Cours de maîtrise de mathématiques : Théorie algébrique des nombres

Bas Edixhoven, Université de Rennes 1
Laurent Moret-Bailly, Université de Rennes 1

Dernière révision : septembre 2004

Ce texte est une version remaniée du polycopié de 2002, entièrement dû à B. Edixhoven. Le degré de détail des démonstrations est très variable. Pour plus de précisions, on pourra consulter les livres mentionnés dans la bibliographie (surtout [Samuel]), et naturellement assister au cours !

L. Moret-Bailly

Table des matières

1 L'équation de Fermat.

1.1 Introduction.

Les principaux objets d'étude de ce cours sont les anneaux d'entiers algébriques. La notion générale d'entier algébrique est introduite au chapitre 4, mais la définition est très simple : un nombre complexe z est un entier algébrique s'il est racine d'un polynôme *unitaire* à coefficients entiers. Exemple : tout nombre entier n (qui est racine de $X - n$), ou encore $\sqrt{2}$, $e^{2i\pi/7}$ et i (qui sont racines respectives de $X^2 - 2$, $X^7 - 1$ et $X^2 + 1$)), mais pas $1/2$, ni π.

Il est vrai, mais pas tout à fait évident (voir la proposition 4.1.4) que les entiers algébriques forment un sous-anneau de $\mathbb{C}$.

Nous commencerons ce cours par illustrer l'importance des anneaux d'entiers algébriques par des exemples : l'anneau $\mathbb{Z}[i]$ des « entiers de Gauss » intervient au chapitre 2 dans le problème des deux carrés (trouver tous els entiers qui sont somme de deux carrés), et l'anneau $\mathbb{Z}[j]$ (où $j = e^{2i\pi/3}$) dans le problème de Fermat en degré 3, résolu par Euler.

Dans ce chapitre, nous allons introduire le « problème de Fermat » général, et traiter quelques cas assez simples : le degré 2, connu depuis l'Antiquité, le degré 4 (résolu par Fermat) et l'équation de Fermat dans $\mathbb{C}[t]$.

L'*equation de Fermat* générale est la suivante :

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

Dans cette équation, n est un entier, supérieur 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 qu'il 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 un anneau A, est simplement l'ensemble des zéros du polynôme $x^n + y^n - z^n$ dans A^3.

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 $\mathbb{Z}^\times = \{1, -1\}$ 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 $\mathrm{Prim}(\mathbb{Z}^r)/\mathbb{Z}^\times$. Ceci est l'analogue sur $\mathbb{Z}$ de la définition usuelle de l'espace projectif $\mathbb{P}(\mathbb{Q}^r) := (\mathbb{Q}^r - \{0\})/\mathbb{Q}^\times$. 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* $\mathbb{P}(\mathbb{Q}^r)$.

En d'autres termes : « toute droite (sous-$\mathbb{Q}$-espace vectoriel de dimension 1) de $\mathbb{Q}^r$ contient un élément de $\mathrm{Prim}(\mathbb{Z}^r)$, unique au signe près ».

La vérification est laissée comme exercice ; disons seulement que l'application inverse est obtenue comme suit : 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.)

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 $\mathbb{Z}^\times = \{1, -1\}$ des inversibles de $\mathbb{Z}$ opère par homothéties sur X, et, de la même façon, $\mathbb{Q}^\times$ opère sur Y. Soient $\overline{X} := X/\mathbb{Z}^\times$ et $\overline{Y} := Y/\mathbb{Q}^\times$ 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 tout anneau A, (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 *triplets pythagoriciens*. Notons que de toute façon, $(a, b, c) \in \mathbb{Z}^3$ 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 $\mathbb{Z}$. 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 a ou 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. On écrit

$$\left(\frac{b}{2}\right)^2 = \frac{c-a}{2}\,\frac{c+a}{2}$$

   et l'on remarque que $(c - a)/2$ et $(c + a)/2$ sont entiers (a et c sont impairs) et premiers entre eux (l'idéal de $\mathbb{Z}$ qu'ils engendrent contient c et a, donc 1). Comme leur produit est un carré, on en déduit (parce que $\mathbb{Z}$ est factoriel et qu'ils sont positifs) que ce sont des carrés : il existe u et v dans $\mathbb{N}$, premiers entre eux, tels que $0 < u < v$, $(c-a)/2 = u^2$ et $(c+a)/2 = v^2$. On en conclut que les triplets pythagoriciens primitifs avec b pair sont les triplets

$$(v^2 - u^2, 2uv, v^2 + u^2) \quad \text{avec} \quad \begin{cases} 0 < u < v \\ u,\ v \text{ premiers entre eux} \\ uv \text{ pair} \end{cases}$$

   (sans la dernière condition, $v^2 - u^2$ et $v^2 + u^2$ seraient pairs et $(v^2 - u^2, 2uv, v^2 + u^2)$ ne serait pas primitif ; réciproquement, avec u et v premiers entre eux le seul nombre premier qui puisse diviser $v^2 - u^2$ et $v^2 + u^2$ est 2, ce qui est exclu si uv est 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 ». À 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 point de C est dit *rationnel* si ses deux coordonnées sont rationnelles. En considérant les droites passant par le point rationnel évident $(-1, 0)$, 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 écrivant $t=u/v$ avec u et v des entiers premiers entre eux, on obtient de nouveau la classification des triplets pythagoriciens primitifs obtenue plus 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 à l'équation de Fermat dans $\mathbb{Z}^3$, en tout degré ≥ 3. Malheureusement, la démonstration est beaucoup trop difficile pour être expliquée 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 (*$\operatorname{pgcd}(a,b,c)=1$*), 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 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 non nuls, premiers entre eux dans leur ensemble (vu la minimalité) donc premiers entre eux deux à deux (même argument que dans $\mathbb{Z}$), 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 à deux, car pour $\zeta \neq \zeta'$ les polynômes $c-\zeta b$ et $c-\zeta' b$ sont $\mathbb{C}$-linéairement indépendants dans $\mathbb{C}[t]$, donc le sous-$\mathbb{C}$-espace vectoriel qu'ils engendrent contient b et c qui sont premiers entre eux. 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 constantes non nulles, qui sont elles-mêmes des puissances n-ièmes. Il existe donc des polynômes x_ζ dans $\mathbb{C}[t]$ tels que

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

Comme les $c-\zeta b$ sont premiers entre eux deux à 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 quel triplet x, y, et z parmi les x_ζ (c'est possible parce que

$n \geq 3$). Comme x^n, y^n et z^n appartiennent au sous-espace de $\mathbb{C}[t]$ engendré 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 $\mathbb{C}$, non 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, non 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. □

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 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, en langage géométrique, des cubiques planes ou « courbes elliptiques »).

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

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

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

Preuve. Raisonnons par l'absurde (en laissant les détails au lecteur). 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 étapes :

1. x, y et z sont deux à deux premiers entre eux (vérifiez : attention, l'équation n'est pas homogène !).
2. L'équation dit donc que (x^2, y^2, z) est un triplet pythagoricien primitif. Après permutation, si nécessaire, de x et y, on a x et z impairs, y pair. Il existe alors u et v dans $\mathbb{N}$, premiers entre eux, avec $u > v$, tels que :

$$\begin{aligned} (2.1) \quad x^2 &= u^2 - v^2 \\ (2.2) \quad y^2 &= 2\,uv \\ (2.3) \quad z &= u^2 + v^2. \end{aligned}$$

3. La relation (2.1) dit que (x, v, u) est pythagoricien primitif ; comme x est impair, il existe a et b positifs et premiers entre eux tels que

$$\begin{aligned} (3.1) \quad x &= a^2 - b^2 \\ (3.2) \quad v &= 2\,ab \\ (3.3) \quad u &= a^2 + b^2. \end{aligned}$$

4. En combinant (2.2) et (2.3), on trouve

$$(y/2)^2 = uab$$

avec a et b premiers entre eux, et premiers avec u (car $2ab = v$, premier avec u). Comme en outre a, b et u sont positifs ce sont donc des carrés :

$$u = c^2, \quad a = e^2, \quad b = f^2$$

ce qui, reporté dans (3.3), donne $c^2 = e^4 + f^4$. On a donc une nouvelle solution non triviale (e, f, c) de l'équation de départ. Pour arriver à une contradiction, il reste à voir que $c < z$: mais l'équation (2.3) implique $z > u^2$, c'est-à-dire $z > c^4 > c$, d'où la contradiction cherchée.

□

2 Les entiers de Gauss 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.

Bien entendu, $\mathbb{Z}[i]$ désigne la sous-$\mathbb{Z}$-algèbre (c'est-à-dire le sous-anneau) de $\mathbb{C}$ engendré par i, c'est-à-dire l'ensemble des nombres complexes de la forme $P(i)$, pour $P \in \mathbb{Z}[X]$. Ses éléments sont souvent appelés « entiers de Gauss ». On voit tout de suite que ce sont les nombres complexes de la forme $a+ib$, avec a et b *entiers* (en effet ceux-ci sont évidemment dans $\mathbb{Z}[i]$, et ils forment déjà un sous-anneau de $\mathbb{C}$). Plus précisément :

2.1.1 Proposition. *Notons $A := \mathbb{Z}[i]$.*

(i) *L'homomorphisme de $\mathbb{Z}[X]$ dans A donné par $P \mapsto P(i)$ induit par passage au quotient un isomorphisme*
$$\mathbb{Z}[X]/(X^2+1) \xrightarrow{\sim} A.$$
En particulier, A est un $\mathbb{Z}$-module libre de rang 2 (plus précisément, $(1, i)$ est une base de ce $\mathbb{Z}$-module).

(ii) *Le groupe des automorphismes de l'anneau A est $\{\mathrm{Id}, \sigma\}$, où σ désigne la conjugaison complexe.*

(iii) *L'application « carré du module » induit une application, appelée « norme » :*
$$\begin{array}{rccc} N: & A & \longrightarrow & \mathbb{N} \\ z = a+ib & & \longmapsto & N(z) := z\,\overline{z} = a^2+b^2 \end{array}$$
(où a et b sont supposés entiers !). Cette application respecte la multiplication, et l'on a $N(z) = 0$ si et seulement si $z = 0$.

(iv) *Pour $z \in A$, on a l'équivalence :*
$$z \in A^\times \Leftrightarrow N(z) = 1.$$
On a $A^\times = \{\pm 1, \pm i\}$; c'est un groupe cyclique d'ordre 4.

(v) *L'anneau A est euclidien (donc principal, donc factoriel).*

Preuve. (i) Notons $\varphi : \mathbb{Z}[X] \to A$ l'homomorphisme en question. Il est clair que φ est surjectif (par définition de A), et d'autre part $\varphi(X^2+1) = 0$, donc φ passe au quotient en un morphisme surjectif d'anneaux $\overline{\varphi} : \mathbb{Z}[X]/(X^2+1) \to A$. Notons x la classe de X dans $\mathbb{Z}[X]/(X^2+1)$ Comme X^2+1 est unitaire, la division euclidienne par X^2+1 dans $\mathbb{Z}[X]$ montre que tout élément de $\mathbb{Z}[X]/(X^2+1)$ s'écrit de façon unique sous la forme $a+bx$ (avec a et b entiers). Comme $\overline{\varphi}$ est surjectif, on en déduit que tout $z \in A$ peut s'écrire sous la forme $z = \overline{\varphi}(a+bx) = a+ib$; l'unicité de cette écriture est immédiate, et montre

en outre que $\overline{\varphi}$ est injectif, donc finalement bijectif. (Bien entendu, ces arguments peuvent être rendus complètement élémentaires : exercice !).

(ii) Il est immédiat que σ est un automorphisme de A ; pour voir que c'est le seul (outre l'identité), il suffit de remarquer qu'un automorphisme τ est déterminé par $\tau(i)$ (en vertu de (i)), et que l'on doit avoir $\tau(i)^2 = \tau(i^2) = \tau(-1) = -1$, donc $\tau(i) = \pm i$.

(iii) est immédiat et laissé au lecteur.

(iv) Comme $N(1) = 1$ et que N respecte la multiplication, si z est inversible dans A alors $N(z)$ est inversible dans $\mathbb{N}$ donc égal à 1. Réciproquement si $z \in A$ vérifie $N(z) = 1$, alors $z\,\overline{z} = 1$ donc $z \in A^\times$ (avec pour inverse $\overline{z} = \sigma(z)$).

En conséquence, $A^\times$ est l'ensemble des $z = a + ib$ avec a et b dans $\mathbb{Z}$ et $a^2 + b^2 = 1$; on en déduit immédiatement que $A^\times = \{\pm 1, \pm i\}$.

(v) Montrons que l'application $N : A \to \mathbb{N}$ est une « jauge euclidienne », c'est-à-dire que :

(a) pour tout $z \in A$, on a $N(z) = 0$ si et seulement si $z = 0$;

(b) pour tous a et $b \in A$ avec $b \neq 0$, il existe q et r dans A tels que $a = bq + r$ et $N(r) < N(b)$.

La première assertion a déjà été vue. Pour la seconde, considérons le nombre complexe $z = a/b$. Les conditions ci-dessus s'écrivent $z = q + (r/b)$ et $|r/b| < 1$. Il s'agit donc de trouver (étant donné $z \in \mathbb{C}$) un élément q de A tel que $|q - z| < 1$, ce que le lecteur fera à l'aide d'un dessin (en fait on peut trouver q tel que $|q - z| \leq \sqrt{2}/2$). □

Vu l'assertion (v) ci-dessus, la question naturelle qui se pose est de trouver les éléments irréductibles (ou « premiers ») de A. La réponse est fournie par le théorème suivant (où l'on pose encore $A = \mathbb{Z}[i]$) :

2.1.2 Théorème. (1) *Soit p un nombre premier. Alors :*

(i) *si $p = 2$, alors $p = (1+i)(1-i) = i\,(1-i)^2$; de plus $1 - i$ est irréductible dans A, de norme 2 (et il en est de même de $1 + i$, qui lui est associé) ;*

(ii) *si $p \equiv -1 \pmod 4$, alors p est irréductible dans A (de norme p^2) ;*

(iii) *si $p \equiv 1 \pmod 4$, alors $p = \pi\overline{\pi}$, où $\pi \in A$ et son conjugué $\overline{\pi}$ sont irréductibles de norme p, et non associés entre eux.*

(2) *Inversement, tout élément irréductible de A est :*

(a) *soit associé à $1 - i$ (et de la forme $\pm 1 \pm i$), et de norme 2 ;*

(b) *soit associé à un nombre premier $p \equiv -1 \pmod 4$, et de norme p^2 ;*

(c) *soit de norme p, nombre premier congru à 1 modulo 4, et associé à un élément π comme en* (iii) *ci-dessus.*

Preuve. (On rappelle que deux éléments x et y de A sont *associés* s'il existe $u \in A^\times$ tel que $y = ux$.)

(1) Remarquons que si $z \in A$ et si $N(z)$ est un nombre premier, alors z est irréductible : ceci résulte des assertions (iii) et (iv) de 2.1.1.

(i) est immédiat.

Pour montrer (ii) et (iii), on remarque d'abord que (puisque A est principal) un élément b non nul de A est irréductible si et seulement si l'anneau A/bA est un corps. Or il résulte de 2.1.1 (i) que, si $b \in \mathbb{Z}$, on a $A/bA \cong \mathbb{F}_p[X]/(X^2+1)$. On a alors le résultat bien connu suivant (voir cours de licence) :

2.1.3 Lemme. *Soit p un nombre premier impair. On a alors les équivalences :*

$p \equiv 1 \pmod 4 \quad \Leftrightarrow \quad -1$ *est un carré dans* $\mathbb{Z}/p\mathbb{Z} \quad \Leftrightarrow \quad X^2+1$ *n'est pas irréductible dans* $(\mathbb{Z}/p\mathbb{Z})[X]$. □

Revenons à 2.1.2, et montrons (ii) : d'après le lemme, si $p \equiv -1 \pmod 4$, alors l'anneau A/pA est un corps (puisque X^2+1 est irréductible dans $\mathbb{F}_p[X]$), donc p est bien irréductible.

(iii) Si $p \equiv -1 \pmod 4$, alors, toujours d'après le lemme, X^2+1 a une racine α dans $\mathbb{F}_p$ (et en fait deux racines distinctes), d'où un morphisme d'anneaux

$$\varphi : A \cong \mathbb{Z}[X]/(X^2+1) \longrightarrow \mathbb{F}_p$$

envoyant la classe de X (c'est-à-dire l'élément i de A) sur α, et de façon générale la classe d'un polynôme P sur $P(\alpha)$. Ce morphisme est évidemment surjectif (car son image contient 1, qui engendre $\mathbb{F}_p$ comme groupe additif).

Comme A est principal le noyau de φ est engendré par un élément π, et ce noyau contient évidemment p de sorte que π divise p dans A. Écrivant $p = \pi\,\pi'$, on remarque que :

- $p^2 = N(p) = N(\pi)\,N(\pi')$ dans $\mathbb{N}$;
- π n'est pas inversible (sinon $\ker\varphi = A$, absurde) donc $N(\pi) \neq 1$;
- π' n'est pas inversible : sinon on aurait $\ker\varphi = p\,A$, mais $|A/\ker\varphi| = |\mathbb{F}_p| = p$, alors que $|A/p\,A| = p^2$ d'après 2.1.1 (i) par exemple. Donc $N(\pi') \neq 1$.

La seule possibilité est donc que $N(\pi) = N(\pi') = p$ (de sorte que π est irréductible, mais on le savait déjà puisque $A/\pi\,A$ est isomorphe à $\mathbb{F}_p$). En outre, vu la définition de la norme, ceci donne $\pi\,\overline{\pi} = p$, comme annoncé en (iii). Il reste à voir que π et $\overline{\pi}$ ne sont pas associés : pour cela, on écrit $\pi = a + ib$ avec a et b entiers et $a^2+b^2 = p$, et on suppose que $\overline{\pi} = u\,\pi$ avec $u \in \{\pm 1, \pm i\}$ (utilisant 2.1.1 (iv)) : il suffit d'éliminer les quatre cas, ce que le lecteur fera bien tout seul.

Montrons la partie (2) de l'énoncé. Soit $\alpha \in A$ irréductible. Bien entendu, α divise (dans A) l'entier $N(\alpha) = \alpha\,\overline{\alpha}$, qui est > 1 puisque α n'est pas inversible (cela fait partie de la définition d'un irréductible). Donc $N(\alpha)$ est un produit (non vide) de nombres premiers ; comme α est irréductible et que A est factoriel, α divise l'un de ces facteurs ; appelons-le p. En particulier $N(\alpha)$ divise $N(p) = p^2$ (et est $\neq 1$, rappelons-le).

Si α est associé à p, alors p est irréductible dans A et l'on est dans le cas (b) de l'énoncé. Sinon, $N(\alpha)$ divise strictement p^2 donc est égal à p, et l'on est dans le cas (a) ou le cas (c). □

2.1.4 Remarque. Pour un nombre premier p, considérons l'anneau A/pA :

– il est isomorphe, comme anneau, à $\mathbb{F}_p[X]/(X^2+1)$ (et, comme groupe abélien, à $\mathbb{Z}^2/p\mathbb{Z}^2 \cong (\mathbb{Z}/p\mathbb{Z})^2$) ;
– si $p \equiv -1 \pmod 4$, on a vu au cours de la démonstration que A/pA est un corps (à p^2 éléments, d'après ce qui précède) ;
– si $p \equiv 1 \pmod 4$, soient $\pm\alpha$ les deux éléments de carré -1 dans $\mathbb{F}_p$: alors on a un isomorphisme d'anneaux

$$A/pA \xrightarrow{\sim} \mathbb{F}_p \times \mathbb{F}_p \quad \text{(anneau produit)}$$

envoyant la classe de i sur $(\alpha, -\alpha)$;
– si $p = 2$, on a $A/pA \cong \mathbb{F}_2[X]/(X^2+1) = \mathbb{F}_2[X]/((X+1)^2) \cong \mathbb{F}_2[Y]/(Y^2)$ (où le dernier isomorphisme envoie X sur $Y-1$).

Le cas $p = 2$ est donc le seul où A/pA ne soit pas réduit (c'est-à-dire admette un élément nilpotent non trivial, en l'occurrence la classe de $1-i$).

2.2 Le théorème des deux carrés.

Si n et un entier et p un nombre premier, on note $v_p(n)$ l'exposant de p dans la décomposition de n en facteurs premiers. (Cette notation sera généralisée plus loin, cf. 3.3.1).

2.2.1 Théorème. *Un nombre premier p est la somme de deux carrés (d'entiers) si et seulement si $p = 2$ ou $p \equiv 1 \pmod 4$ (Fermat).*

Un entier positif n est somme de deux carrés si et seulement si $v_p(n)$ est pair pour tout nombre premier p qui est -1 modulo 4.

Preuve. Bien entendu, $n \in \mathbb{N}$ est somme de deux carrés si et seulement si n est la norme d'un élément de $A = \mathbb{Z}[i]$. On en déduit immédiatement la première assertion (le cas où n est premier), compte tenu du théorème 2.1.2.

Soit n dans $\mathbb{N}$, non nul. Supposons d'abord que $v_p(n)$ est pair pour tout nombre premier $p \equiv -1 \pmod 4$. Alors, d'après l'assertion précédente, n est produit de sommes de deux carrés. Or, dans tout anneau commutatif, l'ensemble des sommes de deux carrés est stable par produit, en raison de l'identité

$$(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2$$

(que l'on retrouve facilement en écrivant « formellement » $a^2+b^2 = (a+ib)(a-ib)$, etc.). Donc n est bien somme de deux carrés.

Réciproquement, supposons que $n = a^2+b^2$ avec a et b dans $\mathbb{Z}$. On a donc $n = N(\alpha)$ avec $\alpha = a+bi \in A$. Comme A est factoriel, α est de la forme $u\,\pi_1 \dots \pi_r$ avec $u \in A^\times$ et les π_i irréductibles dans A. Comme $N(u) = 1$, on a $n = N(\pi_1)\dots N(\pi_r)$. Mais une conséquence de 2.1.2 est que chaque $N(\pi_i)$ est soit 2, soit un nombre premier $\equiv 1 \pmod 4$, soit le *carré* d'un nombre premier $\equiv -1 \pmod 4$, d'où la conclusion. □

On verra en TD un algorithme efficace pour trouver une factorisation dans $\mathbb{Z}[i]$ d'un nombre premier $p \equiv 1 \pmod 4$. 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. (Lagrange) *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 pas car il n'est pas « euclidien » (il est facile de vérifier qu'il n'est pas euclidien pour la norme euclidienne). Le sous-anneau (« ordre ») que l'on prend est celui engendré par i, j, k et $(1 + i + j + k)/2$. Une façon d'écrire cet ordre est :

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

3 Le « théorème de Fermat » en degré 3.

3.1 Introduction.

Nous allons démontrer dans ce chapitre le

3.1.1 Théorème. (Euler) *Soient a, b, c entiers vérifiant $a^3 + b^3 = c^3$. Alors $abc = 0$.*

Ce résultat ne figure pas dans [Samuel]. Nous suivons [I-R, §17.8]. La méthode est la même que dans le cas des polynômes (1.4.1) : factoriser après adjonction des racines cubiques 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 $\mathbb{C}$; on observera l'analogie avec 2.1.1.

3.2 Un peu d'arithmétique dans $\mathbb{Z}[j]$.

On note j le nombre complexe

$$j := \frac{-1 + i\sqrt{3}}{2} = e^{2i\pi/3}.$$

On rappelle que j est une racine cubique primitive de l'unité, et est racine du polynôme $X^2 + X + 1$. (En particulier, $j^2 = (-1 - i\sqrt{3})/2$ est à la fois le carré, l'inverse et le conjugué de j : il est souvent utile de s'en souvenir dans les calculs). On note $A = \mathbb{Z}[j]$ le sous-anneau de $\mathbb{C}$ engendré par j. En utilisant la relation $j^2 = -1 - j$, on voit tout de suite que A est aussi l'ensemble des nombres complexes de la forme $a + bj$, avec a et b entiers. Plus précisément :

3.2.1 Proposition. (i) *L'homomorphisme de $\mathbb{Z}[X]$ dans A donné par $P \mapsto P(j)$ induit par passage au quotient un isomorphisme*

$$\mathbb{Z}[X]/(X^2 + X + 1) \xrightarrow{\sim} A.$$

En particulier, A est un $\mathbb{Z}$-module libre de rang 2 (plus précisément, $(1, j)$ est une base de ce $\mathbb{Z}$-module).

(ii) *Le groupe des automorphismes de l'anneau A est $\{\mathrm{Id}, \sigma\}$, où σ désigne la conjugaison complexe.*

(iii) *L'application « carré du module » induit une application, appelée « norme » :*

$$\begin{array}{rccc} N : & A & \longrightarrow & \mathbb{N} \\ z = a + bj & & \longmapsto & N(z) := z\,\overline{z} = a^2 - ab + b^2 \end{array}$$

(où a et b sont supposés entiers !). Cette application respecte la multiplication, et l'on a $N(z) = 0$ si et seulement si $z = 0$.

(iv) *Pour $z \in A$, on a l'équivalence :*

$$z \in A^\times \Leftrightarrow N(z) = 1.$$

On a $A^\times = \{\pm 1, \pm j, \pm j^2\}$; c'est un groupe cyclique d'ordre 6.

(v) *L'anneau A est euclidien (donc principal, donc factoriel).*

Preuve. La plupart des arguments sont entièrement analogues à ceux de 2.1.1 ; nous laissons donc les détails au lecteur. Pour le calcul de $A^\times$ dans (iv), le plus simple est de remarquer que $a+bj = (a-(b/2)) + ib\sqrt{3}/2$ de sorte que si $|a+bj| = 1$ on a $|b| \leq 1$ d'où $b \in \{0, \pm 1\}$. Pour (v) on montre encore que la norme est une jauge euclidienne, par le même argument que dans 2.1.1 (v). □

Comme A est principal, on peut se poser, comme pour $\mathbb{Z}[i]$, le problème de trouver les irréductibles de A. Nous ne le ferons pas ici ; nous aurons seulement besoin d'un élément irréductible particulier, très analogue à l'élément $1-i$ de $\mathbb{Z}[i]$:

3.2.2 Proposition. *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. La relation $3 = -j^2\lambda^2$ est immédiate ; d'autre part on a $N(\lambda) = 3$, donc λ est premier et $A/\lambda A$ est un corps.

Dans $\mathbb{F}_3$, l'élément 1 est racine (double) du polynôme X^2+X+1, d'où un morphisme d'anneaux $A \cong \mathbb{Z}[X]/(X^2+X+1) \to \mathbb{F}_3$, envoyant j sur 1 et donc λ sur 0, d'où un morphisme $A/\lambda A \to \mathbb{F}_3$, évidemment surjectif donc bijectif puisque $A/\lambda A$ est un corps et $\mathbb{F}_3 \neq \{0\}$. □

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.

3.2.3 Lemme. *Les cubes dans $A/9A = A/\lambda^4 A$ sont 0, ± 1, $\pm\lambda^3$.*

Preuve. On calcule dans $\overline{A} = A/9A$. On remarque d'abord que, pour x et y dans $\overline{A}$, on a $(x+3y)^3 = x^3$: autrement dit, x^3 ne dépend que de la classe de x modulo 3, ou, ce qui revient au même, modulo λ^2.

D'autre part, comme $A/\lambda A = \mathbb{F}_3$, tout élément de A est de la forme $\varepsilon + \lambda a$, avec $\varepsilon \in \{0, \pm 1\}$ et $a \in A$. En recommençant avec a, on en déduit que tout $x \in \overline{A}$ est congru modulo λ^2 à un $\varepsilon + \lambda\varepsilon'$ avec ε et ε' dans $\{0, \pm 1\}$; il suffit donc de voir que

$$\forall (\varepsilon, \varepsilon') \in \{0, \pm 1\}^2, \text{ on a } (\varepsilon + \lambda\varepsilon')^3 \in \{0, \pm 1, \pm\lambda^3\}.$$

C'est clair si $\varepsilon = 0$ ou si $\varepsilon' = 0$. Sinon, on développe :

$$\begin{aligned}(\varepsilon + \lambda\varepsilon')^3 &= \varepsilon^3 + 3\,\lambda\,\varepsilon^2\,\varepsilon' + \lambda^3\,\varepsilon'^3 \quad \text{(formule du binôme, et } 3\,\lambda^2 = 0 \text{ dans } \overline{A}) \\ &= \varepsilon + 3\,\lambda\,\varepsilon' + \lambda^3\,\varepsilon' \qquad (\varepsilon, \varepsilon' \in \{\pm 1\}) \\ &= \varepsilon + (3\,\lambda + \lambda^3)\,\varepsilon'\end{aligned}$$

et un calcul immédiat donne $3\,\lambda + \lambda^3 = 3\,\lambda^2$ qui est nul dans $\overline{A}$, d'où $(\varepsilon + \lambda\varepsilon')^3 = \varepsilon$, cqfd. □

3.3 Preuve du théorème.

Nous allons montrer un résultat plus fort, en travaillant dans $A = \mathbb{Z}[j]$ au lieu de $\mathbb{Z}$ et en introduisant une « inconnue » inversible dans l'équation ; cela est nécessaire pour faire fonctionner la descente infinie (qui se fera cette fois en termes de divisibilité par λ).

3.3.1 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.

En d'autres termes, on a $v_p(a) = \max\{r \in \mathbb{N} \mid p^r \text{ divise } a\}$, et a s'écrit $a = p^{v_p(a)}a'$, avec $a' \in A$ non divisible par p (et donc premier à p).

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

Preuve. Par l'absurde. Supposons donc donnés x, y, z dans A et u dans $A^\times$, avec $x^3+y^3 = uz^3$ 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 $A^\times$, $x^3+y^3 = uz^3$, et $\lambda|z$. Nous allons maintenant produire un tel quadruplet (x', y', z', u') avec $v_\lambda(z') < v_\lambda(z)$; ce sera la contradiction cherchée. Allons-y.

Notons tout d'abord que les classes de x^3 et y^3 dans $A/\lambda^4 A$ sont deux cubes inversibles (car x et y sont premiers avec λ) donc égaux à ± 1 d'après 3.2.3. Comme leur somme est divisible par λ^3 (puisque $x^3 + y^3 = uz^3$), cette somme est nulle. Donc $\lambda^4|uz^3$, donc $\lambda^2|z$. Nous écrivons maintenant :

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

Comme $\lambda^6 | uz^3$, au moins un des facteurs de 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 $v_\lambda(x+jy) = v_\lambda(x+j^2y) = 1$. Pour $x+jy$ par exemple, on écrit :

$$x + jy = (x+y) + (j-1)\,y = (x+y) - \lambda\, y$$

et on remarque que puisque $v_\lambda(x+y) \geq 2$ et $v_\lambda(\lambda\, y) = 1$, le troisième membre est divisible par λ mais pas par λ^2 ; le calcul de $v_\lambda(x+j^2y)$ est analogue (cet argument de « valuation » est typique !). 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 $\det(\begin{smallmatrix} 1 & 1 \\ 1 & j \end{smallmatrix}) = -\lambda$ 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, λ comme pgcd. 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 $A^\times$, 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 :

$$0 = u_1\,\lambda^{3v_\lambda(z)-3}\,\alpha^3 + j\,u_2\,\beta^3 + j^2\,u_3\,\gamma^3.$$

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 $A^\times$ 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 remplaçant y_1 par $-y_1$ si nécessaire, on obtient donc :

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

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

4 Anneaux des entiers dans les corps de nombres.

4.1 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 $\mathbb{Q}$.

4.1.1 Définition. 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 :

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

autrement dit, si b est « racine d'un polynôme *unitaire* à coefficients dans A ».

On dit que B est entier sur A si tout élément de B est entier sur A.

4.1.2 Exemples et remarques.

1. Il est clair que les éléments de A (ou plutôt de son image dans B) sont entiers sur A.
2. Dans la plupart des applications, le morphisme $A \to B$ est injectif. On peut d'ailleurs souvent se ramener à ce cas : il est clair en effet que $b \in B$ est entier sur A si et seulement si il est entier sur l'image de A dans B.
3. Si $\varphi : B \to B'$ est un morphisme de A-algèbres, et si $b \in B$ est entier sur A, il est clair que $\varphi(b)$ est entier sur A (il est annulé par tout polynôme qui annule b).
4. Si $A \to B$ est une extension de corps, on retrouve simplement la notion d'élément *algébrique* sur A.
5. Le cas le plus important dans ce cours est celui où $A = \mathbb{Z}$ et où $B = K$ est une extension (qui sera souvent finie) de $\mathbb{Q}$. Dans ce cas, l'ensemble des éléments de K entiers sur $\mathbb{Z}$ sera noté $K_{\mathbb{Z}}$, et appelé *l'anneau des entiers* de K (on rencontre plus couramment dans la littérature la notation O_K) ; nous allons voir bientôt que c'est bien un sous-anneau de K.
6. Les éléments de $\mathbb{C}_{\mathbb{Z}}$ sont appelés les *entiers algébriques*. Par exemple, $\sqrt{2}$ et i sont des entiers algébriques, mais e et $1/2$ n'en sont pas (pour $1/2$, voir 4.1.3 ci-dessous).

4.1.3 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 entiers premiers entre eux, et $m \neq 0$. 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 $m = \pm 1$ et que a est dans $\mathbb{Z}$.

4.1.4 Proposition. *Soit $A \to B$ un morphisme d'anneaux. Pour b dans B, les conditions suivantes sont équivalentes :*

(i) *b est entier sur A ;*
(ii) *la sous-A-algèbre $A[b]$ de B est un A-module de type fini ;*
(iii) *il existe une sous-A-algèbre C de B, contenant b, et de type fini en tant que A-module ;*
(iv) *il existe un sous-A-module M de B, de type fini, contenant 1 et stable par multiplication par b (i.e., tel que $bM \subset M$).*
(v) *il existe un sous-A-module M de B, de type fini, contenant un élément régulier de B, 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. Rappelons qu'un élément z d'un anneau R est dit *régulier* (ou « non diviseur de zéro ») si la multiplication par z dans R est injective.

Montrons que (i)⇒(ii). 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 $(1, x, \ldots, x^{n-1})$, $n = \deg(f)$. 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 $k < n$).

(ii)⇒(iii) : on peut prendre $C := A[b]$.

(iii)⇒(iv) : on peut prendre $M := C$.

(iv)⇒(v) : on peut prendre « $M := M$ ».

Montrons finalement que (v)⇒(i). Soit donc M un sous-A-module de B, de type fini, contenant un élément régulier, 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 $\sum_j c_{i,j} m_j$, avec les $c_{i,j}$ dans A. Notons N la matrice $b\mathrm{I}_n - (c_{i,j})$ à coefficients dans $A[b]$. Les relations ci-dessus se résument en l'égalité suivante dans le $A[b]$-module M^n :

$$N \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix} = 0.$$

Le lecteur vérifiera que les règles habituelles du produit de matrices s'étendent à ce contexte ; en particulier, si $U \in \mathrm{M}_n(A[b])$ on a encore

$$U\,N \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{pmatrix} = 0.$$

Si l'on prend pour U la transposée de la comatrice de N, on a $U\,N = (\det N)\,\mathrm{I}_n$, et l'on déduit donc de ce qui précède que $(\det N)\,m_i = 0$ pour chaque i. Donc M est annulé par $\det N$ puisque les m_i l'engendrent. Comme M contient un élément régulier, on a donc $\det N = 0$. Mais la définition de N montre que $\det N = P(b)$ où P est unitaire à coefficients dans A (en fait P est le polynôme caractéristique de $(c_{i,j})$), d'où (i).

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 (i) et (iii) montre alors que tout élément de $A[b_1, b_2]$ est entier sur A. □

4.2 Fermeture intégrale, clôture intégrale.

4.2.1 Lemme. *Soient $A \to B \to C$ des morphismes d'anneaux, avec B entier sur A et C entier sur B. Alors C est entier sur A.*

Preuve. Soit $x \in C$. Comme C est entier sur B, on a une relation de la forme

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

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 (pour deux éléments, l'argument a déjà servi dans la preuve de la dernière assertion de 4.1.4). Le critère d'intégralité 4.1.4 (iii) implique alors que x est entier sur A, cqfd. □

4.2.2 Définition. Soient A un anneau et B une A-algèbre. La sous-A-algèbre de B formée des éléments entiers sur A (cf. 4.1.4) est appelée la *fermeture intégrale* de A dans B ; c'est aussi le plus grand sous-anneau de B qui est entier sur A.

Supposons A *intègre*, de corps des fractions K : on appelle *clôture intégrale* de A la fermeture intégrale de A dans K.

On dit qu'un anneau A est *intégralement clos* s'il est intègre et égal à sa clôture intégrale.

4.2.3 Exemple. Si k est un corps, le sous-anneau $A = k[T^2, T^3]$ de $k[T]$ (égal à l'ensemble des polynômes dont le terme en T est nul) est intègre, mais non intégralement clos : son corps des fractions est $k(T)$, et l'élément T est entier sur A (car racine de $X^2 - T^2 \in A[X]$) et n'est pas dans A. Par contre, $k[T]$ est intégralement clos : c'est un cas particulier de 4.2.4 (i) ci-dessous.

4.2.4 Proposition. (i) *Tout anneau factoriel est intégralement clos.*

(ii) (« transitivité de la fermeture intégrale ») *Soient $A \to B \to C$ des morphismes d'anneaux. Soient A_1 la fermeture intégrale de A dans B, et A_2 la fermeture intégrale de A_1 dans C. Alors A_2 est la fermeture intégrale de A dans C.*

(iii) *Soient K un corps et A un sous-anneau de K. La fermeture intégrale de A dans K est un anneau intégralement clos.*

(iv) *Soient K un corps et A un sous-anneau de K. Pour que A soit intégralement clos, il faut et il suffit que la propriété suivante soit satisfaite : « tout élément de K entier sur A et quotient de deux éléments de A appartient à A ».*

Preuve. (i) Exercice : répéter l'argument donné pour $\mathbb{Z}$ en 4.1.3.

(ii) Soit A_2' la fermeture intégrale de A dans C. Alors A_2' est entier sur A, et *a fortiori* sur A_1, donc $A_2' \subset A_2$. Réciproquement, A_2 est entier sur A_1 qui est entier sur A. Donc A_2 est entier sur A d'après 4.2.1, d'où $A_2 \subset A_2'$.

(iii) Soit A' la fermeture intégrale de A dans K. Il est clair que A' est intègre (comme sous-anneau de K). Son corps des fractions F s'identifie à un sous-corps de K, donc la clôture intégrale A'' de A' peut être vue comme un sous-anneau de K (la fermeture intégrale de A' dans F). Par construction, A'' est entier sur A', donc sur A d'après 4.2.1 ; comme c'est un sous-anneau de K il est contenu dans A', donc lui est égal.

(iv) Il suffit de remarquer que le sous-ensemble de K formé des quotients a/b avec $a \in A$ et $b \in A^*$ s'identifie canoniquement au corps des fractions de A. □

4.3 Le cas des corps quadratiques.

Commençons par quelques rappels sur les extensions quadratiques (c'est-à-dire de degré 2) d'un corps. Si K est un corps et L une extension quadratique de K, alors L est engendrée par n'importe quel élément $x \in L \setminus K$, de sorte que $L \cong K[X]/(P)$ où $P \in K[X]$ est unitaire de degré 2 et irréductible (ce qui, en degré 2, équivaut à « sans racine dans K »). Inversement, tout polynôme P de ce type définit une extension quadratique de K.

Un cas particulier important est celui d'un polynôme de la forme $X^2 - d$, où $d \in K$ n'est pas un carré ; l'extension correspondante sera alors notée

$$K(\sqrt{d}) := K[X]/(X^2 - d)$$

et la classe de X dans cette extension sera notée $\sqrt{d}$. Supposons K de caractéristique différente de 2, et soit $P = X^2 + bX + c \in K[X]$. Le calcul habituel montre alors que :

$$P \text{ a une racine dans } K \Leftrightarrow \Delta := b^2 - 4c \text{ est un carré dans } K$$

(lecteur, où utilise-t-on l'hypothèse sur la caractéristique ?). En particulier, si P est irréductible, alors Δ n'est pas un carré dans K, et en est un dans $L = K[X]/(P)$ (où P a une racine) ; explicitement, $\Delta = (2x + b)^2$ où x est la classe de X. On en déduit que $L \cong K(\sqrt{\Delta})$.

Pour $d \in K$ non carré et $r \in K^*$, il est immédiat que $K(\sqrt{d}) \cong K(\sqrt{r^2\, d})$ (il y a en fait deux isomorphismes, envoyant $\sqrt{d}$ sur $\pm r^{-1}\sqrt{r^2\, d}$). Inversement, soient d et d' dans K, non carrés, tels que $K(\sqrt{d}) \cong K(\sqrt{d'})$. Alors d' est un carré dans $K(\sqrt{d})$: on a $d' = (u + v\sqrt{d})^2$ avec u et v dans K, ce qui donne immédiatement en développant que l'on a soit $v = 0$ et $d' = u^2$ (exclu puisque d' n'est pas un carré), soit $u = 0$ et $d' = d\, v^2$.

Nous avons donc établi :

4.3.1 Théorème. *Soit K un corps de caractéristique différente de 2.*
(1) *Toute extension quadratique L de K est isomorphe à $K(\sqrt{d})$, pour un élément $d \in K$ qui n'est pas un carré.*
(2) *Les extensions $K(\sqrt{d})$ et $K(\sqrt{d'})$ de K sont isomorphes si et seulement si d' est de la forme $r^2\,d$, pour un $r \in K^*$.*
(3) *Pour $d \in K$ non carré, les automorphismes de $K(\sqrt{d})$ sont l'identité et la « conjugaison » envoyant $\sqrt{d}$ sur $-\sqrt{d}$.* □

Passons maintenant au cas où $K = \mathbb{Q}$. Il faut d'abord s'attarder un peu sur les notations. Si d est un rationnel qui n'est pas un carré, alors l'équation $X^2 = d$ admet deux racines (opposées) dans $\mathbb{C}$, qui sont réelles si $d > 0$. Le malheur est que, dans ce dernier cas, il est d'usage de désigner la racine *positive* de cette équation par le symbole $\sqrt{d}$, de sorte que le sous-corps de $\mathbb{R}$ engendré par cette racine se note également $\mathbb{Q}(\sqrt{d})$. Il se trouve d'ailleurs que ce sous-corps (notons-le provisoirement $\mathbb{Q}(\sqrt{d})'$) est également engendré par l'autre racine, puisque celle-ci est $-\sqrt{d}$. C'est donc en fait l'unique sous-corps de $\mathbb{C}$ isomorphe à $\mathbb{Q}[X]/(X^2 - d)$. Il n'est donc pas trop gênant de le noter encore $\mathbb{Q}(\sqrt{d})$. Mais si l'on a besoin de fixer un isomorphisme de $\mathbb{Q}(\sqrt{d})$ avec $\mathbb{Q}(\sqrt{d})'$ il faut préciser lequel, c'est-à-dire choisir une racine dans $\mathbb{C}$ de l'équation $X^2 = d$.

Si $d < 0$, on désignera encore par $\mathbb{Q}(\sqrt{d})$ le sous-corps de $\mathbb{C}$ engendré par l'un quelconque des deux nombres complexes $\pm i\sqrt{-d}$. Par contre le symbole $\sqrt{d}$ n'a, rappelons-le, pas de sens dans $\mathbb{C}$ (alors qu'il en a un dans le corps $\mathbb{Q}[X]/(X^2 - d)$).

Nous dirons qu'un entier d est *sans facteur carré* s'il (est non nul et) n'est pas divisible par le carré d'un entier > 1. Il revient au même (exercice) de dire que d est, au signe près, produit d'une famille finie (éventuellement vide) de nombres premiers distincts. On en déduit (exercice encore !) le lemme suivant :

4.3.2 Lemme. *Tout rationnel non nul x s'écrit de façon unique sous la forme*

$$x = r^2\,d$$

où r est un rationnel positif et d un entier sans facteur carré. □

Noter aussi qu'un entier sans facteur carré *et différent de* 1 n'est jamais un carré dans $\mathbb{Z}$ (ni, ce qui revient au même, dans $\mathbb{Q}$).

4.3.3 Théorème. *Soit K une extension quadratique de $\mathbb{Q}$* (ou « corps quadratique »). *Il existe un* unique *entier $d \neq 1$ sans facteur carré tel que $K \cong \mathbb{Q}(\sqrt{d})$.*

Pour $d \neq 1$ sans facteur carré, l'anneau des entiers de $\mathbb{Q}(\sqrt{d})$ est donné par :

$$\mathbb{Q}(\sqrt{d})_{\mathbb{Z}} = \begin{cases} \mathbb{Z}[\sqrt{d}\,] & \text{si } d \not\equiv 1 \pmod 4 \\ \mathbb{Z}[(1+\sqrt{d})/2\,] & \text{si } d \equiv 1 \pmod 4. \end{cases}$$

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

Preuve. La première assertion résulte du théorème 4.3.1 et du lemme 4.3.2.

Fixons $d \neq 1$ sans facteur carré. Il est clair que $\sqrt{d}$ est entier sur $\mathbb{Z}$, et si $d \equiv 1 \pmod 4$ il en est de même de $\frac{1+\sqrt{d}}{2}$ qui est racine du polynôme $X^2 - X + \frac{1-d}{4}$. Donc $\mathbb{Q}(\sqrt{d})_{\mathbb{Z}}$ contient l'anneau donné dans l'énoncé.

Inversement, soit $x = a + b\sqrt{d}$ dans $K_{\mathbb{Z}}$ (avec a et b dans $\mathbb{Q}$). Si σ désigne l'automorphisme non trivial de $\mathbb{Q}(\sqrt{d})$, on a $\sigma(x) = a - b\sqrt{d}$ (cf. 4.3.1 (3)). Comme σ est un automorphisme, on a $\sigma(K_{\mathbb{Z}}) = K_{\mathbb{Z}}$ et donc $\sigma(x) \in K_{\mathbb{Z}}$. Donc $x + \sigma(x) = 2a$ et $x\sigma(x) = a^2 - db^2$ sont entiers sur $\mathbb{Z}$; comme ils sont dans $\mathbb{Q}$, ils sont dans $\mathbb{Z}$. En résumé :

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

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 (en réduisant modulo 4) que x est bien de la forme souhaitée (il est utile de noter que $(2a)^2 - d(2b)^2$ est dans $4\mathbb{Z}$) ; les détails sont laissés au lecteur. □

4.3.4 Exemples. L'anneau des entiers de $\mathbb{Q}(\sqrt{2})$ est $\mathbb{Z}[\sqrt{2}]$; celui de $\mathbb{Q}(\sqrt{5})$ est $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$.

L'anneau des entiers de $\mathbb{Q}(i)$ est l'anneau des entiers de Gauss $\mathbb{Z}[i]$. Celui de $\mathbb{Q}(i\sqrt{3})$ est $\mathbb{Z}[\frac{1+i\sqrt{3}}{2}] = \mathbb{Z}[j]$.

5 Norme, trace, polynôme caractéristique.

5.1 Définitions, premières propriétés.

5.1.1 Notations.

Dans ce paragraphe, on désigne par A un anneau, et par B une A-algèbre qui est *libre de rang fini* en tant que A-module ; on note n ce rang.

Pour tout $b \in B$, on a une application A-linéaire

$$\begin{array}{rccc} \mu_b : & B & \longrightarrow & B \\ & y & \longmapsto & by. \end{array}$$

Noter que μ_b est nulle (resp. injective, resp. bijective) si et seulement si b est nul (resp. régulier dans B, resp. inversible dans B).

L'application $b \mapsto \mu_b : B \to \mathrm{End}_{A-\mathrm{mod}}(B)$ est un morphisme injectif de A-algèbres (non commutatives, en ce qui concerne la seconde). En conséquence, si $P \in A[X]$ alors $\mu_{P(b)} = P(\mu_b)$.

5.1.2 Exemple. Soit $f = X^n + a_{n-1}X^{n-1} + \ldots + a_0$ un polynôme *unitaire* à coefficients dans A. Alors la A-algèbre

$$B := A[X]/(f)$$

vérifie la condition ci-dessus ; plus précisément, la division euclidienne par f dans $A[X]$ (qui existe parce que f est unitaire) montre que $(1, x, \ldots, x^{n-1})$ — où l'on note x la classe de X — est une A-base de B.

Dans cette base, l'endomorphisme μ_x de B a pour matrice

$$\begin{pmatrix} 0 & & & & -a_0 \\ 1 & 0 & & & \vdots \\ & 1 & 0 & & \vdots \\ & & \ddots & \ddots & \vdots \\ & & & 1 & -a_{n-1} \end{pmatrix}$$

qui est appelée *matrice compagnon* du polynôme unitaire f.

5.1.3 Définition. Avec les notations de 5.1.1, on appelle *norme* (resp. *trace*, resp. *polynôme caractéristique*) de $b \in B$ (relativement à A) le déterminant (resp. la trace, resp. le polynôme caractéristique) de μ_b.

Si A est un corps, on appelle *polynôme minimal* de b le polynôme minimal (unitaire) de μ_b. (Lecteur : pourquoi cette restriction sur A ?)

La norme et la trace de b se notent respectivement $\mathrm{N}_{B/A}(b)$ et $\mathrm{Tr}_{B/A}(b)$.

Le polynôme caractéristique de b sera noté ici $\mathrm{Pcar}_{B/A}(b)$ (resp. $\mathrm{Pmin}_{B/A}(b)$; il n'y a pas de notation standard pour ces notions).

(On écrira aussi simplement $\mathrm{N}(b)$, $\mathrm{Tr}(b)$, etc., si aucune confusion n'en résulte).

5.1.4 Propriétés élémentaires.

(i) La norme et la trace sont des éléments de A ; le polynôme caractéristique (et, le cas échéant, le polynôme minimal) sont des polynômes unitaires à coefficients dans A ; le polynôme caractéristique est de degré n (le rang de B comme A-module) ; si l'on écrit

$$\mathrm{Pcar}(b) = X^n + a_{n-1}\,X^{n-1} + \ldots + a_0 \quad (a_i \in A),$$

alors le terme constant $a_0 = \mathrm{Pcar}(b)(0)$ est $(-1)^n\,\mathrm{N}(b)$, et le coefficient « sous-dominant » a_{n-1} est $-\mathrm{Tr}(b)$.

(ii) Le théorème de Cayley-Hamilton implique que b est un zéro de $\mathrm{Pcar}(b)$. Ceci implique notamment que b *divise* $\mathrm{N}(b)$ dans B, puisque $b^n + a_{n-1}\,b^{n-1} + \ldots + a_1\,b = (-1)^{n+1}\,\mathrm{N}(b)$.

(iii) L'application $b \mapsto \mathrm{Tr}(b) : B \to A$ est A-linéaire, et l'on a $\mathrm{Tr}(a) = na$ pour $a \in A$.

(iv) L'application $b \mapsto \mathrm{N}(b) : B \to A$ est multiplicative et l'on a $\mathrm{N}(a) = a^n$ pour $a \in A$.

(v) Un élément b de B est inversible si et seulement si $\mathrm{N}(b) \in A^\times$.

(vi) Supposons que B est l'algèbre *produit* $B_1 \times B_2$, où B_1 et B_2 sont libres de rangs respectifs n_1 et n_2. Alors, pour $b = (b_1, b_2) \in B$, on a

$$\mathrm{Pcar}_{B/A}(b) = \mathrm{Pcar}_{B_1/A}(b_1)\,\mathrm{Pcar}_{B_2/A}(b_2)$$

comme on le voit en choisissant des bases $\mathcal{B}_1$ et $\mathcal{B}_2$ de B_1 et B_2 et en munissant B de la base « juxtaposée » évidente. On en déduit notamment les formules

$$\mathrm{N}_{B/A}(b) = \mathrm{N}_{B_1/A}(b_1)\,\mathrm{N}_{B_2/A}(b_2), \quad \mathrm{Tr}_{B/A}(b) = \mathrm{Tr}_{B_1/A}(b_1) + \mathrm{Tr}_{B_2/A}(b_2).$$

Lorsque A est un corps, on constate par la même méthode que $\mathrm{Pmin}_{B/A}(b)$ est le ppcm (dans $A[X]$) des polynômes minimaux de b_1 et b_2.

(vii) Dans le cas d'une extension finie de corps, remarquer que pour $P \in A[X]$ on a $P(b) = 0$ si et seulement si $P(\mu_b) = 0$, de sorte que $\mathrm{Pmin}(b)$ est caractérisé par les deux propriétés suivantes : il est unitaire et, pour tout $P \in A[X]$, on a l'équivalence :

$$P(b) = 0 \Leftrightarrow \mathrm{Pmin}(b) \text{ divise } P$$

ce qui est la définition habituelle du polynôme minimal d'un élément algébrique. En particulier, $\mathrm{Pmin}(b)$ divise $\mathrm{Pcar}(b)$ dans $A[X]$.

5.1.5 Exemples. Calculer le polynôme caractéristique (et le cas échéant le polynôme minimal) de b :

- lorsque $A = \mathbb{R}$, $B = \mathbb{C}$, b quelconque ;
- lorsque $A = \mathbb{Z}$, $B = \mathbb{Z}[i]$, b quelconque ;
- lorsque $A = \mathbb{Z}$, $B = \mathbb{Z}[j]$, b quelconque ;
- lorsque $A = \mathbb{Q}$, $B = \mathbb{Q}(\sqrt[4]{3})$, $b = \sqrt[4]{3}$ (resp. $b = \sqrt{3}$).

5.1.6 Exemple. Reprenons l'exemple 5.1.2. Par définition de B, les polynômes de $A[X]$ annulant x sont les multiples de f. En particulier, f divise $\mathrm{Pcar}(x)$; comme ces deux polynômes sont unitaires de même degré, ils sont égaux :

$$\mathrm{Pcar}_{B/A}(x) = f.$$

(On peut voir aussi directement, par récurrence sur n, que f est le polynôme caractéristique de sa matrice compagnon ; c'est un bon exercice de développement de déterminants).

On a en particulier $\mathrm{Tr}_{B/A}(x) = -a_{n-1}$ (d'ailleurs, c'est trivial sur la matrice) et $\mathrm{N}_{B/A}(x) = (-1)^n a_0$.

Par exemple, x est inversible dans B si et seulement si a_0 est inversible dans A. *Exercice* : retrouver ce fait de manière élémentaire, sans utiliser de déterminants.

Enfin, si A est un corps, la remarque du début montre que f est aussi le polynôme minimal de x.

Voyons maintenant comment change le polynôme caractéristique de b lorsque l'on change B :

5.1.7 Proposition. *Soit C une B-algèbre qui est libre de rang fini m comme B-module, et soit b un élément de B. Alors :*

(i) *C est un A-module libre de rang mn ;*
(ii) $\mathrm{Pcar}_{C/A}(b) = \mathrm{Pcar}_{B/A}(b)^m$;
(iii) $\mathrm{N}_{C/A}(b) = \mathrm{N}_{B/A}(b)^m$;
(iv) $\mathrm{Tr}_{C/A}(b) = m\,\mathrm{Tr}_{B/A}(b)$;
(v) *si A est un corps et si $C \neq \{0\}$, alors* $\mathrm{Pmin}_{C/A}(b) = \mathrm{Pmin}_{B/A}(b)$.

Preuve. Soient $\mathcal{B} = (e_1, \ldots, e_n)$ une base de B comme A-module, et $\mathcal{B}' = (h_1, \ldots, h_m)$ une base de C comme B-module. Alors on vérifie facilement que $\mathcal{B}'' = (e_i h_j)_{1 \leq i \leq n, 1 \leq j \leq m}$ est une A-base de C (d'où (i)), et que si M est la matrice de $\mu_b : B \to B$ dans la base $\mathcal{B}$, alors la matrice de $\mu_b : C \to C$ dans la base $\mathcal{B}''$ est la matrice diagonale par blocs $\mathrm{diag}(M, \ldots, M)$ (avec m blocs diagonaux). Les assertions (ii) à (iv) en résultent, et (v) est triviale sur la définition (lecteur : que se passe-t-il si $C = \{0\}$?). □

Enfin voici un autre exemple amusant de calcul de polynôme caractéristique :

5.1.8 Proposition. *On reprend les hypothèses et notations de l'exemple* 5.1.2*, et l'on suppose en outre que le polynôme $f \in A[X]$ est* scindé*, c'est-à-dire de la forme*

$$f = \prod_{i=1}^{n} (X - \lambda_i)$$

où les λ_i sont dans A.

Soit $b \in B$ quelconque, classe d'un polynôme $h \in A[X]$: on a donc $b = h(x)$. On a alors les formules :

(i) $\mathrm{Pcar}(h(x)) = \prod_{i=1}^{n}(X - h(\lambda_i))$;
(ii) $\mathrm{N}(h(x)) = \prod_{i=1}^{n} h(\lambda_i)$;
(iii) $\mathrm{Tr}(h(x)) = \sum_{i=1}^{n} h(\lambda_i)$.

Preuve. Il suffit de montrer la première formule, qui entraîne immmédiatement les deux autres. Considérons dans B les éléments :

$$e_0 = 1,\ e_1 = x - \lambda_1,\ e_2 = (x - \lambda_1)(x - \lambda_2), \ldots, e_{n-1=} = (x - \lambda_1)\ldots(x - \lambda_{n-1}).$$

Comme $e_i = x^i +$ (combinaison linéaire de $1, x, \ldots, x^{i-1}$), et que les x^i $(0 \leq i \leq n-1)$ forment une base de B, on voit que $(e_i)_{0\leq i\leq n-1}$ est une base de B. La relation évidente $e_{i+1} = (x - \lambda_{i+1})\, e_i$ donne

$$x\, e_i = \lambda_{i+1}\, e_i + e_{i+1}$$

de sorte que la matrice de x dans la base en question est

$$M = \begin{pmatrix} \lambda_1 & & & \\ 1 & \lambda_2 & & \\ & \ddots & \ddots & \\ & & 1 & \lambda_n \end{pmatrix}.$$

Par suite la matrice de $h(x)$ est $h(M)$, qui est triangulaire inférieure, avec comme éléments diagonaux $h(\lambda_1), \ldots, h(\lambda_n)$. La formule en résulte. □

5.2 La « forme trace ».

On garde les notations de 5.1.1. De la forme linéaire $\mathrm{Tr}_{B/A} : B \to A$ on déduit une forme A-bilinéaire symétrique

$$\begin{array}{rccc} \tau_{B/A} : & B \times B & \longrightarrow & A \\ & (x, y) & \longmapsto & \mathrm{Tr}_{B/A}(xy) \end{array}$$

appelée *forme trace* de B relativement à A. Le résultat suivant, bien que peu évocateur en apparence, est d'une importance cruciale pour la structure des anneaux d'entiers algébriques :

5.2.1 Proposition. *Soit L/K une extension finie de corps de caractéristique nulle. Alors la forme trace*

$$\tau_{L/K} :\ L \times L \longrightarrow K$$

est non dégénérée *(comme forme bilinéaire sur le K-espace vectoriel L).*

Preuve. Soit x un élément du noyau de $\tau_{L/K}$: on a donc, par définition, $\mathrm{Tr}_{L/K}(xy) = 0$ pour tout $y \in L$. Si x n'était pas nul, on aurait notamment $\mathrm{Tr}_{L/K}(xx^{-1}) = 0$: contradiction car $\mathrm{Tr}_{L/K}(1) = [L : K]\, 1 \neq 0$ puisque $\mathrm{car}(K) = 0$. □

5.2.2 Remarques. Soit L/K une extension finie quelconque.

(i) On voit dans la démonstration ci-dessus que la non-dégénérescence de la forme trace équivaut à la propriété que la forme linéaire $\mathrm{Tr}_{L/K}$ soit non nulle.

(ii) L'argument se généralise immédiatement au cas où $[L : K]$ n'est pas divisible par la caractéristique de K.

(iii) De façon générale, on peut montrer que $\tau_{L/K}$ est non dégénérée si et seulement si l'extension L/K est *séparable*.

5.3 Le polynôme caractéristique dans une extension de corps.

5.3.1 Rappels sur les plongements.

Rappelons d'abord que si A est un anneau, si $f \in A[X]$ et si B est une A-algèbre, la donnée d'un morphisme de A-algèbres $\varphi : A[X]/(f) \to B$ équivaut à celle d'un « zéro de f dans B », c'est-à-dire d'un élément b tel que $f(b) = 0$. La correspondance est donnée, dans un sens, par $\varphi \mapsto \varphi(x)$ (avec $x =$ classe de X) ; dans l'autre sens, on associe $b \in B$, zéro de f, l'unique morphisme φ envoyant la classe d'un polynôme P sur $P(b)$.

Soient maintenant K un corps *de caractéristique nulle*, L une extension finie de K, de degré $[L : K] =: d$, et Ω une extension *algébriquement close* de K. On sait alors qu'il existe exactement d K-morphismes ou « K-plongements » $L \to \Omega$ (ils sont automatiquement injectifs, comme morphismes de corps). En outre, si M est une extension finie de L, de degré $[M : L] =: e$, alors chaque K-plongement $L \to \Omega$ admet exactement e prolongements à M ; on obtient ainsi les ed K-plongements de M dans Ω (remarquer que $[M : K] = ed$).

5.3.2 Proposition. *Soient K un corps* de caractéristique nulle, *L une extension finie de K, de degré n, et Ω une extension algébriquement close de K.*

Soit x un élément de L, et soit $f = \mathrm{Pmin}(x) \in K[X]$ son polynôme minimal sur K. On considère la suite d'extensions

$$K \hookrightarrow K(x) \hookrightarrow L$$

et l'on pose $d = [K(x) : K] = \deg f$ et $e = [L : K(x)]$ (de sorte que $n = ed$).

On note $x_1, \ldots, x_d$ les d racines de f dans Ω (qui sont deux à deux distinctes, car f est irréductible et K de caractéristique nulle). *On note $\varphi_1, \ldots, \varphi_n$ les K-plongements de L dans Ω. Alors :*

(i) $f(X) = \prod_{i=1}^{d}(X - x_i)$;

(ii) $\mathrm{Pcar}_{K(x)/K}(x) = f$;

(iii) $\mathrm{Pcar}_{L/K}(x) = f^e = \prod_{j=1}^{n}(X - \varphi_j(x))$.

Preuve. L'assertion (i) résulte simplement du fait que f est unitaire à racines distinctes. Montrons (ii) : on a un isomorphisme de K-algèbres

$$K[X]/(f) \xrightarrow{\sim} K(x)$$

envoyant la classe de X sur x, de sorte que $\mathrm{Pcar}_{K(x)/K}(x)$ est le polynôme caractéristique de la classe de X dans $K[X]/(f)$, lequel est bien f comme on l'a vu dans 5.1.6.

Pour (iii), le fait que $\mathrm{Pcar}_{L/K}(x) = f^e$ résulte de (ii) et de 5.1.7 (ii). De plus, il résulte des rappels 5.3.1 que les $\varphi_j(x)$ sont les x_i répétés e fois, d'où la dernière égalité. □

5.3.3 Remarques. On voit ainsi que dans le cas d'une extension finie de corps (de caractéristique nulle), *le polynôme caractéristique d'un élément est une puissance de son polynôme minimal*. Ce n'est pas vrai dans une K-algèbre plus générale : ainsi, dans la $\mathbb{R}$-algèbre produit $\mathbb{R}^3$, l'élément $(0,1,1)$ a pour polynôme minimal $X(X-1)$ et pour polynôme caractéristique $X(X-1)^2$.

Le cas le plus important (et le plus simple à retenir) est celui où $L = K(x)$: on a alors $\mathrm{Pcar}(x) = \mathrm{Pmin}(x) = \prod_{i=1}^{d}(X - x_i)$.

La proposition montre aussi que les *valeurs propres* de μ_x dans Ω sont les x_i.

Nous allons maintenant essayer de caractériser, à l'aide de leur polynôme minimal, les éléments de L *entiers* sur un sous-anneau de K.

5.3.4 Proposition. *On garde les notations et hypothèses de* 5.3.2.

(1) *Soit A un sous-anneau de K tel que $f \in A[X]$. Alors :*

(i) *x est entier sur A ;*

(ii) *on a un unique isomorphisme de A-algèbres*

$$A[X]/(f) \xrightarrow{\sim} A[x]$$

envoyant la classe de X sur x ;

(iii) *$(1, x, \ldots, x^{d-1})$ est une base du A-module $A[x]$ (qui est donc libre de rang d) ;*

(iv) *pour tout $z \in A[x]$, on a $\mathrm{Pcar}_{A[x]/A}(z) = \mathrm{Pcar}_{K(x)/K}(z)$.*

(2) (réciproque partielle) *Soit A un sous-anneau de K, ayant K pour corps des fractions, et supposé en outre* intégralement clos. *Si x est entier sur A, alors $f \in A[X]$. En outre, $\mathrm{Pcar}_{L/K}(x) \in A[X]$; en particulier $\mathrm{N}_{L/K}(x)$ et $\mathrm{Tr}_{L/K}(x)$ appartiennent à A.*

Preuve. (1) L'assertion (i) est évidente puisque x est annulé par f (unitaire, à coefficients dans A). Pour (ii), considérons le morphisme de A-algèbres $\varphi : A[X] \to L$ donné par $P \mapsto P(x)$. Il est clair que l'image de φ est $A[x]$, et que son noyau contient l'idéal (f). Inversement, soit $P \in \ker\varphi$: par division euclidienne dans $A[X]$ (rappelons que f est unitaire) on peut écrire $P = fQ + R$ avec Q et R dans $A[X]$ et $\deg R < d$. Comme $P(x) = f(x) = 0$, on a donc $R(x) = 0$, donc f divise R dans $K[X]$. Comme $\deg R < d$ ce n'est possible que si $R = 0$, donc f divise P dans $A[X]$.

(iii) est une conséquence immédiate de (ii). Montrons (iv) (qui d'ailleurs n'a de sens qu'une fois (iii) démontré, pourquoi ?). On sait maintenant que $\mathcal{B} := (1, x, \ldots, x^{d-1})$ est à la fois une A-base de $A[x]$ et une K-base de $K(x)$; si M est la matrice de la multiplication par z dans $A[x]$, relativement à la A-base $\mathcal{B}$, alors M est aussi la matrice de la multiplication par z dans $K(x)$, relativement à la K-base $\mathcal{B}$ de $K(x)$. L'assertion en résulte.

(2) Si x est entier sur A, il en est de même des x_i qui sont les images de x par les plongements de L dans Ω (c'est un cas particulier de 4.1.2 (3)). Comme $f(X) = \prod_{i=1}^{d}(X - x_i)$ (5.3.2 (i)), il en résulte que les coefficients de f sont eux-mêmes entiers sur A. Comme ils sont dans K, qui est le corps des fractions de A, et que A est intégralement clos, ces coefficients sont bien dans A. Donc $f \in A[X]$, et il s'ensuit évidemment que $f^e = \mathrm{Pcar}_{L/K}(x) \in A[X]$. □

5.3.5 Remarque. On observera que dans le cas particulier des corps quadratiques, le raisonnement fait en (2) ci-dessus est exactement le début de la preuve de 4.3.3.

Résumons, dans le cas particulier où $A = \mathbb{Z}$ et $K = \mathbb{Q}$:

5.3.6 Corollaire. *Soit L un corps de nombres et x un élément de L. Alors $x \in L_{\mathbb{Z}}$ si et seulement si le polynôme minimal de x sur $\mathbb{Q}$ est à coefficients entiers.*

De plus, dans ce cas, $\mathrm{Pcar}_{L/\mathbb{Q}}(x) \in \mathbb{Z}[X]$, et $\mathrm{N}_{L/\mathbb{Q}}(x)$ et $\mathrm{Tr}_{L/\mathbb{Q}}(x)$ sont des entiers, et l'anneau $\mathbb{Z}[x]$ est canoniquement isomorphe à $\mathbb{Z}[X]/(\mathrm{Pmin}_{L/\mathbb{Q}}(x))$. □

5.3.7 Remarque. Nous avons grâce à 5.3.6 un critère commode pour montrer qu'un nombre donné n'est *pas* un entier algébrique. Par exemple, $\sqrt[3]{2}/3$ n'en est pas un, puisque son polynôme minimal $X^3 - \frac{2}{27}$ n'est pas à coefficients entiers.

5.4 Application : structure des anneaux d'entiers de corps de nombres.

5.4.1 Théorème. *Soit K une extension finie de $\mathbb{Q}$. Alors :*

(i) *$K_{\mathbb{Z}}$ est libre de rang $[K : \mathbb{Q}]$ en tant que $\mathbb{Z}$-module ;*

(ii) *toute $\mathbb{Z}$-base de $K_{\mathbb{Z}}$ est une $\mathbb{Q}$-base de K ;*

(iii) *pour tout $z \in K_Z$, on a $\mathrm{Pcar}_{K_{\mathbb{Z}}/\mathbb{Z}}(z) = \mathrm{Pcar}_{K/\mathbb{Q}}(z)$* (et par suite $\mathrm{Tr}_{K_{\mathbb{Z}}/\mathbb{Z}}(z) = \mathrm{Tr}_{K/\mathbb{Q}}(z)$ et $\mathrm{N}_{K_{\mathbb{Z}}/\mathbb{Z}}(z) = \mathrm{N}_{K/\mathbb{Q}}(z)$).

Commençons par une remarque facile :

5.4.2 Proposition. *Soit $\mathbb{Q} \to K$ une extension finie. Alors $K_{\mathbb{Z}}$ engendre K comme $\mathbb{Q}$-espace vectoriel.*

En d'autres termes, $K_{\mathbb{Z}}$ contient une $\mathbb{Q}$-base de K, ou encore : $K_{\mathbb{Z}}$ contient un $\mathbb{Z}$-module libre de rang $[K : \mathbb{Q}]$.

Preuve. Il suffit de remarquer que pour tout $x \in K$, il existe un entier $m > 0$ tel que $mx \in K_{\mathbb{Z}}$ (prendre un polynôme annulateur de x à coefficients entiers, et prendre pour m le coefficient dominant). Si $\mathcal{B}$ est une $\mathbb{Q}$-base quelconque de K, il existe donc $m' > 0$ tel que $m'\mathcal{B} \subset K_{\mathbb{Z}}$. □

5.4.3 Remarques. (i) Généralisation (exercice) : si A est un anneau intègre, K son corps des fractions, et L une extension finie de K, le sous-anneau de L formé des entiers sur A contient un A-module libre de rang $[L : K]$.

(ii) Variante de la démonstration : prendre un $x \in K$ tel que $K = \mathbb{Q}[x]$ (on sait que ça existe) ; comme ci-dessus il existe $m > 0$ tel que $mx \in K_{\mathbb{Z}}$. Alors $\mathbb{Z}[x]$ est libre de rang $[K : \mathbb{Q}]$, d'après 5.3.4. On obtient donc un peu mieux : $K_{\mathbb{Z}}$ contient un *sous-anneau* qui est $\mathbb{Z}$-libre de rang $[K : \mathbb{Q}]$.

Preuve de 5.4.1. (i) Posons $n = [K : \mathbb{Q}]$. Soit M un sous-$\mathbb{Z}$-module de $K_{\mathbb{Z}}$ qui est libre de rang n, et soit $M^* = \mathrm{Hom}_{\mathbb{Z}-\mathrm{mod}}(M, \mathbb{Z})$ son dual. Alors M^* est encore $\mathbb{Z}$-libre de rang n, et l'on a une application $\mathbb{Z}$-linéaire

$$\begin{array}{rccc} \delta : & K_{\mathbb{Z}} & \longrightarrow & M^* \\ & x & \longmapsto & (y \mapsto \mathrm{Tr}_{K/\mathbb{Q}}(xy)) \end{array}$$

(remarquer que $xy \in K_{\mathbb{Z}}$, donc $\mathrm{Tr}_{L/K}(xy) \in \mathbb{Z}$ d'après 5.3.4). Montrons que δ est injective : en effet, si $x \in \ker \delta$, alors $\mathrm{Tr}_{L/K}(xy)$ est nul pour tout $y \in M$, donc pour tout $y \in K$ car M engendre K comme $\mathbb{Q}$-espace vectoriel. Donc $x = 0$ d'après la non-dégénérescence de la trace (5.2.1). Ainsi, $K_{\mathbb{Z}}$ est isomorphe à un sous-$\mathbb{Z}$-module d'un module libre de rang n, donc est lui-même libre de rang $\leq n$. Mais d'autre part, comme il contient M, il est de rang $\geq n$, cqfd.

(ii) Toute $\mathbb{Z}$-base de $K_{\mathbb{Z}}$ engendre K comme $\mathbb{Q}$-espace vectoriel d'après 5.4.2, et est donc une $\mathbb{Q}$-base puisque'elle a le bon nombre d'éléments (il est d'ailleurs très facile de voir directement que toute partie $\mathbb{Z}$-libre de K est $\mathbb{Q}$-libre).

(iii) est conséquence immédiate de (ii) (par le même argument que dans 5.3.4 (1) (iv)). □

5.4.4 Corollaire. *Soit K une extension finie de $\mathbb{Q}$, et soit n son degré. Posons $A = K_{\mathbb{Z}}$. Alors :*

(i) *A est un anneau* noethérien *: tout idéal de A est de type fini.*

(ii) *Pour tout $m \in \mathbb{Z}$, le quotient A/mA est isomorphe, comme groupe abélien, à $(\mathbb{Z}/m\mathbb{Z})^n$.*

(iii) *Pour tout $z \in A$ non nul, on a* $\mathrm{Card}\,(A/z\,A) = |\mathrm{N}_{K/\mathbb{Q}}(z)| = |\mathrm{N}_{A/\mathbb{Z}}(z)|$.

(iv) *Pour tout idéal non nul I de A, l'anneau quotient A/I est* fini.

Preuve. (i) Soit I un idéal de A : alors I est un sous-groupe de A, donc un $\mathbb{Z}$-module de type fini, et *a fortiori* un idéal de type fini.

(ii) Comme $A \cong \mathbb{Z}^n$ comme $\mathbb{Z}$-module, on a $A/mA \cong \mathbb{Z}^n/m\mathbb{Z}^n \cong (\mathbb{Z}/m\mathbb{Z})^n$.

(iii) Pour $z \in A$ non nul, la multiplication par z est un endomorphisme injectif u du $\mathbb{Z}$-module A, qui est libre de rang fini ; on a vu en TD qu'alors $A/\mathrm{Im}\,(u)$ est un groupe fini d'ordre $|\det(u)|$. L'assertion en résulte par définition de la norme (on a $\mathrm{N}_{K/\mathbb{Q}}(z) = \mathrm{N}_{A/\mathbb{Z}}(z)$ d'après 5.4.1 (iii)).

(iv) Soit z un élément non nul de I. Alors A/I est un quotient de $A/z\,A$ qui est fini d'après (iii). □

6 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].

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

1. il est intégralement clos (4.2.2) (et en particulier intègre) ;
2. il est *noethérien :* tout idéal de A est de type fini ;
3. tout idéal premier non nul de A est maximal.

6.1.1 Proposition. (i) *Tout anneau principal est de Dedekind.*

(ii) *Si K est un corps de nombres, l'anneau $K_{\mathbb{Z}}$ des entiers de K est un anneau de Dedekind.*

Preuve. (i) Un anneau principal est trivialement noethérien (tout idéal est engendré par un seul élément) ; il est intégralement clos d'après 4.2.4 (i) ; enfin si I est un idéal premier non nul de A il est engendré par un irréductible p, et l'on sait alors que A/pA est un corps (« tout élément de A non divisible par p est inversible modulo p »).

(ii) $K_{\mathbb{Z}}$ est intégralement clos d'après 4.2.4 (iii) ; il est noethérien d'après 5.4.4 (i). Enfin, soit P un idéal premier non nul de A : alors A/P est intègre, et est *fini* d'après 5.4.4 (iv), donc c'est un corps et P est maximal. □

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

6.1.2 Exemple. Soit k un corps, f dans $k[X, Y]$ irréductible, tel que f et ses dérivées partielles 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 classes de Y et $X - 1$ n'admettent pas de pgcd.

6.2 Généralités noethériennes.

Nous suivons [Samuel, III].

6.2.1 Proposition. *Soient A un anneau et M un A-module. Les conditions suivantes sont équivalentes :*

(i) *toute famille non vide de sous-modules de M possède un élément maximal ;*

(ii) *toute suite croissante de sous-modules de M est stationnaire ;*
(iii) *tout sous-module de M est de type fini.*

Preuve. Les implications (i) $\Longrightarrow$ (ii) et (iii) $\Longrightarrow$ (ii) sont claires (remarquer que la *réunion* d'une suite croissante de sous-modules est encore un sous-module).

Montrons l'implication (ii) $\Longrightarrow$ (i), ou plutôt sa contraposée. Soit $(M_i)_{i\in I}$ 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 $M_i \subsetneqq M_{i'}$. Mais alors il existe une suite strictement croissante $M_{i_0} \subsetneqq M_{i_1} \subsetneqq \ldots$, ce qui contredit (ii).

Montrons (i) $\Longrightarrow$ (iii). Supposons (i), et soit N un sous-module de M. Considérons l'ensemble Φ des sous-modules de type fini de N. Alors Φ n'est pas vide (le sous-module nul appartient à Φ), donc Φ admet un élément maximal P. Il suffit de voir que $P = N$. Sinon, soit $x \in N \setminus P$, et soit P' le sous-module engendré par P et x : alors $P \underset{\neq}{\subset} P' \subset N$, et d'autre part P' est de type fini car P l'est. Ceci contredit le caractère maximal de P, donc $P = N$ comme annoncé. □

6.2.2 Remarque. La preuve de (ii) $\Longrightarrow$ (i) ci-dessus (construction de la suite M_{i_k}) utilise l'axiome du choix.

6.2.3 Définition. Soit A un anneau. Un A-module M est dit *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 de A est de type fini.

6.2.4 Exemples. Tout corps est un anneau noethérien, par manque d'idéaux. L'anneau $\mathbb{Z}$ est noethérien, ainsi, comme on l'a vu, que tout anneau principal et que les $K_{\mathbb{Z}}$ pour les extensions finies K de $\mathbb{Q}$. Si A est noethérien, alors $A[X]$ l'est aussi ; voir un livre d'algèbre pour ce résultat fondamental (nous ne l'utiliserons pas). Tout quotient d'un anneau noethérien est noethérien (trivial !).

L'anneau $\mathbb{Z}[X_1, X_2, \ldots]$ de polynômes en un nombre infini de variables n'est pas noethérien. L'anneau des entiers algébriques, c'est-à-dire la fermeture intégrale $\overline{\mathbb{Z}}$ de $\mathbb{Z}$ dans $\overline{\mathbb{Q}}$ (ou, ce qui revient au même, dans $\mathbb{C}$), ne l'est pas non plus (exercice : considérer les suites d'idéaux données respectivement par $I_n = (X_1, \ldots, X_n)$ et par $J_n = \sqrt[2^n]{2}\,\overline{\mathbb{Z}}$).

6.2.5 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.*

De façon équivalente, sans suites exactes : si M est un A-module et M' un sous-module de M, alors M est noethérien si et seulement si M' et $M'' := M/M'$ 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 de type fini. Supposons maintenant que M' et M'' soient 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. □

6.2.6 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.*

6.3 Produits d'idéaux.

6.3.1 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 finies $\sum_i x_i y_i$, avec x_i dans a et y_i dans b.

6.3.2 Remarques. (i) Le produit d'idéaux est associatif et commmutatif, et admet l'idéal A comme élément neutre ; en outre, il est distributif par rapport à la somme d'idéaux.

(ii) On étend immédiatement cette notion au produit $a_1 \ldots a_n$ d'une suite finie (par récurrence sur n, en partant évidemment du cas $n = 0$, où le produit est l'élément neutre A). Comme le produit est associatif et commutatif, on sait donc définir le produit d'une *famille finie* d'idéaux (indexée par un ensemble fini quelconque, pas forcément ordonné).

(iii) On prendra garde qu'il n'y a pas de produit infini d'idéaux, contrairement à ce qui se passe pour la somme.

(iv) Si x est un élément de A, et b un idéal, alors $(xA)b$ est l'idéal xb. En particulier on a $(xA)(yA) = xyA$ pour x et y dans A (rappelons qu'il est faux en général que $xA + yA = (x + y)A$).

(v) Si a et b sont deux idéaux de A, alors $ab \subset a \cap b$; on n'a pas égalité en général (déjà si $a = b$!)

(vi) Si M est un A-module quelconque, et a un idéal de A, on défnit aM comme le sous-module de M engendré par les xm avec $x \in a$ et $m \in M$; le produit d'idéaux est un cas particulier de cette opération.

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

6.3.3 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 ne soit pas dans p ; mais alors $x_1 \cdots x_n$ est dans $a_1 \cdots a_n$, et pas dans p. □

6.3.4 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 contient un produit d'idéaux premiers non nuls.*

Preuve. La preuve est un exemple typique (donc à méditer !) de l'utilisation de l'hypothèse noethérienne. Montrons par exemple le deuxième énoncé. Soit Φ la famille des idéaux non nuls 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. Alors $a \neq A$ (car A contient le produit vide d'idéaux premiers). Ensuite, 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 existe 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. □

6.4 Idéaux fractionnaires.

6.4.1 Définition. Soit A un anneau intègre, et $A \to K$ son corps des 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 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.

6.4.2 Remarques.

On prendra garde qu'en dépit de la terminologie, un idéal fractionnaire *n'est pas* nécessairement un idéal de A.

On peut encore définir les idéaux fractionnaires comme les ensembles de la forme $\frac{1}{d}a$, où $d \in A^*$ et où a est un idéal de A. Noter que $\frac{1}{d}a$ est isomorphe à a comme A-module ; en particulier il est de type fini si A est noethérien.

Réciproquement (et sans hypothèse noethérienne) tout sous-A-module de type fini M de K est un idéal fractionnaire (si $x_1, \ldots, x_n$ engendrent M, considérer un « dénominateur commun » des x_i).

En résumé, si A est un anneau (intègre et) noethérien, les idéaux fractionnaires de A sont simplement les sous-A-modules de type fini de K.

Parmi les idéaux fractionnaires, ceux de la forme xA, pour $x \in K^*$, sont dits *principaux* ; ce sont ceux qui sont libres de rang 1 comme A-modules. Si A est un anneau principal, alors tous les idéaux fractionnaires non nuls sont principaux (et réciproquement).

Le produit d'idéaux fractionnaires a des propriétés analogues à celles de 6.3.2, que nous laissons au lecteur le soin d'énoncer. En particulier, 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) ; le sous-ensemble $I^+(A)$ formé des idéaux non nuls de A en est un sous-monoïde. Nous utiliserons souvent ces notations ; attention à « non nuls » !

Les idéaux fractionnaires principaux forment aussi un sous-monoïde de $I(A)$, qui est isomorphe à $K^times/A^\times$ et est donc un groupe (l'inverse de xA est $x^{-1}A$).

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

Preuve. Soit m un idéal maximal non nul de A. Notons $A \to K$ le corps des 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 élément régulier. Mais alors, d'après 4.1.4, x est entier sur A, et donc dans A, car A est intégralement clos. On a donc $m' = A$.

Montrons alors que « $m' = A$ » est absurde. 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 $Ax \supset p_1 \cdots p_n$ (on peut appliquer 6.3.4, puisque A est noethérien), 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 $Ax \supset mb$ donc $mbx^{-1} \subset A$ donc (par définition de m') $bx^{-1} \subset m'$. Si l'on suppose $m' = A$ (ce que nous voulons exclure, rappelons-le) ceci donne $bx^{-1} \subset A$, c'est-à-dire $b \subset xA$ ou encore $xA \supset p_2 \cdots p_n$ ce qui contredit le choix minimal de n. □

6.4.4 Remarque. La preuve donnée ci-dessus n'est pas très « parlante ». 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 $K_{\mathbb{Z}}$.

6.5 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 ainsi 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 nombres est égal à l'anneau des entiers, sans avoir à refaire les démonstrations des résultats de ces deux sections.

6.5.1 Définition. Un anneau A est un *D-anneau* si :

1. A est intègre ;
2. A est noethérien ;
3. tout idéal premier non nul de A est maximal et inversible dans $I(A)$.

6.5.2 Remarque. Insistons sur le fait que cette définition est « provisoire » et inventée pour les besoins de la présentation ; nous verrons plus loin que les D-anneaux ne sont autres que les anneaux de Dedekind. Le théorème 6.4.3 implique déjà (compte tenu de la définition des anneaux de Dedekind) que *tout anneau de Dedekind est un D-anneau.*

6.5.3 Théorème. *Soit A un D-anneau, et 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. Si A est un corps, alors P est vide et $I(A)$ a un seul élément (à savoir A), donc tout est clair. On supposera donc que A n'est pas un corps, de sorte que P est l'ensemble, non vide, des idéaux maximaux de A.

Commençons par montrer que tout idéal non nul *de* A est produit d'éléments de P (on aura donc *l'existence* de la décomposition pour les idéaux fractionnaires contenus dans A, plus le fait que les exposants sont ≥ 0 pour ceux-là).

Soit Φ l'ensemble des idéaux non nuls de A qui ne sont pas produits 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 élément de P. Donc a est contenu dans un idéal maximal $p \in P$. Soit p' l'inverse de p. Des inclusions $ap \subset a \subset p \subset A$ on déduit (en utilisant que $pp' = A$) que

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

Si l'on avait $a = ap'$, on en déduirait $ap = a$ en remultipliant par p. Or, puisque a est de type fini, le lemme de Nakayama (6.5.4 ci-dessous) implique que a serait annulé par un élément α de $1 + p$. Comme p est un idéal strict, α est non nul donc régulier dans A, donc $a = \{0\}$, contradiction.

Donc l'inclusion $a \subset ap'$ est stricte et en particulier ap' n'est pas dans Φ, donc 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 $b := da \subset A$. Écrivons $dA = q_1 \cdots q_m$ 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 (qui équivaut à dire que P est une partie libre de $I(A)$). 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 (6.3.3), et est donc égal à l'un des q_i, ce qui est une contradiction. □

6.5.4 Proposition. (Lemme de Nakayama) *Soit A un anneau, I un idéal de A, et M un A-module de type fini. Supposons que $IM = M$. Alors il existe un élément α de $1 + I$ tel que $\alpha M = 0$.*

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 I tels que :

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

Alors on voit, comme dans la preuve de la proposition 4.1.4, que M est annulé par $\alpha := \det(\mathrm{Id} - x)$ (où x désigne la matrice $(x_{i,j})$) ; en développant le déterminant (ou en le réduisant modulo I) on constate qu'il est bien dans $1 + I$. □

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.

6.5.5 Théorème. *Soit A un D-anneau, et soit P l'ensemble des idéaux premiers non nuls de A. Soient a et b des idéaux fractionnaires non nuls de A.*

(i) *Pour tout $p \in P$, on a $v_p(ab) = v_p(a) + v_p(b)$, et $v_p(a^{-1}) = -v_p(a)$.*
(ii) *On a $a \subset b$ si et seulement si $v_p(a) \geq v_p(b)$ pourtout $p \in P$.*
(iii) *On a $a \subset A$ si et seulement si $v_p(a) \geq 0$ pour tout $p \in P$.*
(iv) *Pour tout $p \in P$, on a $v_p(a + b) = \min(v_p(a), v_p(b))$.*
(v) *Pour tout $p \in P$, on a $v_p(a \cap b) = \max(v_p(a), v_p(b))$.*

Preuve. L'énoncé (i) résulte directement du théorème précédent. Pour (ii), on note que $a \subset b$ équivaut à $b^{-1}a \subset A$. Donc avec (i), (ii) résulte de (iii). Montrons (iii). 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 (iv). Cela résulte de (ii) et du fait que $a + b$ est le plus petit idéal fractionnaire de A qui contient a et b. L'énoncé (v) correspond au fait que $a \cap b$ est le plus grand idéal fractionnaire de A contenu dans a et b. □

6.6 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.

6.6.1 Définition. Soient A un D-anneau, 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 :

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

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

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

Preuve. La première égalité résulte directement de ce que $Axy = AxAy$. Montrons (ii). Si $x = 0$, ou $y = 0$, ou $x + y = 0$, c'est clair. Supposons donc les trois non nuls : on a alors par définition $v_p(x + y) = v_p((x + y)A)$. Mais on a $(x + y)A \subset xA + yA$, donc

$$v_p(x + y) = v_p((x + y)A) \geq v_p(xA + yA) = \min(v_p(xA), v_p(yA))$$

en appliquant les assertions (ii) et (iv) de 6.5.5, d'où la conclusion. □

6.6.3 Proposition. *Soient A un D-anneau, K son corps des fractions, et P l'ensemble de ses idéaux premiers non nuls. Soient 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 6.5.5. □

Nous pouvons maintenant démontrer le résultat annoncé plus haut (et « oublier » dorénavant les D-anneaux) :

6.6.4 Corollaire. *Les D-anneaux sont les anneaux de Dedekind.*

Preuve. Il suffit de voir que tout D-anneau A est un anneau de Dedekind ; vu les définitions, la seule chose à montrer est que A est intégralement clos. Notons donc K le corps des fractions de A ; soit x dans K, et supposons que x soit entier sur A. Il existe $n \geq 1$ et des a_i dans A tel que :

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

D'après 6.6.3, 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 $-x^n = a_{n-1}x^{n-1} + \cdots + a_0$. □

6.7 Groupe des unités et groupe des classes d'idéaux.

Soient A un anneau de Dedekind, K son corps de fractions, et P l'ensemble de ses idéaux premiers non nuls. Rappelons 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 aussi que nous avons défini des valuations $v_p \colon K^\times \to \mathbb{Z}$, par $v_p(x) = v_p(Ax)$.

Un idéal fractionnaire non nul a de A est dit *principal* s'il existe x dans K tel que $a = Kx$ (en d'autres termes, si a est libre de rang 1 comme A-module). Nous avons un morphisme de groupes :

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

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

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

Une façon d'interpréter cette suite exacte est de dire que les seules obstructions contre ce que v soit un isomorphisme sont $A^\times$ 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 $K^\times$ avec $v(x) = m$, alors $v^{-1}\{m\} = A^\times x$.

Une autre raison d'être de $C(A)$ est la proposition suivante.

6.7.1 Proposition. *Soit A un anneau de Dedekind. Les conditions suivantes sont équivalentes :*

(i) *le groupe $C(A)$ est trivial ;*
(ii) *A est principal ;*
(iii) *A est factoriel ;*
(iv) *tout idéal premier non nul de A est principal.*

Preuve. (i)⇒(ii) est immédiat : si $C(A)$ est trivial, tout idéal fractionnaire non nul (donc en particulier tout idéal non nul de A) est principal.

(ii)⇒(iii) est bien connu (et est plus facile à montrer pour les anneaux noethériens que dans le cas général).

(iii)⇒(iv) : supposons A factoriel, et soit donc $p \subset A$ premier non nul. Prenons un $x \neq 0$ quelconque dans p, et décomposons x en irréductibles dans A : on a $x = up_1 \cdots p_n$, avec u dans $A^\times$, $n \geq 0$ et les p_i irréductibles. En particulier les idéaux Ap_i sont premiers (« lemme d'Euclide ») et donc $Ax = (Ap_1) \cdots (Ap_n)$ est une décomposition de Ax en produit d'idéaux premiers. Mais comme $x \in p$, on a $v_p(x) > 0$ et p figure donc parmi les Ap_i et est en particulier principal.

(iv)⇒(i) : immédiat puisque $I(A)$ (donc a fortiori $C(A)$) est engendré par les (classes d')idéaux premiers non nuls. □

Dans la résolution de systèmes d'équations polynomiales, les groupes $C(A)$ et $A^\times$ sont des groupes qui compliquent les calculs : par exemple, on a vu dans le cas de l'équation de Fermat en degré 3 l'importance du fait que $\mathbb{Z}[j]$ est principal, et les complications provenant des inversibles de $\mathbb{Z}[j]$. Pour cette raison, il est important de comprendre ces groupes, dans le cas des anneaux d'entiers des corps de nombres. Si K est un corps de nombres, nous montrerons que $C(K_\mathbb{Z})$ est fini, et que $K_\mathbb{Z}^\times$ 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. Ce sont les deux résultats principaux de ce cours.

6.8 Une caractérisation des anneaux de Dedekind.

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 à l'anneau des entiers. Voilà pourquoi on considère le résultat suivant.

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

(i) *A est de Dedekind ;*

(ii) *pour tout idéal premier non nul m de A, le A/m-espace vectoriel m/m^2 est de dimension ≤ 1 (de façon équivalente, il existe $x \in m$ tel que $m = m^2 + Ax$) ;*

(iii) *pour tout idéal premier non nul m de A, on a $\dim_{A/m}(m/m^2) = 1$.*

Preuve. (i)⇒(ii) : le Théorème 6.5.5, partie (2), montre que les seuls sous-A-modules de m qui contiennent m^2 sont m et m^2. En d'autres termes, m/m^2 n'a pas d'autre sous-espace que lui-même et $\{0\}$; il est donc de dimension 0 ou 1.

(ii)⇒(iii) : le lemme de Nakayama montre que $m \neq m^2$, donc $m/m^2 \neq \{0\}$, et (iii) implique donc qu'il est bien de dimension 1.

(iii)⇒(i) (le gros morceau) : supposant (iii), il suffit de voir, d'après 6.6.4, que A est un D-anneau. Notons K le corps de fractions de A, et soit m un idéal premier non nul de A ; montrons que m est inversible dans $I(A)$.

Comme dans la preuve de 6.4.3, le candidat inverse pour m est

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

Toujours par les mêmes raisonnements, on voit que m' est un idéal fractionnaire de A, et que l'on a $m \subset m'm \subset A \subset m'$. Il s'agit de montrer que $m'm = A$; si ce n'est pas le cas, on a $m'm = m$, et il nous suffit donc de montrer que *$m'm$ contient un élément qui n'est pas dans m.*

Soit t dans m et non dans m^2 (noter que $m \neq m^2$ par l'hypothèse (iii), ou encore par Nakayama). Alors la classe de t engendre m/m^2 vu l'hypothèse (iii), de sorte que

$$m = tA + m^2 = tA + (tA + m^2)^2 \subset tA + m^4$$

et en itérant ce calcul on voit que

$$(*) \qquad m = tA + m^N \text{ pour tout entier } N > 0$$

ce qui servira plus loin.

Par le lemme 6.3.4 il existe un entier $r \geq 1$, des idéaux maximaux distincts $m = m_1$, $m_2 \ldots, m_r$ de A, et des entiers $n_1, \ldots, n_r$, tels que :

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

Posons $J = m_2^{n_2} \cdots m_r^{n_r}$ et $n = n_1$, de sorte que

$$(**) \qquad At \supset m^n J.$$

Comme les m_i sont maximaux, on a $m_i + m_j = A$ si $i \neq j$. En prenant des produits, on en déduit que $m^n + J = A$. Il existe donc u dans A tel que

$$\begin{cases} u \in J \\ u \equiv 1 \pmod{m^n}. \end{cases}$$

Nous allons montrer que u « est l'élément cherché », c'est-à-dire :

- $u \in m'm$;
- $u \notin m$.

La seconde condition est évidente puisque $u \equiv 1 \pmod{m^n}$ et $n > 0$. Pour la première il suffit de voir que $u \in tm'$, ou encore que $t^{-1}u \in m'$. Vu la définition de m', c'est encore équivalent à $t^{-1}um \subset A$, ou encore à $um \subset tA$. Comme $u \in J$, il suffit pour cela de voir que $Jm \subset tA$. Mais on sait que $Jm^n \subset tA$ d'après $(**)$, et d'autre part $m = tA + m^n$ d'après $(*)$, de sorte que l'on a

$$Jm = J(tA + m^n) \subset tA + Jm^n \subset tA,$$

ce qui achève la démonstration. □

6.9 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'ait pas (et qu'on ne s'attende pas à en avoir) d'algorithme polynomial 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 nombres premiers divisent $|K_{\mathbb{Z}}/A|$.

Commençons par des propriétés du discriminant, qui est défini en 7.2.1.

6.9.1 Proposition. *Soit K un corps de nombres, et A un sous-anneau d'indice fini de $K_{\mathbb{Z}}$. Alors $p|\mathrm{disc}(A)$ 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 $\mathrm{disc}(A) = 0$ 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. □

6.9.2 Proposition. *Soit K un corps de nombres, et $A \subset K_{\mathbb{Z}}$ un sous-anneau d'indice fini a. Alors* $\mathrm{disc}(A) = a^2 \,\mathrm{disc}(K_{\mathbb{Z}})$.

Preuve. C'est une conséquence immédiate de 7.1.4 plus bas. □

6.9.3 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 :*

(i) $A = K_{\mathbb{Z}}$;

(ii) *A est un anneau de Dedekind ;*

(iii) *pour tout nombre premier p tel que p^2 divise* $\mathrm{disc}(A)$*, et pour tout idéal maximal $m \subset A$ contenant p, on a* $\dim_{A/m}(m/m^2) \leq 1$;

Preuve. L'implication (i) ⇒ (ii) est claire car $K_{\mathbb{Z}}$ est un anneau de Dedekind (6.1.1 (ii)). La réciproque est immédiate : d'abord, puisque A est d'indice fini dans $K_{\mathbb{Z}}$, il existe un entier $d \neq 0$ tel que $d\,K_{\mathbb{Z}} \subset A$, ce qui entraîne que $\mathrm{Frac}\,(A) = \mathrm{Frac}\,(K_{\mathbb{Z}}) = K$. Comme $K_{\mathbb{Z}}$ est entier sur $\mathbb{Z}$, donc sur A et a même corps des fractions, il lui est égal si A est intégralement clos, donc si (ii) est vérifiée.

L'implication (ii) ⇒ (iii) est une conséquence de 6.8.1. Montrons que (iii) implique (ii).

Remarquons d'abord que les hypothèses générales de 6.8.1 sont vérifiées pour A : il est intègre comme sous-anneau de K, noethérien en tant que $\mathbb{Z}$-module de type fini (même raisonnement que dans 5.4.4 (i)) ; on voit de même, comme dans 5.4.4 (iv), que si I est un idéal non nul de A alors A/I est fini ; en particulier si I est premier il est maximal puisque tout anneau intègre fini est un corps.

Supposant (iii), il s'agit donc de voir, d'après 6.8.1, que pour tout idéal premier non nul m de A, le A-module m/m^2 est engendré par un élément. Or m contient un nombre premier p (la caractéristique du corps fini A/m). Si p^2 divise $\mathrm{disc}(A)$, c'est gagné par hypothèse. Sinon, l'indice $|K_{\mathbb{Z}}/A|$ de A dans $K_{\mathbb{Z}}$ est premier à p en vertu de 6.9.2. Ceci entraîne que la multiplication par p^2 dans $K_{\mathbb{Z}}/A$ est bijective ; l'injectivité (resp. la surjectivité) signifie que $A \cap p^2\,K_{\mathbb{Z}} = p^2\,A$ (resp. que $K_{\mathbb{Z}} = A + p^2\,K_{\mathbb{Z}}$). Ces deux conditions entraînent à leur tour que la réduction modulo p^2 induit un isomorphisme d'anneaux :

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

Or considérons, pour un anneau R quelconque, la propriété : « pour tout idéal maximal m de R, le R-module m/m^2 est engendré par un élément ». Il est clair que cette propriété passe au quotient : si elle est vraie pour R elle est vraie pour tout quotient R/I.

Dans notre cas, elle est vraie pour $K_{\mathbb{Z}}$ d'après 6.8.1 ; elle est donc vraie pour $K_{\mathbb{Z}}/p^2K_{\mathbb{Z}}$ donc aussi pour A/p^2A qui lui est isomorphe. Or on a $m \supset m^2 \supset p^2A$ donc m/m^2 s'identifie au quotient $\overline{m}/\overline{m}^2$ où l'on a posé $\overline{m} := m/p^2A$. Ce dernier est un idéal maximal de A/p^2A, donc $\overline{m}/\overline{m}^2$ est engendré par un élément comme A/p^2A-module (donc aussi comme A-module) donc il en est de même de m/m^2. □

6.9.4 Exemple. Traitons 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 (pour calculer ce dernier, on peut utiliser des algorithmes pour le calcul de résultants, mais en degré 3 la formule est bien connue). De toute façon, dans ce cas on trouve $\mathrm{disc}(A) = -3{\cdot}6{\cdot}6 = -2^2 3^3$. Les nombres premiers suspects 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 $A = K_{\mathbb{Z}}$.

7 Le discriminant.

7.1 Discriminant d'une forme bilinéaire symétrique.

7.1.1 Notations, généralités.

Soient A un anneau, et E un A-module libre de rang fini n. On suppose E muni d'une forme bilinéaire symétrique

$$\beta : E \times E \to A.$$

À toute suite finie $\underline{x} = (x_1, \ldots, x_n) \in E^n$, on associe sa « matrice de Gram »

$$\Gamma(\beta, \underline{x}) := (\beta(x_i, x_j))_{1 \leq i \leq n, 1 \leq j \leq n} \in \mathrm{M}_n(A)$$

et l'on pose

$$D(\beta, \underline{x}) := \det \Gamma(\beta, \underline{x}) \in A.$$

Si $\underline{e} = (e_1, \ldots, e_n)$ est une base de E, alors $\Gamma(\beta, \underline{e})$ est simplement la matrice de β dans la base e, et son déterminant $D(\beta, \underline{e})$ s'appelle le *discriminant* de β dans la base $\underline{e}$. En outre, si l'on désigne alors par X la matrice de $\underline{x} \in E^n$ dans cette base (c'est donc une matrice carrée d'ordre n, dont la i-ème colonne est formée des coordonnées des x_i dans $\underline{e}$), alors un calcul immédiat montre que

$$\Gamma(\beta, \underline{x}) = {}^t X \, \Gamma(\beta, \underline{e}) \, X$$

et que par suite

$$D(\beta, \underline{x}) = \det(X)^2 \, D(\beta, \underline{e}).$$

En particulier, si $\underline{e}$ et $\underline{e}'$ sont deux bases de E, on voit que $D(\beta, \underline{e})$ et $D(\beta, \underline{e}')$ sont égaux à multiplication près par le carré d'un inversible de A. Autrement dit, ils ont même classe dans le monoïde (multiplicatif) quotient $A/A^{\times 2}$.

7.1.2 Définition. Avec les hypothèses et notations ci-dessus, le *discriminant* de β, noté

$$\mathrm{disc}(\beta) \in A/A^{\times 2}$$

est la classe dans $A/A^{\times 2}$ de $D(\beta, \underline{e})$, où $\underline{e}$ est une base quelconque de E.

7.1.3 Exemples.

1. Si A est un corps, $\mathrm{disc}(\beta)$ est soit nul, soit inversible ; il est inversible si et seulement si β est *non dégénérée*.
2. Si A est un corps *algébriquement clos*, le monoïde $A/A^{\times 2}$ est isomorphe à $\{0, 1\}$ (muni de la multiplication) ; la seule information donnée par le disccriminant est donc celle vue ci-dessus.
3. Si $A = \mathbb{R}$, alors $A/A^{\times 2}$ est isomorphe à $\{0, 1, -1\}$: le discriminant est un « signe ». *Exercice :* exprimer ce signe en fonction du rang et de la signature de β.
4. Si $A = \mathbb{Z}$, le seul carré inversible est 1, de sorte que le discriminant est un élément *bien défini* de $\mathbb{Z}$.

5. Le discriminant de la forme nulle est 0, *sauf si* $E = \{0\}$: le discriminant de l'unique forme bilinéaire sur le module nul est (la classe de) 1 (qui est le déterminant de la matrice à 0 ligne et 0 colonne).
6. Soient (E_1, β_1) et (E_2, β_2) deux A-modules libres de rang fini, munis de formes bilinéaires symétriques ; soit (E, β) le « produit orthogonal » $(E_1 \times E_2, \beta_1 \times \beta_2)$, avec

$$(\beta_1 \times \beta_2)((x_1, x_2), (y_1, y_2)) = \beta_1(x_1, y_1) + \beta_2(x_2, y_2),$$

alors $\mathrm{disc}(\beta) = \mathrm{disc}(\beta_1)\,\mathrm{disc}(\beta_2)$. (Dans une « base produit » de E, la matrice de β est diagonale par blocs, les deux blocs diagonaux étant les matrices de β_1 et β_2).

Noter que valeur 1 pour le discriminant lorsque $E = \{0\}$ (exemple 5) est la seule compatible avec la formule ci-dessus : c'est une façon de s'en souvenir...

7.1.4 Proposition. *Avec les notations de* 7.1.1, *on suppose en outre que* $A = \mathbb{Z}$. *Soit* $E' \subset E$ *un sous-*$\mathbb{Z}$*-module d'indice fini* a *(et donc aussi libre de rang* n*). Alors*

$$\mathrm{disc}(\beta_{|E'}) = a^2\,\mathrm{disc}(\beta).$$

Preuve. D'après le « théorème de la base adaptée », il existe une base $\underline{e} = (e_1, \ldots, e_n)$ de E et des entiers $d_1, \ldots, d_n$ tels que $\underline{e'} = (d_1 e_1, \ldots, d_n e_n)$ soit une base de E'. On a alors $E/E' \cong \prod_{i=1}^n (\mathbb{Z}/d_i\mathbb{Z})$, de sorte que $a = |\prod_{i=1}^n d_i|$. D'autre part la matrice de $\underline{e'}$ dans la base $\underline{e}$ de E est la matrice diagonale $\mathrm{diag}\,(d_1, \ldots, d_n)$. On a donc

$$\begin{array}{rcl} \mathrm{disc}(\beta_{|E'}) & = & D(\beta, \underline{e'}) \\ & = & \det(\mathrm{diag}\,(d_1, \ldots, d_n))^2\, D(\beta, \underline{e}) \\ & = & (\prod_{i=1}^n d_i)^2\, D(\beta, \underline{e}) \\ & = & a^2\,\mathrm{disc}(\beta), \end{array}$$

d'où la conclusion. □

7.2 Discriminant d'une algèbre.

Soient A un anneau, et B une A-algèbre qui est un A-module libre de rang fini n. On applique les considérations précédentes au A-module B muni de la *forme trace* $\tau_{B/A}$ définie en 5.2.

Si $\underline{x} = (x_1, \ldots, x_n) \in B^n$, on posera notamment

$$D_{B/A}(\underline{x}) = D(\tau_{B/A}, (\underline{x})) \in A.$$

On a donc par définition

$$D_{B/A}(\underline{x}) = \det(\mathrm{Tr}_{B/A}(x_i\, x_j))_{1 \le i \le n, 1 \le j \le n}.$$

7.2.1 Définition. Avec les hypothèses et notations ci-dessus, le *discriminant* de B sur A est par définition $\mathrm{disc}(\tau_{B/A}) \in A/A^{\times 2}$.

On le note $\mathrm{disc}(B/A)$ si aucune confusion n'est à craindre.

C'est donc la classe modulo $A^{\times 2}$ de $D_{B/A}(\underline{e})$, où $\underline{e}$ désigne n'importe quelle base de B comme A-module.

7.2.2 Exemples et remarques

1. Le discriminant de la A-algèbre nulle est 1 (7.1.3 (5)). Celui d'une algèbre produit $B_1 \times B_2$ est le produit des discriminants de B_1 et B_2 (utiliser 7.1.3 (6), en remarquant que $\tau_{B_1 \times B_2}$ est produit orthogonal de τ_{B_1} et τ_{B_2}).
2. Par abus de langage, on désigne souvent le discriminant par un élément de A qui le représente. Un cas important où ce n'est pas un abus est celui où $A = \mathbb{Z}$, d'après 7.1.3 (4).
3. Il y a également une situation où le discriminant a un représentant « naturel » : c'est celle des algèbres de la forme $A[X]/(f)$, où $f \in A[X]$ est unitaire. C'est l'objet du paragraphe suivant.

7.3 Discriminant d'un polynôme.

7.3.1 Définition. Soient A un anneau, $f \in A[X]$ un polynôme unitaire à coefficients dans A, et n le degré de f. Notons B la A-algèbre $A[X]/(f)$, et $x \in B$ la classe de X ; on rappelle (cf. 5.1.2) que $(1, x, \ldots, x^{n-1})$ est une base de B comme A-module.

On appelle *discriminant* de f l'élément de A défini par

$$\mathrm{disc}(f) = D_{B/A}(1, x, \ldots, x^{n-1}).$$

7.3.2 Remarques. (i) Bien entendu, dans la situation de 7.3.1, $\mathrm{disc}(B)$ est la classe de $\mathrm{disc}(f)$ modulo les carrés d'inversibles. Insistons sur le fait que, contrairement à celui de B, le discriminant de f est un élément *bien défini* de A.

(ii) Explicitons un peu la définition : on a $\mathrm{disc}(f) = \det(\mathrm{Tr}(x^{i+j}))_{0 \le i \le n-1, 0 \le j \le n-1}$. Par définition de la trace, $\mathrm{Tr}(x^m)$ est la trace de la multiplication par x^m dans B ; c'est donc aussi la trace de C^m où C est la matrice compagnon de f, définie en 5.1.2. On trouve donc

$$\mathrm{disc}(f) = \det \begin{pmatrix} n & \mathrm{Tr}(C) & \mathrm{Tr}(C^2) & \cdots & & \mathrm{Tr}(C^{n-1}) \\ \mathrm{Tr}(C) & \mathrm{Tr}(C^2) & \cdots & & \mathrm{Tr}(C^{n-1}) & \mathrm{Tr}(C^n) \\ \mathrm{Tr}(C^2) & \cdots & & \mathrm{Tr}(C^{n-1}) & \mathrm{Tr}(C^n) & \mathrm{Tr}(C^{n+1}) \\ \vdots & & & & & \vdots \\ \mathrm{Tr}(C^{n-1}) & \mathrm{Tr}(C^n) & & & \cdots & \mathrm{Tr}(C^{2n-2}) \end{pmatrix}.$$

(iii) Sauf en très petit degré (voir 7.3.3 ci-dessous), il est déraisonnable d'appliquer brutalement la formule (ii) telle quelle pour *calculer* un discriminant : il faudrait d'abord écrire la matrice compagnon C (ça, ce n'est rien), puis calculer les puissances C^m ($m \le 2n-2$) (donc $2n-3$ produits de matrices d'ordre n), prendre leurs traces et former la matrice trouvée en (ii) (facile à nouveau), enfin calculer le déterminant. En pratique on passe plutôt par la notion de discriminant d'un polynôme (voir plus loin).

(iv) Même si elle a peu d'intérêt calculatoire, la formule (ii) donne un renseignement précieux. En effet, vu la forme de C donnée en 5.1.2, il est clair que les coefficients de la matrice ci-dessus (et donc aussi son déterminant) sont donnés par des polynômes en les coefficients de f, ne dépendant que de n. En d'autres termes, il existe pour chaque n un polynôme « universel » $\Delta_n(S_0, \ldots, S_{n-1}) \in \mathbb{Z}[S_0, \ldots, S_{n-1}]$ tel que le discriminant du polynôme $X^n + a_{n-1}X^{n-1} + \ldots + a_0$ soit égal à $\Delta_n(a_0, \ldots, a_{n-1})$, quels que soient l'anneau A et les coefficients a_i.
D'ailleurs, le polynôme Δ_n n'est autre que le discriminant du polynôme « universel » $X^n + S_{n-1}X^{n-1} + \ldots + S_0$, à coefficients dans $\mathbb{Z}[S_0, \ldots, S_{n-1}]$.

7.3.3 Exemples. En degré 1, on a $\Delta_1(S_0) = 1$ (vérifiez !).

Explicitons le calcul de Δ_2. Soit donc $f = X^2 + pX + q$ unitaire de degré 2, à coefficients dans A. La matrice compagnon est $C = \begin{pmatrix} 0 & -q \\ 1 & -p \end{pmatrix}$, de trace $-p$; on a $C^2 = \begin{pmatrix} -q & pq \\ -p & p^2 - q \end{pmatrix}$, de trace $p^2 - 2q$. Le discriminant de f est donc le déterminant $\begin{vmatrix} 2 & -p \\ -p & p^2 - 2q \end{vmatrix}$, égal (surprise) à $p^2 - 4q$. En d'autres termes, $\Delta_2(S_0, S_1) = S_1^2 - 4\,S_0$.

En degré 3, on trouve (avec un logiciel de calcul formel, par exemple) que le discriminant de $X^3 + a\,X^2 + b\,X + c$ est $-4\,a^3\,c + a^2\,b^2 + 18\,a\,b\,c + (-4\,b^3 - 27\,c^2)$. Le cas le plus important (et qu'il est bon de connaître par cœur) est celui où $a = 0$, où le discriminant est $-4\,b^3 - 27\,c^2$: attention au signe !

7.3.4 Remarque. Une conséquence de l'existence de Δ_n (qui lui est d'ailleurs équivalente) est la propriété d'« invariance par changement d'anneau » du discriminant : si f est comme dans 7.3.1 et si $\varphi : A \to A'$ est un morphisme d'anneaux, on peut considérer le polynôme f^φ obtenu en appliquant φ aux coefficients de f. Alors on a

$$\mathrm{disc}(f^\varphi) = \varphi(\mathrm{disc}(f))$$

dans A'.

On peut naturellement montrer cette propriété en « remontant » soigneusement la définition du discriminant ; on a besoin pour cela des propriétés analogues de la trace et du déterminant d'une matrice.

Cette propriété, d'apparence anodine, est très utile. Par exemple, si $A = \mathbb{Z}$, pour voir qu'un entier n divise $\mathrm{disc}(f)$ il suffit de voir que le polynôme f mod n (dans $(\mathbb{Z}/n\mathbb{Z})[X]$) a un discriminant nul. Et, pour A quelconque, on peut, pour calculer $\mathrm{disc}(f)$, remplacer A par n'importe quel anneau contenant A comme sous-anneau.

La proposition suivante fait le lien avec une définition plus traditionnelle du discriminant (et en facilite le calcul) :

7.3.5 Proposition. *Avec les notations de la définition* 7.3.1, *on suppose en outre que f est* scindé, *c'est-à-dire de la forme*

$$f = \prod_{i=1}^{n} (X - \lambda_i)$$

où les λ_i sont des éléments de A. Pour chaque $i \in \{1, \ldots, n\}$, on a donc un morphisme de A-algèbres

$$\varphi_i : B \to A$$

envoyant x sur λ_i (et la classe d'un polynôme $h \in A[X]$ sur $h(\lambda_i)$). Alors :

(i) *Pour $z_1, \ldots, z_n$ quelconques dans B, on a*

$$D_{B/A}(z_1, \ldots, z_n) = \big(\det(\varphi_i(z_j))_{1 \le i,j \le n}\big)^2.$$

En d'autres termes, pour $h_1, \ldots, h_n$ dans $A[X]$, on a

$$D_{B/A}(h_1(x), \ldots, h_n(x)) = \big(\det(h_j(\lambda_i))_{1 \le i,j \le n}\big)^2.$$

(ii) *Le discriminant de f est donné par*

$$\mathrm{disc}(f) \;=\; \prod_{\substack{i,j \in \{1,\ldots,n\} \\ i<j}} (\lambda_i - \lambda_j)^2 \;=\; \varepsilon \prod_{i=1}^{n} f'(\lambda_i) \;=\; \varepsilon\, \mathrm{N}_{B/A}(f'(x))$$

où l'on a posé $\varepsilon = (-1)^{n(n-1)/2}$.

Preuve. (i) Il suffit de montrer la seconde formule. Soit M la matrice $(h_j(\lambda_i)) \in \mathrm{M}_n(A)$, et calculons ${}^tM\,M$: c'est une matrice dont le terme général est

$$\begin{array}{rcll} ({}^tM\,M)_{i,j} & = & \sum_{l=1}^{n} h_i(\lambda_l)\, h_j(\lambda_l) & \\ & = & \sum_{l=1}^{n} (h_i h_j)(\lambda_l) & \\ & = & \mathrm{Tr}_{B/A}((h_i h_j)(x)) & \text{(d'après 5.1.8 (iii))} \\ & = & \mathrm{Tr}_{B/A}(h_i(x)\, h_j(x)). & \end{array}$$

Par définition de $D_{B/A}$, on a donc $D_{B/A}(h_1(x), \ldots, h_n(x)) = \det({}^tM\,M) = \det(M)^2$, cqfd.
(ii) La partie (i), appliquée à $z_i = x^{i-1}$ (ou, si l'on préfère, à $h_i = X^{i-1}$) et la définition du discriminant donnent

$$\mathrm{disc}(f) = \begin{vmatrix} 1 & \lambda_1 & \cdots & \lambda_1^{n-1} \\ 1 & \lambda_2 & \cdots & \lambda_2^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \lambda_n & \cdots & \lambda_n^{n-1} \end{vmatrix}^2 = \prod_{\substack{i,j \in \{1,\ldots,n\} \\ i<j}} (\lambda_i - \lambda_j)^2$$

(Vandermonde), d'où la première égalité. En remarquant que $(\lambda_i - \lambda_j)^2$ peut aussi s'écrire $-(\lambda_i - \lambda_j)(\lambda_j - \lambda_i)$, on en tire :

$$\begin{aligned}
\mathrm{disc}(f) &= (-1)^{n(n-1)/2} \prod_{\substack{i,j\in\{1,\dots,n\}\\ j\neq i}} (\lambda_i - \lambda_j) \\
&= (-1)^{n(n-1)/2} \prod_{i=1}^{n} \prod_{\substack{j\in\{1,\dots,n\}\\ j\neq i}} (\lambda_i - \lambda_j) \\
&= (-1)^{n(n-1)/2} \prod_{i=1}^{n} f'(\lambda_i)
\end{aligned}$$

puisque $f'(X) = \sum_i \prod_{j\neq i}(X - \lambda_j)$. Enfin, le produit des $f'(\lambda_i)$ est égal à $\mathrm{N}_{B/A}(f'(x))$ en vertu de 5.1.8 (ii), d'où la dernière égalité. □

La partie (ii) de la proposition ci-dessus fournit plusieurs façons, toutes utiles, de calculer le discriminant. Par exemple, lorsque A est un corps, on obtient :

7.3.6 Corollaire. *Soient K un corps, $f \in K[X]$ unitaire de degré n, B la K-algèbre $K[X]/(f)$, $x \in B$ la classe de X, L une extension de K telle que f soit scindé dans $L[X]$* (par exemple un corps de décomposition de f, ou une clôture algébrique de K).

(1) *Soient λ_i $(1 \leq i \leq n)$ les racines de f dans L, comptées avec multiplicités. On a dans L les égalités (avec $\varepsilon = (-1)^{n(n-1)/2}$)*

$$\mathrm{disc}(f) \;=\; \prod_{\substack{i,j\in\{1,\dots,n\}\\ i<j}} (\lambda_i - \lambda_j)^2 \;=\; \varepsilon \prod_{i=1}^{n} f'(\lambda_i) \;=\; \varepsilon\, \mathrm{N}_{B/K}(f'(x))$$

(2) *Les conditions suivantes sont équivalentes :*

(i) $\mathrm{disc}(f) \neq 0$;

(ii) *la forme trace $\tau_{B/K}$ est non dégénérée ;*

(iii) *f n'a pas de racine multiple dans L (ou dans une clôture algébrique de K) ;*

(iv) *f et f' n'ont pas de racine commune dans L (ou dans une clôture algébrique de K) ;*

(v) *f et f' sont premiers entre eux dans $K[X]$.*

Preuve. La première égalité de (1) résulte immédiatement de 7.3.5 (ii), puisque $\mathrm{disc}(f)$ se calcule aussi bien dans L que dans K, et que dans $L[X]$ on a $f = \prod_{i=1}^{n}(X - \lambda_i)$. Pour la seconde, posons $B_L := L[X]/(f)$: alors 7.3.5 (ii) donne $\mathrm{disc}(f) = \varepsilon\, \mathrm{N}_{B_L/L}(f'(x))$, et il suffit de remarquer que si $z \in B$, alors $\mathrm{N}_{B/K}(z) = \mathrm{N}_{B_L/L}(z)$ (en effet $(1, x, \dots, x^{n-1}$ est à la fois une K-base de B et une L-base de B_L, et la matrice de z est la même dans ces deux bases).

(2) L'équivalence (i)⇔(ii) a déjà été remarquée (7.1.3). Les équivalences (iii)⇔(iv)⇔(v) sont (on l'espère) bien connues. Enfin, (i)⇔(iii) (ou, si l'on préfère, (i)⇔(iv)) est une conséquence de (1). □

Dans la proposition 7.3.5, la dernière formule, $\mathrm{disc}(f) = \varepsilon\,\mathrm{N}(f'(x))$, se distingue par le fait que les λ_i n'y figurent pas, et qu'elle garde donc un sens sans l'hypothèse que f soit scindé. On peut (on doit !) donc se demander si elle est vraie sans cette hypothèse, et de fait :

7.3.7 Corollaire. *Sous les hypothèses de* 7.3.1 (et sans supposer f scindé)*, on a la formule*

$$\mathrm{disc}(f) = (-1)^{n(n-1)/2}\,\mathrm{N}_{B/A}(f'(x)).$$

Preuve. Écrivons $f = X^n + a_{n-1}X^{n-1} + \ldots + a_0$. Le premier membre est $\Delta_n(a_0, \ldots, a_{n-1})$, où $\Delta_n \in \mathbb{Z}[S_0, \ldots, S_{n-1}]$ est le polynôme de 7.3.2 (iv). De même, le membre de droite est un « polynôme universel » en les a_i (à coefficients entiers, et ne dépendant que de n) : en effet il est égal à $\det(f'(C))$ où C est la matrice compagnon C de f ; il est clair que les coefficients de f' sont polynomiaux en les a_i, de même que ceux de C, donc aussi ceux de la matrice $f'(C)$ et finalement son déterminant. L'identité de l'énoncé est donc de la forme

$$\Delta_n(a_0, \ldots, a_{n-1}) = \Phi_n(a_0, \ldots, a_{n-1})$$

où Δ_n et Φ_n sont dans $\mathbb{Z}[\underline{S}] = \mathbb{Z}[S_0, \ldots, S_{n-1}]$, et sont indépendants de f (et de A). Il suffit donc d'établir dans $\mathbb{Z}[\underline{S}]$ l'identité $\Delta_n = \Phi_n$, ce qui revient à démontrer 7.3.7 dans le cas (dit « universel ») où A est l'anneau $A_u = \mathbb{Z}[\underline{S}]$ et où f est le polynôme $f_u = X^n + S_{n-1}X^{n-1} + \ldots + S_0$. Pour cela, on peut en outre remplacer A_u par un anneau le contenant, par exemple (puisqu'il est intègre) par son corps des fractions K_u. Mais il existe une extension L de K_u telle que f_u soit scindé dans $L[X]$, et sur laquelle on peut donc appliquer 7.3.5 (ii). □

7.3.8 Remarque. Voici une variante de l'argument ci-dessus, que nous laissons comme exercice. Pour $f \in A[X]$ unitaire de degré n, on montre qu'il existe une A-algèbre A' contenant A (et, si l'on veut, libre de rang $n!$ comme A-module) telle que f soit scindé dans $A'[X]$: la formule est donc vraie dans A', et donc aussi dans A par le même argument que ci-dessus.

Pour trouver A', on copie l'argument bien connu (du moins on l'espère) dans le cas où A est un corps : on remarque que si l'on pose encore $B = A[X]/(f)$, et si x est la classe de X dans B, alors $f(x) = 0$ donc $f = (X - x)\,g(X)$ avec $g \in B[X]$ unitaire de degré $n - 1$; on conclut alors par récurrence sur n.

7.4 Retour aux algèbres : algèbres séparables.

7.4.1 Définition. Soient K un corps, et B une K-algèbre (commutative) de dimension finie. On dit que B est *séparable* si $\mathrm{disc}(B/K) \neq 0$ (ou, de façon équivalente, si la forme trace $\tau_{B/K}$ est non dégénérée, cf. 1 1).

7.4.2 Exemples et remarques.

(i) On dit en particulier qu'une *extension* finie de K est séparable si c'est une K-algèbre séparable.

(ii) Soit $f \in K[X]$ unitaire : alors, d'après 7.3.6 (2), la K-algèbre $K[X]/(f)$ est séparable si et seulement si f n'a pas de racine multiple dans une clôture algébrique de K (on dit alors parfois que f est un *polynôme séparable*).

(iii) Soient B_1 et B_2 deux K-algèbres de dimenson finie. Alors $B_1 \times B_2$ est séparable si et seulement si B_1 et B_2 le sont : ceci résulte de 7.2.2 1.

(iv) Soit B une K-algèbre de dimension finie et soit $x \in B$ un élément *nilpotent*. Alors x est de trace nulle (exercice d'algèbre linéaire : considérer le polynôme caractéristique de x, ou ses valeurs propres comme endomorphisme). Mais, pour tout $y \in B$, xy est encore nilpotent (B est commutative), de sorte que $\mathrm{Tr}\,(xy) = 0$ pour tout y et que x est dans le noyau de la forme trace.
On en conclut que *toute K-algèbre séparable est réduite*, c'est-à-dire sans élément nilpotent non nul.

La partie (3) de la proposition ci-dessous donne une réciproque partielle à 7.4.2 (iii) :

7.4.3 Proposition. *Soient K un corps, et B une K-algèbre (commutative) de dimension finie.*
(1) *Les conditions suivantes sont équivalentes :*

(i) *B est réduite ;*

(ii) *B est isomorphe à un produit $L_1 \times \cdots \times L_r$ d'extensions finies de K.*

(2) *Les conditions suivantes sont équivalentes :*

(iii) *B est séparable ;*

(iv) *B est isomorphe à un produit $L_1 \times \cdots \times L_r$ d'extensions finies séparables de K.*

(3) *On suppose que K est fini ou de caractéristique nulle. Alors toute extension finie de K est séparable. En conséquence, les conditions* (i) *à* (iv) *ci-dessus sont équivalentes.*

Preuve. (1) L'implication (ii)⇒(i) est triviale.

Sans même supposer B réduite, soit $J \subset B$ l'intersection de tous les idéaux maximaux de B. Comme B est de dimension finie, J est intersection d'une famille finie $(m_1, \ldots, m_r)$ d'idéaux maximaux distincts. Le lemme chinois implique que le morphisme naturel

$$\varphi : B \to \prod_{i=1}^{r} B/m_i$$

est surjectif (on voit en particulier que $r \leq \dim_K B$, mais peu importe ici). Il est clair d'autre part que $\ker \varphi = J$.

Montrons que J est le « nilradical » de B, c'est-à-dire l'ensemble des nilpotents. Si $x \in B$ est nilpotent, il est clair que $\varphi(x) = 0$, donc $x \in J$. Réciproquement, soit $x \in J$: puisque

$\dim B < \infty$, x est annulé par un polynôme non nul, de la forme $P(X) = X^d(XQ(X) + \lambda)$ avec $\lambda \neq 0$ dans K ; on a donc $0 = x^d(xQ(x)+\lambda)$. Mais x est dans tous les idéaux maximaux de B, donc $xQ(x) + \lambda$ n'est dans aucun, donc est inversible. La relation ci-dessus implique donc $x^d = 0$, cqfd.

Si B est réduite, on en déduit que φ est injectif, donc bijectif, d'où (ii).

(2) L'implication (iv)⇒(iii) est immédiate par 7.4.2 (iii). Inversement, si B est séparable, elle est réduite d'après 7.4.2 (iv) ; elle est donc produit d'extensions finies de K, automatiquement séparables par 7.4.2 (iii).

(3) Soit L une extension finie de K.

Si K est de caractéristique nulle, le théorème de l'élément primitif assure que L est engendrée par un élément (comme extension de K) donc est de la forme $K[X]/(f)$ où $f \in K[X]$ est irréductible. Mais ceci entraîne que f est séparable : en effet, comme $\operatorname{car} K = 0$, la dérivée f' de f n'est pas nulle ; comme $\deg f' < \deg f$ et que f est irréductible, les polynômes f et f' sont donc premiers entre eux, donc L est séparable d'après 7.3.6 (2).

Si K est fini, on sait que le groupe L^* est cyclique, d'ordre n premier à la caractéristique p de K. Soit x un générateur de L^*. Alors $L = K(x)$, et comme ci-dessus il suffit de voir que le polynôme minimal f de x n'a pas de racine multiple. Or x est racine du polynôme $X^n - 1$, qui n'a pas de racine multiple (sa dérivée est nX^{n-1} donc a pour seule racine 0 puisque $n \neq 0$ dans K). Il en est donc de même de f, qui divise $X^n - 1$. □

7.4.4 Remarque. L'assertion (3) s'étend en fait à tout corps de caractéristique $p > 0$ dont tout élément est une puissance p-ième (ces corps, ainsi que les corps de caractéristique nulle, sont dits *parfaits*).

Réciproquement, si $\operatorname{car} K = p > 0$ et si $a \in K$ n'est pas une puissance p-ième, alors on montre facilement que le polynôme $X^p - a$ est irréductible dans $K[X]$; comme il est clair qu'il a une racine d'ordre p dans une clôture algébrique de K (d'ailleurs sa dérivée est nulle), on voit que $L := K[X]/(X^p - a)$ est une extension finie de K qui n'est pas séparable.

8 Finitude du groupe des classes d'idéaux.

Si K est 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.

8.1 La norme d'un idéal.

8.1.1 Définition. Soient K une extension finie de $\mathbb{Q}$, et a un idéal non nul de $K_\mathbb{Z}$. On définit la *norme* $\mathrm{N}_{K/\mathbb{Q}}(a)$ de a par :

$$\mathrm{N}_{K/\mathbb{Q}}(a) := |K_\mathbb{Z}/a|.$$

On la note aussi $\mathrm{N}(a)$ si aucune confusion n'est à craindre.

8.1.2 Proposition. *Avec les notations ci-dessus, posons $A = K_\mathbb{Z}$.*

(i) *Si x est un élément non nul de A, alors $\mathrm{N}_{K/\mathbb{Q}}(xA)$ est égal à $|\mathrm{N}_{K/\mathbb{Q}}(x)|$.*

(ii) *Si a et b sont des idéaux non nuls de A, 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 A.*

Preuve. L'assertion (i) a déjà été vue, cf. 5.4.4 (iii). Pour (ii), 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 :

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

Il suffit donc de voir que $|a/am| = |A/m|$, ou encore, que a/am est un $K_\mathbb{Z}/m$-espace vectoriel de dimension un. Or le théorème de décomposition des idéaux montre que a/am n'a pas de sous-A-module autre que lui-même et 0, et qu'il n'est pas nul, d'où la conclusion. □

8.1.3 Remarques. (i) Avec les notations de 8.1.1 et 8.1.2, il résulte de la définition que l'entier $\mathrm{N}(a)$ annule le groupe A/a. Donc $\mathrm{N}(a).1_{A/a} = 0$, de sorte que $\mathrm{N}(a)$ *est un élément de a.*
Inversement, soit m un entier positif appartenant à a : alors A/a est un quotient de A/mA, donc $\mathrm{N}(a)$ divise le cardinal de A/mA, qui est $m^{[K:\mathbb{Q}]}$ d'après 5.4.4 (ii).

(ii) Si a est *maximal*, alors la caractéristique du corps $K_\mathbb{Z}/a$ est un nombre premier p, qui est l'unique nombre premier appartenant à a ; la norme de a est alors une puissance de p (elle divise même $p^{[K:\mathbb{Q}]}$ d'après (i) ci-dessus).
On voit donc que, si p est un nombre premier, *les idéaux maximaux de A contenant p sont exactement les idéaux maximaux dont la norme est une puissance de p.*
On prendra garde que, pour un idéal a, le fait que $\mathrm{N}(a)$ soit une puissance d'un nombre premier p n'implique évidemment pas que a soit maximal (sauf si $\mathrm{N}(a) = p$, bien entendu).

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

Nous considérons $\mathbb{Q}(\sqrt{-5})$ comme sous-anneau de $\mathbb{C}$, en envoyant $\sqrt{-5}$ vers $i\sqrt{5}$. 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 applications suivantes :

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

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

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

8.3 Application.

8.3.1 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. □

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 $n \geq 1$).

8.4 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 $\mathrm{disc}(A)$ 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 :

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

On conclut que :

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

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

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

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 sur un dessin, où l'on voit qu'il 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 :

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

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 :

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

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 :

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

On en conclut le résultat suivant.

8.4.1 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 $2^{-1}|\mathrm{disc}(K_{\mathbb{Z}})|^{1/2}$.*

8.4.2 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.

8.5 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 $d = r_1 + 2r_2$.

8.5.1 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 $\mathbb{C}^{r_2} \to \mathbb{R}^{2r_2}$:

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

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 :

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

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 :

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

8.5.2 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.

8.5.3 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 $a\log(x) + b\log(y) \leq \log(ax + by)$. □

8.5.4 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 $K_{\mathbb{Z}}$.

8.5.5 Lemme. *Soit M un $\mathbb{Z}$-module libre de rang fini, et b: $M \times M \to \mathbb{Z}$ 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* $\mathrm{disc}(b)$*, comme étant cet entier.*

8.5.6 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 $K_\mathbb{Z}$.

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

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

Preuve. 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

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

□

8.5.8 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 :*

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

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

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

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 $K_\mathbb{Z}/nK_\mathbb{Z}$. □

Nous terminons cette section avec un exemple amusant.

8.5.9 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 $f := x^4 - x + 41$, 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 ($\mathrm{disc}(A) = -163$). 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 $-40 < n < 41$. □

9 La réciprocité quadratique.

9.1 Décomposition des nombres premiers.

Soient K un corps de nombres, et p un nombre premier. L'anneau $K_{\mathbb{Z}}/pK_{\mathbb{Z}}$ est alors une $\mathbb{F}_p$-algèbre de dimension $d := \dim_{\mathbb{Q}}(K)$. Nous allons relier sa structure à la décomposition de $pK_{\mathbb{Z}}$ en produit d'idéaux premiers, et d'autre part au discriminant de $K_{\mathbb{Z}}$.

Commençons par une remarque valable dans tout anneau de Dedekind :

9.1.1 Proposition. *Soient A un anneau de Dedekind, I un idéal non nul de A. Les conditions suivantes sont équivalentes :*

(i) *l'anneau A/I est (isomorphe à) un produit de corps ;*
(ii) *l'anneau A/I est* réduit *;*
(iii) *pour tout idéal premier non nul m de A, on a $v_m(I) \in \{0, 1\}$* (où $v_m(I)$ est l'exposant de m dans la décomposition de I, cf. 6.5.3).

Preuve. L'implication (i) $\Rightarrow$ (ii) est triviale (pour n'importe quel anneau).

Écrivons $I = m_1^{e_1} \cdots m_r^{e_r}$, où les m_i sont des idéaux premiers non nuls de A, deux à deux distincts (et où tous les e_i sont > 0). En particulier les idéaux $m_i^{e_i}$ sont étrangers deux à deux, de sorte que l'on a (lemme chinois) :

$$A \xrightarrow{\sim} \prod_{i=1}^{r} (A/m_i^{e_i}).$$

(ii) $\Rightarrow$ (iii) : supposons (iii) fausse, par exemple $e_1 \geq 2$. L'idéal $I' = m_1\, m_2^{e_2} \cdots m_r^{e_r}$ contient I, est différent de I (par unicité de la décomposition), et vérifie $I'^{e_1} \subset I$. Soit alors $x \in I' \backslash I$: alors la classe de x dans A/I est un élément non nul (puisque $x \notin I$) et nilpotent (puisque $x^{e_1} \in I'^{e_1} \subset I$, donc A/I n'est pas réduit.

(iii) $\Rightarrow$ (i) : si chaque e_i vaut 1, alors chaque $A/m_i^{e_i} = A/m_i$ est un corps, donc A/I est bien un produit de corps. □

9.1.2 Proposition. *Soit B un anneau qui est un $\mathbb{Z}$-module libre de type fini, et soit p un nombre premier. Les conditions suivantes sont équivalentes :*

(i) *l'anneau B/pB est un produit de corps ;*
(ii) *l'anneau B/pB est réduit ;*
(iii) *p ne divise pas* $\mathrm{disc}(B/\mathbb{Z})$.

Preuve. La classe modulo p de $\mathrm{disc}(B/\mathbb{Z})$ est le discriminant de la $\mathbb{F}_p$-algèbre B/pB, et ce dernier est nul si et seulement si B/pB est réduit (ou encore un produit de corps), d'après 7.4.3 (3). □

9.1.3 Cas des entiers d'un corps de nombres.

Soient K un corps de nombres et p un nombre premier. On pose $A = K_{\mathbb{Z}}$, et l'on considère la décomposition de pA en produit d'idéaux premiers :

$$pA = m_1^{e_1} \cdots m_r^{e_r}$$

où les m_i sont les idéaux premiers (distincts) de A contenant p, et où chaque $e_i = v_{m_i}(p)$ est un entier positif. Pour chaque i, le quotient A/m_i est un corps fini de caractéristique p (puisque $p \in m_i$), donc on a

$$\mathrm{N}(m_i) = |A/m_i| = p^{f_i}$$

où $f_i = [A/m_i : \mathbb{F}_p]$ est un entier > 0.

9.1.4 Proposition. *Avec les hypothèses et notations de* 9.1.3, *les conditions suivantes sont équivalentes :*

(i) *p ne divise pas* $\mathrm{disc}(K_{\mathbb{Z}})$ *;*
(ii) *A/pA est réduit ;*
(iii) *tous les e_i sont égaux à* 1.

De plus, on a la relation

$$\sum_{i=1}^{r} e_i f_i = [K : \mathbb{Q}].$$

Preuve. L'équivalence de (ii) et (iii) (resp. de (i) et (ii)) résulte de 9.1.1 (resp. de 9.1.2).

Pour montrer la dernière assertion, posons $n = [K : \mathbb{Q}]$. Alors on a

$$\begin{array}{rcll} p^n & = & \mathrm{N}_{K/\mathbb{Q}}(p) & \\ & = & \mathrm{N}(pA) & \text{(proposition 8.1.2 (i))} \\ & = & \prod_{i=1}^{r} \mathrm{N}(m_i)^{e_i} & \text{(proposition 8.1.2 (ii))} \\ & = & \prod_{i=1}^{r} p^{e_i f_i} & \text{(définition de } f_i\text{)} \\ & = & p^{\sum_{i=1}^{r} e_i f_i} & \end{array}$$

d'où la conclusion. □

9.1.5 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.

Nous utiliserons un peu plus loin le résultat suivant.

9.1.6 Proposition. *Soient $\mathbb{Q} \to K \to L$ des extensions finies, d'anneaux d'entiers respectifs A et B.*

(i) *Pour tout $x \in A$, on a $xB \cap A = xA$. En d'autres termes, l'homomorphisme naturel d'anneaux $A/xA \to B/xB$ est injectif.*
(ii) *Soit p un nombre premier. Si p est ramifié dans K, il l'est dans L.*

Preuve. (i) Soit $x \in A$ et soit $z \in xB \cap A$. Si $x = 0$, tout est clair. Sinon, $z/x \in B \cap K$; donc z est un élément de K entier sur $\mathbb{Z}$. Donc $z \in A$, cqfd.

(ii) En appliquant (i) à $x = p$, on conclut que A/pA est (isomorphe à) un sous-anneau de B/pB. Donc si A/pA n'est pas réduit, B/pB non plus. □

9.2 Le cas des corps quadratiques.

On suppose maintenant que K est un corps quadratique. Il est donc de la forme $K = \mathbb{Q}(\sqrt{d})$, où $d \neq 1$ est un entier sans facteur carré, déterminé de façon unique par K. L'anneau des entiers A de K est donné par le théorème 4.3.3 ; comme le polynôme minimal de $\sqrt{d}$ (resp. $\frac{1+\sqrt{d}}{2}$) est $X^2 - d$ (resp. $X^2 - X - \frac{d-1}{4}$), on en déduit que

$$A \cong \mathbb{Z}[X]/(f), \text{ avec } f = \begin{cases} X^2 - d & \text{si } d \not\equiv 1 \pmod 4 \\ X^2 - X - \frac{d-1}{4} & \text{si } d \equiv 1 \pmod 4 \end{cases}$$

et que par suite, le discriminant de A sur $\mathbb{Z}$ (qui est celui de f) est donné par

$$\operatorname{disc}(A/\mathbb{Z}) = \Delta = \begin{cases} 4d & \text{si } d \not\equiv 1 \pmod 4 \\ d & \text{si } d \equiv 1 \pmod 4. \end{cases}$$

On remarquera au passage que d, et donc K, est entièrement déterminé par Δ.

Soit alors p un nombre premier. Vu la relation $\sum_{i=1}^{r} e_i f_i = [K : \mathbb{Q}]$ de 9.1.4, les seules possibilités pour la décomposition de pA sont, puisqu'ici $[K : \mathbb{Q}] = 2$:

- $pA = m^2$ (m maximal de norme p) ;
- $pA = m_1 m_2$ (m_1 et m_2 maximaux distincts de norme p) ;
- $pA = m$ (maximal de norme p^2).

Le premier cas est celui où p est ramifié ; dans le second cas, on dit que p est *décomposé* dans K. Dans le troisième, on dit que p est *inerte* dans K (c'est le cas où p est encore irréductible dans $K_{\mathbb{Z}}$).

Ces trois cas sont décrits dans le tableau suivant, où $\overline{A} = A/pA$, $\overline{\Delta} = \Delta \bmod p$, et $\overline{f} \in \mathbb{F}_p[X]$ est le polynôme f réduit modulo p :

p ramifié	**p décomposé**	**p inerte**
Racines de $\overline{f}$ dans $\mathbb{F}_p$:		
une racine double	deux racines	aucune racine
Structure de $\overline{A}$:		
$\overline{A} \cong \mathbb{F}_p[Y]/(Y^2)$	$\overline{A} \cong \mathbb{F}_p \times \mathbb{F}_p$	corps à p^2 éléments
Condition sur le discriminant (si $p \neq 2$) :		
$\overline{\Delta} = 0$	$\overline{\Delta}$ est un carré non nul	$\overline{\Delta}$ n'est pas un carré
Condition sur le discriminant (si $p = 2$) :		
$\Delta \equiv 0 \pmod 4$	$\Delta \equiv 1 \pmod 8$	$\Delta \equiv 5 \pmod 8$

Seule la dernière ligne mérite une explication. Si 2 est ramifié, Δ est pair, donc divisible par 4 (formule ci-dessus). Sinon, d est nécessairement $\equiv 1 \pmod 4$, et égal à Δ ; si l'on écrit $d = \Delta = 1 + 4\delta$, le polynôme $\overline{f}$ est égal à $X^2 + X + \overline{\delta} \in \mathbb{F}_2[X]$. Si $\Delta \equiv 1 \pmod 8$, alors $\overline{\delta} = 0$ et $\overline{f} = X(X+1)$ a deux racines distinctes, donc 2 est décomposé. Sinon, $\overline{f} = X^2 + X + 1$ est irréductible et 2 est inerte.

Ce tableau montre que le type de décomposition de p dans K ne dépend que de la classe du discriminant de K modulo p (ou modulo 8, si $p = 2$). À l'aide de la réciprocité quadratique nous exprimerons cette propriété en termes de la classe de p modulo le discriminant de K.

9.3 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.

9.3.1 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*

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

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 K un corps de décomposition de $X^p - 1$ sur $\mathbb{Q}$, 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 $\sigma(\zeta_p)$. □

9.3.2 Théorème. *Soit p un nombre premier et $\mathbb{Q}(\zeta_p)$ comme ci-dessus. 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 6.9.3. Comme ζ_p est entier sur $\mathbb{Z}$, $\mathbb{Z}[\zeta_p]$ est contenu dans $\mathbb{Q}(\zeta_p)_{\mathbb{Z}}$. 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 (qui est celui de $\mathbb{Z}[\zeta_p]=\mathbb{Z}[X]/(\Phi_p)$) est, au signe près, une puissance de p, et qu'il en est de même de $\mathrm{disc}(\mathbb{Q}(\zeta_p)_{\mathbb{Z}})$ qui le divise. 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 $\dim_{A/m}(m/m^2)\leq 1$. L'anneau $\mathbb{Z}[\zeta_p]/p\mathbb{Z}[\zeta_p]$ 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 :

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

En « faisant $Y=\zeta_p-1$ on en déduit que $p\in m^2$, ce qui implique que m/m^2 est engendré par ζ_p-1, donc de dimension au plus un. □

9.3.3 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 $\mathbb{Q}$. Il est donc de la forme $\mathbb{Q}(\sqrt{d})$, avec $d\neq 1$ sans facteur carré. De plus, on sait, d'après 9.1.6 et 9.3.2,que le seul nombre premier ramifié dans K est p. Donc le discriminant de K est, au signe près, une puissance de p. La formule donnant le discriminant de $\mathbb{Q}(\sqrt{d})$ implique immédiatement le résultat. □

9.4 Réciprocité quadratique.

9.4.1 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 :*

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

L'application $\left(\frac{\cdot}{p}\right):\mathbb{F}_p\to\{-1,0,1\}\subset\mathbb{Z}$ s'appelle le symbole de Legendre. *Pour $a\in\mathbb{F}_p$ on a :*

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

L'application $a\mapsto\left(\frac{a}{p}\right)$ induit un morphisme de groupes de $\mathbb{F}_p^*$ dans $\mathbb{Z}^\times$.

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 $\mathbb{Z}^\times$. 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 $\mathbb{F}_p^{*,2}$. □

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

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

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

(iii) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Remarquer que, « concrètement », l'énoncé peut se formuler ainsi :

9.4.3 Corollaire. (i) *Si p et q sont premiers, impairs et distincts, alors :*

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

(ii) *Si p est premier impair, alors :*

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

(iii) *Si p est premier impair, alors :*

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

Preuve. L'assertion (ii) est déjà connue (9.4.1). Pour montrer (i) et (iii), fixons p et q premiers distincts, avec $p \neq 2$ (mais on n'exclut pas que $q = 2$).

Considérons le corps $L = \mathbb{Q}(\zeta_p)$. D'après la proposition 9.3.3, l'unique sous-corps quadratique de L est $K := \mathbb{Q}(\sqrt{p^*})$, avec $p^* = \left(\frac{-1}{p}\right) p$; on posera $x = \sqrt{p^*} \in K$. Notons que le discriminant de K est p^* ; en particulier, q est non ramifié dans K et, d'après 9.2, on a :

– si $q \neq 2$:

$$\begin{aligned} q \text{ est décomposé dans } K &\Leftrightarrow \left(\tfrac{p^*}{q}\right) = 1 \\ q \text{ est inerte dans } K &\Leftrightarrow \left(\tfrac{p^*}{q}\right) = -1. \end{aligned}$$

– si $q = 2$:

$$\begin{aligned} 2 \text{ est décomposé dans } K &\Leftrightarrow p^* \equiv 1 \pmod 8 \\ 2 \text{ est inerte dans } K &\Leftrightarrow p^* \equiv 5 \pmod 8. \end{aligned}$$

Par définition de p^*, on remarque que $\left(\frac{p^*}{q}\right) = (-1)^{\frac{p-1)(q-1)}{2}} \left(\frac{p}{q}\right)$ si q est impair, et que $p^* \equiv 1 \pmod 8$ (resp. $p^* \equiv 5 \pmod 8$) équivaut en fait à $p \equiv \pm 1 \pmod 8$ (resp. à $p \equiv \pm 3 \pmod 8$). Les assertions à démontrer peuvent donc, dans tous les cas, se résumer ainsi :

$$\begin{aligned} q \text{ est décomposé dans } K &\Leftrightarrow \left(\tfrac{q}{p}\right) = 1 \\ q \text{ est inerte dans } K &\Leftrightarrow \left(\tfrac{q}{p}\right) = -1. \end{aligned} \qquad (?)$$

Montrons donc (?). Nous avons un diagramme commutatif :

$$\begin{array}{ccccc} L = \mathbb{Q}(\zeta_p) & \longleftarrow & \mathbb{Z}[\zeta_p] \cong \mathbb{Z}[Y]/(\Phi_p(Y)) & \longrightarrow & \mathbb{F}_q[Y]/(\Phi_p(Y)) = \mathbb{Z}[\zeta_p]/(q) \\ \uparrow & & \uparrow & & \uparrow \\ K = \mathbb{Q}(\sqrt{p^*}) & \longleftarrow & \mathbb{Z}[x] \cong \mathbb{Z}[X]/(f) & \longrightarrow & \mathbb{F}_q[X]/(f) = \mathbb{Z}[x]/(q) \\ \uparrow & & \uparrow & & \uparrow \\ \mathbb{Q} & \longleftarrow & \mathbb{Z} & \longrightarrow & \mathbb{F}_q \end{array}$$

avec $f = X^2 - X - (p^* - 1)/4$. Les anneaux $\mathbb{Z}[Y]/(\Phi_p)$ et $\mathbb{Z}[X]/(f)$ sont les anneaux d'entiers respectifs de L et K ; l'application de $\mathbb{F}_q[X]/(f)$ vers $\mathbb{F}_q[Y]/(\Phi_p(Y))$ est injective d'après 9.1.6 (ii).

Par la Proposition 9.3.1, $\mathrm{Gal}(L/\mathbb{Q})$ s'identifie à $\mathbb{F}_q^*$. D'autre part, $\mathrm{Gal}(K/\mathbb{Q})$ admet un unique isomorphisme avec $\mathbb{Z}^*$. Ceci nous donne un diagramme :

$$\begin{array}{ccc} \mathrm{Gal}(L/\mathbb{Q}) & \xrightarrow[\sim]{h} & \mathbb{F}_p^* \\ \downarrow g & & \downarrow (\frac{\cdot}{p}) \\ \mathrm{Gal}(K/\mathbb{Q}) & \xrightarrow{\sim} & \mathbb{Z}^\times \end{array}$$

qui est *nécessairement commutatif* car il n'existe qu'un morphisme surjectif d'un groupe cyclique d'ordre pair vers $\{\pm 1\}$.

On voit donc que le sous-groupe des carrés dans $\mathbb{F}_p^*$ est l'image par h de $\mathrm{Gal}(L/K)$ (qui est le noyau de g).

En particulier, notons σ_q l'élément de $\mathrm{Gal}(L/\mathbb{Q})$ qui correspond à la classe de q dans $\mathbb{F}_p^*$: on a donc l'équivalence :

$$(\tfrac{q}{p}) = 1 \Leftrightarrow \sigma_q \in \mathrm{Gal}(L/K) \Leftrightarrow (\sigma_q)_{|K} = \mathrm{Id}.$$

Or $\sigma_q(\zeta_p) = \zeta_p^q$, donc σ_q induit l'endomorphisme de Frobenius de $\mathbb{F}_q[Y]/(\Phi_p)$. Donc il induit le frobenius de $\mathbb{F}_q[X]/(f)$.

Regardons donc le frobenius de $\mathbb{F}_q[X]/(f) = K_{\mathbb{Z}}/qK_{\mathbb{Z}}$: comme q n'est pas ramifié dans K, on a deux possibilités :

– q est décomposé dans K : alors $\mathbb{F}_q[X]/(f) \cong \mathbb{F}_q \times \mathbb{F}_q$, et le frobenius est l'identité ;
– q est inerte dans K : alors $\mathbb{F}_q[X]/(f)$ est un corps à q^2 éléments, dont le frobenius n'est pas l'identité.

Si $(\frac{q}{p}) = 1$, σ_q induit l'identité sur K ; a fortiori il induit l'identité sur $\mathbb{F}_q[X]/(f)$ donc on est dans le premier cas, et q est décomposé.

Si $(\frac{q}{p}) = -1$, σ_q n'est pas l'identité sur K donc envoie $\sqrt{p^*}$ sur $-\sqrt{p^*}$ et la racine x de f sur $1 - x$. Donc il n'induit pas l'identité sur $\mathbb{F}_q[X]/(f)$, et q est inerte dans K. On a donc bien montré (?) □

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- Soient $n \in \mathbb{N}$ et $a = (a_1, \ldots, a_n) \in \mathbb{Z}^n$, non nul. On note $\Delta = \mathbb{Z}a$ le sous-$\mathbb{Z}$-module de $\mathbb{Z}^n$ engendré par a. Montrer que les conditions suivantes sont équivalentes :

(i) a est primitif ;
(ii) $\mathbb{Z}^n/\Delta$ est un $\mathbb{Z}$-module sans torsion ;
(iii) $\mathbb{Z}^n/\Delta$ est un $\mathbb{Z}$-module libre ;
(iv) Δ a un supplémentaire dans $\mathbb{Z}^n$;
(v) a fait partie d'une base de $\mathbb{Z}^n$.

-3- Soient A un anneau factoriel, n un entier naturel, et a, b, c des éléments non nuls de A. On suppose que $ab = c^n$ et que a et b sont premiers entre eux. Montrer qu'il existe $u \in A^\times$, $\alpha \in A$ et $\beta \in A$ tels que $a = u\alpha^n$ et $b = u^{-1}\beta^n$.

-4- Soient K un corps, et n un entier supérieur 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 : considérer, par l'absurde, 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.)

Où sert 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 congrus à -1 modulo 4. (Supposer le contraire : à l'aide du produit des nombres premiers en question, fabriquer alors un entier qui n'est divisible par aucun d'eux et qui est congru à -1 modulo 4).

Même question modulo 6.

Si l'on applique la méthode aux congruences modulo n (donné et ≥ 3), quel résultat obtient-on ?

-6- Soit p un nombre premier impair. Montrer que $x^2 + 1$ a une racine dans $\mathbb{F}_p$ si et seulement si $p \equiv 1 \pmod 4$. (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- Donner une caractérisation des nombres premiers congrus à 1 modulo 3, analogue à celle de l'exercice précédent. En déduire qu'il y a une infinité de nombres premiers congrus à 1 modulo 3.

-8- 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 application. Alors f est une* jauge euclidienne *si son image est minorée 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 jauge euclidienne sur A.*

1. (Juste pour mémoire.) Montrer qu'un anneau euclidien est principal.
2. Montrer que pour tout $a \neq 0$ dans A on a $f(a) > f(0)$.
3. Montrer que $f\colon \mathbb{Z} \to \mathbb{Z}$, $n \mapsto |n|$, est une jauge euclidienne.
4. Soit K un corps. Montrer que $f\colon K[x] \to \mathbb{Z}$, $a \mapsto \deg(a)$ est euclidienne. Ici on convient que $\deg(0) = -1$. (Si on veut que $\deg(0) = -\infty$, on pourrait introduire l'ensemble ordonné $\mathbb{N} \cup \{-\infty\}$, et la notion de jauge euclidienne à valeurs dans $\mathbb{N} \cup \{-\infty\}$.
5. Soit A un anneau intègre, et $f\colon A \to \mathbb{Z}$ une application. Montrer que f est euclidienne si et seulement si $f + 1$ (la fonction donnée par $a \mapsto f(a) + 1$) l'est.
6. (Plus difficile.) Soit A un anneau intègre et $\phi\colon A \to \mathbb{Z}$ une jauge euclidienne. Montrer que $f\colon A \to \mathbb{Z}$, $a \mapsto \min\{\phi(ax) \,|\, 0 \neq x \in A\}$, est une jauge euclidienne, et a la propriété supplémentaire que $f(ab) \geq f(a)$ pour tous a et b avec b non nul.

-9- Montrer que l'anneau $\mathbb{Z}[i]$ est euclidien pour la jauge $d\colon \mathbb{Z}[i] \to \mathbb{N}$, $z \mapsto z\overline{z}$. Même question pour $\mathbb{Z}[j]$. Montrer que $\mathbb{Z}[i\sqrt{5}]$ ne l'est pas : d'abord directement, puis en montrant qu'il n'est pas factoriel.

-10- Soit σ l'automorphisme non trivial de $\mathbb{Q}(\sqrt{2})$. Évidemment, 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 jauge euclidienne. (Pour les courageux : quels sont les corps quadratiques dont l'anneau des entiers est euclidien pour la norme ainsi définie ?)

-11- Donner (et le cas échéant programmer) des algorithmes de division euclidienne dans $\mathbb{Z}[i]$ et $\mathbb{Z}[j]$; en déduire des algorithmes de calcul de pgcd dans ces anneaux.

-12- Le but de cet exercice est de donner un algorithme efficace (en un sens « probabiliste ») pour trouver, pour un nombre premier $p \equiv 1 \pmod 4$, un élément d'ordre 4 dans $\mathbb{F}_p^*$ (c'est-à-dire un solution dans $\mathbb{F}_p$ de l'éuation $x^2 = -1$). Soit donc p premier, congru à 1 mod 4.

1. Ecrivons $p - 1 = 2^n m$ avec m impair (notez que $n \geq 2$). Pour a dans $\mathbb{F}_p^*$, l'ordre de a^m divise 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 $b \neq \pm 1$.

2. 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.
3. 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]).

-13- Factoriser en irréductibles : $7 + i$ dans $\mathbb{Z}[i]$, et $5 + j$ dans $\mathbb{Z}[j]$.

-14- Chercher un nombre premier p qui est congru à 1 modulo 4 et raisonnablement grand (disons au moins 1000), et l'écrire comme somme de deux carrés.

-15- Soit p premier, avec $p \equiv 1 \pmod 4$. On se propose de donner un algorithme calculant des entiers a et b tels que $p = a^2 + b^2$.

Pour cela on commence par trouver c dans $\mathbb{Z}$ tel que $|c| < p/2$ et que $c^2 \equiv -1 \pmod p$, grâce à l'algorithme de l'exercice **12** par exemple.

Notons alors $f\colon \mathbb{Z}[i] \to \mathbb{F}_p$ le morphisme d'anneaux tel que $f(i) = c \bmod p$. Montrer 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 $a + ib$ de $\ker(f)$. Montrer que l'on a alors $a^2 + b^2 = p$.

Remarque : l'algorithme obtenu (en utilisant celui de l'exercice **12**) est probabiliste, et le temps moyen qu'il nécessite est $O(\log(p)^3)$. (Le nombre moyen de a à essayer dans l'exercice **12** 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- « Calculer » $\mathbb{Z}[i]/(a + bi)\mathbb{Z}[i]$ en tant que $\mathbb{Z}$-module, pour des $a + bi$ (a et b dans $\mathbb{Z}$) de votre choix. Par exemple, pour ceux avec $|a| \leq 3$, $|b| \leq 3$.

-17- Trouver des isomorphismes d'anneaux de $\mathbb{F}_{19}[X]/(X^2 + 2X - 4)$ sur $\mathbb{F}_{19} \times \mathbb{F}_{19}$, et de $\mathbb{F}_{19}[X]/(X^2 + 1)$ sur $\mathbb{F}_{19}[Y]/(2Y^2 + 2Y + 1)$.

-18- Généraliser le théorème des deux carrés en donnant un critère pour qu'un *rationnel* x soit somme de deux carrés dans $\mathbb{Q}$, en termes de la décomposition de x en facteurs premiers.

En déduire qu'un entier n est somme de deux carrés dans $\mathbb{Z}$ si et seulement si il est somme de deux carrés dans $\mathbb{Q}$.

-19- Soit p un nombre premier. En s'inspirant du cas de $\mathbb{Z}[i]$, étudier la décomposition de p dans $\mathbb{Z}[j]$ en fonction de la classe de p modulo 3.

-20- 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 $\mathbb{Q}(\sqrt{5})_{\mathbb{Z}}$.

-21- Soient A un anneau, B une A-algèbre, S une partie de B. On note $A[S] \subset B$ l'intersection de toutes les sous-A-algèbres de B contenant S.

(i) Montrer que $A[S]$ est la plus petite sous-A-algèbre de B contenant S. On l'appelle la sous-A-algèbre de B *engendrée par* S. Si $A = \mathbb{Z}$, on dira aussi « le sous-anneau de B engendré par S ». La notation $A[S]$ est traditionnelle mais très mauvaise (confusion avec les algèbres de polynômes).

(ii) Montrer que $A[S]$ est engendré *comme A-module* par les « monômes » $s_1^{e_1} \dots s_r^{e_r}$ avec $r \in \mathbb{N}$, les s_i dans S et les e_i dans $\mathbb{N}$.

(iii) Quelle est la sous-A-algèbre de B engendrée par $\emptyset$? par B ? Si B est l'algèbre de polynômes $A[X_1, \dots, X_n]$, quelle est la sous-A-algèbre de B engendrée par $\{X_1, \dots, X_n\}$?

(iv) Si $S = \{s_1, \dots s_n\}$ est *fini*, montrer que $A[S]$ est l'image du morphisme de A-algèbres $A[X_1, \dots, X_n] \to B$ donné par $P \mapsto P[s_1, \dots s_n]$.

(v) Pour S quelconque, montrer que $A[S]$ est la réunion des $A[T]$ où T parcourt les parties finies de S. Si vous connaissez les polynômes en une infinité d'indéterminées, généralisez (iv) aux parties S quelconques.

(vi) On dit que B est une *A-algèbre de type fini* s'il existe $S \subset B$ fini tel que $A[S] = B$. Montrer que si B est une A-algèbre de type fini, c'est un A-module de type fini, mais que la réciproque est fausse.
Une A-algèbre B est de type fini si et seulement si elle est isomorphe à un quotient d'une algèbre de polynômes $A[X_1, \dots, X_n]$.

(vii) Tout quotient d'une A-algèbre de type fini est une A-algèbre de type fini. Si B est une A-algèbre de type fini et C une B-algèbre de type fini, alors C est une A-algèbre de type fini.

(viii) Si B est une A-algèbre de type fini, engendrée par une partie S non nécessairement finie, alors il existe $T \subset S$ fini tel que $B = A[T]$.

(ix) Montrer que $\mathbb{Q}$ n'est pas une $\mathbb{Z}$-algèbre de type fini. (Utiliser (viii) en prenant pour S, par exemple, l'ensemble des $1/n$ pour n entier non nul).

-22- Montrer « à la main » que $\sqrt{2} + \sqrt[3]{3}$ est un entier algébrique.

-23- Parmi les nombres complexes suivants, lesquels sont des entiers algébriques ?

$$\sqrt[9]{7} \qquad \frac{6}{\sqrt{3}} \qquad \sqrt{6} + \frac{1}{\sqrt{3}} \qquad e^{2i\pi/561} \qquad e + \pi$$

-24- Soit B l'anneau de toutes les fonctions de $\mathbb{R}$ dans $\mathbb{R}$, et soit A le sous-anneau de B formé des fonctions continues. Soit X une partie de $\mathbb{R}$, et soit $\chi_X \in B$ la fonction caractéristique de X. À quelle(s) condition(s) sur X l'élément χ_X est-il entier sur A ?

-25- Soit d un entier sans facteur carré, avec $d \equiv 1 \pmod 4$. Montrer de deux manières que $A := \mathbb{Z}[\sqrt{d}]$ n'est pas factoriel :

(i) en remarquant qu'il n'est pas intégralement clos ;

(ii) en remarquant que $(1 + \sqrt{d})(1 - \sqrt{d}) = 1 - d$ et que 2 est irréductible dans A (pour ce dernier point on pourra utiliser la norme $\mathrm{N}(a + b\sqrt{d}) = a^2 - db^2$).

-26- Soit A un anneau factoriel. Montrer que A est intégralement clos.

-27- Donner des exemples d'anneaux intègres non intégralement clos.

-28- Soient K un corps, et $(A_i)_{i\in I}$ une famille de sous-anneaux intégralement clos de K. Montrer que $\bigcap_{i\in I} A_i$ est intégralement clos.

-29- Soient $x \in \mathbb{C}$ un entier algébrique, $A = \mathbb{Z}[x]$, $K = \mathbb{Q}(x)$. Montrer l'équivalence :

$$A \text{ est intégralement clos} \Leftrightarrow A = K_{\mathbb{Z}}.$$

-30- Soient A un anneau et B une A-algèbre de type fini. Montrer l'équivalence :

$$B \text{ est entière sur } A \Leftrightarrow B \text{ est un } A\text{-module de type fini.}$$

-31- Soient X et Y deux $\mathbb{Z}$-modules libres de même rang n, et soit $u : X \to Y$ un homomorphisme. Si B_1 et B_2 sont des bases de X et Y respectivement, on peut représenter u par une matrice $M_{B,B'}(u) \in \mathrm{M}_n(\mathbb{Z})$. Montrer que :

(i) $|\det(M_{B,B'}(u))|$ est indépendant de B et B' ;

(ii) u est injectif si et seulement si $\det(M_{B,B'}(u)) \neq 0$;

(iii) si u est injectif alors $|\det(M_{B,B'}(u))| = |Y/u(X)|$ (utiliser le « théorème de la base adaptée »).

-32- Soient K un corps, $n \geq 0$ un entier, et $a_0, \ldots, a_{n-1}$ dans K. Montrer que :

$$\det \begin{pmatrix} t & & & & a_0 \\ -1 & t & & & \vdots \\ & -1 & \ddots & & \vdots \\ & & \ddots & t & a_{n-2} \\ & & & -1 & t + a_{n-1} \end{pmatrix} = t^n + a_{n-1}t^{n-1} + \cdots + a_0.$$

Indication : on peut procéder de deux façons au moins. Développer suivant la première ligne et faire une 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 indéteerminées, alors le polynôme en question est irréductible.

-33- Soient A un anneau, et soit

$$f = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in A[X]$$

un polynôme unitaire de degré n à coefficients dans A.

(1) Montrer qu'il existe une A-algèbre C avec les propriétés suivantes :

(i) C est un A-module libre de rang $n!$;

(ii) il existe $\lambda_1, \ldots, \lambda_n \in C$ tels que $f = \prod_{i=1}^{n}(X - \lambda_i)$ dans $C[X]$.

(Indication : on procédera par récurrence sur n, en s'inspirant de la preuve de l'existence d'un corps de décomposition pour un polynôme à coefficients dans un corps).

(2) Soit $B = A[X]/(f)$, et soit $z \in B$. En utilisant (1), justifier la méthode suivante pour calculer (par exemple) la norme $\mathrm{N}_{B/A}(z)$:

– on écrit $z = h(x) = h(X) \bmod f$ (avec x = classe de X dans B, et $h \in A[X]$) ;
– on calcule le polynôme $S = \prod_{i=1}^{n} h(L_i) \in A[L_1, \ldots, L_n]$ où les L_i sont des indéterminées ;
– on écrit $S = T(\sigma_1, \ldots, \sigma_n)$ où les σ_i sont les polynômes symétriques élémentaires en les L_i, et où T est à coefficients dans A ;
– on renvoie $\mathrm{N}_{B/A}(z) = T(-a_{n-1}, a_{n-2}, \ldots, (-1)^n a_0)$.

-34- Soient A un anneau intègre, K son corps des fractions, L une K-algèbre, x un élément de L entier sur A. Montrer que les coefficients du polynôme minimal P de x sur K sont entiers sur A. (Indication : montrer que toute racine de P dans une extension de K est entière sur A).

Qu'en déduit-on si A est intégralement clos (par exemple si $A = \mathbb{Z}$) ?

-35- Soient A un anneau intégralement clos, K son corps des fractions, et $f \in A[X]$ un polynôme unitaire. On suppose que $f = gh$ avec g et h unitaires dans $K[X]$. Montrer que g et h sont dans $A[X]$. (Indication : considérer les racines de f dans une clôture algébrique de K).

-36- En utilisant l'exercice **33**, généraliser l'exercice **35** comme suit :

Soient A un anneau, R une A-algèbre, P et Q deux polynômes unitaires dans $R[X]$. Si les coefficients de PQ sont entiers sur A, les coefficients de P et de Q le sont aussi.

-37- Soient A un anneau et R une A-algèbre. Soit $P \in R[X]$. Montrer que P est entier sur $A[X]$ si et seulement si ses coefficients sont entiers sur A.

(Indication : supposons P racine de $Q(Y) = Y^m + F_1 Y^{m-1} + \cdots + F_m$, avec les F_i dans $A[X]$. On pose $P_1 = P - X^r$ avec r assez grand. Alors P_1 est racine de $Q_1(Y) = Q(Y + X^r) = Y^m + G_1 Y^{m-1} + \cdots + G_m$. On en déduit que $(-P_1)(P_1^{m-1} + \cdots + G_{m-1}) = G_m$ dans $R[X]$. Pour r convenable, $G_m = Q(X^r)$ est unitaire, ainsi que $-P_1$. On en déduit que le facteur $P_1^{m-1} + \cdots + G_{m-1}$ est aussi unitaire, puis, en appliquant l'exercice **36**, que P_1, et donc P, est à coefficients entiers sur A).

-38- Soient A un anneau, R une A-algèbre, n un entier naturel, A' la fermeture intégrale de A dans R. Déduire de l'exercice **37** que la fermeture intégrale de $A[X_1, \ldots, X_n]$ dans $R[X_1, \ldots, X_n]$ est $A'[X_1, \ldots, X_n]$.

En déduire que si A est intégralement clos, alors $A[X_1, \ldots, X_n]$ est intégralement clos.

-39- Soit $K = \mathbb{Q}[X]/(X^3 - 2)$ (isomorphe à $K' = \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$), et soit $x \in K$ la classe de X (correspondant à l'élément $\sqrt[3]{2}$ de K'). Soient $A = \mathbb{Z}[x]$, et B l'anneau des entiers de K. On se propose de montrer que $A = B$.

(1) Montrer que $A \subset B$, et donner une base du $\mathbb{Z}$-module A.

(2) Soit $z = a + b\,x + c\,x^2 \in K$, avec $a, b, c \in \mathbb{Q}$. Calculer le polynôme caractéristique de z. Calculer les traces de z, $x\,z$ et $x^2\,z$ et en déduire que $6B \subset A$.

(3) Soit z comme ci-dessus, supposé dans B. Écrivant $a = a'/6$, $b = b'/6$ et $c = c'/6$ avec $a', b', c' \in \mathbb{Z}$, montrer en utilisant les calculs de (2) que $a', b', c' \in 6\mathbb{Z}$ et conclure.

-40- Soient A un anneau, B une A-algèbre qui est libre de rang fini n comme A-module, z un élément de B. On suppose connu le polynôme $f := \mathrm{Pcar}_{B/A}(z) \in A[X]$. Comment calculer « simplement » le polynôme caractéristique de z^2 ?

-41- Soient $K \subset L$ une extension de corps, z un élément de L algébrique sur K, $f \in K[X]$ son polynôme minimal. Pour $\lambda \in K$, quel est le polynôme minimal de λz ? Et celui de $1/z$, si $z \neq 0$?

-42- Soient $z \in \mathbb{C}^*$ un entier algébrique, f son polynôme minimal sur $\mathbb{Q}$. Montrer que $1/z$ est un entier algébrique si et seulement si $f(0) = \pm 1$. Montrer qu'alors $1/z \in \mathbb{Z}[z]$.

-43- Soient A un anneau intègre, K son corps des fractions, L une K-algèbre, d un élément non nul de A. On considère la sous-A-algèbre $A[1/d]$ de K engendrée par $1/d$.

(i) Montrer que $A[1/d] = \bigcup_{n\in\mathbb{N}} d^{-n}A$.

(ii) Soit z un élément de L. Montrer que z est entier sur $A[1/d]$ si et seulement si il existe $n \in \mathbb{N}$ tel que $d^n z$ soit entier sur A.

(iii) Soit B la fermeture intégrale de A dans L. Montrer que la fermeture intégrale de $A[1/d]$ dans L est $B[1/d]$.

(iv) Si A est intégralement clos, en est-il de même de $A[1/d]$?

-44- On garde les notations de l'exercice **43**.

(i) Montrer que $A[1/d]$ est isomorphe (comme A-algèbre) à $A[X]/(dX-1)$. (On pourra soit procéder directement, soit utiliser la question (iii)).

(ii) Pour $d_1, \ldots, d_r$ non nuls dans A, montrer que $A[\frac{1}{d_1}, \cdots, \frac{1}{d_r}] = A[\frac{1}{d_1 \ldots d_r}]$.

(iii) Soit $f : A \to R$ un morphisme d'anneaux. Montrer que pour que f se prolonge en un morphisme d'anneaux $f_1 : A[1/d] \to R$, il faut et il suffit que $f(d)$ soit inversible dans R. Montrer que le prolongement f_1 est alors unique.

(iv) On suppose que A est factoriel. Soit P un système de représentants des irréductibles de A, et soit $P' = \{p \in P | p \text{ ne divise pas } d\}$. Montrer que $A[1/d]$ est factoriel et admet P' comme système de représentants des irréductibles.

(v) On suppose que A est principal. Soit $x = u/v$ un élément de K, avec u et v dans A premiers entre eux. Montrer que $A[x] = A[1/v]$. En déduire que toute sous-A-algèbre rde type fini de K est de la forme $A[1/f]$, pour $f \in A$ convenable.

-45- On garde les notations de l'exercice **43**.

(i) Soit J un idéal de $A[1/d]$. Montrer que $J \cap A$ est un idéal de A, et que J est l'idéal de $A[1/d]$ engendré par $J \cap A$.

(ii) Montrer que si A est noethérien, il en est de même de $A[1/d]$.

(iii) Montrer que si A est un anneau de Dedekind, il en est de même de $A[1/d]$. (Si $J \subset J'$ sont deux idéaux premiers non nuls de $A[1/d]$, considérer l'inclusion $J \cap A \subset J' \cap A$).

-46- Un $\mathbb{Z}$-module M est dit *sans torsion* si pour tout $n \in \mathbb{Z}$ et tout $x \in M$, l'égalité $nx = 0$ implique $n = 0$ ou $x = 0$.

Montrer que tout $\mathbb{Z}$-module libre est sans torsion, et que tout $\mathbb{Z}$-module de type fini sans torsion est libre.

Montrer que $\mathbb{Q}$ est sans torsion mais n'est pas libre.

-47- Soient M un $\mathbb{Z}$-module libre de type fini, x un élément de M, n un entier. On suppose que nx fait partie d'une base de M. Montrer que $n = \pm 1$.

Réciproquement, soit $y \in M$ tel que l'équation $nz = y$ (en $n \in \mathbb{Z}$ et $z \in M$) n'ait que les solutions évidentes (i.e. $n = \pm 1$). Montrer que y fait partie d'une base de M. (Indication : montrer que le $\mathbb{Z}$-module $M/\mathbb{Z}y$ est sans torsion, et utiliser l'exercice **46**).

-48- Soit K un corps. On appelle *valuation* (discrète) sur K une application $v : K \to \mathbb{Z} \cup \{+\infty\}$ ayant les propriétés suivantes (avec les conventions évidentes pour l'addition et l'ordre dans $\mathbb{Z} \cup \{+\infty\}$) : pour x et y dans K et

(i) $v(x) = +\infty \Leftrightarrow x = 0$;

(ii) $v(xy) = v(x) + v(y)$ (en particulier v induit un morphisme de groupes $K^* \to \mathbb{Z}$) ;

(iii) $v(x + y) \geq \min\{v(x), v(y)\}$.

L'application valant 0 sur K^* et $+\infty$ en 0 est une valuation sur K, dite *triviale*.

On dit qu'une valuation v est *normalisée* si elle est surjective (ou, de façon équivalente, s'il existe $x \in K$ tel que $v(x) = 1$). Montrer que toute valuation non triviale v est de la forme $k\, v_0$, pour une unique valuation normalisée v_0.

Soient A un anneau factoriel, K son corps des fractions, p un élément irréductible de A. Montrer que l'application v_p définie par

$$v_p(x) = \begin{cases} \text{l'exposant de } p \text{ dans la décomposition de } x \text{ en irréductibles} & \text{si } x \neq 0 \\ +\infty & \text{si } x = 0 \end{cases}$$

est une valuation normalisée sur K.

-49- Soient K un corps et v une valuation sur K (cf. exercice **48**).

(i) Montrer que $v(-1) = 0$.

(ii) Soient x et y dans K, tels que $v(x) \neq v(y)$. Montrer que l'inégalité $v(x + y) \geq \min\{v(x), v(y)\}$ est alors une égalité. (Déduire de (i) la formule $v(z-t) \geq \min\{v(z), v(t)\}$, puis l'appliquer avec z et t convenables).

(iii) Pour tout $m \in \mathbb{Z}$, soit $V_n := \{x \in K | v(x \geq n\}$. Montrer que V_0 est un sous-anneau de K, de corps des fractions K, et que, pour tout n, V_n est un sous-V_0-module de K, qui est libre de rang 1.

-50- Montrer que les seules valuations normalisées sur $\mathbb{Q}$ sont les v_p, pour p premier.

Indications : si v est une telle valuation, noter d'abord que v est ≥ 0 sur $\mathbb{Z}$, et qu'il existe un entier n tel que $v(n) = 1$. Montrer alors qu'il existe un unique facteur premier p de n tel que $v(p) = 1$, puis, en utilisant l'identité de Bézout, que $v(q) = 0$ pour tout q premier différent de p.

-51- Soit A un anneau principal. Généraliser l'exercice **50** comme suit : les seules valuations normalisées sur $\mathrm{Frac}(A)$ qui sont ≥ 0 sur A sont les v_p, pour p irréductible dans A.

-52- Soit k un corps. Montrer que les seules valuations normalisées sur $k(X)$ qui sont triviales sur k sont :

- les v_P, pour $P \in k[X]$ irréductible ;
- v_∞ définie par $v_\infty(F/G) := \deg G - \deg F$ pour F et G non nuls dans $k[X]$.

Indications : si v est une valuation qui est ≥ 0 sur $k[X]$, utiliser l'exercice **51**. Sinon, remarquer que $a := v(1/X)$ est strictement positif, et en déduire que $v(F) = -a \deg(F)$ pour tout polynôme $F \neq 0$.

-53- Soient A un anneau intègre, K son corps des fractions, M un sous-A-module non nul de K.

(i) Montrer que tout morphisme de A-modules $f : M \to K$ est de la forme $x \mapsto a\,x$, pour un unique $a \in K$.

(ii) En déduire un isomorphisme canonique entre le dual $M^* := \mathrm{Hom}_A(M, A)$ de M et le sous-A-module $M' := \{x \in K \mid xM \subset A\}$ de K.

(iii) On suppose que M est inversible, c'est-à-dire qu'il existe un sous-A-module N de K tel que $MN = A$. Montrer que M et N sont des idéaux fractionnaires, et que $N = M'$.

(iv) On suppose que A est un anneau de Dedekind. Montrer que deux éléments M_1 et M_2 de $I(A)$ ont même classe dans $C(A)$ si et seulement si ils sont isomorphes comme A-mocdules.

-54- Soient I un ensemble et A un anneau. Montrer que l'anneau A^I n'est noethérien que dans les cas suivants :

(i) $A = \{0\}$;

(ii) A est noethérien et I est fini.

-55- Soit X un intervalle de $\mathbb{R}$, non vide et non réduit à un point. Montrer que l'anneau $\mathcal{C}(X, \mathbb{R})$ n'est pas noethérien. (Utiliser une suite strictement décroissante de fermés de X).

-56- Généraliser **55** au cas d'un espace métrique infini.

-57- Soit V un voisinage de 0 dans R. Dans l'anneau $\mathcal{C}(V, \mathbb{R})$, montrer que l'idéal J des fonctions nulles en 0 n'est pas de type fini. (Indication : si $f_1, \ldots, f_n \in J$, considérer la fonction $(\sum_i |f_i|)^{1/2}$).

Montrer que l'idéal similaire dans l'anneau $\mathcal{C}^\infty(V, \mathbb{R})$ (en supposant V ouvert) est engendré par un élément, mais que $\mathcal{C}^\infty(V, \mathbb{R})$ n'est pas noethérien.

-58- Soit U un ouvert de $\mathbb{C}$. On note $H(U)$ l'anneau des fonctions holomorphes sur U.

(i) Montrer que $H(U)$ est intègre si et seulement si U est connexe et non vide.

(ii) On suppose U connexe non vide. Pour tout $p \in U$ et tout $f \in H(U)$, on note $\mathrm{ord}_p(f) \in \mathbb{N} \cup \{\infty\}$ l'ordre de f en p. Montrer que ord_p se prolonge en une valuation (encore notée ord_p) sur le corps des fractions $M(U)$ de $H(U)$. Pour $f \in M(U)$, montrer que $f \in H(U)$ si et seulement si $\mathrm{ord}_p(f) \geq 0$ pour tout $p \in U$. En déduire que $H(U)$ est intégralement clos.

(iii) Montrer que $H(\mathbb{C})$ n'est pas noethérien. (Pour chaque $n \in \mathbb{N}$, considérer l'idéal I_n des fonctions qui s'annulent en tous les entiers $\geq n$, et utiliser les fonctions $[\sin 2\pi(z-n)]/(z-n)$).

-59- Soient A un anneau noethérien, et B une A-algèbre qui est un A-module de type fini. Montrer que B est un anneau noethérien.

-60- Soient A un anneau, I et J deux idéaux de A. On dit que I et J sont *étrangers* si $I + J = A$.

(i) (« lemme chinois ») Si I et J sont étrangers, alors $I \cap J = IJ$ et $A/(I \cap J) \xrightarrow{\sim} (A/I) \times (A/J)$.

(ii) Si I et J sont étrangers, et si I et K sont étrangers, alors I et JK sont étrangers.

(iii) Si I et J sont étrangers, alors I^m et J^n sont étrangers (m et n quelconques dans $\mathbb{N}$). (On donnera deux démonstrations : l'une par récurrence en utilisant (ii), l'autre en partant d'une relation $1 = i + j$ avec $i \in I$ et $j \in J$, et en en déduisant une relation $1 = i' + j'$ avec $i' \in I^m$ et $j' \in J^n$).

-61- Deux éléments a et b d'un anneau A sont dits *étrangers* si les idéaux aA et bA sont étrangers (cf. exercice **60**). Expliciter cette condition. Montrer qu'elle implique que a et b sont « premiers entre eux » (tout diviseur commun est inversible), et que la réciproque est vraie si A est principal. Donner un exemple où elle est fausse (avec A intègre).

-62- Soit A un anneau de Dedekind.

(i) Soit p un idéal premier non nul de A, et soit $e \in \mathbb{N}$. Montrer que p/p^e est engendré par un élément (commencer par $e = 2$). En déduire que tout idéal de A/p^e est engendré par un élément.

(ii) Soit J un idéal non nul de A. Montrer que tout idéal de A/J est engendré par un élément. (Utiliser la décomposition en idéaux premiers, la question précédente et l'exercice **60**).

-63- Généralisation de l'exercice **51** : soient A un anneau de Dedekind, et K son corps des fractions. Montrer que toute valuation normalisée v sur K qui est positive ou nulle sur A est de la forme v_p, où p est un idéal premier non nul de A, uniquement déterminé par v).

Indications : on pose $p = \{x \in A \mid v(x) > 0\}$. C'est un idéal premier non nul de A ; on va montrer que $v = v_p$.

On fixe $\pi \in A$ tel que $v(\pi) = 1$. Alors π est dans p mais pas dans p^2, ce qui entraîne que $p = \pi A + p^2$ (cf. exercice **62** (i)), et que $p^e = \pi^e A + p^{e+1}$ pour tout $e \in \mathbb{N}$. Soit alors

$x \in A$ non nul, et soit $e = v_p(x)$. On en déduit que $x \equiv y\pi^e \pmod{p^{e+1}}$, où $y \in A$ vérifie $v_p(y) = 0$. On en tire $v(x) = e$ en utilisant l'exercice **49** (ii).

-64- Soient k un corps, et A une k-algèbre de dimension finie n en tant que k-espace vectoriel.

(i) 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.)

(ii) 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 (c'est-à-dire sans sous-module non trivial), et qu'alors $s \leq n$.

(iii) 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.

(iv) Soient $x_1, \ldots, x_n$ dans l'intersection des m_i. Montrer que $x_1 \cdots x_n = 0$. Indication : montrer que $x_1 \cdots x_i A \subset M_i$.

(v) 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 aux 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.

-65- 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 **64** 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.

-66- Dans cet exercice nous nous intéressons aux idéaux de $A := \mathbb{Z}[\sqrt{-5}]$, l'anneau des entiers 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 $\mathbb{Z}[x]$.

(i) 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 $\mathbb{Z}[x]/(f)$.

(ii) 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 $p = 5$.

(iii) 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.

(iv) 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 $(\mathbb{Z}/20\mathbb{Z})^\times$. Mieux, il existe un morphisme de groupes $g\colon (\mathbb{Z}/20\mathbb{Z})^\times \to \{1,-1\}$ 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 si c'est un carré modulo p_2).

(v) 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 $2A = m_2^2$.

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

(vii) 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 $m_3\overline{m_3}$ (et aussi m_3^2). Ceci explique les différentes factorisations de 6.

(viii) 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-il s'expliquer en termes du groupe $C(A)$?

-67- (extrait du partiel de mars 2002) On désigne par m un entier positif, *impair* et sans facteur carré. On note K le corps quadratique $\mathbb{Q}(\sqrt{-2m}) = \mathbb{Q}[X]/(X^2+2m)$ (on désigne par $\sqrt{-2m} \in K$ la classe de X) et $A = K_\mathbb{Z}$ l'anneau des entiers de K. (1) Soit I l'idéal de A engendré par 2 et $\sqrt{-2m}$. Montrer que $N(I) = 2$. (Indication : on pourra calculer A/I, ou bien montrer que $I^2 = 2A$).

(2) On suppose que $m > 1$. Montrer que A ne contient aucun élément de norme 2, puis que A n'est pas factoriel.

-68- (extrait de l'examen de mai 2003) Soit $f = X^3 + 3X + 1 \in \mathbb{Z}[X]$. Soient A l'anneau $\mathbb{Z}[X]/(f)$, et K l'anneau $\mathbb{Q}[X]/(f)$. On notera x la classe de X dans A, et l'on posera $y = x + 1$.

(i) Montrer que f est irréductible dans $\mathbb{Z}[X]$.

(ii) Calculer le discriminant de f.

(iii) Trouver (en en donnant des générateurs) les idéaux maximaux de A contenant 2, et donner leurs normes.

(iv) Même question pour les idéaux maximaux de A contenant 3.

(v) Soit I l'idéal $(3, y)$ de A. Montrer que $3 \in I^2$ (on pourra chercher une relation vérifiée par y).

(vi) Montrer que A est l'anneau des entiers de $\mathbb{Q}[X]/(f)$.

(vii) Quels sont les nombres premiers ramifiés dans A ?

(viii) Quelle est la décomposition de $3A$ en produit d'idéaux maximaux de A ?

-69- Soit A un anneau.

(i) Calculer $\mathrm{disc}(X^3+X^2)$.

(ii) Pour $n \in \mathbb{N}$ et $a \in A$, montrer que $\mathrm{disc}(X^n - a) = (-1)^{(n-1)(n-2)/2}\, n^n\, a^{n-1}$.

(iii) Pour $f \in A[X]$ unitaire et $a \in A$, on pose $g(X) = f(X+a)$. Calculer $\mathrm{disc}(g)$ en fonction de $\mathrm{disc}(f)$ et de a.

-70- Soit K un corps, et soient f et g unitaires dans $K[X]$.

(i) Montrer qu'il existe $r \in K$ tel que $\mathrm{disc}(fg) = r^2\,\mathrm{disc}(f)\,\mathrm{disc}(g)$. (On distinguera suivant que f et g sont ou non premiers entre eux ; s'ils le sont, on considérera $K[X]/(fg)$).

(ii) Si $B = K[X]/(f)$, montrer que l'on peut prendre $r = \mathrm{N}_{B/K}(g(x))$, où x est la classe de x. (On pourra considérer les racines de f et de g dans une extension convenable de K).

(iii) Généraliser au cas où K est un anneau quelconque.

-71- Soit $f \in \mathbb{R}[X]$ unitaire. Calculer le signe de $\mathrm{disc}(f)$ en fonction du nombre de racines réelles (resp. nulles, resp. non réelles) de f.

-72- Soient p un nombre premier, et soit q une puissance de p. On pose $f = X^q - p \in \mathbb{Z}[X]$. Montrer que f est irréductible dans $\mathbb{Z}[X]$, et que l'anneau des en,tiers de $\mathbb{Q}(\sqrt[q]{p})$ est $\mathbb{Z}[\sqrt[q]{p}]$.

-73- Soit $f = X^3 - X^2 - 1 \in \mathbb{Z}[X]$. Montrer que f est irréductible, que $\mathrm{disc}(f) = -31$, et que $\mathbb{Z}[X]/(f)$ est un anneau de Dedekind.

-74- Calculer les symboles de Legendre suivants, par exemple en utilisant la réciprocité quadratique : $(\frac{19}{229})$, $(\frac{2}{229})$, $(\frac{38}{229})$, $(\frac{51}{229})$.

-75- Soit p premier, $p > 2$.

1. 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^*.)
2. 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.
3. Montrer que $(x+1/x)^2 = 2$.
4. 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 $(x+1/x)^p = x+1/x$.)
5. Retrouver la formule du cours pour $\left(\frac{2}{p}\right)$.

-76- Le symbole de Jacobi (extrait de l'examen de septembre 2002).

On note M l'ensemble des entiers positifs impairs ; on le munit de la structure de monoïde commutatif donnée par la multiplication.

On note Σ le monoïde multiplicatif $\{0, 1, -1\}$.

On considère les applications $\chi, \omega : M \to \mathbb{Z}/2\mathbb{Z}$ définies par

$$\begin{aligned} \chi(n) &= \tfrac{n-1}{2} \mod 2 \\ \omega(n) &= \tfrac{n^2-1}{8} \mod 2. \end{aligned}$$

(1) Montrer que χ et ω sont des morphismes de monoïdes de $(M, \times)$ dans $(\mathbb{Z}/2\mathbb{Z}, +)$.

Soient a et b deux entiers, avec $b \in M$. On définit le *symbole de Jacobi* $\left(\frac{a}{b}\right) \in \Sigma$ de la façon suivante : on écrit $b = \prod_{i=1}^{r} p_i$ où les p_i sont premiers impairs, et l'on pose

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

où $\left(\frac{a}{p_i}\right) \in \Sigma$ est le symbole de Legendre. En particulier, $\left(\frac{a}{b}\right)$ coïncide avec le symbole de Legendre si b est premier.

(2) Vérifier les propriétés suivantes (en indiquant leur domaine de validité) :

(i) $\left(\frac{a}{b}\right)$ ne dépend que de la classe de a modulo b

(ii) $\left(\frac{a}{b}\right) \neq 0 \Leftrightarrow a$ et b sont premiers entre eux

(iii) $\left(\frac{a}{1}\right) = 1$ (iv) $\left(\frac{a}{bb'}\right) = \left(\frac{a}{b}\right)\left(\frac{a}{b'}\right)$

(v) $\left(\frac{1}{b}\right) = 1$ (vi) $\left(\frac{aa'}{b}\right) = \left(\frac{a}{b}\right)\left(\frac{a'}{b}\right)$

(3) Soient a et $b \in M$. Prouver les identités :

(i) $\left(\frac{-1}{b}\right) = (-1)^{\chi(b)}$ (ii) $\left(\frac{2}{b}\right) = (-1)^{\omega(b)}$ (iii) $\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\chi(a)\,\chi(b)}$.

(4) Soit $a \in \mathbb{Z}$ et soit $p > 2$ un nombre premier. Expliquer comment trouver si a est un carré modulo p, en utilisant les questions précédentes, et sans décompostition en facteurs premiers. Où sert l'hypothèse que p est premier ?

-77- 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 $\mathrm{disc}(K)$. (On pourra commencer par un exemple, disons $\mathbb{Q}(\sqrt{15})$).

On pourra exprimer les résultats à l'aide du symbole de Jacobi.

-78- Soit p un nombre premier ; on considère le polynôme cyclotomique $\Phi_p(X) = \frac{X^p-1}{X-1} = 1 + X + \ldots + X^{p-1}$.

(1) Si k est un corps de caractéristique différente de p, quelles sont les racines de Φ_p dans k ? Que se passe-t-il en caractéristique p ?

(2) Soit $l \neq p$ un nombre premier. Montrer que Φ_p a une racine dans $\mathbb{F}_l$ si et seulement si $l \equiv 1 \pmod{p}$.

(3) Montrer qu'il existe une infinité de nombres premiers congrus à 1 modulo p.

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.