-3)$ avec la notation du cours. Comme X et $X+1$ sont les facteurs irréductibles distincts de P dans $\mathbb{Z}/2\mathbb{Z}[X]$, le cours affirme que D et $\overline{D}$ sont les deux seuls idéaux premiers de $A = \mathbb{Z}[\alpha]$ contenant 2, qu'ils sont distincts, et de norme 2 (car $X, X-1$ sont de degré 1). Le même argument assure que S et $\overline{S}$ sont les ideaux premiers distincts de A contenant 7, et qu'ils sont de norme 7. De plus, comme $A = \mathbb{Z}[\alpha]$ est l'anneau des entiers de $\mathbb{Q}(\alpha)$, un autre théorème du cours donne $2A = \overline{D}D$ et $7A = S\overline{S}$.

(x) (5) On a $\mathrm{N}(2+\alpha) = \mathrm{N}((2+\alpha) = 4 + 2 + 22 = 28$. Les idéaux premiers contenant (=divisant car A est de Dedekind) $2+\alpha$ contiennent $28 = 4 \cdot 7$ et donc 2 ou 7. D'après le (ix), ils sont donc de la forme $D, \overline{D}, S, \overline{S}$. Par la propriété de Dedekind (qui s'applique par le (viii)) et la multiplicativité de la norme, on a donc $(2+\alpha) = D^a\overline{D}^b S^c \overline{S}^d$ avec $a+b = 2$ et $1 = c+d$. Mais $2+\alpha$ n'est pas dans $\overline{D} = 2A + (\alpha-1)A$, car sinon $1 = (2+\alpha) - (-1+\alpha) - 2$ serait dans $\overline{D}$, i.e.$\overline{D} = A$: absurde ($\overline{D}$ est de norme 2). Autrement dit, $\overline{D}$ ne divise pas $2+\alpha$: on a donc $b = 0$. Comme $2+\alpha$ est manifestement dans S on a que S divise $(2+\alpha) : c = 1$ et donc $d = 0$. On a montré $(2+\alpha) = D^2$.

(xi) (5) La méthode du cours (i.e. un argument d'indice) montre que $2, \alpha$ est une $\mathbb{Z}$-base directe de D, et aussi que $7, 2+\alpha$ est une $\mathbb{Z}$-base directe de T. On a donc $\mathrm{q}_{2,\alpha}(x,y) = \frac{1}{2}\mathrm{N}(2x+\alpha y) = 2x^2+xy+11y^2$ et $\mathrm{q}_{7,\alpha+2}(x,y) = \frac{1}{7}\mathrm{N}(7x+(2+\alpha)y) = \frac{1}{7}(49x^2+7\cdot 5xy+28y^2) = 7x^2+5xy+4y^2$. D'autre part, on a les équivalences propres

$$(7,5,4) \overset{+}{\sim} (4,-5,7) \overset{+}{\sim} (4,3,6).$$

La définition de Dedekind montre donc $\mathrm{q}_D = [(2,1,11)]$ et $\mathrm{q}_S = [(4,3,6)]$.

(xii) (3) D'après Dedekind et le (viii), l'application $[I] \mapsto \mathrm{q}_I$ est un isomorphisme de groupes $\mathrm{P}(A) = \mathrm{Cl}(A) \xrightarrow{\sim} \mathrm{P}(-87)$. D'après (iv) et (v), le groupe de droite est cyclique d'ordre 6 engendré par $[(2,1,11)]$. Mais cette classe est q_D par le (xi), ce qui conclut.

(xiii) (3) D'après (ix) et (x) on a $[S][\overline{S}] = 1$ et $[D]^2[S] = 1$, on a donc $[D]^2 = [S]^{-1} = [\overline{S}] = [S]^{\mathrm{opp}}$. Le groupe $\mathrm{P}(-87)$ étant cyclique d'ordre 6 engendré par $C = [(2,1,11)]$, il suffit d'identifier les puissances de C. Pour des raisons d'ordre, on savait déjà $C^0 = [(1,1,22)]$, $C^3 = [(3,3,8)]$ et $C^{-1} = C^5 = [(2,-1,11)]$. Il ne reste qu'à déterminer C^2, puisque l'on a $C^4 = C^{-2} = (C^2)^{-1}$. Mais la relation $[D]^2 = [S]^{\mathrm{opp}}$ s'écrit $C^2 = [(2,1,11)]^2 = [(4,-3,6)]$ par (xi).

Problème 2. (i) (3) Soit ζ une racine 7ème de l'unité, avec $\zeta \neq 1$. On a $1+\zeta+\zeta^{-1}+\zeta^2+\zeta^{-2}+\zeta^3+\zeta^{-3} = 0$. De plus, on a $(\zeta+\zeta^{-1})^2 = \zeta^2+\zeta^{-2}+2$ et $(\zeta+\zeta^{-1})^3 = \zeta^3+\zeta^{-3}+3(\zeta+\zeta^{-1})$. On en déduit que l'élément $\zeta+\zeta^{-1}$ est racine du polynôme $P = X^3+X^2-2X-1$. On conclut car pour $\zeta = e^{2i\pi/7}$ on a $\zeta+\zeta^{-1} = \alpha$. Le polynôme P n'a pas de racine rationnelle : si p/q est racine avec $(p,q) = 1$ alors q et p divise 1, mais ± 1 n'est pas racine. Comme $\deg P = 3$ on en déduit que P est irréductible dans $\mathbb{Q}[X]$: c'est le polynôme minimal de α et $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$.

(ii) (2) On prend $\zeta = e^{2ik\pi/7}$ avec $0 < k < 7$, on a vu que $\zeta+\zeta^{-1} = 2\cos\frac{2k\pi}{7}$ est racine de P. On trouve 3 racines réelles distinctes en prenant $k = 1,2,3$. Donc $r_1 = 3$ et $r_2 = 0$. Autre méthode : on a $P(-1) = 1$, $P(1) = -1$ et $P(\pm\infty) = \pm\infty$, donc P s'annule sur $]-\infty,1[$, $]-1,1[$ et $]1,\infty[$.

(iii) (4) On applique la théorie de Minkowski à l'ordre $A = \mathbb{Z}[\alpha]$ de K (noter que l'on a $\alpha \in \overline{\mathbb{Z}}$ par le (i)). Par le (ii), la constante de Minkowski de A est $\mathrm{C}(A) = C(0,3)\sqrt{|\mathrm{disc}A|}$, avec $C(0,3) = 3!/3^3 = 2/9$. De plus, on a $\mathrm{disc}A = \mathrm{disc}P = 49$ (donnée). On a donc $C(A) = 14/9 < 2$. D'après Minkowski, tout idéal non nul de A est équivalent à un idéal contenant un entier N avec $1 \leq N \leq C(A) < 2$, i.e. à l'idéal A : tout idéal non nul est principal.

(iv) (3) On a $\mathbb{Z}[\alpha] \subset \mathcal{O}_K$ car $\alpha \in \overline{\mathbb{Z}}$ (d'après (i)). Comme $\mathbb{Z}[\alpha]$ est principal, il est factoriel, et donc intégralement clos. Cette dernière propriété entraîne en particulier que $\mathbb{Q}(\alpha) \cap \overline{\mathbb{Z}}$ (i.e. $\mathcal{O}_K$ par définition) est inclus dans $\mathbb{Z}[\alpha]$.

Problème 3. (i) (3) (exercice donné à faire à la maison) Comme D est fondamental, il ne s'écrit pas de la forme n^2D' avec D' discriminant d'une forme, i.e. $D' \equiv 0,1 \bmod 4$. Si $D \equiv 1 \bmod 4$, et $D = n^2D'$ on a nécessairement $D' \equiv 1 \bmod 4$, donc D fondamentak ssi D est sans facteur carré, auquel cas A_D est l'anneau des entiers de $\mathbb{Q}(\sqrt{D})$ par le cours. Si $D = 4d$ on voit que D fondamental entraîne $d \equiv 2,3 \bmod 4$ (prendre "$n = 2$") et d sans facteur carré, et on conclut encore par le cours.

(1) D'après (i), I est inversible, ce qui justifie l'existence de J.

(ii) (2) Par définition, si u, v est une $\mathbb{Z}$-base directe de J on a $[\mathrm{q}_{u,v}] = \mathrm{q}_J$ et $\mathrm{q}_{u,v}(x,y) = \frac{\mathrm{N}(ux+vy)}{\mathrm{N}(J)}$. On conclut par l'identité $\mathrm{N}(z) = \mathrm{N}((z))$ pour $z \neq 0$.

(iii) (3) Si $[I] = [I']$ alors $[I'J] = [I][J] = 1$ et donc $I'J$ est principal, manifestement inclus dans J. L'application de l'énoncé est donc bien définie. Elle est injective car J est inversible. Si on a $(z) \subset J$, alors par contenir c'est diviser (J inversible) on a $(z) = JI'$. On a $[I'] = [J]^-1 = [I]$: c'est la surjectivité.

(iv) (5) Dans la bijection précédente, si $JI' = (z)$ on a $\frac{\mathrm{N}((z))}{\mathrm{N}(J)} = \mathrm{N}(I')$ par multiplicativité de la norme (qui vaut par (i) car A_D est de Dedekind). La première assertion en découle. Pour la seconde, il ne reste qu'à montrer que si on a $I'J = (z)$ principal non nul, alors on a équivalence entre :

(a) $I' = mI''$ pour $m \geq 2$ et I'' idéal,
(b) $z = mz'$ avec $m \geq 2$ et $z' \in J$.

Cela vient du fait que dans la bijection du (iii), l'ensemble but et l'ensemble source sont stables par multiplication par tout entier $m \in \mathbb{Z}$ (noter en particulier $[mI'] = [I']$), et que cette bijection induit donc une bijection, pour tout $m \geq 2$, entre idéaux de la forme mI' avec $[I'] = [I]$, et idéaux de la forme $m(z)$ avec $z \in J - \{0\}$. Cela prouve (a) $\Leftrightarrow$ (b).

(v) (2) On a $[I][J] = 1$ donc $\mathrm{q}_I = \mathrm{q}_J^{-1}$. Or $\mathrm{q}_J^{-1} = \mathrm{q}_J^{\mathrm{opp}}$ par le cours, donc q_I et q_J sont équivalentes. La seconde assertion découle du fait que deux formes équivalentes représentent les même entiers.

(vi) (4) On écrit $\mathrm{A}_D = \mathbb{Z} + \mathbb{Z}\alpha$ avec α comme dans le cours. Comme A_D est l'anneau des entiers de $\mathbb{Q}(\sqrt{D})$ par (i), un résultat du cours montrer qu'il suffit de voir que le polynôme minimal de α (qui est de degré 2) est scindé à racines distinctes mod p. Il y a deux cas.

– Si $D = 4d$ alors on a $\alpha = \sqrt{d}$ de polynôme minimal $X^2 - d$. L'hypothèse sur p sécrit que $p \neq 2$ et d carré modulo p, de sorte que $X^2 - d$ est de la forme $(X - u)(X + u)$ dans $(\mathbb{Z}/p\mathbb{Z})[X]$ avec $u \neq 0$.

– Sinon on a $D \equiv 1 \bmod 4$, et $\alpha = \frac{1+\sqrt{D}}{2}$ est de polynôme minimal $P = X^2 - X + \frac{1-D}{4}$. Si $p = 2$ l'hypothèse s'écrit $D \equiv 1 \bmod 8$, i.e. $P \equiv X(X - 1) \bmod 2$, et conclut. Si p est impair on a $4P = (2X - 1)^2 - D$ et D est un carré non nul mod p, et on conclut encore.

(vii) (3) Toute classe de forme est égale à q_I pour un certain idéal non nul I, par Dedekind. Le (v) montre que q_I représente p si, et seulement si, I est équivalent à un idéal de norme p. Les seuls idéaux de norme p contiennent p, et sont P et P' par le cours et l'analyse du (vi).

(viii) (4) Soit I un idéal de (l'anneau de Dedekind) A_D de norme p^m. Ses facteurs premiers contiennent p^m et donc p : ils sont donc de la forme P ou P' par le (vi). On a donc $I = P^a(P')^b$. Si a et b sont tous les deux non nuls, on constate que I est divisible par $PP' = (p) : I$ n'est pas primitif. On a donc $I = P^a$ ou $I = (P')^b$, avec $a = b = m$ en prenant la norme.

(ix) (2) On applique le (viii) et le (v).

(x) (2) L'ordre de q_P (resp. $\mathrm{q}_{P'}$) est le plus petit entier $m \geq 1$ tel que $(\mathrm{q}_P)^m$ est la forme principale. On conclut par le (ix).

(xi) (4) Sous l'hypothèse sur n, $D = 9 - 2^{n+3}$ est $\equiv 1 \bmod 4$ et sans facteur carré donc fondamental. La forme $q = (2, 1, 2^n - 1)$ est de discriminant $1 - 8(2^n - 1) = 9 - 2^{n+3} = D$. La forme principale q' de ce discriminant est $(1, 1, 2^{n+1} - 2)$. Elle représente primitivement $1 + 1 + 2^{n+1} - 2 = 2^{n+1}$. On a $4q'(x, y) = (2x + y)^2 + (2^{n+3} - 9)y^2$. Ses représentations primitives différentes de 4 ont un y non nul, et sont $\geq 2^{n+3} - 9$. Pour $n \geq 2$, la plus petite puissance de 2 après $2^{n+3} - 9$ est 2^{n+3}. Elle est atteinte pour $x = y = 1$.

(xii) (2) D'après le (ix), p^2 est primitivement représenté par la forme principale si, et seulement si, q_P^2 est la classe principale. D'après le cours, c'est équivalent à q_P ambiguë.

16. Corrigé de l'examen 2018-2019

Problème 1. (i) (5) D'après Gauss, des représentants distincts sont donnés par les réduites de discriminant -155. Si (a,b,c) est une telle réduite, on a $|b| \leq a \leq \sqrt{155/3} < \sqrt{52}$, donc $|b| \leq 7$. D'autre part b est impair. La méthode de Gauss donne $ac = 39$ pour $b = \pm 1$, $ac = 41$ pour $b = \pm 3$, $ac = 45$ pour $b = \pm 5$, $ac = 51$ pour $b = \pm 7$. On trouve les réduites $(1,1,39)$, $(3,\pm 1,13)$ et $(5,5,9)$. La première et la dernière sont les seules ambigues.

(ii) (3) Toutes les classes ci-dessus sont primitives, donc $\mathrm{P}(-155) = \mathrm{Cl}(-155)$ est un groupe abélien d'ordre 4. Soit x la classe de $(3,1,13)$. Comme x n'est pas ambigue on a $x^2 \neq 1$. Mais $x^4 = 1$ donc x est d'ordre 4 et $\mathrm{P}(-155) \simeq \mathbb{Z}/4\mathbb{Z}$.

(iii) On a $A = A_{-155}$. D'après Dedekind on a $\mathrm{Pic}(A) \simeq \mathrm{P}(-155) \simeq \mathbb{Z}/4\mathbb{Z}$.

(iv) A est un ordre de $K = \mathbb{Q}(\sqrt{-155})$ ($r_1 = 0$, $r_2 = 1$) et on a $\mathrm{disc} A = \mathrm{disc} t^2 - t + 39 = -155$, puis $\mathrm{C}(A) \leq \frac{2}{\pi}\sqrt{155} < 8$. D'après Minkowski, tout idéal non nul de A est équivalent à un idéal contenant N avec $1 \leq N \leq 7$.

(v) Comme $-155 = -5 \cdot 31$ est sans facteur carré et $\equiv 1 \bmod 4$, on sait que A est l'anneau des entiers de K. Ainsi, $\mathrm{Cl}(A) = \mathrm{Pic}(A)$ est un groupe, recouvert part les classes des diviseurs de (N) avec $1 \leq N \leq 7$. Par la propriété de Dedekind, ces classes sont engendrées par les classes des idéaux premiers contenant N avec $N = 2, 3, 5$ et 7.

(vi) Le polynôme $t^2 - t + 39$ est $\equiv t(t-1) \bmod 3$ (factorisation en irréductibles dans $\mathbb{Z}/3\mathbb{Z}[t]$), et on conclut par la proposition du cours que $T = \mathrm{I}_3(t)$ et $T' = \mathrm{I}_3(t-1)$ sont les deux idéaux premiers de A contenant 3, et vérifient $(3) = TT'$ (par exemple car $A = \mathcal{O}_K$ et un théorème du cours).

(vii) Le polynôme $R = t^2 - t + 39$ est irréductible dans $\mathbb{Z}/2\mathbb{Z}[t]$ et dans $\mathbb{Z}/7\mathbb{Z}[t]$ (il n'a pas de racine dans $\mathbb{Z}/2$, et son disciminant $-155 \equiv -1 \bmod 7$ n'est pas un carré dans $\mathbb{Z}/7\mathbb{Z}$). On en déduit que $(2) = \mathrm{I}_2(R)$ et $(7) = \mathrm{I}_7(R)$ sont premiers (les seuls contenant respectivement 2 et 7). De même, $t^2 - t + 39 \equiv (t+2)^2 \bmod 5$ montre $(5) = C^2$ avec $C = (5, \alpha + 2)$ l'unique idéal premier contenant 5.

(viii) On a $\mathrm{N}(\alpha - 3) = 3^2 - 3 + 39 = 45 = 5 \cdot 9$, de sorte que $\alpha - 3$ est produit d'idéaux premiers contenant 5 ou 3. Remarquons que $\alpha - 3$ n'est pas dans T', car sinon on aurait $(\alpha - 1) - (\alpha - 3) - 3 = 1$ dans T' : absurde (on sait que T' est de norme $3^1 = 3$). Donc T' ne divise pas $\alpha - 3$, et la seule possibilité est donc $(\alpha - 3) = CT^2$. Si $C = (z)$ alors $\mathrm{N}(z) = \mathrm{N}(C) = 5$, donc $x^2 + xy + 39y^2$ représente 5. Cela entraine que 20 est de la forme $(2x+y)^2 + 155y^2$, puis $y = 0$ et 20 est un carré : absurde, C n'est pas principal.

(ix) D'après le (v), (vi) et (vii), $\mathrm{Pic}(A)$ est engendré par les classes de T, T', (2), (7) et C. Comme $[T][T'] = [3A] = [A]$, $[T']$ est l'inverse de $[T]$ (et donc une puissance de $[T]$). De même $[C]^2 = [A]$ et $[C][T]^2 = [A]$ par (viii), donc $[C] = [C]^{-1}] = [T]^2$ et $[T]^4 = [A]$. Ainsi $\mathrm{Pic}(A)$ est engendré par $[T]$, dont l'ordre divise 4. Mais $[T]^2 = [C] \neq [A]$ car C n'est pas principal : on a montré $\mathrm{Pic}(A) \simeq \mathbb{Z}/4\mathbb{Z}$.

Problème 2. (i) Le plongement $\sigma_{|\mathbb{Q}(x)}$ (dans $\Sigma(\mathbb{Q}(x))$) se prolonge d'exactement $[K : \mathbb{Q}(x)] > 1$ manière à K d'après le cours. Un de ces prolongements est σ. Il suffit donc d'en considérer un autre, et de l'appeler τ.

(ii) La justification vient du fait $|\Sigma(K)| = [K : \mathbb{Q}] = r_1$ si K est totalement réel. On considère le plongement canonique $\iota(x) = (\sigma_1(x), \ldots, \sigma_n(x))$ de K dans $\mathbb{R}^n$. On sait que $\iota(\mathcal{O}_K)$ est un réseau de covolume $\sqrt{d}$. On considère le compact C constitué des n-uples $(x_1, \ldots, x_n)$ dans $\mathbb{R}^n$ avec $|x_1| \leq 2^{n-1}\sqrt{d}$ et $|x_i| \leq 1/2$ pour $i > 2$. C'est un convexe symétrique de volume de Lebesgue $2^n\sqrt{d} = 2^n \mathrm{covol}(\iota(\mathcal{O}_K))$. Par le lemme du corps convexe on a donc l'existence de $\iota(x) \in \iota(\mathcal{O}_K)$ non nul comme dans l'énoncé.

(iii) Comme x est non nul et dans $\mathcal{O}_K$, sa norme $\mathrm{N}_{K/\mathbb{Q}}(x) = \prod_i \sigma_i(x)$ est un entier non nul : il est donc ≥ 1 en valeur absolue. On en déduit $1 \leq |\sigma_1(x)|/2^{n-1}$, puis l'énoncé (on a utilisé $|\sigma_i(x)| \leq 1/2$ pour $i > 1$).

(iv) Par le (iii), on a $|\sigma_1(x)| \neq |\sigma_i(x)|$ pour $i \neq 1$, le (i) entraîne donc $K = \mathbb{Q}(x)$.

(v) Le $n-i$-eme coefficient du polynome caractéristique de x est majoré par $\binom{n}{i} M^i$ où $M = 2^{n-1}\sqrt{d}$ (ses racines sont $\leq M$ en valeur absolue). Comme ce polynôme caractéristique est à coefficients entiers, il vit dans un ensemble fini ne dépendant que de n et d. Mais x en est une racine : il n'y a qu'un nombre fini de possibilités pour x. D'arès le (iv), il n'y a qu'un nombre fini de possibilités pour K.

Problème 3. (i) D'après le cours, on a $R \in \mathbb{Z}[X]$ (unitaire) et l'anneau $\mathbb{Z}[x]$ est isomorphe au quotient de $\mathbb{Z}[X]$ par (R). Se donner un morphisme d'anneaux $\mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}$ est donc équivalent à se donner un morphisme d'anneaux $\varphi : \mathbb{Z}[X] \to \mathbb{Z}/p\mathbb{Z}$ vérifiant $\varphi(R) = 0$. Les morphismes d'anneaux $\varphi : \mathbb{Z}[X] \to \mathbb{Z}/p\mathbb{Z}$ sont clairement ceux de la forme $P(X) \mapsto P(a)$ avec $a \in \mathbb{Z}/p\mathbb{Z}$: il y en a donc exactement p. Un tel morphisme d'annule sur R si, et seulement si, on a $R(a) = 0$, c'est à dire si a est racine de R dans $\mathbb{Z}/p\mathbb{Z}$.

(ii) Par hypothèse $\mathcal{O}_K/P_i$ a p éléments, ce qui entraîne $\mathcal{O}_K/P_i \simeq \mathbb{Z}/p\mathbb{Z}$ (par exemple, c'est un corps de caractéristique p à p éléments...). On dispose donc d'un morphisme d'anneaux surjectif $\varphi_i : \mathcal{O}_K \to \mathcal{O}_K/P_i \to \mathbb{Z}/p\mathbb{Z}$, dont le noyau est P_i. Ces φ_i sont distincts car leurs noyaux le sont.

(iii) Ainsi, on a $|\mathrm{Hom}(\mathcal{O}_K, \mathbb{Z}/p\mathbb{Z})| \geq r$ par le (ii), et si $\mathcal{O}_K$ est de la forme $\mathbb{Z}[x]$ on a $|\mathrm{Hom}(\mathcal{O}_K, \mathbb{Z}/p\mathbb{Z})| \leq p$ par le (i) (au pire des cas, tous les éléments de $\mathbb{Z}/p\mathbb{Z}$ sont racines, et il y en a p...). On a donc bien $r \leq p$.

(iv) Par définition $\mathrm{N}_{K/\mathbb{Q}}(t-x)$ est le déterminant de l'endomorphisme K de multiplication par $t-x$, soit encore $\det(t\mathrm{id} - \mathrm{m}_x)$. On reconnaît $\chi_{x,K/\mathbb{Q}}(t)$. Mais comme on a $K = \mathbb{Q}(x)$, on a aussi $R = \chi_{x,K/\mathbb{Q}}$ d'après le cours.

(v) On a $\mathrm{Tr}_{K/\mathbb{Q}} = \sum_i \sigma_i$ où les σ_i parcourent les $[K : \mathbb{Q}]$ plongements de K. Comme $K = \mathbb{Q}(x)$, les $\sigma_i(x) = x_i$ sont exactement les conjugués de x sur $\mathbb{Q}$ (et il y en a $[K : \mathbb{Q}]$), i.e. $R(t) = \prod_i (t - x_i)$. Ainsi, la trace cherchée est $\sum_i \sigma_i(\frac{1}{1-x}) = \sum_i \frac{1}{1-x_i}$. On conclut par la formule bien connue $R'(t)/R(t) = \sum_i 1/(t - x_i)$. Notez que x, et donc tous les x_i sont différents de 1.

(vi) Le polynôme $R(t) = t^3 - t - 8$ est de degré 3, donc s'il est réductible il a une racine n dans $\mathbb{Q} \cap \overline{\mathbb{Z}} = \mathbb{Z}$. Mais $n^3 - n = 8$ est impossible pour n dans $\mathbb{Z}$ (regarder mod 3). Donc R est irréductible et $[K : \mathbb{Q}] = \deg R = 3$.

(vii) Soit Q un idéal premier de $\mathcal{O}_K$ contenant 2, il contient donc $2 \cdot 4 = 8 = \alpha(\alpha-1)(\alpha+1)$. Comme Q est premier, il contient $\alpha, \alpha+1$ ou $\alpha-1$. Mais $\alpha - 1 = \alpha + 1 - 2$, donc il contient $\alpha - 1$ si et seulement si il contient $\alpha + 1$. Comme $1 = (\alpha+1) - \alpha$ il ne peut contenir à la fois $\alpha+1$ et α (par convention on a $Q \neq \mathcal{O}_K$).

(viii) Par le (iv) on a $\mathrm{N}_{K/\mathbb{Q}}(2-\alpha) = R(2) = -2$. D'après le cours on a $\mathrm{N}(2-\alpha) = |\mathrm{N}_{K/\mathbb{Q}}(2-\alpha)| = 2$.

(ix) D'après le théorème de Dedekind, un idéal de norme première est forcément premier. Donc P est premier. Réciproquement, si un idéal premier contient 2 et α, il contient $P = (2-\alpha)$, qui est maximal (car premier non nul), et donc on a $P = (2-\alpha)$.

(x) D'après le (iv) on a $\mathrm{N}_{K/\mathbb{Q}}(\pm 1 - \alpha) = -8$, donc $\mathrm{N}_{K/\mathbb{Q}}(\alpha \pm 1) = (-1)^3 . -8 = 8$. Ainsi, l'idéal $(\alpha \pm 1)$ est de norme 8. Ses facteurs premiers divisent donc 2, et contiennent $\alpha \pm 1$. Par hypothèse, il y a un seul tel premier, à savoir Q, et donc $(\alpha \pm 1)$ est une puissance de Q. Par multiplicativité de la norme, c'est la même puissance dans les deux cas.

(xi) On a $aA \subset bA$ si, et seulement si, b divise a quand A est intègre. On a donc $\beta \in \mathcal{O}_K$ par le (x).

(xii) On a $\beta = \frac{1+\alpha}{1-\alpha} = \frac{2}{1-\alpha} - 1$. Sa trace est donc $-2 \cdot 2/8 - 3 = -7/2$ par le (v).

(xiii) Cette trace n'est pas entière, donc β n'est pas dans $\mathcal{O}_K$. Donc il existe au moins deux idéaux premiers de $\mathcal{O}_K$ contenant 2 et $\alpha + 1$, disons Q_1 et Q_2.

(xiv) Par le (vii), (x) et (xiii), les trois idéaux P, Q_1 et Q_2 sont premiers distincts et contiennent 2 (donc sont de norme ≥ 2). Donc PQ_1Q_2 divise (2). Mais la norme de 2 est $2^3 - 8$ par le (vi), cela montre que $\mathrm{N}(P)\mathrm{N}(Q_1)\mathrm{N}(Q_2)$ divise 8, ce qui entraîne $\mathrm{N}(P) = \mathrm{N}(Q_1) = \mathrm{N}(Q_2) = 2$, puis $(2) = PQ_1Q_2$ (on a utilisé la propriété de Dedekind et la multiplicativité de la norme).

(xv) On a au moins 3 idéaux premiers de norme 2 dans $\mathcal{O}_K$: c'est impossible si $\mathcal{O}_K = \mathbb{Z}[x]$ par le (iii).

(xvi) Le (ix) montre $(\alpha) = P^3$.

(xvii) Les idéaux premiers contenant $\alpha + 1$ (resp. $\alpha - 1$) contiennent 2, et sont Q_1 et Q_2, donc Q_1Q_2 divise $\alpha + 1$ et $\alpha - 1$. De plus, $(\alpha + 1) \neq (\alpha - 1)$ par l'argument déjà donné au (xii).

(xviii) On en déduit que $(\alpha(\alpha+1)) = (2)P^2Q_1$, puis $\gamma := \alpha(\alpha+1)/2$ dans $\mathcal{O}_K$.

(xix) Soit $L = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\gamma$. On a montré $\mathcal{O}_K \supset L = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\gamma \supset \mathbb{Z}[\alpha]$. Mais $\operatorname{disc}\mathbb{Z}[\alpha] = \operatorname{disc}(t^3 - t - 8) = 4 - 27 \cdot 8^2 = -1724 = -4 \cdot 431$. Comme $\mathbb{Z}[\alpha]$ est d'indice 2 dans L on en déduit $\operatorname{disc}L = -431$, qui est premier en valeur absolue, donc $L = \mathcal{O}_K$ par le cours (les indices au carré divisent le discriminant).

(xx) $\mathcal{O}_K/2\mathcal{O}_K$ admet pour $\mathbb{Z}/2\mathbb{Z}$-base les classes de 1, α et γ. On a $\alpha^2 = \alpha(\alpha+1) - \alpha \equiv \alpha \bmod 2$, $\alpha\gamma = (\alpha+1-1)\alpha(\alpha+1)/2 = 4+\gamma \equiv \gamma \bmod 2$ et $\gamma^2 = \alpha(\alpha-1+2)\alpha(\alpha+1)/4 = 2\alpha+\alpha\gamma \equiv \alpha\gamma \bmod 2$. Ainsi, si x et y désignent les classes de α et γ modulo 2 on a $x^2 = x$ et $y^2 = y = xy$. Notons A l'anneau $\mathcal{O}_K/2\mathcal{O}_K$. Cela montre que dans l'anneau fini $A := \mathcal{O}_K/2\mathcal{O}_K$ tout élément u vérifie $u^2 = u$. Cela implique (anneau de Boole) que A est isomorphe à l'anneau produit $(\mathbb{Z}/2\mathbb{Z})^m$ nécessairement pour $m = 3$. De manière plus directe, on constate que l'on a $xA = \mathbb{Z}/2\mathbb{Z}x \oplus \mathbb{Z}/2\mathbb{Z}y$ et $(1-x)A = \mathbb{Z}/2\mathbb{Z}(1-x)$, avec $xA(1-x)A = 0$ et $x(y+x) = 0$. L'application $(u,v,w) \mapsto ux + v(y+x) + w(1-x)$ est donc un isomorphisme d'anneaux $(\mathbb{Z}/2\mathbb{Z})^3 \to A$.

Annexe C

Quelques nombres premiers

2	3	5	7	11	13	17	19
23	29	31	37	41	43	47	53
59	61	67	71	73	79	83	89
97	101	103	107	109	113	127	131
137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223
227	229	233	239	241	251	257	263
269	271	277	281	283	293	307	311
313	317	331	337	347	349	353	359
367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457
461	463	467	479	487	491	499	503
509	521	523	541	547	557	563	569
571	577	587	593	599	601	607	613
617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719
727	733	739	743	751	757	761	769
773	787	797	809	811	821	823	827
829	839	853	857	859	863	877	881
883	887	907	911	919	929	937	941
947	953	967	971	977	983	991	997

TABLE 1. Les nombres premiers < 1000

Bibliographie

[Ca] H. Cartan, *Théorie élémentaire des fonctions analytiques d'une ou plusieurs variables*, Hermann (1964).

[C] D. A. Cox, *Primes of the form* $x^2 + ny^2$, Wiley (1989).

[D] H. Davenport, *Multiplicative number theory*, lectures in adv. math. (1967).

[G] K. F. Gauss, *Disquisitiones Arithmeticae*, réédité aux éditions Jacques Gabay (1801).

[H] D. Hilbert, *The theory of algebraic number fields*, Springer monographs in math. (2003). Réédition de *Zahlbericht* (1897).

[I-R] K. Ireland & M. Rosen, *A classical introduction to modern number theory*, Springer GTM 84 (1972).

[L] S. Lang, *Algebra*, 3^{eme} édition, Addison-Wesley (1993).

[M] D. Marcus, *Number fields*, Springer Universitext (1977).

[P] D. Perrin, *Cours d'algèbre*, Ellipse.

[S] P. Samuel, *Théorie algébrique des nombres*, Hermann (1971).

[Se] J.-P. Serre, *Cours d'arithmétique*, P.U.F. (1977).

[S-T] I. Stewart & D. Tall, *Algebraic number theory*, Chapman & Hall (1979).

[Sw] H. P. F. Swinnerton-Dyer, *A brief guide to algebraic number theory*, London Math Soc. student texts **50** (2001).