Cours de maîtrise de mathématiques : “Théorie algébrique des nombres”

Bas Edixhoven, Université de Rennes 1

janvier 2002

Ce texte est une version (légèrement) corrigée et agrandie (d’une section sur le théorème de Wedderburn) du polycopié de 2001. Le polycopié de 2001 était une version réorganisée du texte qui a été distribué en mai 2000. Le texte de mai 2000 était consitué des notes de cours que l’auteur avait écrit pour lui-même, sans avoir l’intention d’en faire un polycopié. Mais vu le temps investi, il lui a semblé quand-même utile d’en faire une version présentable. Néanmoins, le résultat est moins détaillé que le cours. Pour plus de détails, on pourra consulter les livres mentionnés dans la bibliographie, et surtout [Samuel].

Table des matières

1 L'équation de Fermat.

1.1 Introduction.

Nous suivrons le livre de Samuel [Samuel] d'assez près, en complétant par des références au livre de Cohen [Cohen] pour des résultats algorithmiques. En même temps, nous essayerons de motiver le plus possible, par des exemples simples, l'introduction des notions techniques. C'est pour cela que nous commençons par regarder l'équation de Fermat :

$$x^n + y^n = z^n.$$

Dans cette équation, n est un entier, plus grand ou égal à un, et le problème qui se pose est de trouver, pour n donné, toutes les solutions de cette équation, c'est à dire, tous les triplets (a, b, c) dans $\mathbb{Z}^3$ tels que $a^n + b^n = c^n$. Avant de dire quoi que ce soit sur ce problème particulier, remarquons que ce problème garde un sens si on remplace $\mathbb{Z}$ par n'importe quel anneau (les anneaux seront commutatifs et unitaires dans ce cours, sauf mention explicite contraire). En effet, l'ensemble des solutions dans A^3, pour A un anneau, est simplement l'ensemble des racines du polynôme $x^n + y^n - z^n$ dans A^3. Plus tard aujourd'hui, nous allons considérer l'anneau $\mathbb{C}[t]$.

Si $\phi\colon A \to B$ est un morphisme d'anneaux et (a, b, c) dans A^3 une solution de l'équation de Fermat de degré n ci-dessus, alors $(\phi(a), \phi(b), \phi(c))$ dans B^3 est également une solution de la même équation. En fait, cette dernière propriété est vraie pour tout système d'équations polynomiales à coefficients dans $\mathbb{Z}$.

L'équation de Fermat est homogène : tous les monômes y intervenant ont même degré. Une autre façon de dire cela est : si A est un anneau, (a, b, c) dans A^3 et λ dans A non diviseur de zéro, alors (a, b, c) est une solution si et seulement si $(\lambda a, \lambda b, \lambda c)$ l'est. Géométriquement, cela s'exprime en disant que l'ensemble des solutions est un cône, et (au moins sur un corps) la propriété pour (a, b, c) d'être une solution ne dépend que de la "droite" $A(a, b, c)$, donc que de l'image de (a, b, c) dans le "plan projectif" sur A. En général, quand on considère des systèmes d'équations polynomiales homogènes, on a intérêt à considérer les solutions dans l'espace projectif correspondant, car cela fait baisser la dimension du problème (c'est à dire, le nombre de variables) d'un.

L'homogénéité de l'équation de Fermat entraîne également une relation entre les ensembles de solutions dans $\mathbb{Z}$ et dans $\mathbb{Q}$, que nous allons maintenant expliquer.

Pour $r \geq 0$, un élément $(a_1, \ldots, a_r)$ de $\mathbb{Z}^r$ est dit *primitif* si $\mathrm{pgcd}(a_1, \ldots, a_r) = 1$. En particulier, un élément primitif de $\mathbb{Z}^r$ est non nul, et tout a non nul dans $\mathbb{Z}^r$ est de la forme da', avec d dans $\mathbb{Z}$ et a' primitif (d est alors un pgcd des a_i). Le groupe $\mathbb{Z}^* = \{1, -1\}$ des éléments inversibles de $\mathbb{Z}$ opère par homothéties sur l'ensemble $\mathrm{Prim}(\mathbb{Z}^r)$ des éléments primitifs de $\mathbb{Z}^r$, et on nous noterons $\mathbb{P}(\mathbb{Z}^r)$ le quotient $\mathrm{Prim}(\mathbb{Z}^r)/\mathbb{Z}^*$. Ceci est l'analogue sur $\mathbb{Z}$ de la définition usuelle de l'espace projectif $\mathbb{P}(\mathbb{Q}^r) := (\mathbb{Q}^r - \{0\})/\mathbb{Q}^*$. Avec ces définitions, on a la proposition suivante.

1.1.1 Proposition. *L'inclusion de* $\mathrm{Prim}(\mathbb{Z}^r)$ *dans* $\mathbb{Q}^r - \{0\}$ *induit une bijection entre* $\mathbb{P}(\mathbb{Z}^r)$ *et* $\mathbb{P}(\mathbb{Q}^r)$.

La vérification est laissée comme exercice ; disons seulement que l'application inverse est obtenue comme suite : pour a non nul dans $\mathbb{Q}^r$, on prend un dénominateur commun d des a_i, c'est à dire un d dans $\mathbb{Z}$ non nul tel que les da_i sont entiers, et on écrit $da = ea'$ avec e dans $\mathbb{Z}$ et a' dans $\mathbb{Z}^r$ primitif. (Une autre façon de construire l'application inverse est de montrer que pour $a \neq 0$ dans $\mathbb{Q}^r$ l'intersection $\mathbb{Q}{\cdot}a \cap \mathbb{Z}^r$ est un $\mathbb{Z}$-module libre de rang un, et d'en prendre les deux générateurs ; voir la section 9.)

Soit maintenant $n \geq 1$. Notons X l'ensemble des solutions primitives dans $\mathbb{Z}^3$ de l'équation $x^n + y^n = z^n$, et Y l'ensemble des solutions non nulles dans $\mathbb{Q}^3$ de l'équation $x^n + y^n = z^n$. Le groupe $\mathbb{Z}^* = \{1, -1\}$ des inversibles de $\mathbb{Z}$ opère par homothéties sur X, et, de la même façon, $\mathbb{Q}^*$ opère sur Y. Soient $\overline{X} := X/\mathbb{Z}^*$ et $\overline{Y} := Y/\mathbb{Q}^*$ les quotients de ces actions. Alors la proposition précédente implique que l'inclusion de X dans Y induit une bijection de $\overline{X}$ vers $\overline{Y}$.

1.2 L'équation de Fermat, degré 1.

Il n'y a pas grand chose à dire. Pour A n'importe quel anneau, (a, b, c) dans A^3 est une solution si et seulement si $c = a + b$. Autrement dit, nous avons une bijection de A^2 vers l'ensemble des solutions, qui envoie (a, b) vers $(a, b, a + b)$.

1.3 L'équation de Fermat, degré 2, sur $\mathbb{Z}$.

Ici, nous suivons [Samuel, §1.2]. Il s'agit maintenant de l'équation :

$$x^2 + y^2 = z^2.$$

Les solutions (a, b, c) avec a, b et c des entiers positifs et abc non nul, sont appelés des triplets pythagoriciens. Notons que de toute façon, (a, b, c) dans $\mathbb{Z}^3$ est une solution si et seulement si tous les triplets $(\pm a, \pm b, \pm c)$ sont des solutions. Il nous suffit de trouver toutes les solutions dans $\mathbb{N}^3$. Nous allons classifier les triplets pythagoriciens primitifs, à l'aide de la factorialité de l'anneau $\mathbb{Z}$. Comme l'équation que nous considérons est homogène, c'est à dire que tous les termes ont même degré, toute solution (a, b, c) dans $\mathbb{Z}^3$ avec $abc \neq 0$ est de la forme $(\pm da', \pm db', \pm dc')$, avec d dans $\mathbb{N}$ non nul, et (a', b', c') un triplet pythagoricien primitif. On procède par les étapes suivantes.

1. Soit (a, b, c) un triplet pythagoricien. Les conditions suivantes sont équivalentes :
   (a) $\mathrm{pgcd}(a, b, c) = 1$,
   (b) $\mathrm{pgcd}(a, b) = 1$,
   (c) $\mathrm{pgcd}(a, c) = 1$,
   (d) $\mathrm{pgcd}(b, c) = 1$.

   (En effet, si (a, b, c) est pythagoricien et si par exemple un nombre premier p divise a et b, alors p divise $a^2 + b^2$, donc c^2, donc c.)
2. Soit (a, b, c) un triplet pythagoricien primitif. Alors c est impair, et l'un d'entre a et b est pair (pour le voir, on utilise que les carrés dans $\mathbb{Z}/4\mathbb{Z}$ sont 0 et 1).

3. Soit (a, b, c) un triplet pythagoricien primitif avec b pair. En écrivant

$$(b/2)^2 = ((c-a)/2)((c+a)/2),$$

on montre qu'il existe u et v dans $\mathbb{N}$, premiers entre eux, tel que $0 < u < v$, $(c-a)/2 = u^2$ et $(c+a)/2 = v^2$. (En effet, $(c-a)/2$ et $(c+a)/2$ sont premiers entre eux car l'idéal qu'ils engendrent contient c et a, donc 1, et leur produit est un carré.) On conclut que les triplets pythagoriciens primitifs avec b pair sont les triplets $(v^2 - u^2, 2uv, v^2 + u^2)$, avec $0 < u < v$ premier entre eux et uv pair.

Une autre façon de faire la liste de tous les triplets pythagoriciens est la suivante, que l'on pourrait appeler "paramétrisation rationnelle du cercle". A un triplet pythagoricien (a, b, c) on fait correspondre le point $(a/c, b/c)$ du cercle C dans $\mathbb{R}^2$ de rayon un et de centre 0. Un élément de C est dit rationnel si ses deux coordonnées sont rationnelles. En considérant les droites passant par $(-1, 0)$, on montre que tout autre point rationnel de C est de la forme

$$((1-t^2)/(1+t^2), 2t/(1+t^2)),$$

avec t dans $\mathbb{Q}$ (t étant la pente de la droite considérée). En effet, pour t dans $\mathbb{R}$ notons D_t la droite dans $\mathbb{R}^2$ qui passe par $(-1, 0)$ et qui est de pente t, et notons $(x(t), y(t))$ le deuxième point d'intersection de D_t avec le cercle C. Alors t est rationnelle si et seulement si $(x(t), y(t))$ l'est (si $(x(t), y(t))$ est rationnelle, D_t contient deux points rationnels, donc sa pente est rationnelle, si t est rationnelle, le deuxième point d'intersection est de la forme $(-1, 0) + \lambda(1, t)$ avec λ dans $\mathbb{R}$ solution d'une équation de degré deux à coefficients rationnels et avec une racine rationnelle ; un petit calcul donne la formule en haut). En écrivant $t = u/v$ avec u et v des entiers premiers entre eux, on obtient de nouveau la classification des triplets pythagoriciens primitifs obtenue en haut.

1.4 L'équation de Fermat, degré $n \geq 3$, sur $\mathbb{C}[t]$.

En 1993, Andrew Wiles a montré qu'il n'y a pas de solutions non triviales dans $\mathbb{Z}^3$. Malheureusement, la démonstration est beaucoup trop difficile pour l'expliquer dans ce cours. Pour ceux qui veulent voir comment cela marche, voir par exemple le livre de Cornell, Silverman et Stevens [CSS], ou les deux exposés au Séminaire Bourbaki par Serre et Oesterlé, en juin 1995, ou le numéro 22 du magazine "Quadrature", été 1995 (Editions du choix, Argenteuil). Signalons aussi que Kummer, au 19ème siècle, avait déjà démontré le théorème de Fermat pour de nombreux exposants premiers.

Ce que nous pouvons faire avec les techniques à notre disposition, est résoudre ces équations dans l'anneau $\mathbb{C}[t]$.

1.4.1 Théorème. *Soit $n \geq 3$ entier. Si a, b et c dans $\mathbb{C}[t]$ satisfont $a^n + b^n = c^n$ et sont premiers entre eux ($\mathrm{pgcd}(a, b, c) = 1$), alors a, b et c sont de degré zéro, c'est à dire, sont dans $\mathbb{C}$.*

Preuve. La méthode s'appelle "la descente infinie". Supposons donc qu'il existe au moins une solution primitive non constante. Soit alors (a, b, c) une telle solution où le maximum des degrés de a, b et c est minimal. Notons tout d'abord que a, b et c sont premiers entre eux deux par deux, tous non nuls, et qu'au plus un d'entre eux est constant. On a :

$$a^n = c^n - b^n = \prod_{\zeta^n=1} (c - \zeta b).$$

Les facteurs $c - \zeta b$ sont premiers entre eux, deux par deux, car chaque pair d'entre eux forme une base du sous-$\mathbb{C}$-espace vectoriel de $\mathbb{C}[t]$ engendré par b et c (notons que ce sous-espace est de dimension deux car b et c sont non nuls, premiers entre eux et pas tous les deux constant). Par la factorialité de $\mathbb{C}[t]$, nous obtenons que les $c - \zeta b$ sont des puissances $n$ièmes, à des inversibles près. Mais les inversibles sont les constants non nuls, qui sont eux-mêmes des puissances $n$ièmes. Il existe donc des x_ζ dans $\mathbb{C}[t]$ tels que

$$c - \zeta b = x_\zeta^n.$$

Comme les $c - \zeta b$ sont premiers entre eux deux par deux, les x_ζ le sont également. En considérant les termes dominants de c et de b, on voit qu'au plus un des x_ζ est constant. Prenons maintenant n'importe triplet x, y, et z parmi les x_ζ (cela est possible parce que n est au moins 3). Comme x^n, y^n et z^n appartiennent au sous-espace de $\mathbb{C}[t]$ engendre par b et c, il y a une relation linéaire non triviale parmi eux, disons :

$$\alpha x^n + \beta y^n = \gamma z^n,$$

avec α, β et γ dans $\mathbb{C}$, ne pas tous nuls. Mais comme chaque élément de $\mathbb{C}$ est une puissance $n$ième, nous trouvons, en choisissant des racines $n$ièmes de α, β et γ, une relation :

$$x_1^n + y_1^n = z_1^n,$$

avec x_1, y_1 et z_1 premiers entre eux deux à deux, ne pas tous constants, et de même degré que x, y et z, respectivement. Mais cela contredit la minimalité en termes des degrés de la solution (a, b, c) de départ. $\square$

Avant de continuer, notons que nous avons utilisé que l'anneau $\mathbb{C}[t]$ est factoriel, et que tout inversible de $\mathbb{C}[t]$ est une puissance $n$ième. Ce sont exactement ces deux propriétés qui posent un problème pour les anneaux $\mathbb{Z}[e^{2\pi i/n}]$. Le défaut de non factorialité de tels anneaux, ainsi que leurs groupes multiplicatifs, seront étudiés plus tard dans ce cours. Signalons aussi que la méthode qui a conduit à une preuve du théorème de Fermat n'est pas d'étudier en grand détail les anneaux $\mathbb{Z}[e^{2\pi i/n}]$, mais plutôt des anneaux de la forme $\mathbb{Z}[x, y]/(y^2 = x^3 + ax + b)$, c'est à dire, des courbes elliptiques.

Pour montrer que l'on sait démontrer des résultats généraux, citons le suivant, cas spécial d'un théorème de Faltings, auparavant conjecture de Mordell (voir par exemple [Serre1]).

1.4.2 Théorème. *Soit F dans $\mathbb{Q}[x, y, z]$ homogène de degré au moins 4, tel que les dérivées $\partial F/\partial x$, $\partial F/\partial y$ et $\partial F/\partial z$ ne s'annulent pas en un même point de $\mathbb{C}^3 - \{0\}$. Alors l'ensemble $\{(a, b) \in \mathbb{Q}^2 \mid F(a, b, 1) = 0\}$ est fini.*

Ce qui est intéressant dans ce résultat est la condition sur le degré. Le fait que ce degré doit être au moins 4 correspond au fait que la variété des solutions dans $\mathbb{P}(\mathbb{C}^3)$ est une surface compacte connexe et orientable dont le genre (i.e., le nombre de trous) est au moins deux.

1.5 L'équation de Fermat, degré 4, sur $\mathbb{Z}$.

Ici nous suivons [Samuel, §1.2]. Nous allons montrer :

Soient x, y et z dans $\mathbb{Z}$ tels que $x^4 + y^4 = z^2$. Alors $xyz = 0$.

Supposons donc que cet énoncé soit faux, et soit (x, y, z) dans $\mathbb{N}^3$ avec $x^4 + y^4 = z^2$, $xyz \neq 0$, et z minimal. Pour obtenir une contradiction, on procède par les étapes suivantes, où l'on applique ce que nous savons déjà des triplets pythagoriciens (car (x^2, y^2, z) est un tel triplet).

1. x, y et z sont deux à deux premiers entre eux.
2. Après permutation, si nécessaire, de x et y, on a x et z impairs, y pair. Il existe u et v dans $\mathbb{N}$, premiers entre eux, avec $u > v$, tels que :

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

La première équation dit que $x^2 + v^2 = u^2$; comme x est impair, v est pair. La deuxième équation dit que $(y/2)^2 = uv_1$, donc il existe a et b dans $\mathbb{N}$ tels que $u = a^2$ et $v_1 = b^2$. De la première équation on tire qu'il existe c et d dans $\mathbb{N}$, premiers entre eux, tels que :

$$x = c^2 - d^2, \quad v = 2cd, \quad u = c^2 + d^2.$$

La deuxième de ces équations dit que $b^2 = cd$, donc que c et d sont des carrés, disons $c = e^2$ et $d = f^2$ avec e et f dans $\mathbb{N}$. Comme $u = a^2$, on a :

$$e^4 + f^4 = a^2,$$

et comme $a^2 = u$ et $z > u^2$, on a $z > u^2 \geq a^4 \geq a$. Contradiction avec la minimalité de z.

1.6 L'équation de Fermat, degré 3, sur $\mathbb{Z}$.

Ceci n'est pas fait dans [Samuel]. Nous suivons [I-R, §17.8]. La méthode est toujours la même : factoriser après adjonction des racines 3èmes de l'unité, et descente infinie. Nous commençons par quelques résultats sur le sous-anneau $A := \mathbb{Z}[j]$, avec $j^2 + j + 1 = 0$, de $\mathbb{C}$.

1.6.1 Proposition. *La conjugaison complexe $z \mapsto \overline{z}$ induit sur A un automorphisme d'anneau. L'application $N\colon A \to \mathbb{N}$, $a \mapsto a\overline{a} = |a|^2$ est multiplicative et s'appelle la norme de la $\mathbb{Z}$-algèbre A. L'anneau A est euclidien pour la fonction N ; A est donc factoriel. Le groupe A^* de ses éléments inversibles est $\{\pm 1, \pm j, \pm j^2\}$, et est cyclique d'ordre 6. L'élément $\lambda := 1 - j$ de A est premier, et le quotient $A/\lambda A$ est un corps à trois éléments. Une factorisation de 3 dans A est la suivante : $3 = -j^2\lambda^2$.*

Preuve. Comme A est un sous-anneau de $\mathbb{C}$, A est intègre. Pour voir que $N\colon A \to \mathbb{C}$, $a \mapsto |a|^2$ prend ses valeurs dans $\mathbb{Z}$, faisons le calcul suivant :

$$N(n + mj) = (n + mj)(n + mj^2) = n^2 + nm(j + j^2) + m^2 = n^2 - nm + m^2.$$

C'est donc vrai que N prend ses valeurs dans $\mathbb{N}$. Pour montrer que A est euclidien pour la fonction N, il faut montrer que pour tous a et b dans A avec b non nul, il existe q et r dans A avec $a = qb + r$ et $N(r) < N(b)$. Soient a et b dans A, avec $b \neq 0$. Soit q alors un des éléments de A le plus proche de a/b. Alors on a :

$$|a/b - q| \leq 1/\sqrt{3} < 1.$$

(Pour l'expliquer, faire un dessin du réseau A dans $\mathbb{C}$; ce réseau est l'ensemble des sommets d'un pavage de $\mathbb{C}$ par des triangles de cotés un.) Posons $r := a - qb$. On alors :

$$|r| = |a - qb| = |b| \cdot |a/b - q| < |b|,$$

d'où $N(r) = |r|^2 < |b|^2 = N(b)$.

Soit a dans A. Alors a est inversible si et seulement s'il existe b dans A tel que $ab = 1$. En particulier, si a est dans A^*, il existe b dans A tel que $1 = N(1) = N(ab) = N(a)N(b)$, d'où $N(a) = 1$. D'autre part, si a est dans A et $N(a) = 1$, on a $1 = a\overline{a}$, donc a est dans A^* (et $a^{-1} = \overline{a}$). Les inversibles de A sont les a dans A avec $N(a) = 1$, c'est à dire, les a dans l'intersection de A et le cercle unité.

Pour voir ce qu'est $A/\lambda A$, notons que $A = \mathbb{Z}[t]/(t^2+t+1)$, ce qui nous donne un morphisme surjectif $A \to \mathbb{F}_3$, en envoyant t vers 1 (en effet, l'image de t^2+t+1 est alors 0). Par construction, l'image de λ dans $\mathbb{F}_3$ est nulle, donc le morphisme $A \to \mathbb{F}_3$ se factorise par $A/\lambda A$ ce qui donne une surjection de $A/\lambda A$ sur $\mathbb{F}_3$. Le fait que $N(\lambda) = 3$ implique que λ est irréductible, donc premier (car A euclidien donc factoriel). Mais alors $A/\lambda A$ est un corps (c'est le quotient d'un anneau principal par un idéal premier non nul), donc le morphisme $A/\lambda A \to \mathbb{F}_3$ est injectif, et donc un isomorphisme.

Calculons : $\lambda^2 = (1-j)^2 = 1 - 2j + j^2 = 1 + j + j^2 - 3j = -3j$. □

Faisons quelques exemples de factorisation dans A. Factorisons par exemple $3 + j$ et $4 - j$. D'abord, $N(3+j) = 3^2 - 3 + 1 = 7$ est premier, donc $3+j$ est premier, ainsi que $\overline{3+j} = 2 - j$. La factorisation de $4 - j$ est plus intéressante. On a $N(4-j) = 4^2 + 4 + 1 = 21 = 3{\cdot}7$. On essaie alors de diviser $4 - j$ par un élément de norme 3, par exemple $1 - j$. On trouve :

$$\frac{4-j}{1-j} = \frac{4-j}{1-j} \cdot \frac{1-j^2}{1-j^2} = \frac{4 - 4j^2 - j + 1}{3} = 3 + j.$$

Comme $3+j$ est premier, on a la factorisation $4 - j = (1-j)(3+j)$ en éléments premiers de A.

1.6.2 Lemme. *Les puissances troisièmes dans $A/9A = A/\lambda^4 A$ sont $0, \pm 1, \pm\lambda^3$.*

Preuve. Comme $A/\lambda A = \mathbb{F}_3$, tout élément de A est d'une des formes $1 + \lambda a$, $-1 + \lambda a$, λa (avec a dans A). On calcule les puissances troisièmes de ces bêtes, en utilisant que même les a en haut s'écrivent encore sous la forme $a_1 + \lambda a'$ avec a_1 dans $\{0, 1, -1\}$ (et on utilise le "petit théorème de Fermat"). □

Nous allons montrer un résultat plus fort que l'énoncé que pour tout (x, y, z) dans $\mathbb{Z}^3$ avec $x^3 + y^3 = z^3$ on ait $xyz = 0$; cela est nécessaire pour faire la descente infinie. Cette fois, la descente sera en termes de divisibilité par λ.

1.6.3 Notation. Soit A un anneau factoriel, a dans A non nul, et p dans A premier. Nous notons alors $v_p(a)$ le nombre de facteurs p dans la décomposition de A en facteurs irréductibles. Plus précisément, on a $a = p^{v_p(a)}a'$, avec p ne pas divisant a'. (On utilise la lettre v pour valuation.)

1.6.4 Théorème. *Supposons que x, y et z sont dans A et que u est dans A^* tels que $x^3+y^3 = uz^3$. Alors $xyz = 0$.*

Preuve. Par contradiction. Supposons donc que x, y, z et u sont dans A, avec u dans A^*, $x^3 + y^3 = uz^3$ et $xyz \neq 0$. Par l'argument habituel, nous pouvons supposer que x, y et z sont deux à deux premiers entre eux.

Montrons que $\lambda | xyz$, et que si $\lambda | xy$, alors $u = \pm 1$. Supposons donc que $\lambda | xy$. Alors λ ne divise pas uz^3, donc on a $\pm 1 = \pm u$ dans $A/\lambda^3 A$. Cela veut dire que λ^3 divise $u-1$ ou $u+1$. Il en résulte que $u = \pm 1$. (Par exemple, on peut utiliser que $|u \pm 1| \leq 2$ tandis que $|\lambda^3| = 3\sqrt{3} > 2$.) Nous avons donc montré la deuxième assertion. Montrons la première. Supposons que λ ne divise pas xyz. Alors $\{x^3, y^3, z^3\} \subset \{1, -1\}$ dans $A/\lambda^4 A$. Mais alors on a $u = \pm 2$ dans $A/\lambda^4 A$. Cela veut dire que λ^4 divise $u-2$ ou $u+2$. Mais $1 \leq |u \pm 2| \leq 3$ tandis que $|\lambda^4| = 9$, ce qui est une contradiction.

Ceci nous ramène au cas où nous avons x, y, z et u dans A, avec u dans A^*, $x^3 + y^3 = uz^3$, et $\lambda | z$. Nous allons maintenant produire un tel quadruplet (x', y', z', u') avec $v_\lambda(z') < v_\lambda(z)$; c'est ça la contradiction cherchée. Allons-y.

Notons tout d'abord que dans $A/\lambda A$ nous avons $x^3 + y^3 = 0$, donc que $x + y = 0$ (dans $A/\lambda A$, bien sûr). Mais alors $x^3 + y^3 = 0$ dans $A/\lambda^4 A$ (utiliser ce que nous savons des cubes dans $A/\lambda^4 A$), donc $\lambda^4 | uz^3$, donc $\lambda^2 | z$. Nous écrivons maintenant :

$$(x+y)(x+jy)(x+j^2y) = x^3 + y^3 = uz^3.$$

Comme $\lambda^6 | uz^3$, au moins un des facteurs à gauche est divisible par λ^2 ; en remplaçant y par jy ou j^2y si nécessaire, on a $\lambda^2 | (x+y)$ (notons que ces substitutions ne changent pas z, ce qui est important pour notre argument).

Montrons qu'alors $v_\lambda(x+jy) = v_\lambda(x+j^2y) = 1$. Comme l'image de j dans $\mathbb{F}_3$ est 1, il est clair que λ divise $x + jy$ et $x + j^2y$. Supposons que $\lambda^2 | (x+jy)$. Alors $x + y = x + jy$ dans $A/\lambda^2 A$, donc $0 = (1-j)y = \lambda y$ dans $A/\lambda^2 A$. Comme y est dans A^*, cela entraîne que $\lambda^2 | \lambda$, ce qui est faux. De même pour $x + j^2y$: λ^2 ne divise pas $1 - j^2$. Nous avons donc :

$$v_\lambda(x+y) = 3v_\lambda(z) - 2, \quad v_\lambda(x+jy) = 1, \quad v_\lambda(x+j^2y) = 1.$$

Le fait que $\det\left(\begin{smallmatrix} 1 & 1 \\ 1 & j \end{smallmatrix}\right) = -\lambda$ montre que $(x+y)A + (x+jy)A = \lambda A$, et de même on trouve que $x+y$, $x+jy$ et $x+j^2y$ ont, deux à deux, plus grand commun diviseur λA. La factorialité de A donne l'existence d'éléments α, β et γ de A qui sont premiers à λ et premiers entre eux deux à deux, et d'éléments u_1, u_2 et u_3 de A^*, tels que :

$$x + y = u_1 \lambda^{3v_\lambda(z)-2}\alpha^3, \quad x + jy = u_2 \lambda \beta^3, \quad x + j^2y = u_3 \lambda \gamma^3.$$

La combinaison linéaire avec coefficients 1, j et j^2 de ces trois équations, divisée par λ, donne :

$$0 = u_1 \lambda^{3v_\lambda(z)-3}\alpha^3 + ju_2\beta^3 + j^2u_3\gamma^3.$$

On pose maintenant $x_1 := \beta$, $y_1 := \gamma$, et $z_1 := \lambda^{v_\lambda(z)-1}\alpha$. Alors on a, avec ε_1 et ε_2 dans A^* convenables :

$$x_1^3 + \varepsilon_1 y_1^3 = \varepsilon_2 z_1^3.$$

Comme $\lambda^3 | z_1^3$ (car $v_\lambda(z) \geq 2$), on a $\varepsilon_1 = \pm 1$ dans $A/\lambda^3 A$, ce qui montre que $\varepsilon_1 = \pm 1$ (dans A). En replaçant y_1 par $-y_1$ si nécessaire, on obtient donc :

$$x_1^3 + y_1^3 = \varepsilon_2 z_1^3,$$

avec $v_\lambda(z_1) = v_\lambda(z) - 1$. $\square$

2 L'anneau $\mathbb{Z}[i]$ et le théorème des deux carrés.

2.1 Un peu d'arithmétique dans $\mathbb{Z}[i]$.

Le but de cette section est d'abord de comprendre comment se factorisent les nombres premiers dans $\mathbb{Z}[i]$, et d'appliquer le résultat pour déterminer quels entiers sont somme de deux carrés. Les résultats de cette section se trouvent dans [Samuel, §5.6], mais y sont démontrés de façon moins élémentaire.

2.1.1 Proposition. *La conjugaison complexe $z \mapsto \overline{z}$ induit sur $\mathbb{Z}[i]$ un automorphisme d'anneau. L'application $N\colon \mathbb{Z}[i] \to \mathbb{N}$, $a \mapsto a\overline{a} = |a|^2$ est multiplicative et s'appelle la norme de la $\mathbb{Z}$-algèbre $\mathbb{Z}[i]$. L'anneau $\mathbb{Z}[i]$ est euclidien pour la fonction N ; $\mathbb{Z}[i]$ est donc factoriel. Le groupe $\mathbb{Z}[i]^*$ de ses éléments inversibles est $\{\pm 1, \pm i\}$, et est cyclique d'ordre 4.*

La démonstration est analogue à celle que nous avons déjà faite pour $\mathbb{Z}[j]$.

2.1.2 Théorème. *Soit p un nombre premier. Alors p est encore premier dans $\mathbb{Z}[i]$ si et seulement si $p = -1$ modulo 4. Pour 2 on a : $2 = (1+i)(1-i) = i(1-i)^2$. Un nombre premier p congru à 1 modulo 4 se factorise comme : $p = (a+bi)(a-bi)$, en deux facteurs premiers non associés. Les éléments premiers de $\mathbb{Z}[i]$ sont ceux dont la norme est un nombre premier (forcément 1 modulo 4 ou égal à 2) ou le carré d'un nombre premier qui est -1 modulo 4.*

Preuve. Montrons d'abord les assertions sur la factorisation dans $\mathbb{Z}[i]$ des nombres premiers. Supposons donc p premier dans $\mathbb{Z}$ et non premier dans $\mathbb{Z}[i]$. Soit alors α premier dans $\mathbb{Z}[i]$ tel que $\alpha|p$; notons que p/α n'est pas inversible dans $\mathbb{Z}[i]$. Ecrivons $\alpha = a + bi$ avec a et b dans $\mathbb{Z}$. Alors $a^2 + b^2 = N(\alpha)|N(p) = p^2$. On en conclut que $N(\alpha) = p$, et donc que p n'est pas -1 modulo 4. La situation de 2 se vérifie par un calcul. Montrons maintenant que les premiers p qui sont 1 modulo 4 se factorisent en deux premiers non associés. Soit donc p premier, congru à 1 modulo 4. Les deux racines distinctes de x^2+1 dans $\mathbb{F}_p$ (ce sont les éléments d'ordre 4 du groupe cyclique $\mathbb{F}_p^*$) nous donnent deux morphismes d'anneaux de $\mathbb{Z}[i]$ vers $\mathbb{F}_p$. Soit α un générateur du noyau de l'un des deux. Alors α est premier dans $\mathbb{Z}[i]$, il divise p, et il n'est pas associé à p (par exemple car $\mathbb{Z}[i]/p\mathbb{Z}[i]$ est de cardinal p^2). Comme $N(\alpha)|N(p) = p^2$, on a $\alpha\overline{\alpha} = N(\alpha) = p$.

Montrons que tout premier de $\mathbb{Z}[i]$ est un diviseur d'un unique premier positif de $\mathbb{Z}$. Pour cela, supposons que α dans $\mathbb{Z}[i]$ soit premier. Alors $\mathbb{Z}[i]/\mathbb{Z}[i]\alpha$ est intègre (car α premier), et même un corps car en plus $\mathbb{Z}[i]$ principal. (En fait, nous n'utiliserons pas que c'est un corps.) Considérons le morphisme d'anneaux $\mathbb{Z} \to \mathbb{Z}[i]/\mathbb{Z}[i]\alpha$. Son noyau contient $N(\alpha) = \alpha\overline{\alpha}$ qui est non nul, et son image est intègre. Il en résulte que le noyau est engendré par un nombre premier p. Bien sûr, on a $\alpha|p$. D'autre part, si p est premier dans $\mathbb{Z}$ et $\alpha|p$, p est un générateur du noyau de $\mathbb{Z} \to \mathbb{Z}[i]/\mathbb{Z}[i]\alpha$.

Pour finir, montrons la classification des premiers de $\mathbb{Z}[i]$ en termes de la norme. Supposons que α dans $\mathbb{Z}[i]$ soit premier. Notons p l'unique nombre premier divisible par α. En utilisant la factorisation de p en premiers dans $\mathbb{Z}[i]$, on voit que si p n'est pas -1 modulo 4, $N(\alpha) = p$, et que sinon $N(\alpha) = p^2$. D'autre part, il est clair que si α dans $\mathbb{Z}[i]$ est tel que $N(\alpha)$ est premier, alors α est premier. Supposons que α dans $\mathbb{Z}[i]$ est tel que $N(\alpha) = p^2$ avec $p = -1$ modulo 4. Comme $p^2 = N(\alpha) = \alpha\overline{\alpha}$, on a $\alpha|p$. Mais comme p est premier dans $\mathbb{Z}[i]$, α l'est aussi. $\square$

2.2 Le théorème des deux carrés.

2.2.1 Théorème. *Un nombre premier p est la somme de deux carrés si et seulement si p est congru à 1 modulo 4 (Fermat). Soit n dans $\mathbb{N}$. Alors n est une somme de deux carrés si et seulement si $v_p(n)$ est pair pour tout nombre premier p qui est -1 modulo 4.*

Preuve. La première assertion a été vue dans la section 2.1 : $a^2+b^2 = (a+bi)(a-bi)$ dans $\mathbb{Z}[i]$. Montrons la deuxième assertion. Soit n dans $\mathbb{N}$, non nul. Supposons d'abord que $v_p(n)$ est pair pour tout nombre premier p qui est -1 modulo 4. Pour chaque premier $p = 1$ mod 4, choisissons a_p et b_p dans $\mathbb{Z}$ tels que $p = a_p^2 + b_p^2$. Alors on a $n = (a + bi)(a - bi)$ où :

$$a + bi = (1 + i)^{v_2(n)} \prod_{p\equiv 1(4)} (a_p + b_p i)^{v_p(n)} \prod_{p\equiv -1(4)} p^{v_p(n)/2}.$$

D'autre part, supposons que $n = a^2 + b^2$ avec a et b dans $\mathbb{Z}$. On écrit alors $n = \alpha\overline{\alpha}$, avec $\alpha = a + bi$. Soit p premier, avec $p = -1$ modulo 4, donc premier dans $\mathbb{Z}[i]$. Il existe v dans $\mathbb{N}$ et β dans $\mathbb{Z}[i]$ premier à p tels que $\alpha = p^v\beta$. Alors on a $\overline{\alpha} = p^v\overline{\beta}$, et donc, avec $m := \beta\overline{\beta}$ dans $\mathbb{N}$: $n = p^{2v}m$, avec p ne pas divisant m dans $\mathbb{Z}[i]$, donc pas non plus dans $\mathbb{Z}$. Cela montre bien que $v_p(n)$ est pair. $\square$

Dans le TD on verra un algorithme efficace pour trouver une factorisation dans $\mathbb{Z}[i]$ d'un nombre premier p dans $\mathbb{N}$ qui est 1 modulo 4. Cet algorithme est assez simple, et utilise des particularités de $\mathbb{Z}[i]$ (être engendré par une racine de l'unité d'ordre 4, et être euclidien). Dans des cas plus généraux, signalons qu'il existe des algorithmes efficaces pour factoriser des polynômes sur les corps finis (algorithme de Berlekamp) et pour trouver des éléments courts dans des réseaux (LLL : Lenstra-Lenstra-Lovász) ; pour ces algorithmes, voir [Cohen].

2.2.2 Théorème. *Tout n dans $\mathbb{N}$ est somme de quatre carrés.*

Pour la preuve, que nous ne donnerons pas ici par manque de temps, voir [Samuel, §5.7]. L'idée de la preuve est la même que celle du théorème des deux carrés, mais on remplace $\mathbb{Z}[i]$ par un sous-anneau convenable de la $\mathbb{Q}$-algèbre (non commutative) des quaternions : $\mathbb{Q}\oplus\mathbb{Q}i\oplus\mathbb{Q}j\oplus\mathbb{Q}k$, avec $i^2 = j^2 = k^2 = -1$, et $ij = -ji = k$. Cette $\mathbb{Q}$-algèbre est une algèbre à division : tout élément non nul admet un inverse. Le sous-anneau $\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}k$ ne suffit car il n'est pas "euclidien" (il est facile de vérifier qu'il n'est pas euclidien pour la norme euclidienne). Le sous-anneau que l'on prend est celui engendré par i, j, k et $(1 + i + j + k)/2$. Une façon d'écrire cet ordre est :

$$\{(a + bi + cj + dk)/2 \mid a, b, c, d \in \mathbb{Z}, a = b = c = d \bmod 2\}.$$

3 Anneaux des entiers dans les corps de nombres.

3.1 Eléments entiers.

Maintenant que nous avons vu quelques applications non triviales de l'arithmétique dans des anneaux tels que $\mathbb{Z}[i]$ et $\mathbb{Z}[j]$, nous allons introduire de tels anneaux dans tous les corps de nombres. Par corps de nombres, on entend extension finie de $\mathbb{Q}$.

3.1.1 Définition. Soit $\mathbb{Q} \to K$ une extension finie. Un élément x de K est dit entier sur $\mathbb{Z}$ s'il est racine d'un polynôme unitaire à coefficients dans $\mathbb{Z}$. Autrement dit, x dans K est entier sur $\mathbb{Z}$ s'il existe $n \geq 1$ et des a_i dans $\mathbb{Z}$, $0 \leq i < n$, tels que :

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0.$$

L'ensemble de tels éléments sera noté $K_\mathbb{Z}$. Une notation plus courante pour $K_\mathbb{Z}$ est O_K.

3.1.2 Exemple. Montrons que $\mathbb{Q}_\mathbb{Z} = \mathbb{Z}$. Il est évident que $\mathbb{Q}_\mathbb{Z}$ contient $\mathbb{Z}$. Soit a dans $\mathbb{Q}_\mathbb{Z}$, et écrivons $a = n/m$, avec n et $m > 0$ des entiers premiers entre eux. Prenons f dans $\mathbb{Z}[x]$ unitaire tel que $f(a) = 0$. Ecrivons $f = x^r + a_{r-1}x^{r-1} + \cdots + a_0$. Cela donne :

$$n^r + a_{r-1}n^{r-1}m + \cdots + a_0 m^r = 0.$$

Supposons qu'un nombre premier p divise m. Alors p divise $a_{r-1}n^{r-1}m + \cdots + a_0 m^r$, donc n^r, donc n, ce qui contredit que n et m sont premiers entre eux. Il en résulte que $m = 1$ et que a est dans $\mathbb{Z}$.

La définition d'intégralité est clairement une généralisation de la notion d'élément algébrique dans une extension de corps. Nous allons montrer tout de suite que $K_\mathbb{Z}$ est en fait un sous-anneau de K, contenant $\mathbb{Z}$. Le fait que $K_\mathbb{Z}$ contient $\mathbb{Z}$ est de toute façon évident.

3.1.3 Proposition. *Soit $A \to B$ un morphisme d'anneaux. Un élément b de B est dit entier sur A s'il existe $n \geq 1$ et des a_i dans A, $0 \leq i < n$, tel que :*

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0.$$

Pour b dans B, les conditions suivantes sont équivalentes :

1. *b est entier sur A ;*
2. *la sous-A-algèbre $A[b]$ de B est un A-module de type fini ;*
3. *il existe une sous-A-algèbre C de B, contenant b, et de type fini en tant que A-module ;*
4. *il existe un sous-A-module M de B, de type fini, contenant 1 et stable par multiplication par b (i.e., tel que $bM \subset M$).*
5. *il existe un sous-A-module M de B, de type fini, contenant un non diviseur de zéro et stable par multiplication par b.*

Soit B' l'ensemble des b dans B qui sont entiers sur A. Alors B' est une sous-A-algèbre de B.

Preuve. Montrons que $(1) \Rightarrow (2)$. Soit f dans $A[x]$ unitaire, tel que $f(b) = 0$. Alors le sous-anneau $A[b]$ de B est l'image du morphisme de A-algèbres $A[x] \to B$ qui envoie x vers b. Comme f est unitaire, on peut diviser avec reste par f dans $A[x]$, ce qui montre que le A-module $A[x]/(f)$ est libre de base $(1, x, \ldots, x^{n-1})$, avec n le degré de f. Il en résulte que $A[b]$ est engendré, en tant que A-module, par 1, b, ... , b^{n-1}. Bien sûr, ceci se voit également en notant que dans $A[b]$ les b^m avec $m \geq n$ sont combinaisons linéaires des b^k avec $k < m$, donc des b^k avec $k < n$.

$(2) \Rightarrow (3)$: on peut prendre $C := A[b]$.

$(3) \Rightarrow (4)$: on peut prendre $M := C$.

$(4) \Rightarrow (5)$: on peut prendre "$M := M$".

Montrons finalement que $(5) \Rightarrow (1)$. Soit M un sous-A-module de B, de type fini, contenant un non diviseur de zéro x, et stable par multiplication par b. Soient $n \geq 0$ et $m_1, \ldots, m_n$ des générateurs de M. Pour tout i, bm_i s'écrit comme $\sum_j a_{j,i}m_j$, avec les $a_{j,i}$ dans A. Notons e la base canonique du A-module libre A^n, et considérons le morphisme $g\colon A^n \to M$ qui envoie e_i vers m_i. Comme les m_i engendrent M, ce morphisme est surjectif. Nous avons alors un diagramme commutatif :

$$\begin{array}{ccc} A^n & \xrightarrow{g} & M \\ {\scriptstyle a\cdot}\downarrow & & \downarrow{\scriptstyle b\cdot} \\ A^n & \xrightarrow{g} & M \end{array}$$

où $b\cdot$ est l'endomorphisme $m \mapsto bm$ de M, et où $a\cdot$ est l'endomorphisme $v \mapsto av$ de A^n. Soit f dans $A[x]$ le polynôme caractéristique $\det(x\mathrm{I}_n - a)$ de a. Par définition, f est unitaire, de degré n. Le théorème de Cayley-Hamilton (voir ci-dessous) dit que $f(a) = 0$ dans $\mathrm{End}_A(A^n)$. Il en résulte que l'endomorphisme $m \mapsto f(b)m$ de M est nul. En particulier, $f(b)x = 0$, et comme x n'est pas un diviseur de zéro, $f(b)$ est nul.

Montrons maintenant le deuxième énoncé. Il faut donc montrer que B' est une sous-A-algèbre de B. Soient donc b_1 et b_2 dans B'. Alors la sous-A-algèbre $A[b_1, b_2]$ de B engendrée par b_1 et b_2 est un A-module de type fini (car engendré par les $b_1^i b_2^j$ avec $0 \leq i < n$ et $0 \leq j < m$ si b_1 et b_2 sont racines de polynômes unitaires à coefficients dans A de degrés n et m respectivement). L'équivalence entre les conditions 1 et 3 montre alors que tout élément de $A[b_1, b_2]$ est entier sur A. $\square$

3.1.4 Théorème. (Cayley-Hamilton) *Soit A un anneau commutatif, $n \geq 0$ un entier, et a dans $\mathrm{M}_n(A)$. Soit f dans $A[t]$ le polynôme caractéristique $\det(t\mathrm{I}_n - a)$ de a. Alors $f(a) = 0$ dans $\mathrm{M}_n(A)$.*

Preuve. C'est clair si a est diagonale ; nous allons nous ramener à ce cas. Fixons pour l'instant l'anneau A, mais pensons aux coefficients de a comme des variables. Alors les coefficients de $f(a)$ sont des fonctions polynomiales des $a_{i,j}$, à coefficients dans $\mathbb{Z}$. Il suffit donc de montrer l'identité pour $A := \mathbb{Z}[\{x_{i,j} \mid 1 \leq i,j \leq n\}]$, et a la matrice x. Plongeons A d'abord dans son corps des fractions K, et ensuite dans un corps de décomposition L de f (f vu comme élément de $K[t]$). Si le discriminant de f est non nul, a a n valeurs propres distinctes dans L, est donc diagonalisable sur L, et le résultat est clair. Pour voir que le discriminant est non nul, il suffit de le voir après un choix convenable de valeurs pour les $x_{i,j}$. On peut prendre par exemple pour x la matrice diagonale $\mathrm{diag}(1, 2, \ldots, n)$. $\square$

3.2 Les corps quadratiques.

3.2.1 Théorème. *Toute extension de degré 2 de $\mathbb{Q}$ est isomorphe à une sous-extension de $\mathbb{Q} \to \mathbb{C}$ de la forme $\mathbb{Q} \to \mathbb{Q}(\sqrt{d})$ pour un unique $d \neq 1$ dans $\mathbb{Z}$ sans facteur carré : $e^2|d$ implique $e = \pm 1$. Soit $d \neq 1$ un entier sans facteur carré. Alors $\mathbb{Q}(\sqrt{d})$ est une extension de degré 2 de $\mathbb{Q}$. On a :*

$$\mathbb{Q}(\sqrt{d})_{\mathbb{Z}} = \mathbb{Z}[\sqrt{d}] \text{ si } d \not\equiv 1 \text{ mod } 4, \qquad \mathbb{Q}(\sqrt{d})_{\mathbb{Z}} = \mathbb{Z}[(1+\sqrt{d})/2] \text{ si } d \equiv 1 \text{ mod } 4.$$

Dans le premier cas, $(1, \sqrt{d})$ est une $\mathbb{Z}$-base de $\mathbb{Q}(\sqrt{d})_{\mathbb{Z}}$. Dans le deuxième cas, $(1, (1+\sqrt{d})/2)$ est une $\mathbb{Z}$-base de $\mathbb{Q}(\sqrt{d})_{\mathbb{Z}}$.

Preuve. Soit K une extension de degré 2 de $\mathbb{Q}$. Prenons x dans K tel que $K = \mathbb{Q}\cdot 1 \oplus \mathbb{Q}\cdot x$. Il existe a et b dans $\mathbb{Q}$ tels que $x^2 + ax + b = 0$. On pose $y := x + a/2$ (2 est bien inversible dans $\mathbb{Q}$), et on a $y^2 = d' := a^2/4 - b$. On a bien $K = \mathbb{Q}(y)$. On écrit $d' = c^2 d$ avec c dans $\mathbb{Q}$ et d dans $\mathbb{Z}$ et sans facteur carré. En posant $z := y/c$, on a $K = \mathbb{Q}(z)$, avec $z^2 = d$; $d \neq 1$ car K est de degré deux. Ceci montre donc l'existence.

Supposons que d et d' sont des entiers $\neq 1$ sans facteur carré, tels que les $\mathbb{Q}$-algèbres $\mathbb{Q}(\sqrt{d})$ et $\mathbb{Q}(\sqrt{d'})$ soient isomorphes. Il existe alors a et b dans $\mathbb{Q}$ tels que $d' = (a + b\sqrt{d})^2$, ce qui donne : $2ab = 0$ et $a^2 + b^2 d = d'$. Si $a = 0$, on a $b^2 d = d'$ et on a $d = d'$. Si $b = 0$, on a $a^2 = d'$, ce qui contredit le fait que d' n'est pas un carré dans $\mathbb{Q}$. Ceci établit l'unicité.

Soit maintenant $d \neq 1$ un entier sans facteur carré. Soit par la théorie de Galois, soit en remarquant que $x^2 - d$ a deux racines distinctes $\sqrt{d}$ et $-\sqrt{d}$ dans $K := \mathbb{Q}(\sqrt{d})$, on voit que K a un unique automorphisme non trivial σ, donné par $\sigma(a + b\sqrt{d}) = a - b\sqrt{d}$, pour tout a et b dans $\mathbb{Q}$. Comme σ est un automorphisme, on a $\sigma(K_{\mathbb{Z}}) = K_{\mathbb{Z}}$. Pour tout x dans K, on a :

$$0 = (x - x)(x - \sigma(x)) = x^2 - (x + \sigma(x))x + x\sigma(x),$$

avec $x + \sigma(x)$ et $x\sigma(x)$ dans $\mathbb{Q}$. Soit x dans $K_{\mathbb{Z}}$. Alors $\sigma(x)$ est dans $K_{\mathbb{Z}}$ donc $x + \sigma(x)$ et $x\sigma(x)$ sont entiers sur $\mathbb{Z}$; comme ils sont dans $\mathbb{Q}$, ils sont dans $\mathbb{Z}$. En écrivant $x = a + b\sqrt{d}$, avec a et b dans $\mathbb{Q}$, cela donne :

$$2a \in \mathbb{Z}, \quad a^2 - db^2 \in \mathbb{Z}.$$

En particulier, cela implique que $4db^2$ est dans $\mathbb{Z}$. On en déduit que $2b$ est dans $\mathbb{Z}$ (car d est sans facteur carré). Ensuite, on distingue les trois cas $d = 1$, -1 et 2 modulo 4, et on trouve que x est bien de la forme souhaitée (il est utile de noter que $(2a)^2 - d(2b)^2$ est dans $4\mathbb{Z}$). D'autre part, on vérifie directement que les x de cette forme sont entiers sur $\mathbb{Z}$. Les détails sont laissées au lecteur. $\square$

3.3 La trace.

Notre but suivant est de montrer que pour $\mathbb{Q} \to K$ une extension finie, $K_{\mathbb{Z}}$ est libre de rang $\dim_{\mathbb{Q}} K$ en tant que $\mathbb{Z}$-module. Nous allons donner deux démonstrations de cela. La première sera plutôt algébrique, en utilisant une forme quadratique qui s'appelle la forme trace de K sur $\mathbb{Q}$. La deuxième démonstration fait appel à des résultats bien connus sur les sous-groupes discrets de $\mathbb{R}$-espaces vectoriels de dimension finie. Introduisons maintenant la trace.

3.3.1 Définition. Soit A un anneau, et B une A-algèbre qui est libre de rang fini en tant que A-module. Pour b dans B on appelle trace de b sur A la trace de l'endomorphisme $\cdot b\colon B \to B$, $x \mapsto xb$ du A-module B ; c'est un élément de A que l'on notera $\mathrm{Tr}_{B/A}(b)$. L'application $\mathrm{Tr}_{B/A}$ de B vers A est un morphisme de A-modules, on l'appellera le morphisme trace de la A-algèbre B. L'application $(b_1, b_2) \mapsto \mathrm{Tr}(b_1 b_2)$ de B^2 vers A est A-bilinéaire, et est appelée la forme trace de la A-algèbre B ; nous la noterons $(b_1, b_2) \mapsto \langle b_1, b_2\rangle_{B/A}$.

Pour que la forme trace nous soit utile, nous avons besoin de savoir qu'elle est non dégénérée.

3.3.2 Théorème. *Soit $K \to L$ une extension finie de corps. Alors la forme trace est non dégénérée si et seulement si l'extension est séparable.*

Preuve. Supposons que $K \to L$ soit séparable. Alors il existe des éléments primitifs pour cette extension ; prenons en un, disons b, et soit f dans $K[x]$ son polynôme minimal sur K. Soit $K \to K'$ une extension qui scinde f : $f = (x-b_1)\cdots(x-b_d)$ dans $K'[x]$. Notons $L' := K' \otimes_K L$ la K'-algèbre obtenue de $K \to L$ par extension des scalaires de K à K' (voir la section 9 pour la définition du produit tensoriel d'algèbres sur un corps). Alors $\langle \cdot, \cdot\rangle_{L'/K'}$ est simplement la forme bilinéaire déduite de $\langle \cdot, \cdot\rangle_{L/K}$ par la même extension des scalaires. D'autre part, la K'-algèbre L' est isomorphe à $(K')^d$ via :

$$K[x]/(f) \xrightarrow{\sim} L, \qquad L' \xrightarrow{\sim} K'[x]/(f) \xrightarrow{\sim} (K')^d.$$

Maintenant on calcule directement. Une façon de dire ce qui se passe ici, est de dire que cette extension des scalaires ne change rien aux matrices qui donnent le morphisme et la forme trace, par rapport à une K-base de L, et à la K'-base de L' en déduite, mais qu'après cette extension de K à K', il existe une base beaucoup mieux adaptée au problème que nous voulons résoudre : la base canonique de $(K')^d$.

Nous ne montrons pas l'implication dans l'autre sens. Voir des livres d'algèbre, par exemple celui de Lang (Algebra). □

Nous allons maintenant montrer que pour K une extension finie de $\mathbb{Q}$, la trace $\mathrm{Tr}_{K/\mathbb{Q}}\colon K \to \mathbb{Q}$ envoie $K_{\mathbb{Z}}$ dans $\mathbb{Z}$.

3.3.3 Lemme. *Soit A un anneau, et $f\colon B_1 \to B_2$ un morphisme de A-algèbres. Soit b dans B_1 entier sur A. Alors $f(b)$ est entier sur A.*

Preuve. Immédiat car $f(b)$ est annulé par tout polynôme qui annule b. □

3.3.4 Proposition. *Soit K une extension finie de $\mathbb{Q}$, et notons $d := \dim_{\mathbb{Q}} K$. Il existe alors exactement d morphismes de K dans $\mathbb{C}$, disons $\phi_1, \ldots, \phi_d$. Soit x dans K, et soit f dans $\mathbb{Q}[t]$ son polynôme minimal sur $\mathbb{Q}$. Alors :*

1. $(t - \phi_1(x)) \cdots (t - \phi_d(x)) = f^{\dim_{\mathbb{Q}(x)} K}$;

2. *Si x est dans $K_{\mathbb{Z}}$, f est dans $\mathbb{Z}[t]$;*
3. *Le polynôme caractéristique de $\cdot x\colon \mathbb{Q}(x) \to \mathbb{Q}(x)$ est f ;*
4. *Le polynôme caractéristique de $\cdot x\colon K \to K$ est $f^{\dim_{\mathbb{Q}(x)} K}$;*
5. *Si x est dans $K_{\mathbb{Z}}$, $\mathrm{Tr}_{K/\mathbb{Q}}(x)$ est dans $\mathbb{Z}$.*

Preuve. Le fait qu'il existe exactement d morphismes de $\mathbb{Q}$-algèbres de K dans $\mathbb{C}$ a été montré en premier semestre. Rappelons nous le principe de la démonstration : on montre, par récurrence sur d, l'énoncé suivant : soit $K \to L$ une extension de corps, séparable, de degré d, et soit $\overline{K}$ une clôture algébrique, alors il existe exactement d morphismes de K-algèbres de L dans $\overline{K}$.

Soient maintenant $\phi_1, \ldots, \phi_d$ les plongements de notre K dans $\mathbb{C}$. Montrons la formule 1 en haut. Soit donc x dans K. L'identité se voit alors en regroupant les $\phi_i(x)$ qui sont égaux. Chaque racine de f dans $\mathbb{C}$ intervient $\dim_{\mathbb{Q}(x)} K$ fois. Ceci montre la première partie.

Soit x dans $K_{\mathbb{Z}}$. On applique la première partie à $\mathbb{Q}(x)$. En notant $d_x := \dim_{\mathbb{Q}} \mathbb{Q}(x)$ on a :

$$f = (t - \phi_1(x)) \cdots (t - \phi_{d_x}(x)),$$

avec $\phi_1, \ldots, \phi_{d_x}$ les plongements de $\mathbb{Q}(x)$ dans $\mathbb{C}$. Les $\phi_i(x)$ sont entiers sur $\mathbb{Z}$, donc les coefficients de f, qui sont des sommes de produits de $\phi_i(x)$, sont eux aussi entiers sur $\mathbb{Z}$. Mais comme ils sont dans $\mathbb{Q}$, ils sont dans $\mathbb{Z}$. Ceci termine la démonstration de la deuxième partie.

Par rapport ła $\mathbb{Q}$-base $(1, x, \ldots, x^{d_x-1})$ de $\mathbb{Q}(x)$, la matrice de $\cdot x$ est :

$$\begin{pmatrix} & & & & -a_0 \\ 1 & & & & \vdots \\ & 1 & & & \vdots \\ & & \ddots & & \vdots \\ & & & 1 & -a_{d_x-1} \end{pmatrix},$$

où nous avons écrit $f = t^{d_x} + \sum_{i<d_x} a_i t^i$. On montre, par récurrence sur la taille de cette matrice, que son polynôme caractéristique est f (c'est un exercice). Une autre façon de démontrer la troisième partie est de dire que le polynôme caractéristique de $\cdot x$ est dans $\mathbb{Q}[t]$, unitaire, de degré d_x, et, par Cayley-Hamilton, annule x, donc égale f. Encore une autre façon de faire est d'étendre les scalaires de $\mathbb{Q}$ à $\mathbb{C}$, et de choisir une base mieux adaptée au calcul, c'est à dire, une base où $\cdot x$ est diagonale.

Soit $(y_1, \ldots, y_e)$ une $\mathbb{Q}(x)$-base de K. On a donc $ed_x = d$. Alors les $x^i y_j$ forment une $\mathbb{Q}$-base de K, que l'on ordonne comme suite : $(y_1, xy_1, \ldots, x^{d_x-1}y_1, y_2, \ldots)$. Par rapport à cette base, la matrice de $\cdot x$ est constituée de e blocs, chacun égal à la matrice de la partie précédente. Cela démontre donc la quatrième partie.

La cinquième partie résulte directement des parties précédentes. □

3.4 Première démonstration de la liberté de $K_{\mathbb{Z}}$.

Pour montrer que $K_{\mathbb{Z}}$ est libre de rang $\dim_{\mathbb{Q}} K$ en tant que $\mathbb{Z}$-module, nous allons montrer que $K_{\mathbb{Z}}$ contient un sous-anneau avec cette propriété. Ensuite, en utilisant la forme trace, nous montrerons, par un argument de dualité, que $K_\mathbb{Z}$ est contenu dans un sous-$\mathbb{Z}$-module libre de rang $\dim_\mathbb{Q} K$ de K. Par le résultat qui dit que tout sous-module d'un $\mathbb{Z}$-module libre de rang n est libre de rang au plus n, cela implique que $K_\mathbb{Z}$ est libre, de rang $\dim_\mathbb{Q} K$.

3.4.1 Proposition. *Soit $\mathbb{Q} \to K$ une extension finie. Alors $K_\mathbb{Z}$ contient un sous-anneau qui est libre de rang $d := \dim_\mathbb{Q} K$ en tant que $\mathbb{Z}$-module.*

Preuve. Prenons x dans K un élément primitif : $K = \mathbb{Q}(x)$. En le remplaçant par nx avec $n > 0$ un entier convenable, on a x entier sur $\mathbb{Z}$. Il est clair que $\mathbb{Z}[x]$ a les propriétés voulues. □

3.4.2 Théorème. *Soit K une extension finie de $\mathbb{Q}$. Alors $K_\mathbb{Z}$ est libre de rang $\dim_\mathbb{Q} K$ en tant que $\mathbb{Z}$-module.*

Preuve. Soit A un sous-anneau de $K_\mathbb{Z}$ qui est déjà du bon rang sur $\mathbb{Z}$. Notons que pour tout x dans $K_\mathbb{Z}$ et y dans A, on a $\langle x, y\rangle_{K/\mathbb{Q}}$ dans $\mathbb{Z}$. Cela nous donne un morphisme de $\mathbb{Z}$-modules de $K_\mathbb{Z}$ vers $\mathrm{Hom}_\mathbb{Z}(A, \mathbb{Z})$:

$$x \mapsto (y \mapsto \langle x, y\rangle_{K/\mathbb{Q}}).$$

Comme A contient une $\mathbb{Q}$-base de K (car A est libre du bon rang ; appliquer la définition d'indépendance linéaire), et que la forme trace $\langle\cdot,\cdot\rangle_{K/\mathbb{Q}}$ est non dégénérée, ce morphisme est injectif. Donc $K_\mathbb{Z}$ est isomorphe à un sous-module de $\mathrm{Hom}_\mathbb{Z}(A, \mathbb{Z})$, qui est lui-même libre de rang $\dim_\mathbb{Q} K$. Comme tout sous-module d'un $\mathbb{Z}$-module libre de rang fini n est libre de rang au plus n, cela nous donne que $K_\mathbb{Z}$ est libre de rang au plus $\dim_\mathbb{Q} K$. Mais comme il contient A, il est de rang $\dim_\mathbb{Q} K$. □

3.5 Deuxième démonstration de la liberté de $K_\mathbb{Z}$.

Soit K une extension finie de $\mathbb{Q}$, $d := \dim_\mathbb{Q} K$, et $\phi_1, \ldots, \phi_d$ les plongements de K dans $\mathbb{C}$. Nous numérotons les ϕ_i de la façon suivante : ceux qui ont image dans $\mathbb{R}$ sont $\phi_1, \ldots, \phi_{r_1}$, et ensuite tel que $\phi_{r_1+r_2+i} = \overline{\phi_{r_1+i}}$, où $\overline{\phi}$ signifie ϕ suivi de la conjugaison complexe. Nous posons :

$$\Phi\colon K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}, \quad x \mapsto (\phi_1(x), \ldots, \phi_{r_1+r_2}(x)).$$

Cette application Φ, qui est un morphisme injectif de $\mathbb{Q}$-algèbres, s'appelle le plongement canonique de K (pas si canonique, car il faut numéroter les ϕ_i). De ce qui précède, il résulte que si on a x dans $K_\mathbb{Z}$, et $\Phi(x) = (x_1, \ldots, x_{r_1+r_2})$, alors le polynôme

$$(t - x_1)\cdots(t - x_{r_1})(t - x_{r_1+1})(t - \overline{x_{r_1+r_2+1}})\cdots(t - x_{r_1+r_2})(t - \overline{x_{r_1+2r_2}})$$

est de la forme $t^d + a_{d-1}t^{d-1} + \cdots + a_1 t + a_0$, avec les a_i dans $\mathbb{Z}$. Même, les a_i sont des sommes de produits de x_i et de $\overline{x_i}$. Cela implique que $\Phi(K_\mathbb{Z})$ est discret, et donc, par le théorème suivant, que $\Phi(K_\mathbb{Z})$ est libre de rang au plus d.

3.5.1 Théorème. *Soit H un sous-groupe discret d'un $\mathbb{R}$-espace vectoriel V de dimension finie n. Alors H est un $\mathbb{Z}$-module libre de rang au plus n. En plus, toute $\mathbb{Z}$-base de H est une suite $\mathbb{R}$-linéairement indépendante de V. Si H est de rang n, on l'appelle un réseau.*

Preuve. Voir [Samuel, IV, Thm 1]. Mais la preuve donnée là-bas ne me plait pas trop ; elle ne donne pas d'algorithme pour calculer une base du sous-groupe discret. Pour cette raison, je donne une autre preuve.

Nous remplaçons V par son sous-$\mathbb{R}$-espace vectoriel engendré par H.

Soient donc V et H comme dans le théorème. Nous devons montrer que H est libre de rang n, et que toute $\mathbb{Z}$-base de H est une $\mathbb{R}$-base de V. Récurrence sur n. Pour $n = 0$, c'est clair. Supposons donc que $n \geq 1$. Choisissons un produit scalaire $\langle \cdot, \cdot \rangle$ sur V, et notons $||\cdot||$ la norme associée. Prenons h_0 dans H non nul, avec $||h_0||$ minimal (c'est possible car H est discret, donc d'intersection finie avec tout sous-ensemble borné de V). Notons V' l'orthogonal de $\mathbb{R}h_0$, et $p \colon V \to \mathbb{R}h_0$ et $p' \colon V \to V'$ les projections orthogonales.

Montrons d'abord que $\mathbb{Z}h_0 = H \cap \mathbb{R}h_0$. Soit h dans $H \cap \mathbb{R}h_0$. On a $h = \lambda h_0$ pour un λ dans $\mathbb{R}$. Ecrivons $\lambda = m + \varepsilon$ avec $0 \leq \varepsilon < 1$. Alors $\varepsilon h_0 = h - mh_0$ est dans H, et $||\varepsilon h_0|| < ||h_0||$, donc $\varepsilon = 0$, et h est dans $\mathbb{Z}h_0$.

Montrons maintenant que $p'H$ est discret (dans V', bien sûr). Pour cela, il faut montrer qu'il existe $\varepsilon > 0$ tel que si h est dans H mais pas dans $\mathbb{R}h_0$, alors $||p'(h)|| > \varepsilon$. Soit donc h dans H mais pas dans $\mathbb{R}h_0$. En translatant par un élément de $\mathbb{Z}h_0$, nous pouvons supposer que $||p(h)|| \leq (1/2)||h_0||$ (faire un dessin, avec la bande des tels h, et la boule de rayon $||h_0||$). Comme $||h_0||$ est minimal, on a $||p'(h)|| \geq (1/2)\sqrt{3}||h_0||$.

Par récurrence, $p'H$ est libre, de rang au plus $n-1$, et toute $\mathbb{Z}$-base de $p'H$ est une $\mathbb{R}$-base de V'. Soient $h_1, \ldots, h_r$ dans H tel que $(p'(h_1), \ldots, p'(h_r))$ soit une $\mathbb{Z}$-base de $p'H$. On montre qu'alors $h := (h_0, h_1, \ldots, h_r)$ est une $\mathbb{Z}$-base de H (exercice). Il est clair que $(h_0, h_1, \ldots, h_r)$ est une $\mathbb{R}$-base de V. Par rapport à cette $\mathbb{Z}$-base de H, toute $\mathbb{Z}$-base de H est donnée par un élément de $\mathrm{GL}_n(\mathbb{Z})$, donc en particulier par un élément de $\mathrm{GL}_n(\mathbb{R})$, ce qui termine la démonstration. $\square$

4 Les anneaux de Dedekind.

Nous voulons démontrer que dans l'anneau d'entiers $K_{\mathbb{Z}}$ d'un corps de nombres K on a factorisation unique des idéaux non nuls en idéaux premiers. Cela remplacera, dans les applications, la factorialité perdue. Pour voir que la factorialité est perdue, considérer le cas $K = \mathbb{Q}(\sqrt{-5})$. La généralité naturelle de ce que nous voulons faire est le cadre des anneaux de Dedekind. Nous allons suivre [Samuel, III].

4.1 Définition. Un anneau A est dit de Dedekind si :

1. il est intègre ;
2. noethérien : tout idéal est de type fini ;
3. intégralement clos : tout élément du corps de fractions qui est entier sur l'anneau, est dans l'anneau ;
4. tout idéal premier non nul est maximal (la dimension de Krull est au plus un).

4.2 Les $K_{\mathbb{Z}}$ sont de Dedekind.

Avec ce que nous avons déjà vu, il est clair que tout anneau principal est de Dedekind. Le but de cette section est de montrer que les anneaux d'entiers des corps de nombres sont de Dedekind. Par définition, ces anneaux sont intègres. Le fait qu'ils sont libres de rang fini en tant que $\mathbb{Z}$-modules entraîne qu'ils sont noethériens : tout idéal est un sous-module d'un $\mathbb{Z}$-module libre de rang fini, donc libre de rang fini, donc engendré, même en tant que $\mathbb{Z}$-module, par un nombre fini d'éléments. Reste donc à voir qu'ils sont intégralement clos, et que tout idéal premier non nul est maximal.

4.2.1 Proposition. *Soit K un corps de nombres. Soit p un idéal premier non nul de $K_{\mathbb{Z}}$. Alors p est maximal.*

Preuve. Soit x dans p non nul (existe car p non nul). Comme $K_{\mathbb{Z}}$ est intègre, l'application $K_{\mathbb{Z}} \to p$, $y \mapsto xy$, est injective. Cela montre que p est libre de même rang que $K_{\mathbb{Z}}$ en tant que $\mathbb{Z}$-module, donc que $K_{\mathbb{Z}}/p$ est fini. Comme un anneau intègre fini est un corps, p est un idéal maximal. $\square$

4.2.2 Lemme. *Soit $A \to B \to C$ des morphismes d'anneaux, avec B entier sur A : tout b dans B est entier sur A. Soit x dans C, entier sur B. Alors x est entier sur A.*

Preuve. Prenons une relation de dépendance intégrale pour x sur B :

$$x^n + b_{n-1}x^{n-1} + \cdots + b_0 = 0,$$

avec les b_i dans B. Notons que la sous-A-algèbre $A[b_0, \ldots, b_{n-1}, x]$ de C est de type fini en tant que A-module, car engendré par des monômes $b_0^{i_0} \cdots b_{n-1}^{i_{n-1}} x^{i_n}$ avec tous les exposants bornés. Le critère d'intégralité du cours 3 implique que x est entier sur A. $\square$

4.2.3 Proposition. *Soit K un corps de nombres. Alors $K_{\mathbb{Z}}$ est intégralement clos.*

Preuve. Il n'y a qu'à appliquer le lemme précédent dans le cas $\mathbb{Z} \to K_{\mathbb{Z}} \to K$. □

4.3 Autres exemples d'anneaux de Dedekind.

Les anneaux de Dedekind ne se manifestent pas uniquement en théorie des nombres, mais également en géométrie algébrique, comme le montre l'exemple suivant.

4.3.1 Exemple. Soit k un corps, f dans $k[x,y]$ irréductible, tel que f et ses dérivés partiels f_x et f_y engendrent l'idéal $k[x,y]$ de $k[x,y]$. Alors l'anneau $A := k[x,y]/(f)$ est de Dedekind. En termes géométriques : l'anneau de coordonnées d'une courbe algébrique affine non singulière est de Dedekind. Un tel anneau A peut être non factoriel, donc le fait qu'il soit encore de Dedekind est important. Par exemple, $\mathbb{R}[x,y]/(x^2+y^2-1)$ n'est pas factoriel. Ce dernier fait n'est pas difficile à démontrer. Par exemple, les éléments y et $x-1$ n'admettent pas de pgcd.

4.4 Généralités noethériennes.

Nous suivons [Samuel, III].

4.4.1 Proposition. *Soit A un anneau, et M un A-module. Les conditions suivantes sont équivalentes :*

1. *toute famille non vide de sous-modules de M possède un élément maximal, c'est à dire, si I est un ensemble non vide et, pour tout i dans I, M_i un sous-module de M, alors il existe i dans I tel que pour tout j dans I, M_i n'est pas contenu strictement dans M_j ;*
2. *toute suite croissante de sous-modules de M est stationnaire : si $M_1 \subset M_2 \subset \cdots$ est une suite de sous-modules de M, on a $M_i = M_{i+1}$ pour tout i assez grand ;*
3. *tout sous-module de M est de type fini.*

Preuve. Les implications $(1) \implies (2)$, $(2) \implies (3)$ et $(3) \implies (2)$ sont claires. Montrons, pour finir, que $(2) \implies (1)$. Cela se fait par contradiction : supposons que toute suite croissante de sous-modules de M est stationnaire, et que M_i, pour i dans I, soit une famille non vide de sous-modules de A, qui n'admet pas d'élément maximal. Alors, pour tout i dans I, il existe un i' dans I avec $M_{i'}$ strictement plus grand que M_i. Mais alors il existe une suite strictement croissante $M_{i_0} \subset M_{i_1} \cdots$, ce qui contredit que toute suite croissante est stationnaire. □

4.4.2 Définition. Soit A un anneau. Un A-module M est noethérien si tout sous-module de M est de type fini. L'anneau A est dit noethérien s'il l'est en tant que A-module, c'est à dire, si tout idéal est de type fini.

4.4.3 Exemples. L'anneau $\mathbb{Z}$ est noethérien, ainsi que les $K_{\mathbb{Z}}$ pour les extensions finies K de $\mathbb{Q}$. Tout corps est noethérien, par manque d'idéaux. Si A est noethérien, alors $A[x]$ l'est aussi ; voir un livre d'algèbre pour ce résultat fondamental (nous ne l'utiliserons pas). L'anneau $\mathbb{Z}[x_1, x_2, \ldots]$

de polynômes en un nombre infini de variables n'est pas noethérien, ainsi que la clôture intégrale $\overline{\mathbb{Z}}$ de $\mathbb{Z}$ dans $\overline{\mathbb{Q}}$.

4.4.4 Proposition. *Soit A un anneau et $0 \to M' \to M \to M'' \to 0$ une suite exacte courte de A-modules. Alors M est noethérien si et seulement si M' et M'' le sont.*

Preuve. Si M est noethérien, alors M' et M'' le sont, car tout sous-module de M' est un sous-module de M, et tout sous-module de M'' est l'image d'un sous-module de M, donc tous de type fini. Supposons maintenant que M' et M'' sont noethériens. Soit N un sous-module de M, N' son intersection avec M' et N'' son image dans M'. Alors N' et N'' sont de type fini. Prenons des éléments $n'_1, \ldots, n'_r$ et $n''_1, \ldots, n''_s$ de N tels que $n'_1, \ldots, n'_r$ engendrent N', et les images de $n''_1, \ldots, n''_s$ dans M'' engendrent N''. Alors $n'_1, \ldots, n'_r$ et $n''_1, \ldots, n''_s$ engendrent N. $\square$

4.4.5 Corollaire. *Soit A un anneau. Si $M_1, \ldots, M_n$ sont des A-modules noethériens, alors leur produit $M_1 \times \cdots \times M_n$ est noethérien. Si A est noethérien, alors tout A-module de type fini est noethérien.*

4.5 Produits d'idéaux.

4.5.1 Définition. Soit A un anneau, et a et b des idéaux de A. On définit alors le produit ab comme étant l'idéal engendré par les xy, avec x dans a et y dans b. Ce produit ab est l'ensemble des sommes finis $\sum_i x_i y_i$, avec x_i dans a et y_i dans b.

Le lemme suivant dit que, pour cette multiplication, les idéaux premiers se comportent comme des éléments premiers.

4.5.2 Lemme. *Soit A un anneau, p un idéal premier, et $a_1, \ldots, a_n$ des idéaux. Supposons que $p \supset a_1 \cdots a_n$. Alors $p \supset a_i$ pour un i convenable.*

Preuve. Sinon, pour tout i, il existe x_i dans a_i tel que x_i n'est pas dans p ; mais alors $x_1 \cdots x_n$ est dans $a_1 \cdots a_n$, et pas dans p. $\square$

4.5.3 Lemme. *Soit A un anneau noethérien. Alors tout idéal de A contient un produit d'idéaux premiers. Et aussi : tout idéal non nul de A différent de A contient un produit d'idéaux premiers non nuls.*

Preuve. La preuve est un exemple typique de l'utilisation, assez magique, de l'hypothèse noethérienne. Montrons par exemple le deuxième énoncé. Soit Φ la famille des idéaux non nuls de A différents de A qui ne contiennent pas de produit d'idéaux premiers non nuls. Supposons que Φ soit non vide. Soit alors a dans Φ maximal. Certainement, a n'est pas premier, car $a \supset a$. Donc (comme A/a est non nul et non intègre) il existe x et y dans A, non dans a, tel que xy soit dans a. Comme $a + Ax$ et $a + Ay$ sont strictement plus grands que a, il existent des idéaux premiers non nuls $p_1, \ldots, p_r$ et $q_1, \ldots, q_s$, tels que $a + Ax \supset p_1 \cdots p_r$ et $a + Ay \supset q_1 \cdots q_s$. Mais alors :

$$a \supset (a + Ax)(a + Ay) \supset p_1 \cdots p_r q_1 \cdots q_s,$$

ce qui est une contradiction. Donc Φ est bien vide. $\square$

4.6 Idéaux fractionnaires.

4.6.1 Définition. Soit A un anneau intègre, et $A \to K$ son corps de fractions. Un *idéal fractionnaire* de A est un sous-A-module a de K tel qu'il existe d dans A non nul avec $da \subset A$. Si A est intègre et noethérien, les idéaux fractionnaires sont les sous-A-modules de type fini de K. Si a et b sont des idéaux fractionnaires de A, leur produit ab est le sous-A-module de K engendré par les xy avec x dans a et y dans b ; c'est encore un idéal fractionnaire de A, et, si a et b sont des idéaux de A, c'est le produit défini précédemment. De même, si a et b sont des idéaux fractionnaires de A, leur somme $a + b$ est un idéal fractionnaire de A.

4.6.2 Lemme. *Soit A un anneau intègre. L'ensemble $I(A)$ des idéaux fractionnaires non nuls de A est un monoïde pour la multiplication, c'est à dire, cette multiplication est associative, et admet un élément neutre (c'est A).*

Bien qu'on a deux opérations sur l'ensemble des idéaux fractionnaires d'un anneau intègre A, à savoir le produit et la somme, et que l'on a même $a(b + c) = ab + ac$, cet ensemble ne devient pas un anneau, car il manque l'inverse pour l'addition.

4.6.3 Théorème. *Soit A un anneau de Dedekind. Alors tout idéal maximal non nul de A est inversible dans le monoïde $I(A)$ d'idéaux fractionnaires non nul de A.*

Preuve. Soit m un idéal maximal non nul de A. Notons $A \to K$ le corps de fractions de A. Posons :

$$m' := \{x \in K \mid xm \subset A\}.$$

Alors m' est un sous-A-module de K. Pour tout y dans m on a $ym' \subset A$, donc m' est un idéal fractionnaire de A. Il suffit donc de montrer que $m'm = A$. Comme $m' \supset A$, on a $m \subset m'm \subset A$, donc soit $m'm = A$, soit $m'm = m$. Supposons que $m'm = m$.

Soit x dans m'. Alors m est un sous-A-module de K, de type fini, stable par multiplication par x, et contenant un non diviseur de 0. Par notre critère d'intégralité, x est entier sur A, donc dans A, car A est intégralement clos. On a donc $m' = A$. Ceci va contredire que tout les idéaux premiers non nuls de A sont maximaux.

Soit x dans m non nul. Soient $n \geq 1$ entier et $p_1, \ldots, p_n$ des idéaux premiers non nuls de A tels que $Ax \supset p_1 \cdots p_n$, avec n minimal. Comme $m \supset Ax \supset p_1 \cdots p_n$, on a $m \supset p_i$ pour un certain i, disons pour $i = 1$. Mais m et p_1 sont maximaux, donc $p_1 = m$. Posons $b := p_2 \cdots p_n$. Alors on a $Ax \supset mb$ et $Ax \not\supset b$ par minimalité de n. Prenons alors y dans b, non dans Ax. Alors on a $yx^{-1} \notin A$, et $yx^{-1}m \subset A$, autrement dit : $yx^{-1} \in m'$. Contradiction. □

4.6.4 Remarque. Je trouve que la preuve donnée ci-dessus n'est pas conceptuelle du tout. On peut suivre ligne par ligne que cela marche, mais comprendre ce qui se passe, c'est bien autre chose. Si on dispose de l'outil de localisation, on peut faire une preuve plus conceptuelle, par exemple, comme Serre dans son livre [Serre3]. Tout d'abord, m'/A est $(K/A)^{m=0}$, le plus grand sous-module de K/A annulé par m. Ensuite, dans le cas local, on a pour tout x non nul dans m, que $A[x^{-1}] = K$ (le seul idéal premier de A qui est contenu dans Ax est 0). Il en résulte que tout élément de K/A est annulé par une puissance de x. Comme m est de type fini, il en résulte que tout élément de K/A est annulé par une puissance de m. Mais en prenant un sous-module minimal de K/A (ou d'un sous-module non nul de type fini de K/A), on trouve que m'/A est non nul. (Pour l'existence d'un sous-module minimal, on utilise qu'un sous-module de type fini de K/A est artinien.)

Pour finir cette remarque, notons qu'on peut même faire cet argument sans localisation. Voici comment on fait : soit x dans m non nul. Il suffit de voir que $(x^{-1}A/A)^{m=0} \neq 0$. Mais la multiplication par x induit un isomorphisme de $x^{-1}A/A$ vers A/xA. Ce dernier est un anneau noethérien où tous les idéaux premiers sont maximaux, et donc minimaux. Or, dans un anneau noethérien, les idéaux premiers minimaux sont en nombre fini. Soient donc $m = m_1, \ldots, m_r$ les idéaux premiers de $B := A/xA$. Comme dans tout anneau, l'intersection des idéaux premiers est l'idéal des nilpotents (c'est vrai, pour montrer ceci, il est commode de localiser par rapport à un élément de cette intersection). Comme $m_1 \cap \cdots \cap m_r$ est de type fini, c'est un idéal nilpotent. On conclut que B est artinien, et que, pour n assez grand, le morphisme $B \to \prod_i B/m_i^n$ est un isomorphisme. On termine en prenant un sous-module minimal de B/m^n : un tel sous-module est nécessairement isomorphe à B/m, ce qui montre que $B^{m=0} \neq 0$.

Dans les exercices on trouvera une version plus élémentaire des arguments ci-dessus, adaptée spécialement au cas des $K_{\mathbb{Z}}$.

4.7 Factorisation unique des idéaux fractionnaires.

Dans cette section et la suivante, nous allons démontrer certains résultats concernant les anneaux de Dedekind, et en même temps pour un certain type d'anneaux a priori plus généraux dont nous verrons plus tard que ce sont eux aussi des anneaux de Dedekind. La raison de procéder comme ceci est que cela nous permet de démontrer plus loin un critère pratique pour savoir si un sous-anneau d'un anneau d'entiers dans un corps de nombre est égal à l'anneau des entiers, sans avoir à refaire les démonstrations des résultats de ces deux sections.

4.7.1 Théorème. *Soit A un un anneau de Dedekind, ou un anneau intègre, noethérien dont tout idéal premier non nul est maximal et inversible dans $I(A)$. Soit P l'ensemble des idéaux premiers non nuls de A. Alors tout idéal fractionnaire non nul a de A s'écrit de façon unique sous la forme :*

$$a = \prod_{p \in P} p^{v_p(a)},$$

avec les $v_p(a)$ dans $\mathbb{Z}$, presque tous nuls. Si a est un idéal non nul de A, on a $v_p(a) \geq 0$ pour tout p dans P.

Le monoïde $I(A)$ est un groupe : tout idéal fractionnaire non nul a de A admet un inverse pour la multiplication d'idéaux fractionnaires. Nous avons donc un isomorphisme de groupes :

$$v\colon I(A) \xrightarrow{\sim} \bigoplus_P \mathbb{Z} = \mathbb{Z}^{(P)}, \qquad a \mapsto (p \mapsto v_p(a)).$$

Preuve. Soit Φ l'ensemble des idéaux non nuls de A qui ne sont pas produit d'un nombre fini d'éléments de P. Supposons que $\Phi \neq \emptyset$. Soit a un élément maximal de Φ. Alors $a \neq A$, car A

est le produit de zéro éléments de P. Donc il existe p dans P tel que $a \subset p$ (prendre p maximal parmi les idéaux différents de A et contenant a). Soit p' l'inverse de p. On a :

$$a \subset ap' \subset pp' = A.$$

Si $a = ap'$, on a $p' = A$ (comme dans la preuve du théorème précédent si A est de Dedekind, et en utilisant le lemme 4.11.2 sous l'autre hypothèse sur A). Donc ap' n'est pas dans Φ. Donc ap' s'écrit sous la forme $ap' = p_1 \cdots p_n$, avec les p_i dans P. Mais alors on a :

$$a = aA = ap'p = p_1 \cdots p_n p,$$

ce qui est une contradiction. Donc Φ est bien vide, et tout idéal non nul de A est un produit d'éléments de P.

Soit a un idéal fractionnaire non nul de A. Soit d non nul dans A tel que $b := da \subset A$. Ecrivons $dA = q_1 \cdots q_m$ et $b = p_1 \cdots p_n$ avec les p_i et q_j dans P. Alors on a $a = p_1 \cdots p_n q_1^{-1} \cdots q_m^{-1}$, ce qui montre que tout idéal fractionnaire non nul est un produit de puissances d'éléments de P.

Le fait que $I(A)$ est un groupe commutatif, engendré par P, est maintenant clair. Montrons l'unicité de la factorisation. Cela équivaut à ce que P soit libre. Supposons qu'il existe une relation non triviale $\prod_p p^{n_p} = A$. En séparant les exposants positifs et négatifs, on obtient une relation non triviale de la forme :

$$p_1^{n_1} \cdots p_r^{n_r} = q_1^{m_1} \cdots q_s^{m_s},$$

avec les exposants > 0 et les p_i et q_j tous distincts. Mais alors p_1 contient $q_1^{m_1} \cdots q_s^{m_s}$, donc contient l'un des q_i, et est donc égal à l'un des q_i, ce qui est une contradiction. □

Pour pouvoir travailler avec cette factorisation des idéaux fractionnaires, nous avons besoin d'en traduire les propriétés les plus importantes en termes de cette factorisation. D'où le formulaire suivant.

4.7.2 Théorème. *Soit A un un anneau de Dedekind, ou un anneau intègre, noethérien dont tout idéal premier non nul est maximal et inversible dans $I(A)$. Soit P l'ensemble des idéaux premiers non nuls de A. Soient a et b des idéaux fractionnaires non nuls de A.*

1. *Pour tout p dans P : $v_p(ab) = v_p(a)v_p(b)$.*
2. *On a $a \subset b$ si et seulement si $v_p(a) \geq v_p(b)$ pour tout p dans P.*
3. *On a $a \subset A$ si et seulement si $v_p(a) \geq 0$ pour tout p dans P.*
4. *Pour tout p dans P : $v_p(a + b) = \min(v_p(a), v_p(b))$.*
5. *Pour tout p dans P : $v_p(a \cap b) = \max(v_p(a), v_p(b))$.*

Preuve. L'énoncé (1) résulte directement du théorème précédent. Pour (2), on note que $a \subset b$ équivaut à $b^{-1}a \subset A$. Donc avec (1), (2) résulte de (3). Montrons (3). Si les $v_p(a)$ sont tous ≥ 0, a est un produit d'idéaux, donc un idéal. Si $a \subset A$, tous les $v_p(a)$ sont ≥ 0 par le théorème précédent. Montrons (4). Cela résulte de (2) plus le fait que $a + b$ est le plus petit idéal fractionnaire de A qui contient a et b. L'énoncé (5) correspond au fait que $a \cap b$ est le plus grand idéal fractionnaire de A contenu dans a et b. □

4.8 Valuations sur les anneaux de Dedekind.

En pratique, on travaille plutôt directement avec les éléments du corps de fractions d'un anneau de Dedekind qu'avec les idéaux fractionnaires. Pour cela, il est commode d'introduire les valuations induites par les idéaux premiers non nuls.

4.8.1 Définition. Soit A un un anneau de Dedekind, ou un anneau intègre, noethérien dont tout idéal premier non nul est maximal et inversible dans $I(A)$. Soit K son corps de fractions, et P l'ensemble de ses idéaux premiers non nuls. Pour tout p dans P, la *valuation sur K en p* est l'application :

$$v_p \colon K \to \mathbb{Z} \cup \{\infty\}, \quad x \mapsto v_p(Ax) \text{ si } x \neq 0, 0 \mapsto \infty.$$

4.8.2 Proposition. *Dans la situation de la définition précédente, les applications v_p de K vers $\mathbb{Z} \cup \{\infty\}$ ont les propriétés suivantes :*

1. *$v_p(xy) = v_p(x) + v_p(y)$ pour tous x et y dans K^* ; autrement dit : $v_p \colon K^* \to \mathbb{Z}$ est un morphisme de groupes ;*
2. *$v_p(x + y) \geq \min(v_p(x), v_p(y))$, avec égalité si $v_p(x) \neq v_p(y)$.*

Preuve. La première égalité résulte directement de ce que $Axy = AxAy$. Montrons (2). Si $x = 0$, ou $y = 0$, ou $x + y = 0$, c'est clair. Supposons donc les trois non nuls. Ecrivons $Ax = p^{v_p(x)}a$ et $Ay = p^{v_p(y)}b$. Supposons que $v_p(x) \leq v_p(y)$. Alors $v_p(a) = 0 = v_p(b)$. Nous avons :

$$Ax = p^{v_p(x)}a \subset p^{v_p(x)}(a + b), \quad Ay = p^{v_p(y)}b \subset p^{v_p(y)}(a + b) \subset p^{v_p(x)}(a + b).$$

Il en résulte que $Ax + Ay = p^{v_p(x)}(a+b)$. Le Théorème 4.7.2 dit que $v_p(a+b) = 0$, ce qui donne bien

$$v_p(x + y) = v_p(A(x + y)) \geq v_p(Ax + Ay) = v_p(x).$$

Si $v_p(y) > v_p(x)$, alors $x+y$ n'est pas dans $p^{v_p(x)+1}(a+b)$, car sinon x serait dans $p^{v_p(x)+1}(a+b)$, ce qui n'est pas le cas. □

Ces propriétés justifient le nom de valuation pour les v_p. Nous ne donnerons pas ici la définition générale de ce qu'est une valuation, mais nous voulons plutôt insister sur l'analogie avec l'ordre d'une fonction méromorphe en une variable en un point.

Considérons par exemple l'anneau $\mathbb{C}[x]$. Alors, pour $f \neq 0$ dans le corps des fractions $\mathbb{C}(x)$, et a dans $\mathbb{C}$, on a bien que l'ordre de f en a est l'exposant de $x - a$ dans la factorisation en irréductibles de f.

Pour manipuler facilement les $v_p(x)$, il est commode de penser à x comme une fonction, et à $v_p(x)$ comme l'ordre de x en p. A vrai dire, en géométrie algébrique on dispose de ce qu'il faut pour rendre tout ceci rigoureux. En particulier, si A est l'anneau des fonctions régulières sur une courbe algébrique affine non singulière, cette interprétation est tout à fait correcte.

Le résultat suivant est l'analogue de ce qu'une fonction rationnelle sans pôle est régulière.

4.8.3 Proposition. *Soit A un un anneau de Dedekind, ou un anneau intègre, noethérien dont tout idéal premier non nul est maximal et inversible dans $I(A)$. Soit K son corps de fractions, et P l'ensemble de ses idéaux premiers non nuls. Soit x dans K et a dans $I(A)$. Pour que x soit dans a il faut et il suffit que $v_p(x) \geq v_p(a)$ pour tout p dans P. En particulier, pour que x soit dans A il faut et il suffit que $v_p(x) \geq 0$ pour tout p.*

Preuve. Ceci résulte directement de la définition de $v_p \colon K^* \to \mathbb{Z}$ et des parties (2) et (3) du Théorème 4.7.2. $\square$

4.9 Groupe des unités et groupe de classes d'idéaux.

Soit A un anneau de Dedekind, K son corps de fractions, et P l'ensemble de ses idéaux premiers non nuls. Rappelons nous que $I(A)$ est le groupe des idéaux fractionnaires non nuls, et que nous avons un isomorphisme $v \colon I(A) \xrightarrow{\sim} \mathbb{Z}^{(P)}$ donné par $a = \prod_p p^{v_p(a)}$. Rappelons nous aussi que nous avons défini des valuations $v_p \colon K^* \to \mathbb{Z}$, par $v_p(x) = v_p(Ax)$.

Un idéal fractionnaire a de A est dit principal s'il est principal, c'est à dire, s'il existe x dans K tel que $a = Kx$. Nous avons un morphisme de groupes :

$$K^* \longrightarrow I(A), \qquad x \mapsto Ax.$$

L'image de ce morphisme est le sous-groupe $P(A)$ des idéaux fractionnaires principaux. Le quotient $I(A)/P(A)$ est appelé le groupe de classes d'idéaux de A, et est noté $C(A)$. Avec ces définitions, il est clair que nous avons une suite exacte :

$$0 \longrightarrow A^* \longrightarrow K^* \xrightarrow{v} \mathbb{Z}^{(P)} \longrightarrow C(A) \longrightarrow 0.$$

Une façon d'interpréter cette suite exacte est de dire que les seules obstructions contre ce que v soit un isomorphisme sont A^* et $C(A)$. Plus exactement, soit $m \colon P \to \mathbb{Z}$ dans $\mathbb{Z}^{(P)}$. Alors m est dans l'image de v si et seulement si l'image de m dans $C(A)$ est nulle. Si tel est le cas, et si x dans K^* avec $v(x) = m$, alors $v^{-1}\{m\} = A^*x$. Dans le cas où A est l'anneau de fonctions régulières sur une courbe algébrique affine non singulière, le groupe $C(A)$ est l'obstruction quand on veut construire de telles fonctions avec des ordres de pôles et de zéros donnés en tous les points, et on l'appelle le groupe de Picard de la courbe. Une autre raison d'être de $C(A)$ est la proposition suivante.

4.9.1 Proposition. *Soit A un anneau de Dedekind. Alors A est factoriel si et seulement si $C(A)$ est trivial.*

Preuve. Si $C(A)$ est trivial, tout idéal premier non nul est principal, donc tout x non nul dans A s'écrit comme $up_1 \cdots p_n$, avec u dans A^*, $n \geq 0$ et les p_i premiers. Donc, dans ce cas, A est factoriel.

Supposons que A est factoriel. Alors tout x non nul dans A s'écrit sous la forme $up_1 \cdots p_n$, avec u dans A^*, $n \geq 0$ et les p_i premiers, et donc Ax s'écrit comme $(Ap_1) \cdots (Ap_n)$, c'est à dire, comme un produit d'idéaux premiers principaux. L'unicité de la factorisation des idéaux non nuls en idéaux premiers non nuls implique donc que tous les idéaux premiers qui interviennent dans la factorisation d'un tel Ax sont principaux. Pour montrer que $C(A)$ est nul, il suffit donc de montrer que tout idéal premier p non nul intervient dans la factorisation d'un Ax. Soit p un idéal premier non nul. Prenons x dans p, non dans p^2 (c'est possible, car $p \supset p^2$ et par l'unicité des factorisations, $p \neq p^2$). Alors $v_p(x) = 1$. $\square$

Dans la résolution de systèmes d'équations polynomiales, les groupes $C(A)$ et A^* sont des groupes qui nous embêtent, et pour cette raison, il est important de les comprendre un peu mieux, dans le cas des anneaux d'entiers dans les corps de nombres. Pour K un corps de nombres, nous montrerons que $C(K_{\mathbb{Z}})$ est fini, et que $K_{\mathbb{Z}}^*$ est, à des racines de l'unité près, libre de rang $r_1 + r_2 - 1$, où r_1 est le nombre de plongements réels de K dans $\mathbb{C}$, et $2r_2$ le nombre de plongements non réels. Voilà les deux résultats principaux de ce cours.

4.10 Quelques conditions équivalentes.

Pour que toute la théorie des anneaux d'entiers dans les corps de nombres soit utile, il faut disposer de critères pratiques pour qu'un sous-anneau de l'anneau des entiers d'un corps de nombres soit égal á l'anneau des entiers. Voilà pourquoi on considère le résultat suivant.

4.10.1 Théorème. *Soit A un anneau intègre noethérien, dont tout idéal premier non nul est maximal. Alors les conditions suivantes sont équivalentes :*

1. *A est de Dedekind ;*
2. *tout idéal premier non nul m de A est inversible dans $I(A)$;*
3. *pour tout idéal premier non nul m de A, le A/m-espace vectoriel m/m^2 est de dimension un.*

Preuve. Le fait que (1) implique (2) est le théorème 4.6.3.

Montrons que (2) implique (3). Considérons le morphisme quotient $p\colon m \to m/m^2$. L'application qui à un sous-A-module de m/m^2 associe son image réciproque dans m est une bijection entre l'ensemble des sous A-modules de m/m^2 et l'ensemble des sous A-modules de m qui contiennent m^2. Par le Théorème 4.7.2, partie (2), les seuls sous A-modules de m qui contiennent m^2 sont m et m^2, et ces deux ne sont pas égaux par l'unicité de la factorisation dans le Théorème 4.7.1. Comme en plus les sous A-modules de m/m^2 sont les sous A/m-espaces vectoriels, on constate que la dimension de m/m^2 est bien un.

Montrons que (3) implique (2). Soit donc m un idéal premier non nul de A. Notons K le corps de fractions de A, et posons $m' := \{x \in K \mid xm \subset A\}$. Alors m' est un idéal fractionnaire : c'est un sous A-module de K, et pour tout d non nul dans m on a $dm' \subset A$. Nous allons montrer que $m'm = A$, ce qui montre bien que m est inversible dans $I(A)$. Par construction on a $m'm \subset A$. Comme $m' \supset A$, on a $m \subset m'm$. Donc on a $m'm = m$ ou $m'm = A$, et il nous suffit de montrer que $m'm$ contient un élément qui n'est pas dans m. Soit t dans m et non dans m^2. Par le Lemme 4.5.3 il existe $r \geq 1$ un entier, et $m = m_1, m_2 \ldots, m_r$ des idéaux maximaux distincts de A, et des entiers $n_1, \ldots, n_r$, tel que :

$$At \supset m_1^{n_1} \cdots m_r^{n_r}.$$

Comme les m_i sont maximaux, on a $m_i + m_j = A$ si $i \neq j$. En prenant des puissances, on a $m_i^{n_i} + m_j^{n_j} = A$ si $i \neq j$. Le théorème Chinois donne un isomorphisme :

$$f\colon A/m_1^{n_1} \cdots m_r^{n_r} \xrightarrow{\sim} A/m_1^{n_1} \times \cdots \times A/m_r^{n_r}, \quad \overline{x} \mapsto (x_1, \ldots, x_r),$$

où x_i est la classe de x modulo $m_i^{n_i}$. Prenons u dans A tel que $(u_1, \ldots, u_r) = (1, 0, \ldots, 0)$. Montrons que $t^{-1}u$ est dans m', c'est à dire, que pour tout x dans m on a $t^{-1}ux$ dans A. La condition $t^{-1}ux \in A$ est équivalente à $ux \in tA$, et encore équivalente à $\overline{ux} \in \overline{tA}$, avec $\overline{A} = A/m_1^{n_1} \cdots m_r^{n_r}$. Via l'isomorphisme f, la dernière condition devient : $x_1 \in (t_1)$ dans l'anneau A/m^{n_1}. Comme t est dans m et non dans m^2, et que m/m^2 est de dimension un, il existe a_1 dans a tel que $x = a_1 t + x_2$, avec x_2 dans m^2. Ensuite, pour tout $n \geq 1$, t^n engendre m^n/m^{n+1}, ce qui fait qu'il existe des a_i dans A tels que $x = a_1 t + \cdots + a_n t^n + x_{n+1}$ avec x_{n+1} dans m^{n+1}. En prenant $n \geq n_1$ on obtient que dans A/m^{n_1} on a l'identité $x = a_1 t + \cdots + a_n t^n$, donc que $x_1 \in (t_1)$. On sait donc que $t^{-1}u$ est dans m'. Mais alors $u = tt^{-1}u$ est dans $m'm$. Comme u n'est pas dans m (car $u_1 = 1$) on conclut que $m'm = A$.

Montrons que (2) implique (1). Par définition, il nous faut montrer que A est intégralement clos. Soit donc x dans K et supposons que x soit entier sur A. Alors il existe $n \geq 1$ et des a_i dans A tel que :

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

Vu la Proposition 4.8.3, pour montrer que x est dans A, il suffit de montrer que $v_m(x) \geq 0$ pour tout idéal premier non nul m de A. Supposons donc que m soit un tel idéal et que $v_m(x) < 0$. Alors on a, par les propriétés de v_m :

$$v_m(x^n) = nv_m(x) < v_m(x^{n-1}) \leq v_m(a_{n-1}x^{n-1} + \cdots + a_0),$$

ce qui contredit que $-x^n = a_{n-1}x^{n-1} + \cdots + a_0$. □

4.11 Quelques critères pour que $A = K_{\mathbb{Z}}$.

Pour que les beaux résultats que l'on vient de voir, et ceux que nous verrons, soient exploitables, il faudra aussi avoir un moyen de calculer, pour un K donné, l'anneau des entiers $K_{\mathbb{Z}}$. Bien qu'on n'a pas (et on ne s'attend pas à l'avoir un jour) d'algorithme polynômial pour faire un tel calcul (en fait, il faudrait d'abord expliciter les données de départ, et le format dans lequel on aimerait la réponse), il est utile d'avoir quelques critères pour voir si un sous-anneau A de $K_{\mathbb{Z}}$ est égal à $K_{\mathbb{Z}}$, ou pour voir quels premiers divisent $|K_{\mathbb{Z}}/A|$.

Commençons par une propriété du discriminant, qui est défini dans le lemme 5.5.5 et la définition 5.5.6.

4.11.1 Proposition. *Soit K un corps de nombres, et A un sous-anneau d'indice fini de $K_{\mathbb{Z}}$. Alors $p|\mathrm{discr}(A)$ si et seulement si A/pA n'est pas réduit.*

Preuve. En effet, si k est un corps, et A une k-algèbre de dimension finie en tant que k-espace vectoriel, on a $\mathrm{discr}(A) = 0$ si A n'est pas réduit, car la forme trace est alors dégénérée. D'autre part, si k est parfait, comme $\mathbb{F}_p$ par exemple, une k-algèbre de dimension finie et réduite est un produit fini d'extensions séparables de k, donc telle que la forme trace est non dégénérée. □

4.11.2 Proposition. (Lemme de Nakayama) *Soit A un anneau, m dans A un idéal maximal, et M un A-module de type fini. Supposons que $mM = M$. Alors il existe un élément a de A qui n'est pas dans m tel que $aM = 0$.*

Preuve. Soient $m_1, \ldots, m_n$ des générateurs de M. Soit $f\colon A^n \to M$ le morphisme de A-modules tel que $f(e_i) = m_i$. Par hypothèse, il existe des $x_{i,j}$ dans m tels que :

$$m_i = \sum_j x_{i,j} m_j.$$

Alors on voit, comme dans la preuve de la Proposition 3.1.3, que M est annulé par $\det(1-x)$, qui n'est pas dans m. $\square$

4.11.3 Théorème. *Soit K un corps de nombres, et $A \subset K_{\mathbb{Z}}$ un sous-anneau d'indice fini. Alors les conditions suivantes sont équivalentes :*

1. *$A = K_{\mathbb{Z}}$;*
2. *pour tout idéal maximal m de A, on a $\dim_{A/m}(m/m^2) = 1$;*
3. *pour tout idéal maximal m de A, on a $\dim_{A/m}(m/m^2) \leq 1$;*
4. *pour tout premier p tel que p^2 divise $\mathrm{discr}(A)$, et pour tout tout idéal maximal $m \subset A$ contenant p, on a $\dim_{A/m}(m/m^2) \leq 1$;*

Preuve. Le Théorème 4.10.1 montre que (1) et (2) sont équivalentes. Il est clair que (2) implique (3) et que (3) implique (4). D'après la Proposition précédente, on a $m^2 \neq m$ pour tout idéal maximal m de A, donc les conditions $\dim_{A/m}(m/m^2) \leq 1$ et $\dim_{A/m}(m/m^2) = 1$ sont équivalentes. Il ne reste donc qu'à montrer que (4) implique (3).

Soit donc p un nombre premier tel que p^2 ne divise pas $\mathrm{discr}(A)$ et soit m un idéal maximal de A contenant p. Nous devons montrer que $\dim_{A/m}(m/m^2) \leq 1$. Posons $n := |K_{\mathbb{Z}}/A|$. Alors on montre dans les exercices que $\mathrm{discr}(A) = n^2 \mathrm{discr}(K_{\mathbb{Z}})$. On voit donc que p ne divise pas n. Il en résulte que la réduction modulo p^2 induit un isomorphisme d'anneaux :

$$A/p^2A \xrightarrow{\sim} K_{\mathbb{Z}}/p^2K_{\mathbb{Z}}.$$

On en déduit que les idéaux maximaux de A qui contiennent p sont en bijection avec ceux de $K_{\mathbb{Z}}$, et que les m/m^2 sont de dimension un. $\square$

4.11.4 Exemple. Traitons par exemple le cas de $K = \mathbb{Q}(2^{1/3}) = \mathbb{Q}[x]/(f)$, avec $f = x^3 - 2$. Prenons notre candidat $A := \mathbb{Z}[2^{1/3}]$ pour $K_{\mathbb{Z}}$, et appliquons le critère. Il y a deux façons de calculer le discriminant de A : on peut le faire avec la définition, c'est à dire, en calculant le déterminant de la forme trace de A, ou en calculant de discriminant de f (en TD on verra que les deux sont égaux). Pour calculer le discriminant, on peut utiliser des algorithmes pour le calcul de résultants. De toute façon, dans ce cas on trouve $\mathrm{discr}(A) = -3{\cdot}6{\cdot}6 = -2^2 3^3$. Les premiers dont nous nous méfions sont donc 2 et 3. Comme $A/2A = \mathbb{F}_2[x]/(x^3)$, il n'y a qu'un seul idéal maximal de A qui contient 2, à savoir $m_2 := (2, \overline{x})$, mais celui-là est engendré par $\overline{x}$ tout seul, car dans A on a $2 = \overline{x}^3$, donc m_2/m_2^2 est de dimension au plus un sur A/m_2. Comme

$A/3A = \mathbb{F}_3[x]/(x^3+1)$ et que $x^3+1 = (x+1)^3$ sur $\mathbb{F}_3$, on pose $y = x+1$, et l'on calcule : $x^3-2 = y^3-3y^2+3y-3$, donc $A = \mathbb{Z}[y]/(y^3-3y^2+3y-3)$, (polynôme d'Eisenstein !) et on voit qu'il n'y a qu'un seul idéal maximal de A qui contient 3, à savoir $m_3 = (3, y)$. Ici encore, m_3 est principal, car engendré par $\overline{y}$, donc m_3/m_3^2 est de dimension au plus un sur A/m_3. On conclut que $A = K_{\mathbb{Z}}$.

5 Finitude du groupe des classes d'idéaux.

Pour K une extension finie de $\mathbb{Q}$, nous avons défini le groupe de classes d'idéaux $C(K_{\mathbb{Z}})$ comme le quotient $I(K_{\mathbb{Z}})/P(K_{\mathbb{Z}})$. Le but est maintenant de montrer que les $C(K_{\mathbb{Z}})$ sont finis. Pour le faire, nous allons montrer que tout élément de $C(K_{\mathbb{Z}})$ est représenté par un idéal a de $K_{\mathbb{Z}}$ qui est "petit" dans le sens que $K_{\mathbb{Z}}/a$ est petit. Le cardinal de $K_{\mathbb{Z}}/a$ sera appelé la norme de a.

5.1 La norme.

5.1.1 Définition. Soit A un anneau, et B une A-algèbre qui est libre de rang fini en tant que A-module. Pour b dans B on appelle norme de b sur A le déterminant de l'endomorphisme $\cdot b\colon B \to B$, $x \mapsto xb$ du A-module B ; c'est un élément de A que l'on notera $\mathrm{N}_{B/A}(b)$. Pour tous b_1 et b_2 dans B on a $\mathrm{N}_{B/A}(b_1 b_2) = \mathrm{N}_{B/A}(b_1)\mathrm{N}_{B/A}(b_2)$.

5.1.2 Remarque. Par rapport à une A-base de B, $\mathrm{N}_{B/A}\colon B \to A$ est donné par un polynôme homogène de degré $\mathrm{rang}_A(B)$ en $\mathrm{rang}_A(B)$ variables.

Soit maintenant K une extension finie de $\mathbb{Q}$, d son degré, et $\phi_1, \ldots, \phi_d$ les d plongements de K dans $\mathbb{C}$.

5.1.3 Proposition.
1. *Pour tout x dans K on a :* $\mathrm{Tr}_{K/\mathbb{Q}}(x) = \phi_1(x) + \cdots + \phi_d(x)$.
2. *Pour tout x dans K on a :* $\mathrm{N}_{K/\mathbb{Q}}(x) = \phi_1(x) \cdots \phi_d(x)$.
3. *Pour tout x dans $K_{\mathbb{Z}}$, $\mathrm{Tr}_{K/\mathbb{Q}}(x)$ et $\mathrm{N}_{K/\mathbb{Q}}(x)$ sont dans $\mathbb{Z}$.*
4. *Pour tout x dans $K_{\mathbb{Z}}^*$, $\mathrm{N}_{K/\mathbb{Q}}(x)$ est 1 ou -1.*
5. *Pour $x \neq 0$ dans $K_{\mathbb{Z}}$, on a $|K_{\mathbb{Z}}/xK_{\mathbb{Z}}| = |\mathrm{N}_{K/\mathbb{Q}}(x)|$.*

Preuve. On utilise la proposition 3.3.4 pour les parties 1 et 2. La partie 3 résulte des propriétés d'intégralité. La partie 4 résulte de 3. La dernière partie a déjà été vue en TD (c'est à dire, figure parmi les exercices). □

5.1.4 Définition. Pour a un idéal non nul de $K_{\mathbb{Z}}$, nous définissons sa *norme* $\mathrm{N}_{K/\mathbb{Q}}(a)$ par : $\mathrm{N}_{K/\mathbb{Q}}(a) := |K_{\mathbb{Z}}/a|$.

Pour x dans $K_{\mathbb{Z}}$ on a donc : $|\mathrm{N}(x)| = \mathrm{N}(K_{\mathbb{Z}}x)$.

5.1.5 Proposition. *Si a et b sont des idéaux non nuls de $K_{\mathbb{Z}}$, on a $\mathrm{N}(ab) = \mathrm{N}(a)\mathrm{N}(b)$. En particulier, on a $\mathrm{N}(a) = \prod_p \mathrm{N}(p)^{v_p(a)}$, où p parcourt l'ensemble des idéaux maximaux de $K_{\mathbb{Z}}$.*

Preuve. Il suffit de le montrer dans le cas où b est un idéal maximal m. Dans ce cas, on a une suite exacte de $K_{\mathbb{Z}}$-modules :

$$0 \longrightarrow a/am \longrightarrow K_{\mathbb{Z}}/am \longrightarrow K_{\mathbb{Z}}/a \longrightarrow 0.$$

Ensuite, on utilise que a/am est un $K_{\mathbb{Z}}/m$-espace vectoriel de dimension un. □

5.2 Le cas de $\mathbb{Q}(\sqrt{-5})$.

Nous considérons $\mathbb{Q}(\sqrt{-5})$ comme sous-anneau de $\mathbb{C}$, en envoyant $\sqrt{-5}$ vers $\sqrt{5}i$. L'anneau des entiers de $\mathbb{Q}(\sqrt{-5})$ est $\mathbb{Z}[\sqrt{-5}]$, de $\mathbb{Z}$-base $(1, \sqrt{-5})$.

Soit a un idéal non nul de $\mathbb{Z}[\sqrt{-5}]$. Essayons de trouver un élément $x \neq 0$ de a tel que $|x|$ soit petit, et de voir après à quoi cela peut bien servir. Pour $r > 0$ réel, notons $B(r)$ la boule fermée $\{z \in \mathbb{C} \mid |z| \leq r\}$. Nous considérons, pour $r \geq 0$, les morphismes suivants :

$$B(r) \hookrightarrow \mathbb{C} \longrightarrow \mathbb{C}/a,$$

de groupes additifs (a n'est pas un idéal dans $\mathbb{C}$!). On a :

$$\mathrm{Vol}(B(r)) = \pi r^2, \quad \mathrm{Vol}(\mathbb{C}/\mathbb{Z}[\sqrt{-5}]) = \sqrt{5}, \quad \mathrm{Vol}(\mathbb{C}/a) = \mathrm{N}(a)\sqrt{5}.$$

Pour la dernière égalité, utiliser la suite exacte :

$$0 \longrightarrow \mathbb{Z}[\sqrt{-5}]/a \longrightarrow \mathbb{C}/a \longrightarrow \mathbb{C}/\mathbb{Z}[\sqrt{-5}] \longrightarrow 0,$$

ou raisonner en termes de domaines fondamentaux (celui pour a est réunion disjointe de $\mathrm{N}(a)$ copies de celui de $\mathbb{Z}[\sqrt{-5}]$). Prenons maintenant r tel que $\mathrm{Vol}(B(r)) > \mathrm{Vol}(\mathbb{C}/a)$, c'est à dire :

$$r > r_0 = \left(\frac{\mathrm{N}(a)\sqrt{5}}{\pi}\right)^{1/2}.$$

Alors l'application ci-dessus de $B(r)$ vers $\mathbb{C}/a$ n'est pas injective, donc il existe y et z dans $B(r)$, distincts, tel que $x := y - z$ est dans a. Nous avons donc obtenu un $x \neq 0$ dans a avec $|x| \leq 2r$. Ceci vaut pour tout $r > r_0$. Comme les $B(2r)$ sont compactes, les $B(2r) \cap (a - \{0\})$ le sont aussi, donc leur intersection, prise sur tous les $r > r_0$, n'est pas vide (car aucune intersection finie n'est vide). Donc, en fait, nous avons montré l'existence d'un $x \neq 0$ dans a avec $|x| \leq 2r_0$. Considérons maintenant la suite d'inclusions d'idéaux :

$$\mathbb{Z}[\sqrt{-5}] \supset a \supset \mathbb{Z}[\sqrt{-5}]x = ab,$$

où la dernière égalité est la définition de b. Cela montre que a^{-1} est égal à b dans $C(\mathbb{Z}[\sqrt{-5}])$, et que :

$$\mathrm{N}(b) = \mathrm{N}(\mathbb{Z}[\sqrt{-5}]x)/\mathrm{N}(a) = \mathrm{N}(x)/\mathrm{N}(a) = |x|^2/\mathrm{N}(a) \leq 4\sqrt{5}/\pi < 3.$$

Nous en concluons que tout élément de $C(\mathbb{Z}[\sqrt{-5}])$ est représenté par un idéal de norme au plus 2 de $\mathbb{Z}[\sqrt{-5}]$. Mais les seuls idéaux de norme au plus 2 sont $\mathbb{Z}[\sqrt{-5}]$ et $m_2 := (2, 1 + \sqrt{-5})$, ce qui montre que $C(\mathbb{Z}[\sqrt{-5}])$ a au plus 2 éléments. Comme m_2 n'est pas principal (la norme de $a + b\sqrt{-5}$ est $a^2 + 5b^2$), on conclut que $C(\mathbb{Z}[\sqrt{-5}]) = \mathbb{Z}/2\mathbb{Z}$.

5.2.1 Théorème. $C(\mathbb{Z}[\sqrt{-5}]) = \mathbb{Z}/2\mathbb{Z}$.

5.3 Application.

5.3.1 Théorème. *L'équation $y^2 = x^3 - 5$ n'a pas de solution dans $\mathbb{Z}$.*

Preuve. Par contradiction. Supposons que x et y sont dans $\mathbb{Z}$, tel que $y^2 = x^3 - 5$. Alors nous avons, dans $\mathbb{Z}[\sqrt{-5}]$:

$$x^3 = y^2 + 5 = (y + \sqrt{-5})(y - \sqrt{-5}).$$

Notons que l'idéal $(y + \sqrt{-5}, y - \sqrt{-5})$ contient $(2\sqrt{-5}) = m_2^2 m_5$. Notons P l'ensemble des idéaux maximaux de $\mathbb{Z}[\sqrt{-5}]$. Alors, si p est dans $P - \{m_2, m_5\}$, au plus l'un d'entre $v_p(y + \sqrt{-5})$ et $v_p(y - \sqrt{-5})$ est > 0, et donc tous ces $v_p(y + \sqrt{-5})$ et $v_p(y - \sqrt{-5})$ sont divisibles par 3. D'autre part, $\overline{m_2} = m_2$ et $\overline{m_5} = m_5$, donc $v_{m_2}(y + \sqrt{-5}) = v_{m_2}(y - \sqrt{-5})$, donc $v_{m_2}(y + \sqrt{-5})$ et $v_{m_2}(y - \sqrt{-5})$ sont divisibles par 3. Le même argument montre que $v_{m_5}(y + \sqrt{-5})$ et $v_{m_5}(y - \sqrt{-5})$ sont divisibles par 3. On en conclut qu'il existe un idéal a de $\mathbb{Z}[\sqrt{-5}]$ tel que $(y + \sqrt{-5}) = a^3$. Comme $C(\mathbb{Z}[\sqrt{-5}])$ est d'ordre 2, a est principal, disons $a = (u)$. Mais alors, quitte à remplacer u par $-u$, on a $u^3 = y + \sqrt{-5}$. En écrivant $u = n + m\sqrt{-5}$, ceci donne rapidement une contradiction. $\square$

On peut voir, mais ce n'est pas facile, qu'il n'y a pas d'obstruction de signe ni de congruence qui permet de montrer ce résultat (en effet, il y a des solutions dans $\mathbb{R}$, et dans tous les $\mathbb{Z}/p^n\mathbb{Z}$ avec p premier et $n \geq 1$).

5.4 Le cas des corps quadratiques réels.

Soit $d > 1$ un entier sans facteur carré. Notons $K := \mathbb{Q}(\sqrt{d})$ et $A := K_\mathbb{Z}$ son anneau des entiers. Rappelons-nous que $A = \mathbb{Z}[(1+\sqrt{d})/2]$ si $d \equiv 1$ modulo 4, et $A = \mathbb{Z}[\sqrt{d}]$ sinon. Notons ϕ_1 et ϕ_2 les deux plongements de K dans $\mathbb{R}$, et $\phi\colon K \to \mathbb{R}^2$ le morphisme d'anneaux donné par $\phi(x) = (\phi_1(x), \phi_2(x))$. Nous observons d'abord que

$$\mathrm{Vol}(\mathbb{R}^2/\phi(\mathbb{Z}[\sqrt{d}])) = \left|\det\begin{pmatrix}1 & \sqrt{d}\\ 1 & -\sqrt{d}\end{pmatrix}\right| = 2\sqrt{d}.$$

On en conclut que $\mathrm{Vol}(\mathbb{R}^2/\phi(A)) = \sqrt{d}$ si $d \equiv 1$ modulo 4, et $2\sqrt{d} = \sqrt{4d}$ sinon. D'autre part, calculons le discriminant $\mathrm{discr}(A)$ de A. Par définition, c'est le déterminant de la matrice de la forme trace par rapport à n'importe quelle $\mathbb{Z}$-base de A (cela ne dépend pas du choix car le déterminant d'un élément g de $\mathrm{GL}_2(\mathbb{Z})$ est ± 1, et la matrice en question change par $m \mapsto g^t m g$). Par rapport à la $\mathbb{Z}$-base $(1, \sqrt{d})$ de $\mathbb{Z}[\sqrt{d}]$, la matrice de la forme trace est $\left(\begin{smallmatrix}2 & 0\\ 0 & 2d\end{smallmatrix}\right)$, donc de déterminant $4d$. Il en résulte que :

$$\mathrm{discr}(A) = \begin{cases} d \text{ si } d \equiv 1 \text{ modulo } 4,\\ 4d \text{ si } d \not\equiv 1 \text{ modulo } 4.\end{cases}$$

On conclut que :

$$\mathrm{Vol}(\mathbb{R}^2/\phi(A)) = |\mathrm{discr}(A)|^{1/2}.$$

Soit maintenant $a \subset A$ un idéal non nul. On a alors :

$$\mathrm{Vol}(\mathbb{R}^2/\phi(a)) = N(a)\mathrm{Vol}(\mathbb{R}^2/\phi(A)) = N(a)|\mathrm{discr}(A)|^{1/2}.$$

Comme dans le cas imaginaire, nous allons nous servir d'une norme $\|\cdot\|$ sur le $\mathbb{R}$-espace vectoriel dans lequel nous travaillons : ici c'est $\mathbb{R}^2$. Nous prenons, comme tout le monde, d'ailleurs, la norme donnée par $\|(x,y)\| = |x| + |y|$. La raison de ce choix devient claire dans un dessin, où l'on voit que ce choix maximise le volume de la "boule" $B(\|\cdot\|, r) := \{z \in \mathbb{R}^2 \mid \|z\| \leq r\}$ sous la condition que cette boule soit contenue dans $\{(x,y) \in \mathbb{R}^2 \mid |xy| \leq 1\}$. (Notons qu'en fait toutes les métriques $\|(x,y)\| = \alpha|x| + \beta|y|$ avec $\alpha\beta = 1$, $\alpha > 0$ et $\beta > 0$ sont aussi bonnes.)

L'identité $(x+y)^2 - 4xy = (x-y)^2$ montre que pour tout x dans K on a :

$$|N(x)| = |\phi_1(x)\phi_2(x)| \leq (1/4)\|\phi(x)\|^2.$$

Comme $B(\|\cdot\|, r)$ est un carré de côté $\sqrt{2}r$, on a :

$$\mathrm{Vol}(B(\|\cdot\|, r)) = 2r^2.$$

Prenons maintenant r_0 tel que $2r_0^2 = \mathrm{Vol}(\mathbb{R}^2/\phi(a))$, donc :

$$r_0 = \left(\frac{N(a)\,|\mathrm{discr}(A)|^{1/2}}{2}\right)^{1/2}.$$

Par le même argument que dans le cas imaginaire, on voit qu'il existe un $x \neq 0$ dans a, tel que $\|x\| \leq 2r_0$. Prenons un tel x. On a alors :

$$|N(x)| \leq (1/4)\|\phi(x)\|^2 \leq (1/4)4r_0^2 = \frac{N(a)\,|\mathrm{discr}(A)|^{1/2}}{2}.$$

D'autre part, on a la suite d'inclusions d'idéaux de A :

$$A \supset a \supset Ax = ab,$$

où la dernière égalité est la définition de b. Pour ce b :

$$N(b) = \frac{|N(x)|}{N(a)} \leq \frac{|\mathrm{discr}(A)|^{1/2}}{2}.$$

On en conclut le résultat suivant.

5.4.1 Théorème. *Soit K un corps quadratique réel. Alors tout élément du groupe de classes d'idéaux $C(K_{\mathbb{Z}})$ a un représentant qui est un idéal de $K_{\mathbb{Z}}$ de norme au plus $2^{-1}|\mathrm{discr}(K_{\mathbb{Z}})|^{1/2}$.*

5.4.2 Exemple. $\mathbb{Z}[\sqrt{7}]$ est principal. En effet, il suffit de voir que tout idéal b de norme au plus $\sqrt{7} < 3$ est principal. Comme $\mathbb{Z}[\sqrt{7}]/(2) = \mathbb{F}_2[x]/(x^2+1)$, il suffit de voir que $(2, 1+\sqrt{7})$ est principal. Comme $N(3+\sqrt{7}) = 3^2 - 7 = 2$, c'est le cas.

5.5 Bornes dans le cas général.

Soit K une extension finie de $\mathbb{Q}$, d son degré, et $\phi_1, \ldots, \phi_d$ les plongements distincts de K dans $\mathbb{C}$, numérotés de la façon suivante : $\overline{\phi_i} = \phi_i$ si $1 \leq i \leq r_1$, et $\overline{\phi_{r_1+i}} = \phi_{r_1+r_2+i}$ si $1 \leq i \leq r_2$. On a donc $d = r_1 + 2r_2$.

5.5.1 Exemple. Prenons $K := \mathbb{Q}(2^{1/3})$. Le polynôme minimal de $2^{1/3}$ est x^3-2, ses trois racines dans $\mathbb{C}$ sont $2^{1/3}$, $2^{1/3}j$, et $2^{1/3}j^2$. On a donc $\phi_1(2^{1/3}) = 2^{1/3}$, et on peut prendre $\phi_2(2^{1/3}) = 2^{1/3}j$ et $\phi_3(2^{1/3}) = 2^{1/3}j^2$.

Nous plongeons K dans $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ en utilisant les ϕ_i :

$$\phi\colon K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}, \quad x \mapsto \phi(x) := (\phi_1(x), \ldots, \phi_{r_1+r_2}(x)).$$

Cette application ϕ est un morphisme de $\mathbb{Q}$-algèbres. Dans la suite, nous utilisons la $\mathbb{R}$-base $(1, i)$ de $\mathbb{C}$ pour passer de $\mathbb{C}$ à $\mathbb{R}^2$. Par exemple, nous noterons également ϕ l'application suivante, obtenue en composant le ϕ en haut par l'isomorphisme $\mathbb{C}^{r_2} \to \mathbb{R}^{2r_2}$:

$$\begin{aligned} &\phi\colon K \to \mathbb{R}^d \\ &\quad x \mapsto (\phi_1(x), \ldots, \phi_{r_1}(x), \mathrm{Re}(\phi_{r_1+1}(x)), \mathrm{Im}(\phi_{r_1+1}(x)), \ldots, \mathrm{Re}(\phi_{r_1+r_2}(x)), \mathrm{Im}(\phi_{r_1+r_2}(x))). \end{aligned}$$

Pour simplifier la notation dans ce qui va suivre, nous posons $K_{\mathbb{R}} := \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Ceci est d'autant plus justifié par le fait que le morphisme naturel de $\mathbb{R}$-algèbres $\mathbb{R} \otimes_{\mathbb{Q}} K \to K_{\mathbb{R}}$ est un isomorphisme (cela se voit en prenant un élément primitif x de K, et en écrivant $K = \mathbb{Q}[t]/(f)$, avec f le polynôme minimal de x). En fait, il est plus naturel de plonger K dans $\mathbb{R} \otimes_{\mathbb{Q}} K$ que dans $K_{\mathbb{R}}$, car cela évite le choix d'une numérotation des ϕ_i.

Nous avons vu que pour tout x dans K, on a :

$$\mathrm{N}_{K/\mathbb{Q}}(x) = |\phi_1(x)| \cdots |\phi_{r_1}(x)| \cdot |\phi_{r_1+1}(x)|^2 \cdots |\phi_{r_1+r_2}(x)|^2.$$

Cela donne donc un diagramme commutatif :

$$\begin{array}{ccc} K & \xrightarrow{\phi} & K_{\mathbb{R}} \\ \Big\downarrow{\scriptstyle \mathrm{N}_{K/\mathbb{Q}}} & & \Big\downarrow{\scriptstyle \mathrm{N}} \\ \mathbb{Q} & \xrightarrow{|\cdot|} & \mathbb{R} \end{array} \quad \mathrm{N}\colon (x, z) \mapsto |x_1| \cdots |x_{r_1}| \cdot |z_1|^2 \cdots |z_{r_2}|^2.$$

Remarquons que l'apparition des exposants 2 au coordonnées qui correspondent aux facteurs $\mathbb{C}$ n'a rien de surprenant, car la norme est le déterminant de la multiplication par l'élément en question (et donc sa valeur absolue mesure le facteur par lequel changent les volumes).

Comme dans le cas des corps quadratiques réels, il faudra choisir une norme sur le $\mathbb{R}$-espace vectoriel $K_{\mathbb{R}}$. Pour rendre optimal les résultats qui suivent, on fait le choix suivant :

$$\|(x, z)\| := |x_1| + \cdots + |x_{r_1}| + 2|z_1| + \cdots + 2|z_{r_2}|.$$

5.5.2 Remarque. Dans [Samuel], on ne voit pas de norme qui apparaît, mais plutôt le choix d'une partie intégrable, convexe et symétrique par rapport à l'origine de $K_{\mathbb{R}}$. Cela revient au même (sauf peut-être si on voulait utiliser de telles parties assez sauvages pour qu'elles ne proviennent pas d'une norme). Si $\|\cdot\|$ est une norme, on lui associe la partie $B(\|\cdot\|, 1)$, la "boule" fermée de rayon un.

5.5.3 Lemme. *Pour tout (x, z) dans $K_{\mathbb{R}}$ on a :*

$$|\mathrm{N}(x, z)|^{1/d} \leq \frac{\|(x, z)\|}{d}$$

Preuve. C'est l'inégalité "moyenne géométrique" $\leq$ "moyenne arithmétique". Elle résulte de la convexité du logarithme. En effet, si $0 < x < y$, le segment de $(x, \log(x))$ à $(y, \log(y))$ est l'ensemble des $(ax + by, a\log(x) + b\log(y))$ avec $a \geq 0$, $b \geq 0$ et $a + b = 1$, d'où $a\log(x) + b\log(y) \leq \log(ax + by)$. □

5.5.4 Lemme. *Pour $r \geq 0$, on a* $\mathrm{Vol}(B(\|\cdot\|, r)) = 2^{r_1}(\pi/2)^{r_2} r^d/d!$.

Preuve. Par récurrence sur r_1 et r_2. Si $r_1 > 0$, on a :

$$\begin{aligned}\mathrm{Vol}(B_{r_1,r_2}(r)) &= \int_{x=-r}^{r} \mathrm{Vol}(B_{r_1-1,r_2}(r - |x|))\, dx = 2\int_{x=0}^{r} \mathrm{Vol}(B_{r_1-1,r_2}(r - x))\, dx = \\ &= 2\int_{x=0}^{r} 2^{r_1-1}\left(\frac{\pi}{2}\right)^{r_2} \frac{(r-x)^{r_1-1+2r_2}}{(r_1 - 1 + 2r_2)!} dx = \cdots\end{aligned}$$

Si $r_1 = 0$ et $r_2 > 0$, on a :

$$\begin{aligned}\mathrm{Vol}(B_{0,r_2}(r)) &= \int_{|z|\leq r/2} \mathrm{Vol}(B_{0,r_2-1}(r - 2|z|))\, dx\, dy = \\ &= 2\pi \int_{\rho=0}^{r/2} \mathrm{Vol}(B_{0,r_2-1}(r - 2\rho))\, d\rho = \cdots,\end{aligned}$$

où nous avons écrit $z = x + iy = \rho e^{i\phi}$. □

La chose suivante que nous voulons est une expression pour $\mathrm{Vol}(K_{\mathbb{R}}/K_{\mathbb{Z}})$.Rappelons que nous avons déjà vu que $K_{\mathbb{Z}}$ est discret dans $K_{\mathbb{R}}$ (ce qui est d'autant plus clair après la remarque que le plongement de $K_{\mathbb{Z}}$ dans $K_{\mathbb{R}}$ est, à un isomorphisme près, celui de $K_{\mathbb{Z}}$ dans $\mathbb{R}\otimes_{\mathbb{Z}} K_{\mathbb{Z}}$. Nous allons voir qu'en effet ce volume s'exprime naturellement en termes du déterminant d'une matrice de la forme trace de $K_{\mathbb{Z}}$.

5.5.5 Lemme. *Soit M un $\mathbb{Z}$-module libre de rang fini, et $b\colon M \times M \to \mathbb{Z}$ une forme bilinéaire. Pour e une base de M, notons $\mathrm{mat}_e(b)$ la matrice de b par rapport à e. Alors les déterminants $\det(\mathrm{mat}_e(b))$, avec e une base de M, sont tous égaux, et on définit le discriminant de b, noté $\mathrm{discr}(b)$, comme étant cet entier.*

5.5.6 Définition. Pour K un corps de nombres on définit le discriminant de $K_{\mathbb{Z}}$ comme le discriminant de la forme trace sur $K_{\mathbb{Z}}$. De même pour des sous-anneaux d'indice fini dans $K_{\mathbb{Z}}$.

5.5.7 Proposition. *Soit K un corps de nombres.*

1. $\mathrm{Vol}(K_{\mathbb{R}}/K_{\mathbb{Z}}) = 2^{-r_2}|\mathrm{discr}(K_{\mathbb{Z}})|^{1/2}$.
2. *Pour tout idéal a non nul de $K_{\mathbb{Z}}$, on a* $\mathrm{Vol}(K_{\mathbb{R}}/a) = 2^{-r_2}|\mathrm{discr}(K_{\mathbb{Z}})|^{1/2}\mathrm{N}(a)$.

Preuve. Bien sûr, le deuxième énoncé résulte directement du premier. Soit $x := (x_1, \ldots, x_d)$ une $\mathbb{Z}$-base de $K_{\mathbb{Z}}$. Alors :

$$\begin{aligned}
\mathrm{Vol}(K_{\mathbb{R}}/K_{\mathbb{Z}}) &= \left|\det \begin{pmatrix} \phi_1(x_1) & \cdots & \phi_1(x_d) \\ \vdots & & \vdots \\ \mathrm{Re}(\phi_{r_1+r_2}(x_1)) & \cdots & \mathrm{Re}(\phi_{r_1+r_2}(x_d)) \\ \mathrm{Im}(\phi_{r_1+r_2}(x_1)) & \cdots & \mathrm{Im}(\phi_{r_1+r_2}(x_d)) \end{pmatrix}\right| \\
&= 2^{-r_2}\left|\det \begin{pmatrix} \phi_1(x_1) & \cdots & \phi_1(x_d) \\ \vdots & & \vdots \\ \phi_{r_1+1}(x_1) & \cdots & \phi_{r_1+1}(x_d) \\ \phi_{r_1+r_2+1}(x_1) & \cdots & \phi_{r_1+r_2+1}(x_d) \\ \vdots & & \vdots \\ \phi_{r_1+r_2}(x_1) & \cdots & \phi_{r_1+r_2}(x_d) \\ \phi_{r_1+2r_2}(x_1) & \cdots & \phi_{r_1+2r_2}(x_d) \end{pmatrix}\right| \\
&= 2^{-r_2}|\det(a)|, \quad \text{avec } a_{i,j} = \phi_i(x_j).
\end{aligned}$$

Vient maintenant l'astuce :

$$(a^t a)_{i,j} = \sum_k (a^t)_{i,k} a_{k,j} = \sum_k a_{k,i} a_{k,j} = \sum_k \phi_k(x_i)\phi_k(x_j) = \mathrm{Tr}_{K/\mathbb{Q}}(x_i x_j).$$

On en conclut que

$$\det(a)^2 = \det(a)\det(a) = \det(a^t)\det(a) = \det(a^t a)) = \mathrm{discr}(K_{\mathbb{Z}}).$$

□

5.5.8 Théorème. *Soit K un corps de nombres, d son degré, r_1 et r_2 le nombre de facteurs $\mathbb{R}$ et $\mathbb{C}$ dans $K_{\mathbb{R}}$.*

1. *Soit a un idéal non nul de $K_{\mathbb{Z}}$. Alors il existe un x non nul dans a tel que :*

$$\mathrm{N}(x) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{d!}{d^d}|\mathrm{discr}(K_{\mathbb{Z}})|^{1/2}\mathrm{N}(a).$$

2. *Tout élément de $C(K_{\mathbb{Z}})$ est représenté par un idéal a de $K_{\mathbb{Z}}$ tel que :*

$$\mathrm{N}(a) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{d!}{d^d}|\mathrm{discr}(K_{\mathbb{Z}})|^{1/2}.$$

3. $C(K_{\mathbb{Z}})$ est fini.

Preuve. On procède comme on l'a déjà fait dans le cas des corps quadratiques réels. Pour la finitude de $C(K_{\mathbb{Z}})$, notons simplement qu'un idéal a de $K_{\mathbb{Z}}$ d'indice n contient n, donc est l'image réciproque de son image dans l'anneau fini $K_{\mathbb{Z}}/nK_{\mathbb{Z}}$. $\square$

Nous terminons cette section avec un exemple amusant.

5.5.9 Théorème. *L'anneau des entiers de $\mathbb{Q}(\sqrt{-163})$ est factoriel. Les nombres $n^2 - n + 41$ avec n entier et $-40 < n < 41$ sont tous des nombres premiers.*

Preuve. On vérifie que 163 est premier, et que -163 est congru à 1 modulo 4. L'anneau des entiers A de $\mathbb{Q}(\sqrt{-163})$ est donc $\mathbb{Z}[u]$, avec $u = (1 + \sqrt{-163})/2$. Le polynôme minimal de u est $f := x^2 - x + 41$, donc $A = \mathbb{Z}[u] = \mathbb{Z}[x]/(f)$.

Montrons que A est factoriel. Comme il est de Dedekind, cela revient à montrer que son groupe de classes d'idéaux est trivial. Le théorème précédent donne qu'il suffit de vérifier que les idéaux de norme au plus $2\sqrt{163}/\pi$ sont principaux ($\mathrm{discr}(A) = -163$). Il suffit donc de vérifier que les idéaux maximaux contenant 2, 3, 5 ou 7 sont principaux. Cela résulte de ce que f est irréductible dans $\mathbb{F}_p[x]$ pour tous les p dans cette liste. On a donc montré que A est factoriel.

Pour montrer le deuxième énoncé sans vérifier cela cas par cas, on utilise une propriété de la norme. Un calcul montre que $N(a + bu) = a^2 + ab + 41b^2 = (a + b/2)^2 + (41 - 1/4)b^2$, pour a et b dans $\mathbb{Q}$. On voit donc que pour a et b dans $\mathbb{Z}$ avec $b \neq 0$, on a $N(a + bu) \geq 41$.

Soit p un nombre premier et supposons que f est réductible dans $\mathbb{F}_p[x]$. Alors A a un idéal de norme p, donc un élément de norme p. Donc f est irréductible dans $\mathbb{F}_p[x]$ si $p < 41$.

Si p est premier et divise un nombre de la forme $n^2 - n + 41$, alors f a une racine dans $\mathbb{F}_p$. On en déduit que si p est premier et divise $n^2 - n + 41$ pour un n dans $\mathbb{Z}$, alors $p \geq 41$. On en conclut que si $|n^2 - n + 41| < 41^2$, alors $n^2 - n + 41$ est premier. Pour finir : on a $|n^2 - n| < 41^2 - 41$ si et seulement si $-40 < n < 41$. $\square$

6 Le théorème des unités.

6.1 Théorème. *Soit K un corps de nombres.*

1. *Pour x dans $K_{\mathbb{Z}}$ on a $x \in K_{\mathbb{Z}}^* \iff \mathrm{N}_{K/\mathbb{Q}}(x) = \pm 1$.*
2. *Le groupe $(K_{\mathbb{Z}}^*)_{\mathrm{tors}}$ est cyclique et fini ; on a $(K_{\mathbb{Z}}^*)_{\mathrm{tors}} = \mu(K) := K_{\mathrm{tors}}^*$, le groupe des racines de l'unité dans K.*
3. *Le quotient $K_{\mathbb{Z}}^*/\mu(K)$ est libre de rang r_1+r_2-1, où r_1 (resp. r_2) est le nombre de facteurs $\mathbb{R}$ (resp. $\mathbb{C}$) dans $K_{\mathbb{R}} = \mathbb{R} \otimes_{\mathbb{Q}} K$.*

Preuve. Soit x dans $K_{\mathbb{Z}}$. Si x est dans $K_{\mathbb{Z}}^*$, alors $1 = \mathrm{N}(1) = \mathrm{N}(x^{-1}x) = \mathrm{N}(x^{-1})\mathrm{N}(x)$, avec $\mathrm{N}(x^{-1})$ et $\mathrm{N}(x)$ dans $\mathbb{Z}$. Si $\mathrm{N}(x) = \pm 1$, alors $\cdot x\colon K_{\mathbb{Z}} \to K_{\mathbb{Z}}$ est un isomorphisme de $\mathbb{Z}$-modules (car de déterminant inversible), donc il existe y dans $K_{\mathbb{Z}}$ tel que $yx = 1$. Les autres assertions prendront plus de temps. Nous numérotons les plongements $\phi_i\colon K \to \mathbb{C}$ comme avant, ainsi que $\phi\colon K \to K_{\mathbb{R}}$. Notons $d := \dim_{\mathbb{Q}}(K)$. Nous considérons le morphisme de groupes suivant :

$$\begin{aligned} L\colon K^* &\xrightarrow{\phi} K_{\mathbb{R}}^* = \mathbb{R}^{*,r_1} \times \mathbb{C}^{*,r_2} \xrightarrow{|\cdot|} (\mathbb{R}_{>0}^*)^{r_1+r_2} \xrightarrow{\log} \mathbb{R}^{r_1+r_2}, \\ x &\mapsto (\log|\phi_1(x)|, \ldots, \log|\phi_{r_1+r_2}(x)|). \end{aligned}$$

Comme pour tout x dans $K_{\mathbb{Z}}^*$ on a $1 = |\mathrm{N}(x)| = |\phi_1(x)\cdots\phi_d(x)|$, on constate que :

$$L(K_{\mathbb{Z}}^*) \subset H := \{x \in \mathbb{R}^{r-1+r_2} \mid x_1 + \cdots + x_{r_1} + 2x_{r_1+1} + \cdots + 2x_{r_1+r_2} = 0\}.$$

6.1.1 Lemme. *Pour tout $r \geq 0$, l'ensemble $\{x \in K_{\mathbb{Z}}^* \mid \forall i\colon |L(x)_i| \leq r\}$ est fini.*

Preuve. Pour un tel x, on a, pour tout i : $|\log|\phi_i(x)|| \leq r$, d'où $e^{-r} \leq |\phi_i(x)| \leq e^r$. Cela donne des bornes sur les coefficients du polynôme minimal f_x de x sur $\mathbb{Q}$; bornes en termes de d et r seulement. Mais f_x est à coefficients dans $\mathbb{Z}$, ce qui implique qu'il n'y a qu'un nombre fini de possibilités pour f_x, donc pour x. □

6.1.2 Corollaire. *Le noyau de $L|_{K_{\mathbb{Z}}^*}\colon K_{\mathbb{Z}}^* \to \mathbb{R}^{r_1+r_2}$ est fini, et $L(K_{\mathbb{Z}}^*)$ est discret dans H.*

6.1.3 Lemme. $\ker(L|_{K_{\mathbb{Z}}^*}) = \mu(K) = (K_{\mathbb{Z}}^*)_{\mathrm{tors}}$.

Preuve. L'inclusion “$\ker(L|_{K_{\mathbb{Z}}^*}) \subset \mu(K)$” vient du corollaire. Si x est dans $\mu(K)$, x est entier sur $\mathbb{Z}$ (car racine d'un $x^n - 1$ avec $n \geq 1$, et $|\phi_i(x)| = 1$ pour tout i). □

Comme $L(K_{\mathbb{Z}}^*)$ est discret dans H, $L(K_{\mathbb{Z}}^*)$ est libre de rang au plus $r_1 + r_2 - 1$. Pour terminer, il suffit donc de montrer que $L(K_{\mathbb{Z}}^*)$ contient $r_1 + r_2 - 1$ éléments $\mathbb{R}$-linéairement indépendants. Donc, en fait, nous montrons quelque chose plus fort que ce qui est demandé dans le théorème : $L(K_{\mathbb{Z}}^*)$ est un réseau dans H. Pour simplifier la notation dans ce qui suit, nous ne traiterons que le cas où $r_2 = 0$ (et $r_1 > 1$). On a alors : $d = r_1$, $K_{\mathbb{R}} = \mathbb{R}^d$, et $r_1 + r_2 - 1 = d - 1$. Nous notons $d_K := |\mathrm{discr}(K)|$ et $l := \log(d_K^{1/2})$ (on a $d_K > 1$ car $K \neq \mathbb{Q}$; voir les exercices).

6.1.4 Proposition. *Pour tout $i < d$ il existe un u_i dans $K_{\mathbb{Z}}^*$ tel que :*

$$\begin{aligned} &|L(u_i)_i| > (d-2)l, \\ &|L(u_i)_j| \leq l \text{ si } i \neq j < d. \end{aligned}$$

Admettons pour l'instant cette proposition, et montrons que $L(u_1), \ldots, L(u_{d-1})$ sont $\mathbb{R}$-linéairement indépendants dans $\mathbb{R}^d$. Notons $a_{i,j} := L(u_i)_j$ pour $1 \leq i, j < d$. Donc a est dans $\mathrm{M}_{d-1}(\mathbb{R})$. On écrit $a = \Delta + r$, avec Δ la partie diagonale de a, et r la partie hors diagonale. Pour $0 \neq v$ dans $\mathbb{R}^{d-1}$ on a alors :

$$\|\Delta v\|_{\sup} > (d-2)l\|v\|_{\sup}, \quad \|rv\|_{\sup} \leq (d-2)l\|v\|_{\sup},$$

d'où $av \neq 0$. Il ne reste maintenant qu'à prouver la proposition.

Preuve. (De la proposition.) Par symétrie, on peut supposer que $i = d-1$. Pour $\lambda > 0$ et $\mu > 0$, nous définissons :

$$B_{\lambda,\mu} := \{x \in \mathbb{R}^d \mid |x_i| \leq 1 \text{ si } i < d-1, |x_{d-1}| \leq \lambda, |x_d| \leq \mu\}.$$

Comme $B_{\lambda,\mu}$ est un produit d'intervalles, le calcul de son volume est immédiat, et donne :

$$\mathrm{Vol}(B_{\lambda,\mu}) = 2^d \lambda\mu.$$

L'argument de Minkowski dit que si $\mathrm{Vol}(\frac{1}{2}B_{\lambda,\mu}) \geq \mathrm{Vol}(\mathbb{R}^d/\phi(K_{\mathbb{Z}}))$, alors $B_{\lambda,\mu}$ contient un élément non nul x de $K_{\mathbb{Z}}$. Par les calculs déjà faits, on sait que $\mathrm{Vol}(\mathbb{R}^d/\phi(K_{\mathbb{Z}})) = d_K^{1/2}$, et $\mathrm{Vol}(\frac{1}{2}B_{\lambda,\mu}) = \lambda\mu$. Nous prendrons donc toujours λ et μ tel que $\lambda\mu = d_K^{1/2}$, et nous noterons $B_{\lambda,\mu}$ simplement par B_λ. Nous prendrons en fait des λ de plus en plus grand.

Pour x non nul dans $B_\lambda \cap K_{\mathbb{Z}}$ on sait :

$$\begin{aligned} 1 \leq |\mathrm{N}(x)| = |\phi_1(x) \cdots \phi_d(x)| \leq \lambda\mu = d_K^{1/2}, \\ |\phi_i(x)| \geq d_K^{-1/2} \quad \text{si } i < d-1, \\ |\phi_{d-1}(x)| \geq \mu^{-1} = \lambda d_K^{-1/2}. \end{aligned}$$

Prenons $c > 0$ assez grand ($c \geq d_K^{(d-1)/2}$ suffira, par exemple). On prend $\lambda_1 := d_K^{1/4}$, par exemple. Cela nous donne x_1 dans $B_{\lambda_1} \cap K_{\mathbb{Z}}$. On prend $\lambda_2 > c\lambda_1$. Cela nous donne x_2. On prend $\lambda_3 > c\lambda_2$, etc. Cela nous donne une suite $x_1, x_2, \ldots$ dans $K_{\mathbb{Z}}$, avec, pour tout i, $|\mathrm{N}(x_i)| \leq d_K^{1/2}$. Mais, pour tout $B > 0$, l'ensemble des idéaux de $K_{\mathbb{Z}}$ d'indice au plus B est fini (un idéal d'indice n contient $nK_{\mathbb{Z}}$, donc provient d'un idéal du quotient fini $K_{\mathbb{Z}}/nK_{\mathbb{Z}}$). Nous prenons $i < j$ tel que $K_{\mathbb{Z}}x_i = K_{\mathbb{Z}}x_j$. Mais alors $u := x_j/x_i$ est dans $K_{\mathbb{Z}}^*$. Vérifions que ce u satisfait aux conditions de la proposition. On sait :

$$\begin{aligned} \text{pour } k < d-1\colon \phi_k(u) = \phi_k(x_j)/\phi_k(x_i), \quad d_K^{-1/2} \leq |\phi_k(x_j)/\phi_k(x_i)| \leq d_K^{1/2}, \\ |\phi_{d-1}(u)| = |\phi_{d-1}(x_j)/\phi_{d-1}(x_i)| \geq \lambda_j d_K^{-1/2}/\lambda_i > c d_K^{-1/2}. \end{aligned}$$

On a donc :

$$\begin{aligned} |L(u)_i| \leq l, \quad \text{si } i < d-1, \\ |L(u)_{d-1}| \geq \log(c) - l. \end{aligned}$$

On veut : $\log(c) - l \geq (d-2)l$, ce qui équivaut à $c \geq l^{d-1}$. □

□

6.1.5 Remarques. 1. Le cas $r_1 = 2, r_2 = 0$ est bien plus facile, et déjà bien intéressant.

2. Comparer à la sphère de Riemann $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$. Si on enlève r points de cette sphère, l'anneau A des fonctions méromorphes sur la sphère et holomorphe en dehors des points enlevés est isomorphe à $\mathbb{C}^* \times \mathbb{Z}^{r-1}$, le facteur $\mathbb{C}^*$ correspond aux fonctions constantes, et le facteur $\mathbb{Z}^{r-1}$ mesure les pôles et zéros. Il paraît donc que les corps de nombres se comportent comme $\mathbb{P}^1(\mathbb{C})$: si, en r points, on n'impose pas de condition, alors l'anneau qui résulte a comme groupe des unités, modulo les unités triviales, rang $r-1$.

3. L'analogue du théorème des unités est vrai pour les courbes algébriques non singulières et projectives.

4. Si $A \subset K_{\mathbb{Z}}$ est un sous-anneau d'indice fini, alors $A^*/\mu(A)$ est encore libre de rang $r_1 + r_2 - 1$ (sans preuve).

5. Avec les outils dont on dispose maintenant, on peut résoudre certaines équations, par exemple l'équation de Fermat en degré 5. En effet, on montre que l'anneau des entiers de $\mathbb{Q}(\zeta_5)$ est $\mathbb{Z}[\zeta_5]$, que le groupe des classes d'idéaux de $\mathbb{Z}[\zeta_5]$ est trivial, et que $\mathbb{Z}[\zeta_5]^*$ est engendré par $-\zeta_5$ et le nombre d'or $\zeta_5 + \zeta_5^{-1}$. Ensuite, on regarde dans [Swin].

6.2 Les corps quadratiques réels.

Soit $d > 1$ sans facteur carré, $K := \mathbb{Q}(\sqrt{d})$. Nous rappelons que $K_{\mathbb{Z}} = \mathbb{Z}[\sqrt{d}]$ si $d \not\equiv 1$ mod 4, et $K_{\mathbb{Z}} = \mathbb{Z}[(1+\sqrt{d})/2]$ si $d \equiv 1$ mod 4. Comme tout corps qui admet un plongement dans $\mathbb{R}$, $\mu(K) = \{1, -1\}$. Le théorème des unités dit donc que $K_{\mathbb{Z}}^*$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.

6.2.1 Définition. On appelle unité fondamentale de $K_{\mathbb{Z}}$ un élément de $K_{\mathbb{Z}}^*$ qui, ensemble avec -1, engendre $K_{\mathbb{Z}}^*$. Il y a donc exactement 4 de telles unités : si u en est un, les autres sont $-u$, u^{-1} et $-u^{-1}$.

Voici comment on peut procéder pour trouver les unités fondamentales. Si $u = x + y\sqrt{d} \neq \pm 1$ (avec x et y dans $\frac{1}{2}\mathbb{Z}$ s'il le faut) est dans $K_{\mathbb{Z}}^*$, $-u$, u^{-1} et $-u^{-1}$ sont des unités, et ce sont les quatre éléments $\pm x \pm y\sqrt{d}$. Exactement un d'entre u, $-u$, u^{-1} et $-u^{-1}$, appelons le v, est tel que $\phi_1(v) > 1$; c'est celui avec $x > 0$ et $y > 0$. Pour L le "plongement" logarithmique $L\colon K_{\mathbb{Z}}^* \to \mathbb{R}\cdot(1,-1) \subset \mathbb{R}^2$, on a $L(-u) = L(u)$, et $L(u^{-1}) = L(-u^{-1}) = -L(u)$. Il en résulte que $u = x + y\sqrt{d}$ dans $K_{\mathbb{Z}}^*$ avec $x > 0$ et $y > 0$ est fondamentale si et seulement si $x + y\sqrt{d}$ est minimal parmi les $u + v\sqrt{d}$ avec $u > 0$ et $v > 0$ tels que $u + v\sqrt{d} \in K_{\mathbb{Z}}$ et $u^2 - dv^2 = \pm 1$.

Par exemple, $1 + \sqrt{2}$ est une unité fondamentale de $\mathbb{Z}[\sqrt{2}]$, et $(1+\sqrt{5})/2$ est une unité fondamentale de $\mathbb{Z}[(1+\sqrt{5})/2]$. Il y a une façon intéressante de calculer des unités fondamentales avec des fractions continues, ce qui n'est pas surprenant, car si $x^2 - dy^2 = \pm 1$, $|x/y - \sqrt{d}|$ est petit ; voir la section suivante pour quelques détails.

Pour comparer $K_{\mathbb{Z}}^*$ à $\mathbb{Z}[\sqrt{d}]^*$, démontrons la proposition suivante.

6.2.2 Proposition. *Si $d \not\equiv -3 \bmod 8$, alors $\mathbb{Z}[\sqrt{d}]^* = K_{\mathbb{Z}}^*$. Si $d \equiv -3 \bmod 8$, $\mathbb{Z}[\sqrt{d}]^*$ est d'indice 1 ou 3 dans $K_{\mathbb{Z}}^*$. Dans tous les cas, $\mathbb{Z}[\sqrt{d}]^*$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.*

Preuve. Si $d \not\equiv 1 \bmod 4$, $K_{\mathbb{Z}} = \mathbb{Z}[\sqrt{d}]$, donc $K_{\mathbb{Z}}^* = \mathbb{Z}[\sqrt{d}]^*$. Supposons donc que $d \equiv 1 \bmod 4$. Le polynôme minimal de $(1+\sqrt{d})/2$ sur $\mathbb{Q}$ est $t^2 - t - (d-1)/4$. Donc $K_{\mathbb{Z}}/2K_{\mathbb{Z}}$ est isomorphe, en tant qu'anneau, à $\mathbb{F}_2[t]/(t^2 - t - (d-1)/4)$. Si $d \equiv 1 \bmod 8$ cela donne $\mathbb{F}_2 \times \mathbb{F}_2$, et si $d \equiv -3 \bmod 8$ cela donne $\mathbb{F}_4$.

D'autre part, notons $f\colon K_{\mathbb{Z}} \to K_{\mathbb{Z}}/2K_{\mathbb{Z}}$ la réduction modulo 2. Comme $\mathbb{Z}[\sqrt{d}]$ est d'indice 2 dans $K_{\mathbb{Z}}$, $\mathbb{Z}[\sqrt{d}]$ contient $2K_{\mathbb{Z}}$, et on a donc $\mathbb{Z}[\sqrt{d}] = f^{-1}f(\mathbb{Z}[\sqrt{d}])$, et $f(\mathbb{Z}[\sqrt{d}])$ est d'indice 2 dans $K_{\mathbb{Z}}/2K_{\mathbb{Z}}$. Comme $f(\mathbb{Z}[\sqrt{d}])$ est une $\mathbb{F}_2$-sous-algèbre de $K_{\mathbb{Z}}/2K_{\mathbb{Z}}$, $f(\mathbb{Z}[\sqrt{d}])$ contient $\mathbb{F}_2$, qui est déjà d'indice 2 ; on conclut que $f(\mathbb{Z}[\sqrt{d}]) = \mathbb{F}_2$. On a donc $\mathbb{Z}[\sqrt{d}] = f^{-1}\mathbb{F}_2$. (Bien sûr, on peut démontrer ceci également par un calcul.) Considérons maintenant la suite de morphismes de groupes :

$$\mathbb{Z}[\sqrt{d}]^* \longrightarrow K_{\mathbb{Z}}^* \longrightarrow (K_{\mathbb{Z}}/2K_{\mathbb{Z}})^*.$$

Il est clair que $\mathbb{Z}[\sqrt{d}]^* \to K_{\mathbb{Z}}^*$ est injectif. Montrons que cette suite est exacte. Soit x dans $\mathbb{Z}[\sqrt{d}]^*$; alors l'image de x dans $(K_{\mathbb{Z}}/2K_{\mathbb{Z}})^*$ est dans $\mathbb{F}_2^*$, donc 1. Soit x dans $K_{\mathbb{Z}}^*$ avec image 1 dans $(K_{\mathbb{Z}}/2K_{\mathbb{Z}})^*$; alors x est dans $f^{-1}\mathbb{F}_2 = \mathbb{Z}[\sqrt{d}]$, et de même pour x^{-1}, ce qui donne $x \in \mathbb{Z}[\sqrt{d}]^*$. Comme $(\mathbb{F}_2 \times \mathbb{F}_2)^*$ est trivial, et $\mathbb{F}_4^*$ d'ordre 3, on obtient ce qu'il faut. $\square$

Pour trouver une unité fondamentale de $\mathbb{Z}[\sqrt{d}]$ on peut procéder comme pour $\mathbb{Q}(\sqrt{d})_{\mathbb{Z}}$, mais en fait, c'est plus simple. Comme dans le cas précédent, on voit qu'il existe une unité fondamentale $u = x + y\sqrt{d}$ avec $x > 0$ et $y > 0$ (x et y entiers, maintenant). Mais on constate alors que si on écrit $u^n = x_n + y_n\sqrt{d}$, alors $y_n > y$ pour $n > 1$. Il en résulte que pour trouver u on teste pour $y = 1, 2, \ldots$ si $dy^2 \pm 1$ est un carré, et on arrête si tel est le cas, avec disons $x^2 - dy^2 = \pm 1$. Alors $x + y\sqrt{d}$ est une unité fondamentale.

Nous sommes maintenant en mesure de dire quelque chose sur l'équation de Pell (ou de Pell-Fermat, en France). Cette équation est la suivante : $x^2 - dy^2 = e$, avec d comme en haut ($d > 1$, sans facteur carré) et e dans $\mathbb{Z}$ donné. L'ensemble des solutions (x, y) dans $\mathbb{R}^2$ est un hyperbole. S'il y a une solution dans $\mathbb{Q}^2$, on obtient toutes les solutions dans $\mathbb{Q}^2$ en intersectant avec des droites passant par la solution de départ. Ce qui nous intéresse ici, est l'ensemble des solutions dans $\mathbb{Z}^2$. Commençons par une remarque immédiate. Pour $(x, y) \in \mathbb{Z}^2$ avec $x^2 - dy^2 = e$, $x + y\sqrt{d}$ est un élément de norme e de $\mathbb{Z}[\sqrt{d}]$, et l'application :

$$\{(x, y) \in \mathbb{Z}^2 \mid x^2 - dy^2 = e\} \longrightarrow \{z \in \mathbb{Z}[\sqrt{d}] \mid \mathrm{N}(z) = e\}, \quad (x, y) \mapsto x + y\sqrt{d}$$

est une bijection.

6.2.3 Théorème. *Soit u une unité fondamentale de $\mathbb{Z}[\sqrt{d}]$.*

1. *Les solutions de l'équation $x^2 - dy^2 = \pm 1$ correspondent alors, via la bijection ci-dessus, aux $\pm u^n$, $n \in \mathbb{Z}$.*
2. *Pour $e \neq 0$ dans $\mathbb{Z}$, $\mathbb{Z}[\sqrt{d}]^*$ opère librement sur l'ensemble $\{z \in \mathbb{Z}[\sqrt{d}] \mid \mathrm{N}(z) = \pm e\}$. Deux éléments z_1 et z_2 de cet ensemble sont dans la même orbite si et seulement si $\mathbb{Z}[\sqrt{d}]z_1 = \mathbb{Z}[\sqrt{d}]z_2$. Ainsi, l'ensemble des orbites de cette action est en bijection avec l'ensemble des idéaux de $\mathbb{Z}[\sqrt{d}]$ qui sont d'indice $|e|$ et principaux.*

6.3 Fractions continues.

Soit $d > 1$ sans facteur carré. Nous avons vu que $\mathbb{Z}[\sqrt{d}]^*$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$. En pratique, pour trouver une unité fondamentale, on utilise le développement de $\sqrt{d}$ en fraction continue. Ici, je veux juste donner quelques indications et un exemple de comment cela marche. Pour des détails, on est invité à consulter les livres [HW] et [Hua].

6.3.1 Définition. Soient $n \geq 0$ un entier, et $a_0, \ldots, a_n$ des variables. La fraction continue associée est la fraction :

$$[a_0, a_1, \ldots, a_n] := a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}}$$

6.3.2 Lemme. *Avec ces notations, on a :*

$$[a_0, a_1, \ldots, a_n] = a_0 + \begin{pmatrix} 0 & 1 \\ 1 & a_1 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & a_{n-1} \end{pmatrix} a_n^{-1} = a_0 + \begin{pmatrix} 0 & 1 \\ 1 & a_1 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & a_n \end{pmatrix} 0,$$

où les matrices opèrent par homographies : $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)x = (ax+b)/(cx+d)$.

6.3.3 Définition. Soit x un nombre réel non rationnel. Le développement de x en fraction continue est défini par : $a_0 := \lfloor x \rfloor$, $x_1 := 1/(x - a_0)$, $a_1 := \lfloor x_1 \rfloor$, $x_2 := 1/(x_1 - a_1)$, etc. Si x est rationnel, on applique le même algorithme, mais on s'arrête quand x_n est entier.

6.3.4 Proposition. *Soit x réel et irrationnel. Soit $a_0, a_1, \ldots$ la suite associée à x par la définition précédente. Ecrivons $[a_0, a_1, \ldots, a_n] = p_n/q_n$. Alors $|p_n/q_n - x| < 1/q_n^2$. Si p et $q > 0$ sont des entiers premiers entre eux et $|p/q - x| < 1/2q^2$, alors il existe n tel que $(p, q) = (p_n, q_n)$. La suite $a_0, a_1, \ldots$ devient périodique (dans le sens qu'il existe N et $m \geq 1$ tels que $a_{n+m} = a_n$ si $n > N$) si et seulement si x est algébrique et de degré deux sur $\mathbb{Q}$. Si $x = \sqrt{d}$ avec $d > 1$ sans facteur carrés, il existe n tel que $p_n^2 - dq_n^2 = \pm 1$, et le premier tel n donne une unité fondamentale $p_n + q_n\sqrt{d}$ de $\mathbb{Z}[\sqrt{d}]$.*

7 La réciprocité quadratique.

7.1 Décomposition des nombres premiers.

Soit K un corps de nombres, et p un nombre premier. L'anneau $A := K_{\mathbb{Z}}/pK_{\mathbb{Z}}$ est alors une $\mathbb{F}_p$-algèbre de dimension $d := \dim_{\mathbb{Q}}(K)$. Nous avons vu dans un exercice que A n'a qu'un nombre fini d'idéaux maximaux, disons $m_1, \ldots, m_r$, et que le morphisme canonique

$$A \to A/m_1^d \times \cdots \times A/m_r^d$$

est un isomorphisme de $\mathbb{F}_p$-algèbres. Définissons des entiers $n_i > 0$ par : $m_i^{n_i - 1} \neq m_i^{n_i} = m_i^{n_i + 1}$. Notons $\widetilde{m_i}$ l'image inverse de m_i dans $K_{\mathbb{Z}}$ via $K_{\mathbb{Z}} \to A \to A/m_i$.

7.1.1 Proposition. *Avec ces notations, on a l'égalité suivante d'idéaux de $K_{\mathbb{Z}}$:*

$$pK_{\mathbb{Z}} = \widetilde{m_1}^{n_1} \cdots \widetilde{m_r}^{n_r}.$$

Preuve. Montrons d'abord que $\widetilde{m_1}^{n_1} \cdots \widetilde{m_r}^{n_r} \subset pK_{\mathbb{Z}}$. En effet, comme

$$m_1^{n_1} \cdots m_r^{n_r} = m_1^{n_1} \cap \cdots \cap m_r^{n_r} = 0$$

dans A, l'image de $\widetilde{m_1}^{n_1} \cdots \widetilde{m_r}^{n_r}$ dans A est nulle. D'où l'inclusion. Il ne reste qu'à montrer que $pK_{\mathbb{Z}}$ et $\widetilde{m_1}^{n_1} \cdots \widetilde{m_r}^{n_r}$ ont même norme. La norme de $pK_{\mathbb{Z}}$ est $|A| = p^d$. Notons k_i le corps $A/m_i = K_{\mathbb{Z}}/\widetilde{m_i}$. Alors, pour tout i, et pour tout $n \geq 0$, $\widetilde{m_i^n}/\widetilde{m_i}^{n+1}$ est un k_i-espace vectoriel de dimension un. Le théorème Chinois dit que l'application canonique :

$$K_{\mathbb{Z}}/\widetilde{m_1}^{n_1} \cdots \widetilde{m_r}^{n_r} \longrightarrow K_{\mathbb{Z}}/\widetilde{m_1}^{n_1} \times \cdots \times K_{\mathbb{Z}}/\widetilde{m_r}^{n_r}$$

est un isomorphisme. Il suffit donc de montrer que $K_{\mathbb{Z}}/\widetilde{m_i}^{n_i}$ est de même cardinal que $A/m_i^{n_i}$. Mais les deux sont de cardinal $|k_i|^{n_i}$: pour le premier, cela est même vrai pour tout exposant, pour le deuxième, il faut utiliser que les inclusions $A \supset m_i \supset \cdots \supset m_i^{n_i}$ sont strictes. □

7.1.2 Proposition. *Avec les mêmes notations, les conditions suivantes sont équivalentes :*

1. *p ne divise pas $\mathrm{discr}(K_{\mathbb{Z}})$;*
2. *A est réduit, i.e., 0 est le seul nilpotent de A ;*
3. *tous les n_i sont 1.*

Preuve. L'équivalence des conditions 1 et 2 a déjà été notée dans la proposition 4.11.1. Montrons l'équivalence des deux dernières. Tout élément de $A/m_i^{n_i}$ qui est dans $m_i/m_i^{n_i}$ est nilpotent. Donc $A/m_i^{n_i}$ est réduit si et seulement si $n_i = 1$. Comme A est le produit des $A/m_i^{n_i}$, A est réduit si et seulement si tous les $A/m_i^{n_i}$ les sont. □

7.1.3 Définition. On dit que p est ramifié dans K, ou dans $K_{\mathbb{Z}}$, si la $\mathbb{F}_p$-algèbre $K_{\mathbb{Z}}/pK_{\mathbb{Z}}$ n'est pas réduite.

Dans la section suivante, nous utiliserons le résultat suivant.

7.1.4 Proposition. *Soient $\mathbb{Q} \to K \to L$ des extensions finies, et p un nombre premier. Si p est ramifié dans K, il l'est dans L.*

Preuve. Supposons que p soit non ramifié dans L. Il nous faut montrer que p est non ramifié dans K. Nous savons donc que $L_{\mathbb{Z}}/pL_{\mathbb{Z}}$ est réduit, et il nous faut montrer que $K_{\mathbb{Z}}/pK_{\mathbb{Z}}$ l'est également. Alors, le morphisme $K \to L$ induit un morphisme $K_{\mathbb{Z}} \to L_{\mathbb{Z}}$. Supposons que x dans $K_{\mathbb{Z}}$ soit dans le noyau de $K_{\mathbb{Z}} \to L_{\mathbb{Z}} \to L_{\mathbb{Z}}/pL_{\mathbb{Z}}$. Cela veut dire que l'image de x dans $L_{\mathbb{Z}}$ est de la forme py, avec y dans $L_{\mathbb{Z}}$. Mais alors x/p est entier sur $\mathbb{Z}$, donc x est dans $pK_{\mathbb{Z}}$. Il en résulte que le morphisme $K_{\mathbb{Z}} \to L_{\mathbb{Z}}$ induit une injection $K_{\mathbb{Z}}/pK_{\mathbb{Z}} \to L_{\mathbb{Z}}/pL_{\mathbb{Z}}$. Cela montre que $K_{\mathbb{Z}}/pK_{\mathbb{Z}}$ est réduit. □

7.1.5 Définition. Soit K une extension de degré deux de $\mathbb{Q}$, et soit p un nombre premier. On dit que p est inerte dans K si $K_{\mathbb{Z}}/pK_{\mathbb{Z}}$ est un corps, ou, ce qui revient au même, si p est premier dans $K_{\mathbb{Z}}$. On dit que p est scindé, ou décomposé dans K si $K_{\mathbb{Z}}/pK_{\mathbb{Z}}$ est isomorphe à $\mathbb{F}_p \times \mathbb{F}_p$, ou, ce qui revient au même, si $pK_{\mathbb{Z}} = m_1 m_2$ avec m_2 et m_2 deux idéaux maximaux distincts de $K_{\mathbb{Z}}$.

7.1.6 Proposition. *Soit $d \neq 1$ un entier sans facteur carré, et $K = \mathbb{Q}(\sqrt{d})$. On a $K_{\mathbb{Z}} = \mathbb{Z}[x]/(f)$, avec $f = x^2 - d$ si $d \neq 1$ mod 4, et avec $f = x^2 - x - (d-1)/4$ si $d = 1$ mod 4. Notons $\overline{f}$ l'image de f dans $\mathbb{F}_p[x]$. Alors :*

1. *p est décomposé dans K si et seulement si $\overline{f}$ a deux racines distinctes dans $\mathbb{F}_p$;*
2. *p est inerte dans K si et seulement si $\overline{f}$ n'a pas de racine dans $\mathbb{F}_p$;*
3. *p est ramifié dans K si et seulement si $\overline{f}$ a exactement une racine dans $\mathbb{F}_p$.*

A l'aide de la réciprocité quadratique nous pourrons montrer que la condition que p soit scindé, inerte ou ramifié ne dépend que de la classe de p modulo le discriminant de K.

7.2 Quel est le sous-corps quadratique de $\mathbb{Q}(\zeta_p)$?

Pour la preuve de la réciprocité quadratique que nous allons donner dans la section suivante, il nous faut un renseignement dont nous nous occupons dans cette section.

7.2.1 Proposition. *Soit p un nombre premier. Soit $\mathbb{Q}(\zeta_p)$ l'extension de $\mathbb{Q}$ engendrée par une racine de l'unité d'ordre p (dans $\mathbb{C}$, par exemple). Alors le polynôme minimal de ζ_p sur $\mathbb{Q}$ est $\Phi_p := (x^p - 1)/(x - 1)$. L'extension $\mathbb{Q} \to \mathbb{Q}(\zeta_p)$ est galoisienne, et on a un isomorphisme de groupes*

$$f\colon \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \longrightarrow \mathbb{F}_p^*,$$

tel que, pour tout σ dans $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$,

$$\sigma(\zeta_p) = \zeta_p^{f(\sigma)}.$$

Preuve. Notons $\mathbb{Q} \to K$ une extension de décomposition de $x^p - 1$, et ζ_p une de ses racines. Comme les racines de $x^p - 1$ sont des puissances de ζ_p, on a $K = \mathbb{Q}(\zeta_p)$. Le polynôme Φ_p est irréductible par le critère d'Eisenstein (on applique ce critère à $\Phi_p(x+1)$ et p). L'extension

$\mathbb{Q} \to K$ est donc de degré $p-1$. Notons G le groupe de Galois de K sur $\mathbb{Q}$. Tout élément de G induit un automorphisme du sous-groupe $\mu_p(K) := \{z \in K \mid z^p = 1\}$ de K^*. Comme $\mu_p(K)$ est d'ordre p, c'est un espace vectoriel de dimension un sur $\mathbb{F}_p$, donc son groupe d'automorphismes est $\mathbb{F}_p^*$. Nous avons donc un morphisme de groupes $f\colon G \to \mathbb{F}_p^*$ tel que pour tout σ dans G, et tout z dans $\mu_p(K)$: $\sigma(z) = z^{f(\sigma)}$. Il reste à montrer que f est un isomorphisme. Comme les deux sont d'ordre $p-1$, il suffit de montrer que f est injectif. Mais cela est clair, car comme K est engendré par ζ_p, tout σ dans G est déterminé par $\sigma(\zeta_p)$. $\square$

7.2.2 Théorème. *Soit p un nombre premier et $\mathbb{Q}(\zeta_p)$ comme en haut. Alors l'inclusion de $\mathbb{Z}[\zeta_p]$ dans $\mathbb{Q}(\zeta_p)_{\mathbb{Z}}$ est une égalité. Tout nombre premier différent de p est non ramifié dans $\mathbb{Q}(\zeta_p)$.*

Preuve. Nous allons appliquer le critère 4.11.3. Comme ζ_p est entier sur $\mathbb{Z}$, $\mathbb{Z}[\zeta_p] \subset \mathbb{Q}(\zeta_p)_{\mathbb{Z}}$. Le fait que la dérivée de $x^p - 1$ soit px^{p-1} implique que dans n'importe quel corps de caractéristique différente de p, $x^p - 1$ n'a pas de racines multiples. Il en résulte que le discriminant de Φ_p est, à un signe près, une puissance de p. Par ce que nous avons vu dans les exercices, cela implique que $\mathrm{discr}(\mathbb{Z}[\zeta_p])$ est, à un signe près, une puissance de p, et que par conséquent, $\mathrm{discr}(\mathbb{Q}(\zeta_p)_{\mathbb{Z}})$ est, à un signe près, une puissance de p. Donc tout premier différent de p est non ramifié dans $\mathbb{Q}(\zeta_p)$.

Pour finir, il nous faut montrer que pour tout idéal maximal m de $\mathbb{Z}[\zeta_p]$ contenant p, on a $\dim_{A/m}(m/m^2) \leq 1$. Ecrivons $\mathbb{Z}[\zeta_p] = \mathbb{Z}[x]/(\Phi_p)$ (avec x s'envoyant vers ζ_p). Cela montre que $\mathbb{Z}[\zeta_p]/p\mathbb{Z}[\zeta_p]$ est isomorphe à $\mathbb{F}_p[x]/(x-1)^{p-1}$, et on en déduit que $\mathbb{Z}[\zeta_p]$ a un unique idéal maximal m contenant p, et qu'on a $m = (p, \zeta_p - 1)$. Posons $y = x - 1$. Alors on a :

$$\Phi_p = \frac{x^p - 1}{x - 1} = \frac{(y+1)^p - 1}{y} = y^{p-1} + py^{p-2} + \cdots + p,$$

qui est un polynôme d'Eisenstein pour le premier p. On voit que p est dans m^2, ce qui implique que m/m^2 est engendré par y, donc de dimension au plus un. $\square$

7.2.3 Proposition. *Soit $p \neq 2$ un nombre premier. Alors $\mathbb{Q}(\zeta_p)$ contient un unique extension quadratique K de $\mathbb{Q}$. On a $K = \mathbb{Q}(\sqrt{p})$ si $p = 1$ mod 4, et $K = \mathbb{Q}(\sqrt{-p})$ si $p = -1$ mod 4.*

Preuve. Le groupe $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ est isomorphe à $\mathbb{F}_p^*$, qui est cyclique d'ordre $p-1$. Comme $p \neq 2$, $p-1$ est pair. Par conséquent, $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ a un unique sous-groupe d'indice 2. Par la correspondance de Galois, $\mathbb{Q}(\zeta_p)$ a un unique sous-corps K de degré 2 sur $\mathbb{Q}$.

Les extensions quadratiques de $\mathbb{Q}$ correspondent aux entiers $d \neq 1$ sans facteur carré. Pour voir pour quel d on a $K \cong \mathbb{Q}(\sqrt{d})$, nous allons utiliser un argument de ramification. Dans les exercices on verra une autre méthode (sommes de Gauss) pour résoudre ce problème.

Par la proposition 7.1.4 et le théorème 7.2.2, K est non ramifié en tous les premiers différents de p. Donc $\mathrm{discr}(K)$ est, à signe près, une puissance de p. Si $d \neq 1$ mod 4, on a $\mathrm{discr}(K) = 4d$, et si $d = 1$ mod 4, on a $\mathrm{discr}(K) = d$. $\square$

7.3 Réciprocité quadratique.

7.3.1 Proposition. *Soit $p \neq 2$ un nombre premier. Le sous-groupe $\mathbb{F}_p^{*,2} := \{a^2 \mid a \in \mathbb{F}_p^*\}$ est d'ordre $(p-1)/2$. Pour a dans $\mathbb{F}_p$, on définit :*

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{si } a \in \mathbb{F}_p^{*,2}, \\ 0 & \text{si } a = 0, \\ -1 & \text{si } a \notin \mathbb{F}_p^{*,2}. \end{cases}$$

La fonction $(\frac{\cdot}{p})\colon \mathbb{F}_p \to \{-1, 0, 1\} \subset \mathbb{Z}$ s'appelle le symbole de Legendre. Pour a dans $\mathbb{F}_p$ on a :

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \quad \text{dans } \mathbb{F}_p.$$

L'application $\mathbb{F}_p^* \to \mathbb{Z}^*$, $a \mapsto (\frac{a}{p})$ est un morphisme de groupes.

Preuve. Considérons le morphisme de groupes $f\colon \mathbb{F}_p^* \to \mathbb{F}_p^*$, $a \mapsto a^2$. Son noyau est $\{1, -1\}$, donc d'ordre 2 ($1 \neq -1$ car $p \neq 2$). L'image de f est $\mathbb{F}_p^{*,2}$, qui est donc d'indice 2. Le quotient $\mathbb{F}_p^*/\mathbb{F}_p^{*,2}$ est donc isomorphe, et cela de manière unique, à $\mathbb{Z}^*$. Considérons le morphisme $g\colon \mathbb{F}_p^* \to \mathbb{F}_p^*$, $a \mapsto a^{(p-1)/2}$. Son noyau est d'ordre $(p-1)/2$, donc son image d'ordre 2 et égale à $\{1, -1\}$. Pour a dans $\mathbb{F}_p^*$, on a $g(a^2) = a^{p-1} = 1$. On a donc $\mathbb{F}_p^{*,2} \subset \ker(g)$, et même égalité car les deux ont même cardinal. Pour conclure : pour a dans $\mathbb{F}_p^*$ on a $g(a) = 1$ si et seulement si a est dans $\mathbb{F}_p^{*,2}$. $\square$

7.3.2 Théorème. *(***Réciprocité quadratique, Gauss.***) Soient p et q deux nombres premiers, différents de 2 et distincts. Alors on a :*

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Preuve. D'après la Proposition 7.2.3, l'unique sous-corps quadratique de $\mathbb{Q}(\zeta_q)$ est $\mathbb{Q}(\sqrt{q^*})$, avec $q^* = (\frac{-1}{q})q$. Nous avons donc un diagramme commutatif :

$$\begin{array}{ccccc}
\mathbb{Q}(\zeta_q) & \longleftarrow & \mathbb{Z}[z]/(\Phi_q) & \longrightarrow & \mathbb{F}_p[z]/(\Phi_q) \\
\uparrow & & \uparrow & & \uparrow \\
\mathbb{Q}(\sqrt{q^*}) & \longleftarrow & \mathbb{Z}[x]/(f) & \longrightarrow & \mathbb{F}_p[x]/(f)\,, \\
\uparrow & & \uparrow & & \uparrow \\
\mathbb{Q} & \longleftarrow & \mathbb{Z} & \longrightarrow & \mathbb{F}_p
\end{array}$$

avec $f = x^2 - x - (q^* - 1)/4$. L'application de $\mathbb{F}_p[x]/(f)$ vers $\mathbb{F}_p[z]/(\Phi_p)$ est une inclusion par un argument que nous avons déjà utilisé dans la preuve de la proposition 7.1.4 (nous utilisons ici que $\mathbb{Z}[z]/(\Phi_p)$ et $\mathbb{Z}[x]/(f)$ sont les anneaux d'entiers dans leurs corps de fractions).

Par la Proposition 7.2.1, $\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$ s'identifie, via l'isomorphisme f, à $\mathbb{F}_q^*$. D'autre part, $\mathrm{Gal}(\mathbb{Q}(\sqrt{q^*})/\mathbb{Q})$ admet un unique isomorphisme avec $\mathbb{Z}^*$. Ceci nous donne un diagramme commutatif :

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) & \xrightarrow[\sim]{f} & \mathbb{F}_q^* \\ \Big\downarrow g & & \Big\downarrow (\frac{\cdot}{q}) \\ \mathrm{Gal}(\mathbb{Q}(\sqrt{q^*})/\mathbb{Q}) & \xrightarrow{\sim} & \mathbb{Z}^\times \end{array}$$

Notons σ_p l'élément de $\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$ qui correspond à l'image de p dans $\mathbb{F}_q^*$. Alors σ_p induit l'endomorphisme de Frobenius de $\mathbb{F}_p[z]/(\Phi_q)$, car $\sigma_p(z) = z^p$ (modulo Φ_q). Donc σ_p induit le Frobenius de $\mathbb{F}_p[x]/(f)$. Notons maintenant que $\sigma_p(\sqrt{q^*})$ est soit égal à $\sqrt{q^*}$, soit à $-\sqrt{q^*}$. On a alors les équivalences :

$$(\tfrac{p}{q}) = 1 \Leftrightarrow g(\sigma_p) = \mathrm{id} \Leftrightarrow p \text{ est scindé dans } \mathbb{Z}[x]/(f) \Leftrightarrow (\tfrac{q^*}{p}) = 1.$$

Donc :

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

□

Pour calculer des symboles de Legendre, il est utile de compléter le théorème ci-dessus par les deux résultats suivants, qui ont été montrés dans le cours et les exercices.

7.3.3 Proposition. *Pour $p \neq 2$ un nombre premier on a :*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \quad \textit{et} \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Concrètement, la réciprocité quadratique se résume en le résultat suivant, qui n'est que la combinaison des deux résultats qui précèdent.

7.3.4 Proposition. *1. Si $p \neq 2$ et $q \neq 2$ sont premiers, on a :*

$$\begin{aligned} \left(\frac{p}{q}\right) &= \left(\frac{q}{p}\right) \quad \textit{si } p \equiv 1(4) \textit{ ou } q \equiv 1(4)\,; \\ &= -\left(\frac{q}{p}\right) \quad \textit{sinon.} \end{aligned}$$

2. Si $p \neq 2$ est premier, on a :

$$\begin{aligned}
\left(\frac{p}{2}\right) &= 1; \\
\left(\frac{2}{p}\right) &= 1 \quad \textit{si } p \equiv \pm 1(8)\,; \\
&= -1 \quad \textit{si } p \equiv \pm 3(8)\,; \\
\left(\frac{-1}{p}\right) &= 1 \quad \textit{si } p \equiv 1(4)\,; \\
&= -1 \quad \textit{si } p \equiv -1(4)\,;
\end{aligned}$$

8 Le théorème de Wedderburn.

Le théorème en question n'est pas tellement un théorème concernant la théorie des nombres, mais plutôt la théorie des corps finis. La preuve que nous donnons ne nécessite qu'un petit peu de théorie sur les groupes opérant sur des ensembles, un peu “d'algèbre linéaire non commutative” (que nous faisons dans un lemme), et le fait que les polynômes cyclotomiques Φ_n ont coefficients dans $\mathbb{Z}$ (nous n'avons pas besoin de leur irréductibilité). Donc si l'on veut, ce théorème pourrait être traité au début du cours.

Dans cette section, on ne suppose *pas* que les anneaux sont commutatifs ; les anneaux sont encore suppposés unitaires. Nous rappelons qu'un corps est par hypothèse un anneau commutatif avec $1 \neq 0$ dans lequel tout élément non nul est inversible. Un anneau (non nécessairement commutatif) dans avec $1 \neq 0$ dans lequel tout élément non nul est inversible est appelé une *algèbre à division*. Un exemple d'une algèbre à division non commutative est donné par les quaternions (sur $\mathbb{Q}$ ou sur $\mathbb{R}$). Les $\mathbb{Q}$-algèbres à division de dimension finie en tant que $\mathbb{Q}$-espace vectoriel jouent un rôle important en théorie des nombres.

8.1 Théorème. *Soit A un anneau fini intègre (non nécessairement commutatif). Alors A est commutatif, et donc un corps. De façon équivalente : toutes les algèbres à division de dimension finie sur un corps fini sont des corps.*

Preuve. Soit A donc un anneau fini intègre. Soit k le centre de A : k est l'ensemble des x dans A tel que $xy = yx$ pour tout y dans A. Alors k est fermé pour l'addition, la multiplication, inversion et opposition ($x \mapsto -x$). Donc k est un corps fini, disons de cardinal q (qui est une puissance d'un nombre premier), et A est une k-algèbre de dimension finie. Notons $n = \dim_k A$. On a donc $|A| = q^n$.

Notons $G = A^*$ le groupe multiplicatif des éléments non nul de A ; donc G est un groupe de cardinal $q^n - 1$. On fait agir G par conjugaison sur lui-même : $(x, y) \mapsto xyx^{-1}$. Considérons la décomposition de G en orbites pour cette action. Ces orbites sont les classes de conjugaison dans G. Les orbites à un éléments sont exactement les $\{x\}$ avec x dans k. Soit R un système de représentants pour les orbites restantes (celles dans $G - k^*$). Pour chaque x dans G, notons $C_x = \{yxy^{-1} \mid y \in G\}$ sa classe de conjugaison et $C(x) = \{y \in G \mid xy = yx\}$ son centralisateur dans G. Pour x dans G, on a une bijection : $G/C(x) \to C_x$, $\overline{y} \mapsto yxy^{-1}$. On a alors :

$$G = k^* \coprod \coprod_{x \in R} C_x, \quad |G| = q - 1 + \sum_{x \in R} \frac{q^n - 1}{|C(x)|}.$$

Pour x dans A, notons $A(x) = \{y \in A \mid yx = xy\}$ le centralisateur de x dans A. Alors $A(x)$ est une sous-k-algèbre de A, et est donc lui aussi une algèbre à division et $C(x) = A(x)^*$. Notons $n(x) = \dim_k A(x)$, on a donc $|A(x)| = q^{n(x)}$, et $|C(x)| = q^{n(x)} - 1$.

La multiplication à gauche sur A par des éléments de $A(x)$ induit une structure de $A(x)$-module sur A. Montrons que A est libre en tant que $A(x)$-module.

8.2 Lemme. *Soit A une algèbre à division et M un A-module de type fini. Alors M est libre.*

Preuve. Soit $m = (m_1, \dots, m_n)$ un système de générateurs de M, avec n minimal. Il suffit de montrer que ce système est libre. Supposons que ce n'est pas le cas, et soit $\lambda_1 m_1 + \cdots + \lambda_n m_n = 0$ une relation non triviale. Quitte à renuméroter les m_i nous avons $\lambda_n \neq 0$, donc :

$$m_n = -\lambda_n^{-1}(\lambda_1 m_1 + \cdots + \lambda_{n-1} m_{n-1}).$$

Ceci implique que $(m_1, \dots, m_{n-1})$ est un système générateur de M, donc contredit la minimalité de n. $\square$

Pour x dans A, notons $r(x) = \mathrm{rang}_{A(x)} A$. On a alors :

$$q^n = |A| = |A(x)^{r(x)}| = |A(x)|^{n(x)} = (q^{n(x)})^{r(x)} = q^{n(x)r(x)},$$

ce qui montre que les $n(x)$ divisent n. (Une autre façon de voir que $n(x)|n$ est de noter que $\mathrm{pgcd}(q^a - 1, q^b - 1) = q^c - 1$ si $c = \mathrm{pgcd}(a, b)$, en regardant l'algoritme d'Euclide.)

Nous entrons maintenant dans la dernière étape de la preuve. Dans $\mathbb{Q}[t]$, nous avons

$$t^n - 1 = \prod_{d|n} \Phi_d(t),$$

avec Φ_d le polynôme unitaire dont les racines (dans $\mathbb{C}$ disons) sont les racines d'unité d'ordre d. Par la théorie de Galois, on sait que les $\Phi_m(t)$ sont en effet dans $\mathbb{Q}[t]$, et comme les racines de l'unité sont entiers sur $\mathbb{Z}$, on voit que les $\Phi_m(t)$ sont dans $\mathbb{Z}[t]$.

Pour x dans R, on a $n(x) \neq n$, car x n'est pas dans le centre k de A. Pour tout entier $m > 0$, nous avons :

$$q^m - 1 = \prod_{d|m} \Phi_d(q).$$

En appliquant ceci à l'identité :

$$q^n - 1 = q - 1 + \sum_{x \in R} \frac{q^n - 1}{q^{n(x)-1}},$$

on obtient que $\Phi_n(q)$ divise $q - 1$, car $\Phi_n(q)$ divise tous les autres termes. En particulier, on trouve que $|\Phi_n(q)| \leq q - 1$. Mais on a :

$$|\Phi_n(q)| = \prod_{a \in (\mathbb{Z}/nZZ)^*} |e^{2\pi i a/n} - 1|.$$

Si $n > 1$, tout facteur dans ce produit est plus grand que $q - 1$ (faire un dessin de l'axe des réels et le cercle unité dans $\mathbb{C}$). Donc $n = 1$, et $A = k$. $\square$

8.3 Exercice. Soit $A = \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}k$ la $\mathbb{Z}$-algèbre des quaternions standard ($i^2 = j^2 = -1$, $ij = -ji = k$). Pour $p \neq 2$ premier il est clair que A/pA n'est pas commutatif, donc ne peut pas être intègre par le théorème de Wedderburn. Pour autant de p que vous voulez, trouvez explicitement des diviseurs de zéro non nuls dans A/pA.

9 Compléments et rappels.

9.1 Produit tensoriel d'algèbres sur un corps.

Le produit tensoriel de modules sur un anneau a été défini dans le cours Algèbre 3, en premier semestre. Le résultat est simplement que pour A un anneau et M et N des A-modules, il existe une forme A-bilinéaire universelle :

$$M \times N \longrightarrow M \otimes_A N, \quad (m, n) \mapsto m \otimes n.$$

Si B et C sont des A-algèbres, alors $B \otimes_A C$ a une structure naturelle de A-algèbre (pour tous b et b' dans B et c et c' dans C, on a $(b \otimes c)(b' \otimes c') = (bb') \otimes (cc')$), et a la propriété universelle suivante : les morphismes de A-modules $B \to B \otimes_A C$ et $C \to B \otimes_A C$ donnés par $b \mapsto b \otimes 1$ et $c \mapsto 1 \otimes c$ sont des morphismes de A-algèbres, et si D est une A-algèbre et $f \colon B \to D$ et $g \colon C \to D$ sont des morphismes de A-algèbres, alors il existe un unique morphisme de A-algèbres $B \otimes_A C \to D$ qui fait commuter le diagramme que l'on devine.

Avec cette propriété universelle, on voit que pour A un anneau et B une A-algèbre, il existe un unique morphisme de B-algèbres $A[x] \otimes_A B \to B[x]$ qui envoie $x \otimes 1$ vers x.

De même façon, on voit, en utilisant des propriétés universelles, que $A[x]/(f) \otimes_A B$ est la même chose que $B[x]/(f)$. Nous utiliserons ceci si $A \to B$ est une extension de corps.

9.1.1 Théorème. *Soit $K \to L$ une extension de corps, et f dans $K[x]$ irréductible, tels que f soit scindé sur L, avec des racines simples. Notons d le degré de f, $r_1, \ldots, r_d$ ses racines dans L, et $\phi_1, \ldots, \phi_d$ les plongements correspondants de $K[x]/(f)$ dans L. Alors le morphisme de K-algèbres :*

$$L \otimes_K K[x]/(f) \longrightarrow L^d, \quad y \otimes z \mapsto (y\phi_1(z), \ldots, y\phi_d(z))$$

est un isomorphisme de L-algèbres. En particulier, si $K \to L$ est galoisienne, de groupe G, et si on note n le cardinal de G, et $g_1, \ldots, g_n$ ses éléments, on a un isomorphisme de L-algèbres :

$$L \otimes_K L \longrightarrow L^n, \quad x \otimes y \mapsto (xg_1(y), \ldots, xg_n(y)).$$

Preuve. Commençons par remarquer que $L \otimes_K K[x]/(f) = L[x]/(f)$ et L^d sont tous les deux de dimension d en tant que L-espace vectoriels. Il suffit donc de montrer que le morphisme en question est soit injectif, soit surjectif. En fait, les deux sont assez faciles. La surjectivité résulte de l'interpolation de Lagrange, et l'injectivité du fait que le noyau de $L[x] \to L^d$ est l'intersection des $(x - r_i)$, donc (f).

Le deuxième énoncé s'obtient du premier en choisissant un élément primitif de L sur K. $\square$

9.2 Modules de type fini sur les anneaux principaux.

Ceci se trouve dans [Samuel, §1.5], mais expliqué d'une façon plus abstraite. D'autre part, cette théorie est dans le programme du cours d'algèbre du semestre précédent. Pour ces raisons, nous irons assez vite.

9.2.1 Théorème. *Soit A un anneau principal et soit $n \geq 0$. Tout sous-module de A^n est libre de rang au plus n. En fait, si M est un sous-module de A^n, il existe une base $(e_1, \dots, e_n)$ de A^n, un entier r tel que $0 \leq r \leq n$ et des éléments $d_1, \dots, d_r$ de A tels que $d_1 | d_2 | \cdots | d_r$ et $(d_1 e_1, \dots, d_r e_r)$ soit une base de M. La suite des d_i n'est pas forcément unique, mais la suite des idéaux $d_1 A \supset d_2 A \supset \cdots \supset d_r A$ l'est.*

Preuve. Nous montrons d'abord, par récurrence sur n, que M est libre de rang au plus n. Pour $n = 0$ rien à faire. Supposons $n \geq 1$. Considérer $p \colon A^n \to A$, projection sur la dernière coordonnée. L'image pM est un sous-module de A, donc un idéal ; comme A est principal, M est libre de rang 0 ou 1. Si c'est 0, M est en fait contenu dans A^{n-1} et on a terminé par récurrence. Supposons donc que pM est de rang 1, de base $p(m)$ pour un m dans M convenable. Alors la suite exacte

$$0 \longrightarrow \ker(p|_M) \longrightarrow M \longrightarrow p(M) \longrightarrow 0$$

est scindée par le morphisme $p(M) \to M$, $p(m) \mapsto m$ (comme $p(m)$ est une base de $p(M)$, il suffit de donner l'image de $p(m)$). Donc M est isomorphe à $(M \cap A^{n-1}) \oplus A$, et on a terminé par récurrence.

Pour montrer l'existence des bases de M et de A^n comme dans l'énoncé, on choisit un nombre fini de générateurs de M, que l'on exprime en termes de la base usuelle de A^n. Ensuite, on fait des opérations élémentaires sur les lignes et les colonnes de la matrice obtenue, pour la rendre de la forme $\mathrm{diag}(d_1, d_2, \dots)$ avec $d_1 | d_2 | \cdots$. Dans le cas de $A = \mathbb{F}_p[t]$, on trouve dans Maple une fonction “Smith” qui fait le calcul (et qui est d'ailleurs au programme pour l'option modélisation de l'oral de l'agreg). Dans le cas $A = \mathbb{Z}$, Maple a la fonction “ismith”. $\square$

Avec ce théorème, on démontre facilement la classification des modules de type fini sur un anneau principal.

10 Exercices.

1. Donner toutes les solutions dans $\mathbb{Z}$ et dans $\mathbb{Q}$ des équations :

   $$x^2 + 2y^2 = 6, \quad x^2 - xy + y^2 = -1, \quad x^2 + y^2 = 7, \quad x^2 + 2y^2 = 7, \quad x^2 - 6y^2 = -1.$$

   Indications : congruences modulo des puissances de deux ; paramétrisation de courbes de degré deux avec un point rationnel.

2. (a) Soit (a, b, c) un triplet pythagoricien primitif. En considérant les carrés dans $\mathbb{Z}/4\mathbb{Z}$, montrer que, quitte à échanger a et b, on a $a \equiv 1\ (2)$, $b \equiv 0\ (2)$ et $c \equiv 1\ (2)$. Montrer qu'alors $a^2 = (c-b)(c+b)$, et que $\mathrm{pgcd}(c-b, c+b) = 1$. (Indication : l'idéal de $\mathbb{Z}$ engendré par $c - b$ et $c + b$ contient $2c$ et $2b$.) En déduire qu'il existe des entiers u et v avec $0 < u < v$, impairs, premier entre eux, tels que $c - b = u^2$ et $c + b = v^2$.

   (b) Conclure que tout triplet pythagoricien primitif (a, b, c) avec b pair s'écrit sous la forme $(uv, (v^2 - u^2)/2, (v^2 + u^2)/2)$, avec $0 < u < v$ dans $\mathbb{N}$ premier entre eux et impairs.

   (c) Montrer que pour u et v dans $\mathbb{N}$ premier entre eux, impairs et tel que $u < v$:

   $$(uv, (v^2 - u^2)/2, (v^2 + u^2)/2)$$

   est un triplet pythagoricien primitif. Conclure que les triplets pythagoriciens primitifs avec b pair sont les triplets $(uv, (v^2 - u^2)/2, (v^2 + u^2)/2)$, avec $u < v$ premier entre eux et uv impair.

3. Montrer que l'anneau $\mathbb{Z}[i]$ est euclidien pour la fonction $d\colon \mathbb{Z}[i] \to \mathbb{N}$, $z \mapsto z\overline{z}$.

4. (Plus difficile.) Soit K un corps, et n un entier plus grand ou égal à 3 et inversible dans K. Montrer que toutes les solutions dans $K[t]$ de l'équation :

   $$a^n + b^n = c^n$$

   avec a, b et c premiers entre eux, sont en fait des solutions dans K. Indication : étendre la méthode donnée en cours, donc : par contradiction ; considérer une solution non constante avec le maximum des degrés de a et b et c minimal parmi toutes les solutions pour tous les corps K. (Il faudra donc peut-être changer de corps pendant la démonstration.) Question : l'hypothèse que n soit inversible dans K est-elle nécessaire ? Plus précisément : en fonction de la caractéristique de K, donner la liste des n pour lesquels il existe des solutions non triviales.

5. Montrer qu'il existe une infinité de nombres premiers p qui sont -1 modulo 4.

6. Soit p un nombre premier. Montrer que $x^2 + 1$ a une racine dans $\mathbb{F}_p$ si et seulement si p n'est pas congru à -1 modulo 4 (indication : le groupe $\mathbb{F}_p^*$ est cyclique, et d'ordre $p - 1$). Montrer que pour n dans $\mathbb{Z}$, tout premier impair qui divise $n^2 + 1$ est congru à 1 modulo 4. Montrer qu'il y a une infinité de nombres premiers qui sont 1 modulo 4.

7. (Pour ceux qui veulent.) Variante des deux questions précédentes, mais pour les classes modulo 3.

8. Factoriser en irréductibles : $7 + i$ dans $\mathbb{Z}[i]$, et $5 + j$ dans $\mathbb{Z}[j]$.
9. Cherchez un nombre premier p qui est congru à 1 modulo 4 et raisonnablement grand (disons au moins 1000), et écrivez le comme somme de deux carrés.
10. Comme la définition de la notion d'anneau euclidien n'est pas la même dans tous les textes, nous donnons une définition ici, et montrons qu'elle est équivalente à une autre que l'on rencontre souvent. Voici donc la définition.

    Soit A un anneau intègre, et $f\colon A \to \mathbb{Z}$ une fonction. Alors f est dite euclidienne si son image est borné inférieurement et si pour tout (a, b) dans A^2 avec $b \neq 0$ il existe q et r dans A avec $a = qb + r$ et $f(r) < f(b)$. Un anneau est dit euclidien s'il existe une fonction euclidienne sur A.

    (a) (Juste pour mémoire.) Montrer qu'un anneau euclidien est principal.

    (b) Montrer que pour tout $a \neq 0$ dans A on a $f(a) > f(0)$.

    (c) Montrer que la fonction $f\colon \mathbb{Z} \to \mathbb{Z}$, $n \mapsto |n|$, est euclidienne.

    (d) Soit K un corps. Montrer que la fonction $f\colon K[x] \to \mathbb{Z}$, $a \mapsto \deg(a)$ est euclidienne. Ici on convient que $\deg(0) = -1$. Si on veut que $\deg(0) = -\infty$, on pourrait introduire l'ensemble ordonné $\mathbb{Z} \cup \{-\infty\}$, et la notion de fonction euclidienne à valeurs dans $\mathbb{Z} \cup \{-\infty\}$.

    (e) Soit A un anneau intègre, et $f\colon A \to \mathbb{Z}$ une fonction. Montrer que f est euclidienne si et seulement si $f + 1$ (la fonction donnée par $a \mapsto f(a) + 1$) l'est.

    (f) (Plus difficile.) Soit A un anneau intègre et $\phi\colon A \to \mathbb{Z}$ une fonction euclidienne. Montrer que la fonction $f\colon A \to \mathbb{Z}$, $a \mapsto \min\{\phi(ax) \mid 0 \neq x \in A\}$, est euclidienne, et a la propriété supplémentaire que $f(ab) \geq f(a)$ pour tous a et b avec b non nul.
11. Montrer directement que $\sqrt{2} + \sqrt{3}$ dans $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ est entier sur $\mathbb{Z}$. Montrer aussi que $1/2$ dans $\mathbb{Q}$ n'est pas entier sur $\mathbb{Z}$. Montrer aussi que $1/2$ dans $\mathbb{Z}/1001\mathbb{Z}$ est entier sur $\mathbb{Z}$.
12. Calculer le morphisme trace et la forme trace pour $\mathbb{Q} \to \mathbb{Q}(2^{1/3})$, disons en termes de matrices par rapport à une base que vous avez choisie. Pareil pour $\mathbb{Q} \to \mathbb{Q}(i)$ et $\mathbb{Q} \to \mathbb{Q}(j)$.
13. Calculer le morphisme trace et la forme trace pour $\mathbb{Q} \to \mathbb{Q}[t]/(t^2)$.
14. Calculer la forme trace pour $\mathbb{Q} \to \mathbb{Q}[x]/(x^3 - x^2 - x + 1)$. Cette forme bilinéaire est-elle non dégénérée ? Le déduire aussi de la décomposition de $x^3 - x^2 - x + 1$ en facteurs irréductibles.
15. Le but de cet exercice est de montrer qu'il y a un algorithme efficace pour trouver, pour un nombre premier p qui est congru à 1 modulo 4, des entiers a et b tels que $p = a^2 + b^2$. Soit donc p premier, et 1 mod 4.

    (a) Ecrivons $p - 1 = 2^n m$ avec m impair (notez que $n \geq 2$). Pour a dans $\mathbb{F}_p^*$, a^m est d'ordre divisant 2^n. On peut donc espérer trouver un élément d'ordre 4 dans $\mathbb{F}_p^*$ en calculant, pour a pris au hasard dans $\mathbb{F}_p^*$, $b := a^m$, et ensuite les $b_i := b^{2^i} = b_{i-1}^2$, $i \geq 0$, jusqu'à ce que $b_k = \pm 1$. En effet, si $k > 0$, alors $b_k = -1$ et b_{k-1} est d'ordre 4. Calculez la probabilité que $b \neq \pm 1$.

(b) Expliquez-vous à vous-même que pour calculer, pour a dans $\mathbb{F}_p$ donné, $b := a^m$, et ensuite les b_i, ne prend au plus qu'environ $n + 2\log_2(m) = O(\log_2(p))$ multiplications dans $\mathbb{F}_p$, si on s'y prend intelligemment.

(c) Expliquez-vous à vous-même que les opérations élémentaires ($+$, $-$, $*$, $/$) dans $\mathbb{F}_p$ se font en au plus $O(\log(p))$, $O(\log(p))$, $O(\log(p)^2)$ et $O(\log(p)^3)$ opérations binaires (c'est à dire, sur des 0 et 1), respectivement. En fait, il existe des méthodes plus efficaces : par exemple, la multiplication de deux nombres $\leq 2^n$ peut se faire en $O(n\log(n)\log(\log(n)))$ opérations binaires (voir [Cohen]).

(d) Soit c dans $\mathbb{Z}$, $|c| < p/2$, tel que $\overline{c}$ dans $\mathbb{F}_p^*$ soit d'ordre 4, et notons $f\colon \mathbb{Z}[i] \to \mathbb{F}_p$ le morphisme tel que $f(i) = \overline{c}$. Montrez que p et $i - c$ engendrent le noyau de f, en tant que $\mathbb{Z}$-module. En appliquant l'algorithme d'Euclide dans $\mathbb{Z}[i]$ à p et $i - c$, on trouve un générateur de $\ker(f)$.

(e) L'algorithme obtenu est probabiliste, et le temps moyen qu'il prend est $O(\log(p)^3)$. (Le nombre moyen de a à essayer est au plus 2, et le nombre d'étapes dans l'algorithme d'Euclide dans $\mathbb{Z}[i]$ à effectuer est au plus $O(\log(p))$.)

16. Soit K un corps, V_1 et V_2 deux K-espaces vectoriels, de dimensions d_1 et d_2, respectivement. Soient u_1 et u_2 des endomorphismes de V_1 et V_2.

(a) Montrer que les polynômes caractéristiques de u_1 et u_2 déterminent celui de l'endomorphisme $u_1 \otimes u_2$ de $V_1 \otimes_K V_2$. Indication : utiliser une extension de K sur laquelle les polynômes caractéristiques de u_1 et u_2 sont scindés.

(b) Donner des formules explicites en termes des coefficients dans les deux cas où $d_2 = 2$ et $1 \leq d_1 \leq 2$.

17. Le produit tensoriel est bien utile pour montrer le fait que deux corps de décomposition pour un polynôme sur un corps sont isomorphes (de façon non unique). En effet, soit K un corps, et f dans $K[x]$ non nul. Soient $K \to K_1$ et $K \to K_2$ deux extensions de décomposition, c'est à dire, sur chacune, f est scindé, et chacune est engendrée par les racines de f.

(a) Montrer que $K_1 \otimes_K K_2$ est une K-algèbre non nulle, et qu'elle a des idéaux maximaux (sans utiliser le lemme de Zorn, si vous le connaissez).

(b) Montrer que la K-algèbre $K_1 \otimes_K K_2$ est engendrée par des racines de f.

(c) Soit K_3 un quotient de $K_1 \otimes_K K_2$ qui est un corps. Montrer que $K \to K_3$ est un corps de décomposition, et que les deux morphismes de K-algèbres $K_1 \to K_3$ et $K_2 \to K_3$ sont des isomorphismes. Cela montre donc que K_1 et K_2 sont isomorphes en tant que K-algèbres.

18. Soit K un corps, $K \to L$ une extension de dimension finie, et $K \to K_1$ et $K \to K_2$ deux sous-extensions. Soit K_3 la sous-extension de L engendrée par K_1 et K_2.

(a) Supposons que $\dim_K K_3 = \dim_K K_1 \dim_K K_2$. Montrer que le morphisme de K-algèbres $f\colon K_1 \otimes_K K_2 \to L$, donné par $f(x \otimes y) = xy$, est injectif, et d'image K_3.

(b) Donner un exemple où le morphisme f n'est pas injectif.

19. Lesquels des anneaux suivants sont des corps :
    (a) $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$,
    (b) $\mathbb{Q}(\sqrt{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{3})$,
    (c) $\mathbb{Q}(\sqrt{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{-1})$,
    (d) $\mathbb{C} \otimes_{\mathbb{Q}} \mathbb{C}$.
20. "Calculer" les $\mathbb{Z}[i]/(a+bi)\mathbb{Z}[i]$ en tant que $\mathbb{Z}$-module, pour des $a+bi$ (a et b dans $\mathbb{Z}$) de votre choix. Par exemple, pour ceux avec $|a| \leq 3$, $|b| \leq 3$.
21. Soit σ l'automorphisme non trivial de $\mathbb{Q}(\sqrt{2})$. Evidemment, σ préserve le sous-anneau $\mathbb{Q}(\sqrt{2})_{\mathbb{Z}} = \mathbb{Z}[\sqrt{2}]$. Soit $d\colon \mathbb{Z}[\sqrt{2}] \to \mathbb{N}$ la fonction donnée par : $d(x) = |x\sigma(x)|$. Montrer que d est une fonction euclidienne. Pour ceux qui veulent : quels sont les corps quadratiques dont l'anneau des entiers est euclidien pour la norme ainsi définie ?
22. Dessiner l'image de $\mathbb{Z}[\sqrt{2}]$ dans $\mathbb{R}^2$ par l'application $a+b\sqrt{2} \mapsto (a+b\sqrt{2}, a-b\sqrt{2})$, avec a et b dans $\mathbb{Z}$. Dessiner aussi la courbe de niveau 1 pour la norme : $|xy| = 1$. Faire l'analogue pour $\mathbb{Q}(\sqrt{5})_{\mathbb{Z}}$.
23. Soit K un corps, $n \geq 0$ un entier, et $a_0, \ldots, a_{n-1}$ dans K. Montrer que :

$$\det \begin{pmatrix} t & & & & a_0 \\ -1 & t & & & \vdots \\ & -1 & \ddots & & \vdots \\ & & \ddots & t & \vdots \\ & & & -1 & t+a_{n-1} \end{pmatrix} = t^n + a_{n-1}t^{n-1} + \cdots + a_0.$$

    Indication : on peut procéder de deux façons au moins. Développer suivant la première ligne et faire récurrence sur n, ou dire qu'il s'agit d'une identité polynomiale en les a_i que l'on démontre en notant que le polynôme en question annule l'endomorphisme en question et que si les a_i sont des variables, alors le polynôme en question est irréductible.
24. Soit $n \geq 0$ entier, et a dans $\mathrm{M}_n(\mathbb{Z})$. Montrer que $\mathbb{Z}^n/a\mathbb{Z}^n$ est fini si et seulement si $\det(a) \neq 0$, et que, dans ce cas, on a $|\mathbb{Z}^n/a\mathbb{Z}^n| = |\det(a)|$.
25. Soit K un corps de nombres. Soit $x \neq 0$ dans $K_{\mathbb{Z}}$, et considérons l'endomorphisme $\cdot x$ du $\mathbb{Z}$-module libre $K_{\mathbb{Z}}$ donné par $y \mapsto xy$. Montrer que :

$$|K_{\mathbb{Z}}/xK_{\mathbb{Z}}| = |\det(\cdot x)| = |a_0|^{(\dim_{\mathbb{Q}} K)/d},$$

    où d et a_0 sont le degré et le terme constant du polynôme minimal de x sur $\mathbb{Q}$.
26. Soit $d \geq 1$. Montrer que si $z_1, \ldots, z_d$ dans $\mathbb{C}$ satisfont à $|z_i| < 1/d$, alors les a_i définis par :

$$(t-z_1)\cdots(t-z_d) = t^d + a_{d-1}t^{d-1} + \cdots + a_1 t + a_0$$

    satisfont à $|a_i| < 1$.
27. Soit A un anneau factoriel (donc intègre). Montrer que A est intégralement clos.

28. Donner un exemple d'un anneau intègre non intégralement clos.
29. Montrer les implications non démontrées en cours dans la proposition qui donne les conditions équivalentes pour qu'un module soit noethérien.
30. Montrer que l'anneau $\mathbb{Z}[x_1, x_2, \ldots]$ de polynômes en un nombre infini de variables n'est pas noethérien. Pareil pour la clôture intégrale $\overline{\mathbb{Z}}$ de $\mathbb{Z}$ dans $\overline{\mathbb{Q}}$.
31. Un sous-anneau d'un anneau noethérien, est-il nécessairement noethérien ? Et un quotient ? Et un sous-module d'un module noethérien ?
32. Soit A un anneau, a et b des idéaux. Montrer que $ab \subset a \cap b$. A-t-on toujours égalité ? (Pour ceux qui veulent : quels sont les anneaux où c'est toujours vrai ?)
33. Soit k un corps, $n \geq 1$, et $A := k[x_1, \ldots, x_n]$. Soit m l'idéal de A, engendré par les x_i. Montrer que pour chaque $d \geq 0$, A/m^d est de dimension finie en tant que k-espace vectoriel. Montrez que cette dimension est le coefficient binomial $\binom{n+d-1}{n}$.
34. Est-ce que l'anneau $\mathbb{Q}[x, y]$ est de Dedekind ?
35. Montrez que tout anneau principal est de Dedekind.
36. Soit k un corps, et A une k-algèbre de dimension finie n en tant que k-espace vectoriel.
    (a) Montrer que le nombre d'idéaux maximaux de A est au plus n. (Si $m_1, \ldots, m_r$ sont des idéaux maximaux distincts, alors le morphisme $A \to A/m_1 \times \cdots \times A/m_r$ est surjectif, par le théorème Chinois.)
    (b) Montrer qu'il existe une suite de sous-A-modules $A = M_0 \supset M_1 \cdots \supset M_s = 0$ tel que les M_j/M_{j+1} avec $0 \leq j < s$ soient simples, et qu'alors $s \leq n$.
    (c) Soient $m_1, \ldots, m_r$ les idéaux maximaux distincts de A. Montrer que tout A-module simple est isomorphe à l'un des A/m_i.
    (d) Soient $x_1, \ldots, x_n$ dans l'intersection des m_i. Montrer que $x_1 \cdots x_n = 0$. Indication : montrer que $x_1 \cdots x_i A \subset M_i$.
    (e) Montrer que $A \to A/m_1^n \times \cdots \times A/m_r^n$ est un isomorphisme.

    Notez que les résultats de cet exercice s'appliquent au sous-k-algèbres commutatives des $\mathrm{M}_n(k)$, donc généralisent la décomposition en sous-espaces caractéristiques pour un endomorphisme au cas d'endomorphismes commutant entre eux, et sans que les polynômes caractéristiques soient scindés.
37. Soit K une extension finie de $\mathbb{Q}$. Soit m un idéal maximal de $K_\mathbb{Z}$. Soit p la caractéristique de $K_\mathbb{Z}/m$ (rappelons que ce dernier est fini). Soit m' l'ensemble des x dans K tels que $xm \subset K_\mathbb{Z}$. En appliquant l'exercice précédent à la $\mathbb{F}_p$-algèbre $K_\mathbb{Z}/pK_\mathbb{Z}$, montrer que $m' \neq K_\mathbb{Z}$. Indication : il suffit de voir qu'il existe un élément non nul de $p^{-1}K_\mathbb{Z}/K_\mathbb{Z}$ annulé par m. La multiplication par p induit un isomorphisme de $K_\mathbb{Z}$-modules de $p^{-1}K_\mathbb{Z}/K_\mathbb{Z}$ vers $K_\mathbb{Z}/pK_\mathbb{Z}$. Ceci donne donc une démonstration plus directe que celle du cours du fait que les idéaux maximaux de $K_\mathbb{Z}$ sont inversibles dans le monoïde des idéaux fractionnaires.
38. Dans cet exercice nous nous intéressons aux idéaux de l'anneau des entiers $A := \mathbb{Z}[\sqrt{-5}]$ de $K := \mathbb{Q}(\sqrt{-5})$. Nous avons déjà vu que cet anneau n'est pas factoriel (6 se factorise

comme $2{\cdot}3$, mais aussi comme $(1+\sqrt{-5})(1-\sqrt{-5})$). La première chose à étudier est comment se factorisent les idéaux pA avec p dans $\mathbb{N}$ premier. Nous allons regarder en détail d'où vient le problème avec les deux factorisations en irréductibles de 6. En même temps, nous anticipons la suite de ce cours : borne pour le groupe $C(A)$, et réciprocité quadratique. Notons $f := x^2+5$, dans $\mathbb{Z}[x]$.

(a) Soit p dans $\mathbb{N}$ premier. Montrer que la $\mathbb{F}_p$-algèbre A/pA est isomorphe à $\mathbb{F}_p \times \mathbb{F}_p$, à $\mathbb{F}_{p^2}$ ou à $\mathbb{F}_p[t]/(t^2)$ suivant le cas où f se décompose dans $\mathbb{F}_p[x]$ en deux facteurs distincts, est irréductible, ou un carré. Indication : considérer $\mathbb{Z}[x]/(f)$.

(b) Montrer que le discriminant de f est -20. Conclure que le dernier des trois cas de l'exercice précédent se produit seulement pour $p=2$ et $p=5$.

(c) Calculer aussi le déterminant de la matrice donnant la forme trace de K sur $\mathbb{Q}$, par rapport à une $\mathbb{Z}$-base de A. Le résultat n'est pas une coïncidence, et montre que ce nombre -20 est un invariant important de A, comme illustre l'exercice suivant.

(d) Soit p dans $\mathbb{N}$ premier, différent de 2 et de 5. La réciprocité quadratique, que nous montrerons plus tard, dit que la condition "-5 est un carré dans $\mathbb{F}_p$" dépend uniquement de l'image de p dans $(\mathbb{Z}/20\mathbb{Z})^*$. Même plus fort, il existe un morphisme de groupes $g\colon (\mathbb{Z}/20\mathbb{Z})^* \to \{1,-1\}$ tel que la condition "$g(p)=1$" équivaut à "-5 est un carré dans $\mathbb{F}_p$". Calculez ce g, et vérifiez ce résultat dans quelques cas (i.e., prendre quelques p_1 et p_2 avec même image dans $\mathbb{Z}/20\mathbb{Z}$, et vérifiez que -5 est un carré modulo p_1 si et seulement s'il est un carré modulo p_2).

(e) En regardant $A/2A$, montrer qu'il existe un unique idéal maximal m_2 de A qui contient 2. Montrer que $m_2 = (2, 1+\sqrt{-5})$, et que $2A = m_2^2$.

(f) Montrer que les idéaux maximaux de A qui contiennent 3 sont $m_3 := (3, -1+\sqrt{-5})$ et $\overline{m_3} = (3, -1-\sqrt{-5})$. Vérifiez que $3A = m_3\overline{m_3}$.

(g) Donner la factorisation de l'idéal $6A$ en idéaux maximaux de A. Montrer que m_2, m_3 et $\overline{m_3}$ ne sont pas principaux, mais que m_2m_3 et $m_2\overline{m_3}$ le sont, ainsi que m_2^2 et $m_3\overline{m_3}$. Ceci explique les différentes factorisations de 6.

(h) Calculer des $\mathbb{Z}$-bases de tous les idéaux maximaux de A qui contiennent un premier p dans $\mathbb{N}$ avec $p \leq 19$. Lesquels sont principaux ? Montrer que si deux d'entre eux ne sont pas principaux, alors leur produit l'est, en calculant cas par cas. Comment cela pourrait s'expliquer en termes du groupe $C(A)$?

39. Soit $d>0$ un entier sans facteur carré, et $K = \mathbb{Q}(\sqrt{-d})$ le corps quadratique imaginaire correspondant.

(a) Calculer le volume de $\mathbb{C}/K_{\mathbb{Z}}$. Indication : quelque soit d modulo 4, il est recommandé de calculer d'abord le volume de $\mathbb{C}/\mathbb{Z}[\sqrt{-d}]$, et de faire ensuite le nécessaire pour obtenir le volume de $\mathbb{C}/K_{\mathbb{Z}}$. (Bien sûr, on peut aussi calculer directement avec une $\mathbb{Z}$-base de $K_{\mathbb{Z}}$.)

(b) Calculer le discriminant $\mathrm{discr}(K_{\mathbb{Z}})$ de K (par définition, c'est le déterminant de la matrice de la forme trace par rapport à n'importe quelle $\mathbb{Z}$-base de $K_{\mathbb{Z}}$). Indication :

comme dans la partie précédente : il est plus simple de faire d'abord le calcul pour $\mathbb{Z}[\sqrt{-d}]$.

(c) Avec la méthode que vous avez vue en cours, montrer que tout idéal non nul a de $K_\mathbb{Z}$ contient un élément x non nul tel que $|x| \leq 2(\pi^{-1}2^{-1}|\mathrm{discr}(K_\mathbb{Z})|^{1/2}\mathrm{N}(a))^{1/2}$.

(d) Montrer que tout élément de $C(K_\mathbb{Z})$ est représenté par un idéal de $K_\mathbb{Z}$ de norme au plus $2\pi^{-1}|\mathrm{discr}(K_\mathbb{Z})|^{1/2}$.

40. Notons $A := \mathbb{Q}(\sqrt{-19})_\mathbb{Z}$. Montrer que A est principal. Indication : utiliser l'exercice précédent pour trouver un entier x tel qu'il suffit de montrer que les idéaux de norme au plus x sont principaux ; ensuite, calculer tous les idéaux de norme au plus x.

41. Soit A un anneau intègre tel que A^* a au plus deux éléments, et tel que tout idéal $a \neq A$ est d'indice au moins 4. Montrer que A n'est pas euclidien. Indication : supposer que $\phi\colon A - \{0\} \to \mathbb{N}$ soit une fonction euclidienne ; soit a dans A non nul et non inversible tel que $\phi(a)$ soit minimal pour de tels éléments ; montrer que A/aA consiste des classes de 0, 1 et -1, car 1 et -1 sont les seuls inversibles de A ; contradiction.

42. Montrer que $A := \mathbb{Q}(\sqrt{-19})_\mathbb{Z}$ n'est pas euclidien. Indication : montrer que pour tout idéal a de A différent de A on a $|A/a| > 3$; utiliser l'exercice précédent.

43. Pour ceux qui veulent : montrer que $A := \mathbb{Q}(\sqrt{-163})_\mathbb{Z}$ est principal. Ceci est directement lié au fait que le polynôme $f := x^2 - x + 41$ a la propriété que $f(n)$ est premier pour $-39 \leq n \leq 40$. (On sait, depuis le début des années 70, que les seuls corps quadratiques imaginaires K avec $K_\mathbb{Z}$ principal sont les $\mathbb{Q}(\sqrt{-d})$ avec d parmi 1, 2, 3, 7, 11, 19, 43, 67, et 163. Voir par exemple le livre [Serre1].)

44. Montrer que l'équation $y^2 = x^5 - 5$ n'a pas de solution dans $\mathbb{Z}$.

45. Soit K une extension finie de $\mathbb{Q}$. Notons $n := \dim_\mathbb{Q}(K)$ son degré et $d := \mathrm{discr}(K_\mathbb{Z})$ son discriminant. Montrer que l'on a :

$$|d| \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}.$$

Indication : utiliser la borne donnée dans le cours pour l'existence de “petits” représentants pour les éléments de $C(K_\mathbb{Z})$. Conclure que si $n > 1$, alors $|d| \geq 3$. Donner un exemple d'un K avec $|d| = 3$. En existe-t-il d'autres ? (En fait, pour chaque entier N, il n'existe (à isomorphisme près) qu'un nombre fini d'extensions finies K de $\mathbb{Q}$ avec $|\mathrm{discr}(K_\mathbb{Z})| \leq N$; c'est le théorème d'Hermite ; voir [Samuel, IV, Thm. 3].)

46. Soit f dans $\mathbb{Z}[x]$ unitaire, disons de degré n. Notons $z_1, \ldots, z_r$ les racines distinctes de f dans $\mathbb{C}$, avec multiplicités $m_1, \ldots, m_r$.

(a) Montrer que la forme trace de $\mathbb{C}[x]/(f)$ sur $\mathbb{C}$ est non dégénérée si et seulement si les z_i sont des racines simples (c'est à dire, si $m_i = 1$ pour tout i).

(b) Supposons à partir de maintenant que les racines de f sont simples. On rappelle que le discriminant de f est défini par : $\mathrm{discr}(f) = \prod_{i<j}(z_i - z_j)^2$. Montrer qu'en effet ce dernier produit ne dépend pas de la numérotation des racines.

(c) Montrer que : $\mathrm{discr}(f) = \mathrm{discr}(\mathbb{Z}[x]/(f)$. Indication : $\mathrm{discr}(\mathbb{Z}[x]/(f)$ est le déterminant de la matrice de la forme trace de la $\mathbb{C}$-algèbre $\mathbb{C}[x]/(f)$, par rapport à la $\mathbb{C}$-base $(1, x, \ldots, x^{n-1})$; le théorème Chinois donne un isomorphisme de $\mathbb{C}[x]/(f)$ vers $\mathbb{C}^n$; comparer l'image de la base $(1, x, \ldots, x^{n-1})$ avec la base canonique.

47. Soit K un corps de nombres, $A \subset B$ deux sous-anneaux d'indice fini de $K_{\mathbb{Z}}$. Montrer que $\mathrm{discr}(A) = |B/A|^2 \mathrm{discr}(B)$. Indication : A et B sont des $\mathbb{Z}$-modules libres de même rang fini ; utiliser ce que vous avez appris.
48. Soit f dans $\mathbb{Z}[x]$ unitaire, irréductible, et de degré au moins 2. Montrer que $|\mathrm{discr}(f)| \geq 3$. Pouvez-vous donner des exemples de f unitaires de degré 2, 3, etc. avec $|\mathrm{discr}(f)| = 1$?
49. Avec la méthode donnée en cours, montrer que $\mathbb{Z}[3^{1/3}]$ est l'anneau des entiers de $\mathbb{Q}(3^{1/3})$. Donner des $\mathbb{Z}$-bases des anneaux d'entiers des $\mathbb{Q}(n^{1/3})$, $4 \leq n \leq 9$.
50. Soit K un corps de nombres. Montrer que K^* n'est pas de type fini.
51. Soit $e \neq 0$ dans $\mathbb{Z}$.
    (a) Montrer que l'équation $x^2 - 2y^2 = e$ a des solutions dans $\mathbb{Z}$ si et seulement si, pour tout premier p tel que $v_p(e) = 1 \bmod 2$, 2 est un carré dans $\mathbb{F}_p$.
    (b) Pouvez vous conjecturer quels sont les p tel que 2 est un carré dans $\mathbb{F}_p$? (Pensez aux congruences modulo le discriminant de $\mathbb{Q}(\sqrt{2})$.)
52. Admettons que $A := \mathbb{Z}[2^{1/3}]$ soit l'anneau des entiers de $\mathbb{Q}(2^{1/3})$.
    (a) Montrer que A^* est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.
    (b) Trouver une unité fondamentale dans A.
    (c) Quelle équation sait-on maintenant résoudre ?
53. Donner une preuve du théorème des unités dans le cas où $r_1 = 0$ et $r_2 = 2$. Pour ceux qui veulent : $r_1 = 0$ et r_2 quelconque.
54. Soit p premier, $p > 2$.
    (a) Montrer que $t^4 + 1$ est scindé sur $\mathbb{F}_{p^2}$. (Indication : les racines de $t^4 + 1$ dans un corps K de caractéristique différente de 2 sont les éléments d'ordre 8 de K^*.)
    (b) Soit x une racine de $t^4 + 1$ dans $\mathbb{F}_{p^2}$. Montrer que x, $-x$, $1/x$ et $-1/x$ sont des racines distinctes de $t^4 + 1$.
    (c) Montrer que $(x + 1/x)^2 = 2$.
    (d) Montrer que $x + 1/x$ est dans $\mathbb{F}_p$ si et seulement si $p = \pm 1 \bmod 8$. (Indication : $x + 1/x \in \mathbb{F}_p$ équivaut à $(x + 1/x)^p = x + 1/x$.)
55. Calculer les symboles de Legendre suivants, par exemple en utilisant la réciprocité quadratique : $(\frac{19}{229})$, $(\frac{2}{229})$, $(\frac{38}{229})$, $(\frac{51}{229})$.
56. Soit $p \neq 2$ en nombre premier, K un corps, et ζ_p d'ordre p dans K^*. Notons τ la somme de Gauss :
$$\tau := \sum_{x \in \mathbb{F}_p^*} \left(\frac{x}{p}\right) \zeta_p^x .$$

Montrer que $\tau^2 = (\frac{-1}{p})p$. Vérifiez ce résultat à la main pour $p = 3$, 5, et 7. Ceci donne donc une démonstration très explicite du fait que le corps quadratique dans $\mathbb{Q}(\zeta_p)$ est $\mathbb{Q}(\sqrt{(\frac{-1}{p})p})$.

57. Soit K un corps quadratique. Montrer que les conditions qu'un premier p soit décomposé, inerte ou ramifié dans K sont données par des congruences modulo $\mathrm{discr}(K)$.
58. Calculer les premiers trois ou quatre approximations rationnelles de π données par la fraction continue associée à π.
59. Soient n et m des entiers. Constatez que le développement en fraction continue de n/m reproduit ce que l'on trouve avec l'algorithme d'Euclide pour calculer le pgcd de n et de m.
60. Soit x un réel irrationnel tel que la fraction continue associée à x devient périodique, dans le sens du cours. Montrez que x est quadratique sur $\mathbb{Q}$.
61. Calculer une unité fondamentale de $\mathbb{Z}[\sqrt{14}]$, avec la méthode des fractions continues.

11 Examens, partiels, etc.

Exemple d'un partiel (printemps 2000).

Durée : 2 heures. Documents autorisés : aucun. Calculettes non autorisées. Les résultats du cours et des feuilles de TD peuvent être utilisés. Justifiez vos réponses.

1. (a) Donner 5 solutions différentes de l'équation $y^2 = 2x^2 - 1$, avec $x > 0$ et $y > 0$ dans $\mathbb{Q}$.

   (b) Donner 5 solutions différentes de l'équation $y^2 = 2x^2 - z^2$, avec x, y et z dans $\mathbb{Z}$, avec $x > 0$, $y > 0$, $z > 0$, $y > z$ et $\mathrm{pgcd}(x, y, z) = 1$.

   (c) L'ensemble des solutions dans $\mathbb{Z}$ de $y^2 = 2x^2 - 1$ est-il fini ?

2. (a) Soit A le sous-anneau $\mathbb{Z}[\sqrt{-7}]$ de $\mathbb{C}$. La fonction $N\colon A \to \mathbb{N}$, $x \mapsto |x|^2$ est-elle euclidienne ?

   (b) Est-ce que l'anneau A est euclidien ?

   (c) Est-ce que l'anneau $B := \mathbb{Z}[(1 + \sqrt{-7})/2]$ est euclidien ?

3. Soit d un entier sans facteurs carrés, différent de 1, et congru à 1 modulo 4. Posons $K := \mathbb{Q}(\sqrt{d})$.

   (a) Donner une $\mathbb{Z}$-base de l'anneau des entiers $K_{\mathbb{Z}}$ de K.

   (b) Donner la matrice, par rapport à votre base, de la forme trace : $(x, y) \mapsto \mathrm{Tr}_{K/\mathbb{Q}}(xy)$.

4. Soit k un corps, V_1 et V_2 des k-espaces vectoriels de dimension finie, u_1 et u_2 des endomorphismes de V_1 et V_2, respectivement. Si u_1 et u_2 sont diagonalisables, est-ce que l'endomorphisme $u_1 \otimes u_2$ de $V_1 \otimes_k V_2$ l'est ?

Partiel du cours “théorie algébrique des nombres”, 17/03/2000.

Durée : 2 heures. Documents autorisés : aucun. Calculettes non autorisées. Les résultats du cours et des feuilles de TD peuvent être utilisés. Justifiez vos réponses.

1. (a) Donner toutes les solutions dans $\mathbb{Q}$ de l'équation $x_1^2 + x_2^2 = 3$.
   (b) Existe-t-il un a dans $\mathbb{Q}$ tel que l'équation $x_1^2 + x_2^2 + x_3^2 = a$ admet des solutions dans $\mathbb{R}$, mais pas dans $\mathbb{Q}$?

2. Soit A le sous-anneau $\mathbb{Z}[2^{1/3}]$ du sous-corps $K := \mathbb{Q}(2^{1/3})$ de $\mathbb{C}$.
   (a) Donner le polynôme minimal de $2^{1/3}$ sur $\mathbb{Q}$.
   (b) Donner une $\mathbb{Z}$-base de A.
   (c) Calculer $r \geq 0$, $1 < d_1 | \cdots | d_r \neq 0$ tels que $A/(-3 + 2^{1/3})A$ est isomorphe, en tant que $\mathbb{Z}$-module, à $\mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_r\mathbb{Z}$.
   (d) Calculer la forme trace de K sur $\mathbb{Q}$ par rapport à votre base.
   (e) Donner une majoration du cardinal du $\mathbb{Z}$-module $K_{\mathbb{Z}}/A$.

3. Soit p un nombre premier, k un corps de caractéristique p, et t dans k. Soit K la k-algèbre $k[x]/(x^p - t)$.
   (a) Supposons que t est une puissance $p$ème dans k. Montrer alors que la forme trace de K sur k est nulle.
   (b) Supposons seulement que t est une puissance $p$ème dans une extension k' de k. Montrer alors que la forme trace de K sur k est nulle.
   (c) Ne supposons plus rien sur t. Montrer que la forme trace de K sur k est nulle.
   (d) Existe-t-il une extension finie de corps telle que sa forme trace soit nulle ?

Corrigé du partiel du 17/03/2000.

1. (a) Supposons que (x_1, x_2) dans $\mathbb{Q}^2$ soit une solution. Ecrivons $x_1 = a/c$ et $x_2 = b/c$ avec a, b et c dans $\mathbb{Z}$ et $\mathrm{pgcd}(a, b, c) = 1$. On a : $a^2 + b^2 = 3c^2$. Mais dans $\mathbb{Z}/4\mathbb{Z}$ les seuls carrés sont 0 et 1, donc a^2, b^2 et c^2 ont image zéro dans $\mathbb{Z}/4\mathbb{Z}$, ce qui contredit $\mathrm{pgcd}(a, b, c) = 1$.

   (b) Oui, on peut prendre $a = 7$. Comme $7 \geq 0$, il y a des solutions dans $\mathbb{R}$. Pour voir qu'il n'y en a pas dans $\mathbb{Q}$, il suffit de voir qu'il n'y a pas de a, b, c et d dans $\mathbb{Z}$ avec $\mathrm{pgcd}(a, b, c, d) = 1$ et $a^2 + b^2 + c^2 = 7d^2$. Cela se voit en notant que les seuls carrés dans $\mathbb{Z}/8\mathbb{Z}$ sont 0, 1 et 4.

2. (a) Le polynôme $x^3 - 2$ dans $\mathbb{Q}[x]$ annule $2^{1/3}$ et est irréductible (Eisenstein avec $p = 2$, ou noter qu'il est de degré trois et n'a pas de racine dans $\mathbb{Q}$) ; c'est donc le polynôme minimal de $2^{1/3}$ sur $\mathbb{Q}$.

   (b) On peut prendre $(1, 2^{1/3}, 2^{2/3})$.

   (c) On calcule la matrice de la multiplication par $-3 + 2^{1/3}$ sur A par rapport à la base que l'on a, et on fait des opérations élémentaires sur les lignes et les colonnes, ce qui donne $\mathbb{Z}/25\mathbb{Z}$. Une autre façon de faire dans ce cas : $A = \mathbb{Z}[x]/(x^3 - 2)$, donc $A/(-3 + 2^{1/3})A = \mathbb{Z}[x]/(x^3 - 2, x - 3) = \mathbb{Z}/(3^3 - 2)$.

   (d) Calcul standard.

   (e) Soit x dans $K_{\mathbb{Z}}$. Ecrivons $x = a + b2^{1/3} + c2^{2/3}$ avec a, b et c dans $\mathbb{Q}$. Alors $\mathrm{Tr}_{K/\mathbb{Q}}(x)$, $\mathrm{Tr}_{K/\mathbb{Q}}(2^{1/3}x)$ et $\mathrm{Tr}_{K/\mathbb{Q}}(2^{2/3}x)$ sont dans $\mathbb{Z}$, ce qui donne $3a \in \mathbb{Z}$, $6b \in \mathbb{Z}$ et $6c \in \mathbb{Z}$. On en conclut que $|K_{\mathbb{Z}}/A| \leq 3{\cdot}6{\cdot}6 = 108$. Notons que cette méthode est la même par laquelle nous avons montré que les $K_{\mathbb{Z}}$ sont des $\mathbb{Z}$-modules libres de rang $\dim_{\mathbb{Q}}(K)$.

3. (a) On a donc $t = s^p$ pour un s dans k. Alors $K = k[x]/(x^p - s^p) = k[x]/((x - s)^p)$, ce qui est isomorphe à $k[y]/(y^p)$. La trace de la multiplication par y^i, avec $i > 0$, est nulle, car y est nilpotent, donc ses valeurs propres sont nulles. La trace de la multiplication par 1 est l'élément p de k, qui est nul car k est de caractéristique p.

   (b) Nous avons vu en cours que la matrice de la forme trace de $K' := k'[x]/(x^p - t)$ sur k' par rapport à la base $(1, x, \ldots, x^{p-1})$ est la même de celle de la forme trace de K sur k par rapport à la base $(1, x, \ldots, x^{p-1})$. Par la première partie, cette matrice est nulle.

   (c) Il suffit de remarquer que $x^p - t$ admet une racine dans une extension convenable de k (une clôture algébrique, ou un corps de décomposition ou de rupture, par exemple). Une autre méthode est de calculer les matrices des $\cdot x^i$, $0 \leq i < p$, par rapport à la base $(1, x, \ldots, x^{p-1})$; cela donne en un seul coup les trois premières parties de cet exercice.

   (d) Oui, par exemple $\mathbb{F}_2(t) \to \mathbb{F}_2(t)[x]/(x^2 - t)$.

Quelques remarques sur la correction.

1. Le correcteur a été surpris par la longueur de certaines copies. Il conseille vivement de faire une version brouillon avant de rédiger la version finale.
2. Le correcteur tient à préciser que $3/2 = 1 + 1/4 + 1/4$, que $6/5 = 1 + 4/25 + 1/25$, et que $4 = 4 + 0 + 0$.
3. C'est vrai qu'une $\mathbb{Z}$-base de A est une $\mathbb{Q}$-base de K, mais il n'est pas vrai que toute $\mathbb{Q}$-base de K est une $\mathbb{Z}$-base de A.
4. Remarque importante : s'il s'agit de faire des opérations élémentaires sur les lignes et les colonnes qui doivent être inversibles sur $\mathbb{Z}$, il faut surtout pas multiplier des lignes ou des colonnes par un entier non inversible. Plus précisément : la matrice $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ n'est pas inversible sur $\mathbb{Z}$, mais $\left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right)$ l'est.
5. La majoration $|K_{\mathbb{Z}}/A| \leq |K/A|$ ne semble pas très utile.
6. Si $A \subset B$ est une inclusion de $\mathbb{Z}$-modules, avec A et B isomorphes (par exemple, les deux libre de même rang), on n'a pas nécessairement $A = B$.
7. Une puissance $p$ème n'est pas la même chose qu'une puissance de p.
8. Remarque importante : il existe des extensions finies de corps qui ne sont pas séparables.
9. Le barème appliqué pendant la correction est : 1 : 3+3, 2 : 2+1+2+1+2, 3 : 1+2+1+2. Ce barème a été choisi avant la correction, en observant que les parties 1a, 2a, 2b, 2c, et 2d donnent déjà 9 points, et n'a pas été modifié depuis.
10. La répartition des notes est comme suite :

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
2	0	0	1	0	1	4	6	6	4	4	4	4	5	4	1	0	0	0	0	0

La moyenne des notes est 9,26.

Exemple d'un examen.

Durée : 3 heures. Documents autorisés : tous. Calculettes non autorisées. Les résultats du cours et des feuilles de TD peuvent être utilisés. Justifiez vos réponses.

1. Soit K un corps de nombres, et m un idéal maximal de son anneau des entiers $K_{\mathbb{Z}}$. Montrer que la norme de m est de la forme p^d avec p un nombre premier, et $d \leq \dim_{\mathbb{Q}}(K)$ un entier. (Indication : utilisez ce que vous savez de $K_{\mathbb{Z}}$ en tant que $\mathbb{Z}$-module.)

2. Donner des exemples d'entiers d tels que l'anneau $\mathbb{Z}[x]/(x^2 - d)$ soit :
   (a) non réduit ;
   (b) intègre, mais non intégralement clos ;
   (c) euclidien, et avec groupe multiplicatif infini ;
   (d) euclidien, et avec groupe multiplicatif fini.

3. Notons A le sous-anneau $\mathbb{Z}[\sqrt{10}]$ de $\mathbb{R}$.
   (a) Combien d'idéaux de norme 2 y a-t-il dans A ?
   (b) Combien d'idéaux de norme 3 y a-t-il dans A ?
   (c) Combien d'idéaux de norme 6 y a-t-il dans A ? (Indication : les questions précédentes peuvent être utiles.)
   (d) Existe-t-il a dans A avec $\mathrm{N}(a) = \pm 2$? Avec $\mathrm{N}(a) = \pm 3$. Et avec $\mathrm{N}(a) = \pm 6$? (Indication : la réduction modulo 5 peut être utile.)
   (e) Calculer l'ordre du groupe de classes d'idéaux $C(A)$.
   (f) Donner les quatre unités fondamentales de A.
   (g) Donner trois solutions de l'équation $x^2 - 10y^2 = 6$, avec x et y des entiers positifs.

4. Est-ce que 30 est un carré dans $\mathbb{Z}/239\mathbb{Z}$? Et dans $\mathbb{Z}/299\mathbb{Z}$?

Examen “théorie algébrique des nombres”, 22/05/2000.

Durée : 3 heures. Documents autorisés : tous. Calculettes non autorisées. Les résultats du cours et des feuilles de TD peuvent être utilisés. Justifiez vos réponses.

1. Est-ce que 15 est un carré dans $\mathbb{Z}/247\mathbb{Z}$? Et dans $\mathbb{Z}/251\mathbb{Z}$?

2. Donner des exemples d'entiers d tels que l'anneau $\mathbb{Z}[x]/(x^2-d)$ soit :
   (a) réduit, mais non intègre ;
   (b) de Dedekind, mais non principal.

3. (a) Soit A le sous-anneau $\mathbb{Z}[\sqrt{-2}]$ de $\mathbb{C}$. La fonction $N\colon A \to \mathbb{N}$, $x \mapsto |x|^2$ est-elle euclidienne ?
   (b) Soit B le sous-anneau $\mathbb{Z}[\sqrt{-3}]$ de $\mathbb{C}$. La fonction $N\colon A \to \mathbb{N}$, $x \mapsto |x|^2$ est-elle euclidienne ?
   (c) Est-ce que l'anneau B est euclidien ?

4. (a) Existe-t-il un corps de nombres K de degré au moins 3 tel que tout élément de $K_{\mathbb{Z}}^*$ soit un cube dans $K_{\mathbb{Z}}$?
   (b) Existe-t-il un corps de nombres K de degré 2 tel que tout élément de $K_{\mathbb{Z}}^*$ soit un cube dans $K_{\mathbb{Z}}$?

5. Notons A l'anneau $\mathbb{Z}[x]/(x^5-1)$.
   (a) Donner une $\mathbb{Z}$-base de A.
   (b) Calculer la matrice de la forme trace de A sur $\mathbb{Z}$, et son déterminant, qui est donc le discriminant de A.
   (c) Pour n dans $\mathbb{N}$, calculer le discriminant de l'anneau $\mathbb{Z}[x]/(x^n-1)$.
   (d) Pour p premier, calculer le discriminant de l'anneau $\mathbb{Z}[x]/(x^{p-1}+\cdots+x+1)$.

Corrigé de l'examen du 22/05/2000.

1. Tout d'abord, on décompose 247 et 251 en facteurs premiers. Cela donne : $247 = 13 \cdot 19$, et 251 est premier car non divisible par tout premier < 16.

   Par le théorème Chinois, 15 est un carré dans $\mathbb{Z}/247\mathbb{Z}$ si et seulement si 15 est un carré dans $\mathbb{Z}/13\mathbb{Z}$ et dans $\mathbb{Z}/19\mathbb{Z}$. Comme 15 est égal à 2 dans $\mathbb{Z}/13\mathbb{Z}$, et que 13 n'est pas ± 1 modulo 8, on sait que 15 n'est pas un carré modulo 13. Conclusion : 15 n'est pas un carré dans $\mathbb{Z}/247\mathbb{Z}$.

   Pour voir si 15 est un carré dans $\mathbb{Z}/251\mathbb{Z}$, on considère le symbole de Legendre. En utilisant la réciprocité quadratique, on voit que : $(\frac{15}{251}) = (\frac{3}{251})(\frac{5}{251}) = -(\frac{-1}{3})(\frac{1}{5}) = 1$.

2. Pour la première partie on peut prendre $d = 1$, et pour la deuxième $d = -5$.

3. (a) Oui, le calcul standard le montre.
   (b) Non, car dans (c) on montre que l'anneau en question n'est pas euclidien.
   (c) Non, car il n'est pas intégralement clos (sa clôture intégrale est $\mathbb{Z}[(1+\sqrt{-3})/2]$).

4. (a) Le théorème des unités de Dirichlet implique que le groupe $K^*_{\mathbb{Z}}$ se surjecte sur $\mathbb{Z}$. Dans $\mathbb{Z}$, la multiplication par 3 n'est pas surjective, donc l'élévation à la puissance 3 dans $K^*_{\mathbb{Z}}$ ne l'est pas non plus.
   (b) Oui, par exemple : $\mathbb{Q}(i)$.

5. (a) On peut prendre $(1, x, x^2, x^3, x^4)$.
   (b) Pour i dans $\mathbb{Z}$, la multiplication par x^i de A vers A agit sur notre base par un 5-cycle si i n'est pas multiple de 5, et par l'indentité si i est multiple de 5. Donc la trace de $\cdot x^i$ est zéro si $5 \not| i$ et est 5 si $5|i$. La matrice de la forme trace par rapport à notre base est donc :
   $$\begin{pmatrix} 5 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 5 \\ 0 & 0 & 0 & 5 & 0 \\ 0 & 0 & 5 & 0 & 0 \\ 0 & 5 & 0 & 0 & 0 \end{pmatrix}$$
   On calcule que le déterminant de cette matrice est -5^5.
   (c) En reprenant le même argument que dans la partie précédente, on voit que ce discriminant est $(-1)^{(n-1)(n-2)/2}n^n$.
   (d) Ceci est plus compliqué. Nous avons vu dans les exercices de TD que pour f dans $\mathbb{Z}[x]$ unitaire, on a $\mathrm{discr}(\mathbb{Z}[x]/(f)) = \mathrm{discr}(f)$. Donc :
   $$\mathrm{discr}(x^p - 1) = (-1)^{(p-1)(p-2)/2}p^p.$$

Ecrivons $x^p - 1 = (x-1)g$. La définition du discriminant en termes de différences de racines donne que $\operatorname{discr}(x^p - 1) = \operatorname{discr}(g)\prod_r (1-r)^2$, où r parcourt l'ensemble de racines de g (dans $\mathbb{C}$, disons). Comme $f = \prod_r (x-r)$ dans $\mathbb{C}[x]$, on a $\prod_r (1-r) = g(1) = p$. On trouve donc : $\operatorname{discr}(g) = (-1)^{(p-1)(p-2)/2} p^{p-2}$. Ici, nous n'avons pas utilisé que p soit premier ; la formule est vraie pour $p \geq 1$.

La répartition des notes est comme suite :

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
2	0	3	3	2	4	2	2	3	2	7	4	2	5	3	1	2	2	0	0	0

La moyenne de ces notes est environ 8.9.

Examen “théorie algébrique des nombres”, 11/09/2000.

Durée : 3 heures. Documents autorisés : tous. Calculettes non autorisées. Les résultats du cours et des feuilles de TD peuvent être utilisés. Justifiez vos réponses.

1. Admettons que $p = 10007$ soit premier. Est-ce que 35 est un carré modulo p ?

2. Notons $n = 5{\cdot}13{\cdot}17{\cdot}29$. Combien de couples (a, b) dans $\mathbb{Z}^2$ existe-t-il tel que $a^2 + b^2 = n$?

3. Notons A le sous-anneau $\mathbb{Z}[\sqrt{15}]$ de $\mathbb{R}$. C’est l’anneau des entiers de $\mathbb{Q}(\sqrt{15})$.
   (a) Combien d’idéaux de norme 2 y a-t-il dans A ?
   (b) Combien d’idéaux de norme 3 y a-t-il dans A ?
   (c) Combien d’idéaux de norme 6 y a-t-il dans A ? (Indication : les questions précédentes peuvent être utiles.)
   (d) Existe-t-il a dans A avec $|\mathrm{N}(a)| = 2$? Avec $|\mathrm{N}(a)| = 3$. Et avec $|\mathrm{N}(a)| = 6$? (Indication : la réduction modulo 5 peut être utile.)
   (e) Calculer l’ordre du groupe de classes d’idéaux $C(A)$.
   (f) Donner un exemple d’une factorisation en irréductibles dans A qui n’est pas unique à des unités près.
   (g) Donner les quatre unités fondamentales de A.
   (h) Donner trois solutions de l’équation $x^2 - 15y^2 = -6$, avec x et y des entiers positifs.

4. Soit p un nombre premier, $n \geq 2$ un entier, et $\mathbb{F}_p \to \mathbb{F}$ une extension de corps de degré n. On sait qu’une telle extension est unique à isomorphisme près, car c’est un corps de décomposition de $x^{p^n} - x$.
   (a) Quel est le cardinal de $\mathbb{F}$?
   (b) Quelle est la dimension de la $\mathbb{F}_p$-algèbre $\mathbb{F} \otimes_{\mathbb{F}_p} \mathbb{F}$?
   (c) Soit G le groupe d’automorphismes de la $\mathbb{F}_p$-algèbre $\mathbb{F} \otimes_{\mathbb{F}_p} \mathbb{F}$. Est-ce que G est cyclique ?
   (d) Est-ce que $\mathbb{F} \otimes_{\mathbb{F}_p} \mathbb{F}$ est un corps ?
   (e) Quel est le cardinal de G ?

Corrigé de l'examen du 11/09/2000.

1. Comme p est premier, on peut appliquer la réciprocité quadratique. On calcule :

$$\left(\frac{35}{10007}\right) = \left(\frac{5}{10007}\right)\left(\frac{7}{10007}\right) = \left(\frac{2}{5}\right)\cdot(-1)\cdot\left(\frac{4}{7}\right) = 1.$$

   Donc 35 est un carré modulo p.

2. Pour p parmi 5, 13, 17 et 29, prenons α_p premier dans $\mathbb{Z}[i]$ tel que $p = \alpha_p\overline{\alpha_p}$ (noter que p est 1 modulo 4). La question est combien de α on a dans $\mathbb{Z}[i]$ avec $n = \alpha\overline{\alpha}$. En regardant la factorisation dans $\mathbb{Z}[i]$ de n, on voit qu'il y a $2^4 4 = 64$ de tels α (pour chaque p il faut choisir entre α_p et $\overline{\alpha_p}$, et tout produit ainsi obtenu peut encore être multiplié par 1, i, -1 ou $-i$).

3. Comme dans "l'exemple d'un examen" à la page 68.

4. (a) Comme $\mathbb{F}$ est isomorphe à $\mathbb{F}_p^n$ en tant que $\mathbb{F}_p$-espace vectoriel, $|\mathbb{F}| = p^n$.
   (b) La dimension du produit tensoriel de deux espaces vectoriels est le produit des deux dimensions. Donc la dimension de $\mathbb{F} \otimes_{\mathbb{F}_p} \mathbb{F}$ est n^2.
   (c) Notons σ l'endomorphisme de Frobenius de $\mathbb{F}$, donc $\sigma(x) = x^p$ pour tout x dans $\mathbb{F}$. Alors σ n'est pas l'identité car $n \geq 2$. Mais alors on a $\sigma \otimes \mathrm{id}$ et $\mathrm{id} \otimes \sigma$ dans G, qui sont tous les deux d'ordre n, mais qui ne sont pas puissances l'un de l'autre. Cela implique que G n'est pas cyclique.
   (d) Non, car si c'était un corps, son groupe d'automorphismes serait cyclique, donc aussi son sous-groupe G. Il y a bien d'autres façons de voir que $\mathbb{F} \otimes_{\mathbb{F}_p} \mathbb{F}$ n'est pas un corps (trop de racines du polynôme $X^{p^n} - X$, par exemple, ou le résultat du cours qui dit que $\mathbb{F} \otimes_{\mathbb{F}_p} \mathbb{F}$ est isomorphe, en tant que $\mathbb{F}$-algèbre, à $\mathbb{F}^n$.
   (e) Utilisant que $\mathbb{F}\otimes_{\mathbb{F}_p}\mathbb{F}$ est isomorphe, en tant qu'anneau, à $\mathbb{F}^n$, on voit que $|G| = n^n \cdot n!$.

La répartition des notes est comme suite :

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
0	0	0	0	1	0	0	3	1	0	2	1	1	0	0	0	0	0	0	0	0

Partiel du cours “théorie algébrique des nombres”, 26/03/2001.

Durée : 2 heures. Documents autorisés : tous. Calculettes autorisées. Les résultats du cours et des feuilles de TD peuvent être utilisés. Justifiez vos réponses. Les exercices avec un astérisque sont probablement plus difficiles. Bonne chance !

Rappel : un élément a d’un anneau A est dit premier si l’idéal qu’il engendre est premier.

1. Factoriser en irréductibles les éléments 29, 31 et $3 + 7i$ de $\mathbb{Z}[i]$.

2. Posons $f := x^3 + x + 1$ dans $\mathbb{Z}[x]$, et $A := \mathbb{Z}[x]/(f)$. Notons u la classe de x dans A.
   - **(a)** Donner une $\mathbb{Z}$-base de A, calculer la matrice de la forme trace par rapport à cette base, et le discriminant de A.
   - **(b)** Calculer la matrice de la multiplication sur A par $u^2 + u - 1$ par rapport à votre base, et calculer les entiers positifs $d_1|d_2|d_3$ tels que $A/(u^2 + u - 1)A$ soit isomorphe à $\mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \oplus \mathbb{Z}/d_3\mathbb{Z}$ en tant que $\mathbb{Z}$-module.
   - **(c)*** L’élément $u^2 + u - 1$ de A est-il premier ?
   - **(d)*** Est-ce que A est intégralement clos ?

3. Soit $K := \mathbb{Q}(\sqrt{-6})$ et $A := \mathbb{Z}[\sqrt{-6}]$ son anneau des entiers.
   - (a) Donner des générateurs pour les idéaux maximaux de A contenant 2.
   - (b) Donner des générateurs pour les idéaux maximaux de A contenant 3.
   - (c) Donner la factorisation en idéaux maximaux de l’idéal $(\sqrt{-6})$.
   - (d) Donner un exemple d’un élément irréductible non premier dans A.
   - (e) Donner un exemple d’un élément a de A et de deux factorisations non équivalentes de ce a en irréductibles.

Corrigé du partiel du 11/04/2001.

1. Comme $29 = 1(4)$ et est premier dans $\mathbb{Z}$, la théorie dit que 29 se factorise en deux facteurs premiers dans $\mathbb{Z}[i]$, et, en effet, on a $29 = 5^2 + 2^2 = (5 + 2i)(5 - 2i)$. Comme 31 est premier dans $\mathbb{Z}$ et -1 modulo 4, 31 est premier (et donc irréductible) dans $\mathbb{Z}[i]$. La norme de $3 + 7i$ est $58 = 2{\cdot}29$. Comme $2 = -i(1 + i)^2$, $3 + 7i$ est divisible par $1 + i$, et on trouve $3 + 7i = (1 + i)(5 + 2i)$.

2. **(a)** Comme $\mathbb{Z}$-base on peut prendre $(1, u, u^2)$. En écrivant les matrices de la multiplication par u et u^2 par rapport à cette base on trouve que $\mathrm{Tr}(u) = 0$ et $\mathrm{Tr}(u^2) = -2$. En utilisant que $u^3 = -u - 1$ et $u^4 = -u^2 - u$, on obtient : $\mathrm{Tr}(u^3) = -3$ et $\mathrm{Tr}(u^4) = 2$. Le déterminant de la matrice de la forme trace est -31.

   (b) Le calcul de la matrice est directe, et les opérations élémentaires sur lignes et colonnes donnent : $d_1 = 1$, $d_2 = d_3 = 3$. Donc $A/(u^2+u-1)A$ est isomorphe à $\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/3\mathbb{Z}$ en tant que $\mathbb{Z}$-module.

   (c)* Comme 3 annule $A/(u^2 + u - 1)A$ (par la partie précédente), on sait que 3 est dans $(u^2 + u - 1)A$. Donc :

   $$A/(u^2+u-1)A = A/(3, u^2+u-1) = \mathbb{F}_3[x]/(x^2+x-1, f) = \mathbb{F}_3[x]/(x^2+x-1),$$

   la dernière égalité résultant du fait que $f = (x - 1)(x^2 + x - 1)$ dans $\mathbb{F}_3[x]$. Comme $x^2 + x - 1$ est irréductible dans $\mathbb{F}_3[x]$, $A/(u^2 + u - 1)A$ est un corps (à 9 éléments), et $u^2 + u - 1$ est donc premier dans A.

   (d)* Comme pour aucun premier p on a $p^2|\mathrm{discr}(A)$, A est intégralement clos par un théorème du cours.

3. (a) On a $A/2A = \mathbb{Z}[x]/(2, x^2 + 6) = \mathbb{F}_2[x]/(x^2)$. Par la correspondance des idéaux d'un anneau et d'un quotient, le seul idéal maximal de A contenant 2 est $m_2 := (2, \sqrt{-6})$.

   (b) On a $A/3A = \mathbb{Z}[x]/(3, x^2 + 6) = \mathbb{F}_3[x]/(x^2)$. Le seul idéal maximal de A contenant 3 est donc $m_3 := (3, \sqrt{-6})$.

   (c) On calcule : $m_2m_3 = (6, 2\sqrt{-6}, 3\sqrt{-6}, -6) = (\sqrt{-6})$.

   (d) Comme $\mathrm{N}(n + m\sqrt{-6}) = n^2 + 6m^2$, il n'y a pas d'élément de norme 2, 3 ou 5 dans A, et $A^\times = \{1, -1\}$. Comme $\mathrm{N}(\sqrt{-6}) = 6 = 2{\cdot}3$, $\sqrt{-6}$ est irréductible. Par la partie précédente, il n'est par premier.

   (e) On a $2{\cdot}3 = 6 = -1{\cdot}\sqrt{-6}^2$. Les 4 facteurs sont bien irréductibles, et les deux factorisations non équivalentes.

Quelques remarques sur la correction.

1. Dans le 2(c), on veut connaître la structure d'anneau de $A/(u^2 + u - 1)A$, mais il faut bien se réaliser que 2(b) ne donne que la structure de $\mathbb{Z}$-module.

2. Quand on demande des exemples, donner le plus simple possible. C'est plus agréable pour le correcteur. Exemple : dans le 3(d), on peut prendre $\sqrt{-6}$, et dans 3(e), deux factorisations de 6.
3. En faisant des opérations sur lignes et colonnes d'une matrice, n'écrivez pas de signes "="entre les matrices, car elles ne sont pas égales. La prochaine fois cela coûtera des points !
4. Dans un anneau quelconque, un élément premier non nul est irréductible ; c'est dans l'autre sens qu'il faut utiliser que l'anneau en question est factoriel.
5. Pour des erreurs énormes (résultat non entier quand il doit être entier, ou argument qui marche dans des cas où l'on sait que la conclusion est fausse) j'ai attribué quelques points négatifs (des -1).
6. Le barème appliqué pendant la correction est : 1 : 4, 2 : 2+2+2+2, 3 : 1+1+2+2+2. Ce barème avait été choisi avant la correction, et n'a pas été modifié depuis.
7. La répartition des notes est comme suite :

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	0	0	1	3	0	1	1	5	2	3	1	10	2	4	1	4	2	0	0	0

La moyenne des notes est $10,8$.

Examen “théorie algébrique des nombres”, 21/05/2001.

Durée : 3 heures. Documents autorisés : tous. Calculettes autorisées. Les résultats du cours peuvent être utilisés sans démonstration. Justifiez vos réponses. Bonne chance !

1. Factoriser en irréductibles 7, $4 - j$ et 29 dans $\mathbb{Z}[j]$ (avec $j = (-1 + i\sqrt{3})/2$).

2. (a) Calculer une unité fondamentale de $\mathbb{Q}(\sqrt{11})_{\mathbb{Z}}$.
   (b) Donner deux solutions dans $\mathbb{Z}$ de l'équation $x^2 - 11y^2 = 1$ avec $x > 0$ et $y > 1$.
   (c) Calculer à la main les quatre premières approximations p_n/q_n de $\sqrt{11}$ données par développement en fraction continue.
   (d) Écrire la fraction continue de $\sqrt{11}$ sous la forme $[a_0, a_1, a_2, a_3, \ldots]$, en indiquant la périodicité ($m > 0$ et N tels que $a_{n+m} = a_n$ si $n \geq N$).

3. Soit A l'anneau $\mathbb{Z}[x]/(x^3 - 5)$, et notons u la classe de x dans A. Notons K le corps des fractions de A.
   (a) Calculer le discriminant de A.
   (b) Donner des générateurs pour les idéaux maximaux de A contenant 3.
   (c) Donner des générateurs pour les idéaux maximaux de A contenant 5.
   (d) Montrer que $A = K_{\mathbb{Z}}$. (Indication : pour traiter les idéaux maximaux contenant 3, faites la substitution $x = y + 2$.)
   (e) Montrer que tout élément du groupe de classes d'idéaux $C(A)$ est représenté par un idéal de norme au plus 7.
   (f) Donner une majoration de $|C(A)|$.
   (g) Est-ce que l'équation $a^3 + 5b^3 + 25c^3 - 15abc = 1$ a des solutions dans $\mathbb{Z}$, autres que $(1, 0, 0)$?

4. Soit K le corps $\mathbb{Q}(\sqrt{13})$.
   (a) Montrer que la condition qu'un nombre premier p soit décomposé dans K ne dépend que de la classe de p modulo 13.
   (b) Donner la liste des éléments a de $\mathbb{Z}/13\mathbb{Z}$ tel qu'il existe un nombre premier p décomposé dans K d'image a dans $\mathbb{Z}/13\mathbb{Z}$.

La répartition des notes était comme suite :

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
3	1	1	1	0	1	1	1	1	1	5	11	5	7	6	2	0	0	0	0	0

La moyenne des notes est $10,15$.

Examen "théorie algébrique des nombres", 13/09/2001.

Durée : 3 heures. Documents autorisés : tous. Calculettes autorisées. Les résultats du cours peuvent être utilisés sans démonstration. Justifiez vos réponses. Bonne chance !

1. On admet que $p = 10039$ est premier. Est-ce que 39 est un carré modulo p ? Est-ce que 35 est un carré modulo p ?

2. (a) Calculer une unité fondamentale de $\mathbb{Z}[\sqrt{15}]$.
   (b) Donner trois solutions dans $\mathbb{Z}$ de l'équation $x^2 - 15y^2 = 1$ avec $x > 0$ et $y > 0$.
   (c) Y a-t-il des solutions dans $\mathbb{Z}$ de l'équation $x^2 - 15y^2 = -1$?
   (d) Y a-t-il des solutions dans $\mathbb{Q}$ de l'équation $x^2 - 15y^2 = -1$?
   (e) Calculer *de façon exacte* la fraction continue de $\sqrt{15}$ sous la forme $[a_0, a_1, a_2, a_3, \dots]$, en indiquant la périodicité ($m > 0$ et N tels que $a_{n+m} = a_n$ si $n \geq N$).
   (f) Calculez, pour $1 \leq n \leq 4$, les approximations p_n/q_n de $\sqrt{15}$ obtenues par le développement en fraction continue (l'utilisation d'homographies est conseillée).

3. Soit A l'anneau intègre $\mathbb{Z}[x]/(x^4 - x - 1)$, et notons u la classe de x dans A. Notons K le corps des fractions de A.
   (a) Calculer le discriminant de A et vérifiez que, à un signe près, il est premier.
   (b) Montrer que $A = K_{\mathbb{Z}}$.
   (c) Calculez les entiers r_1 et r_2 tels que la $\mathbb{R}$-algèbre $\mathbb{R}[x]/(x^4 - x - 1)$ soit isomorphe à $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$.
   (d) Montrer que tout élément du groupe des classes d'idéaux $C(A)$ est représenté par un idéal de norme au plus 2.
   (e) Montrer que A est principal.
   (f) Vérifiez que $x - 3$ divise $x^4 - x - 1$ dans $\mathbb{F}_7[x]$. Est-ce qu'il existe a dans A tel que $|N(a)| = 7$, où $N\colon K \to \mathbb{Q}$ est la norme ? Et si oui, y en a-t-il une infinité, et est-ce qu'il y a un a dans A avec $N(a) = 7$?

4. Soient $r \geq 1$ entier, et $p_1, \dots, p_r$ des nombres premiers distincts et différents de 2. Notons A l'anneau $\mathbb{Z}/p_1 \cdots p_r\mathbb{Z}$.
   (a) Combien de x y a-t-il dans A tel que $x^2 = 1$?
   (b) Combien de x y a-t-il dans A tel que $x^2 = x$?
   (c) Mêmes questions pour $A' := \mathbb{Z}/p_1^2 \cdots p_r^2\mathbb{Z}$.

Les notes étaient : 5, 8, 11 et 12.

Références

[Cohen] H. Cohen. *A course in computational algebraic number theory.* Graduate Texts in Mathematics, 138. Springer-Verlag, Berlin, 1993.

[CSS] *Modular Forms and Fermat's Last Theorem.* G. Cornell, J. Silverman and Glenn Stevens, editors. Springer-Verlag, 1997.

[HW] G.H. Hardy and E.M. Wright. *An introduction to the theory of numbers.* Fifth edition. The Clarendon Press, Oxford University Press, New York, 1979.

[Hua] L.K. Hua. *Introduction to number theory.* Springer-Verlag, Berlin–New York, 1982.

[I-R] K. Ireland and M. Rosen. *A classical introduction to modern number theory.* 2nd edition. Graduate Texts in Mathematics 84, 1990.

[KKS] K. Kato, N. Kurokawa, T. Saito. *Number Theory I, Fermat's dream.* Translations of Mathematical Monographs. AMS, 2000.

[Samuel] P. Samuel. *Théorie algébrique des nombres.* Hermann, Paris, deuxième édition, 1971.

[Serre1] J-P. Serre. *Lectures on the Mordell-Weil theorem.* Apects of Mathematics, E15, Vieweg, 1990 (2nd edition).

[Serre2] J-P. Serre. *Cours d'arithmétique.* Deuxième édition revue et corrigée. Le mathématicien, No. 2. Presses Universitaires de France, Paris, 1977.

[Serre3] J-P. Serre. *Corps Locaux.* Troisième édition. Publications de l'université de Nancago, No. VIII, Hermann, Paris, 1968.

[Swin] H.P.F. Swinnerton-Dyer. *A Brief guide to algebraic number theory.* London Mathematical Society Student Texts, 50. Cambridge University Press, Cambridge, 2001.