THÉORIE ALGÉBRIQUE DES NOMBRES

Martin Debaisieux

Table des matières

1 Anneaux des entiers

Sauf mention contraire, tous les anneaux considérés seront tacitement supposés commutatifs et non nuls. Nous supposons également que le lecteur est familier avec l'ensemble des sujets abordés lors de l'annexe 6.

1.1 Éléments entiers

Définition 1.1. Soient A un anneau intègre et B un anneau le contenant. Un élément β de B est *entier* sur A s'il est racine d'un polynôme monique à coefficients dans A, *i.e.* s'il satisfait une équation de la forme

$$\beta^n + a_1\beta^{n-1} + \cdots + a_n = 0, \quad a_i \in A.$$

Exemple 1.2. Tout élément α d'un anneau A est entier sur A : il suffit de considérer $X - \alpha$.

Exemple 1.3. L'ensemble des éléments de $\mathbf{Q}$ entiers sur $\mathbf{Z}$ correspond précisément à l'anneau $\mathbf{Z}$: il s'agit d'un cas particulier de la proposition 1.12.

Rappel 1.4. Soient A un anneau intègre et B un anneau le contenant. Les éléments de B entiers sur A forment un sous-anneau de B, contenant A.

Définition 1.5. Soient A un anneau intègre et L un corps le contenant A. L'anneau des éléments de L entiers sur A porte le nom de *clôture intégrale* de A dans L. La clôture intégrale de $\mathbf{Z}$ dans un corps de nombres L (*i.e.* une extension finie de $\mathbf{Q}$) est appelée *anneau des entiers* de L et est notée $\mathcal{O}_L$.

Proposition 1.6. *Soit K le corps des fractions d'un anneau intègre A et soit L un corps le contenant. Si $\alpha \in L$ est algébrique sur K, alors il existe un $d \in A$ non nul tel que $d\alpha$ est entier sur A.*

Démonstration. Par hypothèse, l'élément α satisfait une équation de la forme

$$\alpha^m + a_1\alpha^{m-1} + \cdots + a_m = 0, \quad a_i \in K.$$

Soit d un dénominateur commun aux a_i, de manière à ce chaque da_i soit dans A. En multipliant l'équation précédente par d^m, il s'en suit que

$$(d\alpha)^m + a_1 d(d\alpha^{m-1}) + \cdots + a_m d^m = 0.$$

Puisque les coefficients $a_1 d, \ldots, a_m d^m$ sont des éléments de A, $d\alpha$ est entier sur A. □

Corollaire 1.7. *Soit A un anneau intègre dont le corps des fractions est noté K et soit B la clôture intégrale de A dans un corps L contenant K. Si L est une extension algébrique de K, alors il s'agit du corps des fractions de B.*

Démonstration. La proposition précédente implique que tout élément $\alpha \in L$ s'écrit sous la forme $\alpha = \beta/d$ avec $\beta \in B$ et $d \in A$, montrant que L est contenu dans le corps des fractions de B. Puisque ce dernier est le plus petit corps contenant B, l'égalité s'en suit. □

Remarque 1.8. Ce dernier corollaire nous indique que L est le corps des fractions de $\mathcal{O}_L$ pour tout corps de nombres L.

Proposition 1.9. *Soient A un anneau intègre et B sa clôture intégrale dans une extension finie L de son corps des fractions K. Soit S un sous-ensemble multiplicatif de A. L'anneau $S^{-1}B$ est la clôture intégrale de $S^{-1}A$ dans L.*

Démonstration. Soit x un élément de $S^{-1}B$, dès lors il existe un $s \in S$ tel que $sx \in B$ et cet élément est racine d'un polynôme monique à coefficients dans A. Soit n le degré de ce polynôme ; en divisant ses coefficients par s^n, nous obtenons que x est entier sur $S^{-1}A$. Réciproquement, tout élément $x \in L$ entier sur $S^{-1}A$ est racine d'un polynôme monique à coefficients a_i dans $S^{-1}A$. Dès lors, en considérant un dénominateur commun $s \in S$ aux a_i, il s'en suit que sx est entier sur A et donc que $sx \in B$; par conséquent $(sx)/s = x \in S^{-1}B$. □

Définition 1.10. Un anneau est *intégralement clos* s'il est sa propre clôture intégrale dans son corps des fractions.

Exemple 1.11. L'anneau $\mathbf{Z}[\sqrt{5}]$ n'est pas intégralement clos : $(1+\sqrt{5})/2 \in \mathbf{Q}(\sqrt{5})$ est racine du polynôme $X^2 - X - 1 \in \mathbf{Z}[X]$ et est donc entier sur $\mathbf{Z}$; or $(1+\sqrt{5})/2$ n'est pas un élément de $\mathbf{Z}[\sqrt{5}]$.

Proposition 1.12. *Tout anneau factoriel est intégralement clos.*

Démonstration. Soit A un anneau factoriel et considérons a/b un élément de son corps des fractions, entier sur A et mis sous sa forme irréductible. Si b est inversible dans A, alors a/b est un élément de A. Sinon, il existe un irréductible $\pi \in A$ divisant b mais pas a. Comme a/b est entier sur A, il satisfait une équation

$$(a/b)^n + a_1(a/b)^{n-1} + \cdots + a_n = 0, \quad a_i \in A$$

et en la multipliant par b^n, nous obtenons une nouvelle équation montrant que π divise a^n, ce qui est absurde puisque π ne divise pas a. Ainsi b se doit d'être inversible. □

Remarque 1.13. Cette proposition est un moyen efficace de mettre en évidence les anneaux non factoriels. Par exemple, nous savons que l'anneau $\mathbf{Z}[\sqrt{5}]$ n'est pas intégralement clos ; de ce fait il n'est pas non plus factoriel.

Exemple 1.14. Les anneaux $\mathbf{Z}$ et $\mathbf{Z}[i]$ sont intégralement clos puisqu'ils sont tous deux des factoriels. Il s'agit respectivement de la clôture intégrale de $\mathbf{Z}$ dans $\mathbf{Q}$ et $\mathbf{Q}(i)$.

Exemple 1.15. Tout corps k est intégralement clos. De même, tout anneau de polynômes $k[X]$ sur un corps k est principal et est donc intégralement clos.

Remarque 1.16. La réciproque de la proposition 1.12 est cependant fausse : $\mathbf{Z}[i\sqrt{5}]$ est intégralement clos mais il n'est pas factoriel étant donné la décomposition non unique de 6 en 2×3 et en $(1+i\sqrt{5}) \times (1-i\sqrt{5})$.

Remarque 1.17. Le contre-exemple 1.11 et la remarque 1.16 permettent ensemble de justifier les inclusions strictes suivantes :

$$\{\text{anneaux factoriels}\} \subset \{\text{anneaux intégralement clos}\} \subset \{\text{anneaux intègres}\}.$$

Proposition 1.18. *Soit K le corps des fractions d'un anneau intègre A et soit L une extension finie de K. Supposons que A soit intégralement clos. Un élément α de L est entier sur A si et seulement si son polynôme minimal sur K est à coefficients dans A.*

Démonstration. La suffisance est triviale. Pour la nécessité, soit $\alpha \in L$ un élément entier sur A ; alors il satisfait

$$\alpha^m + a_1\alpha^{m-1} + \cdots + a_m = 0, \quad a_i \in A.$$

Considérons $f(X)$ le polynôme minimal de α sur K et soit α' l'une des racines de $f(X)$. Ainsi, il existe un K-isomorphisme $\sigma\colon K(\alpha) \to K(\alpha')$ envoyant α sur α'. L'application de σ à l'équation précédente fournit que

$$\alpha'^m + a_1\alpha'^{m-1} + \cdots + a_m = 0,$$

montrant que α' est également entier sur A. De cette manière, toutes les racines de $f(X)$ sont entières sur A et donc les coefficients de $f(X)$ le sont aussi par 1.4. Il s'agit en outre d'éléments de K et A est intégralement clos ; par conséquent ceux sont des éléments de A et cela conclut la preuve. □

Lemme 1.19. *Soit $A \subseteq B \subseteq C$ une tour d'extensions d'anneaux. Si B est de type fini en tant que A-module et si C est de type fini en tant que B-module, alors C est de type fini en tant que A-module.*

Démonstration. Si $(\beta_1, \ldots, \beta_m)$ est une suite génératrice de B en tant que A-module et $(\gamma_1, \ldots, \gamma_n)$ est une suite génératrice de C en tant que B-module, alors $(\beta_i\gamma_j)_{i,j}$ est une suite génératrice de C en tant que A-module. □

Proposition 1.20. *Si B est entier sur A et de type fini en tant que A-algèbre, alors il est de type fini en tant que A-module.*

Démonstration. Supposons tout d'abord que B est généré en tant que A-algèbre par un élément, disons $B = A[\beta]$. Par hypothèse, β est entier sur A et satisfait donc une équation de la forme

$$\beta^n + a_1\beta^{n-1} + \cdots + a_n = 0, \quad a_i \in A.$$

Tout élément de B peut alors être exprimé comme une somme finie

$$c_0 + c_1\beta + c_2\beta^2 + \cdots + c_N\beta^N, \quad c_i \in A$$

et nous pouvons avoir recours à l'égalité précédente afin de remplacer successivement β^n par une combinaison linéaire de puissances inférieures de β. Ainsi, tout élément de B peut s'exprimer comme une somme finie

$$c_0 + c_1\beta + c_2\beta^2 + \cdots + c_{n-1}\beta^{n-1}, \quad c_i \in A$$

et donc la suite $(1, \beta, \beta^2, \ldots, \beta^{n-1})$ engendre B en tant que A-module. Supposons désormais que $(\beta_1, \ldots, \beta_m)$ engendre B en tant que A-algèbre et considérons la chaîne d'inclusion

$$A \subseteq A[\beta_1] \subseteq A[\beta_1, \beta_2] \subseteq \cdots \subseteq A[\beta_1, \ldots, \beta_m] = B.$$

Donc $A[\beta_1]$ est de type fini en tant que A-module. Étant donné que $A[\beta_1, \beta_2] = A[\beta_1][\beta_2]$ et que β_2 est entier sur $A[\beta_1]$ car il contient A, le même raisonnement montre que $A[\beta_1, \beta_2]$ est de type fini en tant que $A[\beta_1]$-module. Le lemme précédent fournit que $A[\beta_1, \beta_2]$ est de type fini en tant que A-module. En procédant de la même manière, nous obtenons que B est de type fini en tant que A-module. □

Rappel 1.21. Soit $A \subseteq B \subseteq C$ une tour d'extensions d'anneaux intègres. Si B est entier sur A et si C est entier sur B, alors C est entier sur A.

Proposition 1.22. *La clôture intégrale de A dans une extension algébrique L de son corps des fractions est intégralement close.*

Démonstration. Désignons par B la clôture intégrale de A dans L et par C la clôture intégrale de B dans L. Alors C est entière sur A et donc $C \subseteq B$. La réciproque est directe. □

Remarque 1.23. En particulier, l'anneau des entiers d'un corps de nombres est intégralement clos. Il s'agit d'une propriété à laquelle nous tenons étant donné que nous voulons que l'anneau des entiers ait le plus de chance d'être un anneau factoriel (cfr proposition 1.12).

1.2 Exemple : les entiers des corps quadratiques

Définition 1.24. Un *corps quadratique* est un corps de la forme $\mathbf{Q}(\sqrt{d})$, où $d \in \mathbf{Z}$ est sans facteurs carrés.

Remarque 1.25. Il est d'usage d'appeler les entiers $d \in \mathbf{Z}$ qui ne sont divisibles par aucun carré parfait (excepté 1) par entiers sans facteurs carrés. En particulier, des tels éléments satisfont $d \not\equiv 0 \bmod 4\mathbf{Z}$. De manière à exclure le cas où $d = 1$, puisqu'il ne s'agit alors pas d'une extension quadratique de $\mathbf{Q}$, nous ferons également l'hypothèse que $d \neq 1$.

Proposition 1.26. *Soit $\mathbf{Q}(\sqrt{d})$ un corps quadratique.*

(i) Si $d \equiv 2, 3 \bmod 4\mathbf{Z}$, alors l'anneau des entiers de $\mathbf{Q}(\sqrt{d})$ est $\mathbf{Z}[\sqrt{d}]$.

(ii) Si $d \equiv 1 \bmod 4\mathbf{Z}$, alors l'anneau des entiers de $\mathbf{Q}(\sqrt{d})$ est $\mathbf{Z}[(1+\sqrt{d})/2]$.

Démonstration. Remarquons tout d'abord que si x est entier sur $\mathbf{Z}$, alors son conjugué $\sigma(x)$ l'est aussi, où σ est déterminée par $\sqrt{d} \mapsto -\sqrt{d}$. Comme les éléments entiers forment un anneau, $x+\sigma(x)$ et $x\sigma(x)$ sont entiers. Or, en notant $x = a + b\sqrt{d}$ avec a, $b \in \mathbf{Q}$, nous constatons que $x + \sigma(x) = 2a \in \mathbf{Q}$ et $x\sigma(x) = a^2 - db^2 \in \mathbf{Q}$. Comme $\mathbf{Z}$ est intégralement clos, $2a \in \mathbf{Z}$ et $a^2 - db^2 \in \mathbf{Z}$. Ces conditions sont nécessaires pour que x soit entier sur $\mathbf{Z}$; elles sont également suffisantes car alors x est racine de

$$X^2 - 2aX + a^2 - db^2 \in \mathbf{Z}[X].$$

Nous avons également que $(2a)^2 - d(2b)^2 \in \mathbf{Z}$ et, comme $2a \in \mathbf{Z}$, il s'en suit que $d(2b)^2 \in \mathbf{Z}$. Or d est sans facteurs carrés ; si $2b$ n'était pas entier, son dénominateur comporterait un facteur premier p, ce facteur apparaîtrait sous la forme p^2 dans $(2b)^2$ et la multiplication par d ne pourrait pas le ramener dans $\mathbf{Z}$. Par conséquent $2b \in \mathbf{Z}$. Grâce à cela, nous pouvons supposer que $a = u/2$ et $b = v/2$ avec u, $v \in \mathbf{Z}$. Notre condition nécessaire et suffisante revient alors à demander que $u^2 - dv^2 \in 4\mathbf{Z}$. Dès lors, si v est pair, u l'est aussi et donc a, $b \in \mathbf{Z}$. Si v est impair, $v^2 \equiv 1 \bmod 4\mathbf{Z}$; or la classe de $u^2 \bmod 4\mathbf{Z}$ est 0 ou 1 et comme d est sans facteurs carrés, il n'est pas multiple de 4. Nécessairement $u^2 \equiv 1 \bmod 4\mathbf{Z}$ et $d \equiv 1 \bmod 4\mathbf{Z}$. □

Remarque 1.27. Un corps quadratique $\mathbf{Q}(\sqrt{d})$ est dit **réel** lorsque $d > 1$ (puisqu'il est contenu dans $\mathbf{R}$) et **imaginaire** lorsque $d < 0$.

1.3 Exemple : les entiers de Gauss

Cette sous-section est motivée par la recherche d'une caractérisation des nombres premiers impairs pouvant s'écrire comme somme de deux carrés parfaits (voir théorème 1.31). Cette question trouve sa réponse en explorant l'anneau des entiers de Gauss : dans celui-ci, une telle équation $p = a^2 + b^2$ se réécrit en $p = (a+bi)(a-bi)$, réduisant le problème en une détermination du comportement de p dans l'anneau $\mathbf{Z}[i]$.

Rappel 1.28. L'anneau des entiers de Gauss $\mathbf{Z}[i] = \{a+bi \mid a, b \in \mathbf{Z}\}$ est principal ; il est en particulier factoriel.

Remarque 1.29. L'anneau $\mathbf{Z}[i]$ peut être muni d'une application multiplicative, notée Nm et appelée *norme* ; dont la définition est donnée par

$$\mathrm{Nm}\colon \left\{ \begin{array}{ccc} \mathbf{Z}[i] & \longrightarrow & \mathbf{N} \\ a+bi & \longmapsto & a^2+b^2. \end{array} \right.$$

Cette application rend l'anneau $\mathbf{Z}[i]$ euclidien. Le concept de norme sera généralisé et formalisé au cours de la section suivante.

Lemme 1.30. *Un élément α de $\mathbf{Z}[i]$ est inversible si et seulement s'il est de norme* 1.

Démonstration. Lorsque nous supposons l'existence d'un inverse β dans $\mathbf{Z}[i]$ pour α, il s'en suit que

$$1 = \mathrm{Nm}(1) = \mathrm{Nm}(\alpha\beta) = \mathrm{Nm}(\alpha)\,\mathrm{Nm}(\beta)$$

et par conséquent $\mathrm{Nm}(\alpha) = \mathrm{Nm}(\beta) = 1$ puisque ces quantités sont naturelles. Réciproquement, en notant $\alpha = a + bi$ avec a, $b \in \mathbf{Z}$, il suffit de constater que le conjugué de α joue le rôle d'inverse de α et donc $\alpha\overline{\alpha} = \mathrm{Nm}(\alpha) = 1$. □

Théorème 1.31. *Soit $p \in \mathbf{Z}$ un nombre premier impair ; alors*

$$p = a^2 + b^2 \ \ \textit{pour } a, b \in \mathbf{Z} \quad \textit{ssi} \quad p \equiv 1 \bmod 4\mathbf{Z}.$$

Démonstration. Pour la nécessité, remarquons que tout carré parfait est congrue à 0 mod $4\mathbf{Z}$ ou 1 mod $4\mathbf{Z}$. Dès lors, puisque $p = a^2 + b^2$ et qu'il s'agit d'un nombre premier impair,

$$p \equiv 1 \bmod 4\mathbf{Z}.$$

Réciproquement, il suffit de montrer que p n'est plus un nombre premier dans $\mathbf{Z}[i]$: nous aurons alors que $p = \alpha\beta$ pour deux non inversibles de $\mathbf{Z}[i]$ et donc $p^2 = \mathrm{Nm}(\alpha)\,\mathrm{Nm}(\beta)$. Via le lemme 1.30, nous savons que $\mathrm{Nm}(\alpha)$ et $\mathrm{Nm}(\beta)$ sont distincts de 1 ; ils constituent ainsi une factorisation de p^2 dans $\mathbf{Z}$. Ainsi, $p = \mathrm{Nm}(\alpha) = \mathrm{Nm}(\beta)$ et donc $p = a^2 + b^2$ où les coefficients proviennent de $\alpha = a + bi$. Vérifions donc que $p = 1 + 4n$ n'est pas premier dans $\mathbf{Z}[i]$. Notons que l'équation $-1 \equiv x^2 \bmod p\mathbf{Z}$ possède une solution, à savoir $x = (2n)!$: selon le théorème de Wilson [Wil], $-1 \equiv (p-1)! \bmod p\mathbf{Z}$ et donc

$$\begin{aligned} -1 \equiv (p-1)! &= [1 \times 2 \times \cdots \times 2n][(p-1) \times \cdots \times (p-2n)] \\ &\equiv [(2n)!][(-1)^{2n}(2n)!] \\ &= [(2n)!]^2 \bmod p\mathbf{Z}. \end{aligned}$$

Ainsi p divise $x^2 + 1 = (x+i)(x-i)$, cependant $x/p \pm i/p$ n'est pas un élément de $\mathbf{Z}[i]$ et donc p ne divise ni $(x+i)$, ni $(x-i)$; il n'est dès lors plus premier dans $\mathbf{Z}[i]$. □

Proposition 1.32. *Le groupe des inversibles de l'anneau $\mathbf{Z}[i]$ est constitué des racines quatrièmes de l'unité :*

$$\mathbf{Z}[i]^\times = \{1, -1, i, -i\}.$$

Démonstration. Via le lemme 1.30, un élément $\alpha = a + bi \in \mathbf{Z}[i]$ est inversible si et seulement sa norme $\mathrm{Nm}(\alpha) = a^2 + b^2 = 1$, ou encore si et seulement si $a^2 = 1$, $b^2 = 0$ ou $a^2 = 0$, $b^2 = 1$; permettant ainsi de conclure. □

Proposition 1.33. *Les éléments premiers π de $\mathbf{Z}[i]$ sont à inversible près les éléments figurants dans la liste suivante :*

(i) $\pi = 1 + i$,

(ii) $\pi = a + bi$ *avec* $a^2 + b^2 = p$, $p \equiv 1 \bmod 4\mathbf{Z}$, $a > |b| > 0$, *et*

(iii) $\pi = p$ *avec* $p \equiv 3 \bmod 4\mathbf{Z}$

où $p \in \mathbf{Z}$ est un nombre premier.

Démonstration. Les éléments en (i) et (ii) sont premiers puisque qu'une décomposition $\pi = \alpha\beta$ dans $\mathbf{Z}[i]$ implique que $p = \mathrm{Nm}(\pi) = \mathrm{Nm}(\alpha)\,\mathrm{Nm}(\beta)$ pour un certain nombre premier p. Dès lors, soit $\mathrm{Nm}(\alpha) = 1$, soit $\mathrm{Nm}(\beta) = 1$ et donc α ou β est inversible. Les éléments $\pi = p$ où $p \equiv 3 \bmod 4\mathbf{Z}$ sont premiers dans $\mathbf{Z}[i]$ puisqu'une décomposition $p = \alpha\beta$ par deux non inversibles α, β mène à $p^2 = \mathrm{Nm}(\alpha)\,\mathrm{Nm}(\beta)$ et donc, par un argument précédent, à $p = \mathrm{Nm}(\alpha) = a^2 + b^2$ où $\alpha = a + bi$. Le théorème 1.31 implique alors que $p \equiv 1 \bmod 4\mathbf{Z}$.

Employons la terminologie suivante : deux éléments sont associés s'il diffèrent d'un facteur inversible. Il nous reste donc à montrer que tout élément premier π de $\mathbf{Z}[i]$ est associé à l'un des éléments de la liste précédemment constituée. La factorisation dans $\mathbf{Z}$:

$$\mathrm{Nm}(\pi) = \pi \cdot \overline{\pi} = p_1 \cdots p_n$$

où $p_1, \ldots, p_n \in \mathbf{Z}$ sont des nombres premiers, implique que π divise un certain $p := p_j$. Ainsi, $\mathrm{Nm}(\pi)$ divise $\mathrm{Nm}(p) = p^2$ et donc soit $\mathrm{Nm}(\pi) = p$, soit $\mathrm{Nm}(\pi) = p^2$. Dans le premier cas, $\pi = a + bi$ avec $a^2 + b^2 = p$ et alors π est du type (ii) ; ou si $p = 2$, il est associé à $1 + i$. Dans le deuxième cas, π est associé à p puisque p/π est un élément de $\mathbf{Z}$ de norme 1 et est donc inversible. De plus $p \equiv 3 \bmod 4\mathbf{Z}$, sinon $p = 2$ ou $p \equiv 1 \bmod 4\mathbf{Z}$ et par le théorème 1.31, $p = a^2 + b^2 = (a + bi)(a - bi)$ ne pourrait être premier. □

1.4 Traces et normes

Soient deux anneaux $A \subseteq B$ dans lequel B est un A-module libre de rang n. Tout élément β de B définit un endomorphisme A-linéaire

$$m_\beta \colon B \longrightarrow B \colon x \longmapsto \beta x.$$

En considérant C une A-base de B, nous pouvons associer à m_β sa représentation matricielle ; que nous désignerons par $M_C(m_\beta) \in \mathrm{M}_n(A)$.

Exemple 1.34. Soit $d \in \mathbf{Z}$ sans facteurs carrés et supposons dans un premier temps que $d \equiv 2, 3 \bmod 4\mathbf{Z}$. Intéressons-nous à l'extension $\mathbf{Z}[\sqrt{d}]/\mathbf{Z}$ dont une base B est $(1, \sqrt{d})$. Soit $\beta = a + b\sqrt{d}$ un élément de $\mathbf{Z}[\sqrt{d}]$; les coordonnées de β et $\beta\sqrt{d}$ dans la base B sont respectivement (a, b) et (bd, a). De ces égalités, nous en déduisons la représentation matricielle de m_β dans la base B :

$$M_B(m_\beta) = \begin{pmatrix} a & bd \\ b & a \end{pmatrix}.$$

Exemple 1.35. Soit $d \in \mathbf{Z}$ sans facteurs carrés et cette fois-ci faisons l'hypothèse que $d \equiv 1 \bmod 4\mathbf{Z}$. Considérons l'extension $\mathbf{Z}[(1 + \sqrt{d})/2]/\mathbf{Z}$ dont une base B est donnée par $(1, (1 + \sqrt{d})/2)$. Soit $\beta = a + b(1 + \sqrt{d})/2$ un élément de $\mathbf{Z}[(1 + \sqrt{d})/2]$; les coordonnées de β et $\beta(1 + \sqrt{d})/2$ dans la base B sont respectivement (a, b) et $((bd - b)/4, a + b)$. Nous en déduisons la représentation matricielle de m_β dans la base B :

$$M_B(m_\beta) = \begin{pmatrix} a & (bd - b)/4 \\ b & a + b \end{pmatrix}.$$

Définition 1.36. La *trace* et la *norme* de β dans l'extension B/A sont respectivement la trace et le déterminant de l'endomorphisme A-linéaire de multiplication par β :

$$\mathrm{Tr}_{B/A}(\beta) := \mathrm{Tr}(m_\beta) \in A \quad \text{et} \quad \mathrm{Nm}_{B/A}(\beta) := \det(m_\beta) \in A.$$

Remarque 1.37. Si $(e_1, \ldots, e_n)$ est une base de l'extension B/A et si chaque βe_i s'écrit comme $\beta e_i = \sum a_{ij} e_j$, alors

$$\mathrm{Tr}_{B/A}(\beta) = \sum_{i=1}^{n} a_{ii} \quad \text{et} \quad \mathrm{Nm}_{B/A}(\beta) = \det(a_{ij})_{ij}.$$

Noter également que ces notions sont indépendantes du choix de la base.

Exemple 1.38. Soit $d \in \mathbf{Z}$ sans facteurs carrés et tel que $d \equiv 2, 3 \bmod 4\mathbf{Z}$. Considérons un élément $a + b\sqrt{d}$ de $\mathbf{Z}[\sqrt{d}]$. L'exemple 1.34 nous permet d'affirmer que sa trace vaut $\mathrm{Tr}(a + b\sqrt{d}) = 2a$ et que sa norme vaut $\mathrm{Nm}(a + b\sqrt{d}) = a^2 - b^2 d$. Noter qu'en prenant $d = -1$, nous obtenons la définition de norme sur $\mathbf{Z}[i]$ donnée lors de la section précédente.

Exemple 1.39. Soit $d \in \mathbf{Z}$ sans facteurs carrés et supposons que $d \equiv 1 \bmod 4\mathbf{Z}$. Soit un élément $\beta = a + b(1 + \sqrt{d})/2$ de $\mathbf{Z}[(1 + \sqrt{d})/2]$. L'exemple 1.35 nous fournit que sa trace vaut $\mathrm{Tr}(\beta) = 2a + b$ et que sa norme vaut $\mathrm{Nm}(\beta) = a^2 + ab - (b^2 d - b^2)/4$.

Propriété 1.40. *La trace $\mathrm{Tr}_{B/A} \colon B \to A$ est une application A-linéaire. Elle satisfait en particulier, pour tous β, $\beta' \in B$ et $a \in A$:*

$$\mathrm{Tr}(\beta + \beta') = \mathrm{Tr}(\beta) + \mathrm{Tr}(\beta'), \quad \mathrm{Tr}(a\beta) = a\,\mathrm{Tr}(\beta) \quad \textit{et} \quad \mathrm{Tr}(a) = na.$$

Propriété 1.41. *La norme $\mathrm{Nm}_{B/A} \colon B \to A$ est une application multiplicative. Elle satisfait en particulier, pour tous β, $\beta' \in B$ et $a \in A$:*

$$\mathrm{Nm}(\beta\beta') = \mathrm{Nm}(\beta) \cdot \mathrm{Nm}(\beta') \quad \textit{et} \quad \mathrm{Nm}(a) = a^n.$$

Proposition 1.42. *Soit L/k une extension finie de corps, de degré n et soit β un élément de L. Si $f(X)$ désigne le polynôme minimal de β sur k et si $\beta_1 = \beta, \beta_2, \ldots, \beta_m$ sont les racines de $f(X)$ dans un corps algébriquement clos contenant L ; alors*

$$\mathrm{Tr}_{L/k}(\beta) = r(\beta_1 + \cdots + \beta_m) \quad et \quad \mathrm{Nm}_{L/k}(\beta) = (\beta_1 \cdots \beta_m)^r$$

où $r = [L : k(\beta)] = n/m$.

Démonstration. Si $L = k(\beta)$, la matrice de m_β dans la base $B = (1, \beta_1, \cdots, \beta_{n-1})$ de L/k est précisément la matrice compagnon du polynôme $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$:

$$M_B(m_\beta) = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}.$$

Par la formule de la somme et du produit des racines d'un polynôme, la trace est $\beta_1 + \cdots + \beta_n$ et la norme est $\beta_1 \cdots \beta_n$. Le cas général s'obtient par transitivité de la trace et de la norme [Con, §4, thm.1&2]. □

Corollaire 1.43. *Si L/k est une extension finie et séparable de degré n et si $\{\sigma_1, \ldots, \sigma_n\}$ désigne l'ensemble des k-plongements de L dans sa clôture galoisienne ; alors*

$$\mathrm{Tr}_{L/k}(\beta) = \sigma_1(\beta) + \cdots + \sigma_n(\beta) \quad et \quad \mathrm{Nm}_{L/k}(\beta) = \sigma_1(\beta) \cdots \sigma_n(\beta).$$

Démonstration. Chaque β_i apparaît exactement r fois dans la famille $(\sigma_i\beta)_{i=1}^n$. □

Exemple 1.44. Soit $\mathbf{Q}(\sqrt{d})$ un corps quadratique ; puisque toute extension quadratique est galoisienne, le calcul de la trace et de la norme d'un élément s'effectue plus rapidement de la manière suivante : il suffit de déterminer les deux $\mathbf{Q}$-automorphismes de $\mathbf{Q}(\sqrt{d})$, à savoir $\sqrt{d} \mapsto \sqrt{d}$ et $\sqrt{d} \mapsto -\sqrt{d}$.

Exemple 1.45. Soit $p \in \mathbf{Z}$ un nombre premier impair. L'extension $\mathbf{Q}(\zeta_p)/\mathbf{Q}$ est galoisienne, de degré $p - 1$. Dès lors, pour tout $1 \leq j \leq p - 1$,

$$\mathrm{Tr}(\zeta_p^j) = \sum_{i=1}^{p-1} \zeta_p^i = -1 \quad \text{et} \quad \mathrm{Nm}(\zeta_p^j) = \prod_{i=1}^{p-1} \zeta_p^i = \zeta_p^{\frac{(p-1)p}{2}} = 1.$$

Corollaire 1.46. *Soit A un anneau intégralement clos dont le corps des fractions est noté K et soit L une extension finie de K. Si $\beta \in L$ est entier sur A, alors $\mathrm{Tr}_{L/K}(\beta)$ et $\mathrm{Nm}_{L/K}(\beta)$ sont des éléments de A.*

Démonstration. Au moyen de la proposition 1.18, nous pouvons affirmer que si β est entier sur A, alors ses conjugés le sont aussi. Finalement, le fait que A soit intégralement clos permet d'affirmer que tous les conjugés de β (y compris β) sont des éléments de A. □

1.5 Discriminants

Soit L/k une extension finie de corps. En voyant L en tant que k-espace vectoriel, l'application

$$L \times L \longrightarrow k \colon (\alpha, \beta) \longmapsto \mathrm{Tr}_{L/K}(\alpha\beta)$$

est une forme bilinéaire symétrique sur L et le discriminant associé à cette forme est appelé *discriminant* de L/k. Plus généralement :

Définition 1.47. Soient $A \subseteq B$ deux anneaux dans lequel B est un A-module libre de rang m. Le *discriminant* de la suite $(\beta_1, \ldots, \beta_m) \in B^m$ est l'élément de A défini par

$$\mathrm{Disc}_{B/A}(\beta_1, \ldots, \beta_m) = \det \begin{pmatrix} \mathrm{Tr}_{B/A}(\beta_1^2) & \cdots & \mathrm{Tr}_{B/A}(\beta_1\beta_m) \\ \vdots & \ddots & \vdots \\ \mathrm{Tr}_{B/A}(\beta_m\beta_1) & \cdots & \mathrm{Tr}_{B/A}(\beta_m^2) \end{pmatrix}.$$

Exemple 1.48. Soit L une extension quadratique d'un corps k et soit $\alpha \in L \smallsetminus k$; de manière à avoir $L = k(\alpha)$. Considérons le polynôme minimal de α sur k : $X^2 + bX + c$. Alors $\mathrm{Tr}_{L/k}(1) = 2$, $\mathrm{Tr}_{L/k}(\alpha) = -b$ et $\mathrm{Tr}_{L/k}(\alpha^2) = \mathrm{Tr}_{L/k}(-b\alpha - c) = b^2 - 2c$. Par conséquent,

$$\mathrm{Disc}_{L/k}(1, \alpha) = \det \begin{pmatrix} \mathrm{Tr}_{L/k}(1) & \mathrm{Tr}_{L/k}(\alpha) \\ \mathrm{Tr}_{L/k}(\alpha) & \mathrm{Tr}_{L/k}(\alpha^2) \end{pmatrix} = b^2 - 4c$$

coïncidant avec l'appellation classique de discriminant du polynôme $X^2 + bX + c$.

Remarque 1.49. La remarque 6.32 montre que si $(\gamma_1, \ldots, \gamma_m) \in B^m$ est une suite telle que chaque $\gamma_j = \sum_{i=1}^m a_{ij}\beta_j$ avec les coefficients a_{ij} dans A, alors

$$\mathrm{Disc}_{B/A}(\gamma_1, \ldots, \gamma_m) = (\det(a_{ij})_{ij})^2 \ \mathrm{Disc}_{B/A}(\beta_1, \ldots, \beta_m).$$

Dès lors, si $(\beta_1, \ldots, \beta_n)$ et $(\gamma_1, \ldots, \gamma_n)$ sont deux A-bases de B, alors $\det(a_{ij})_{ij}$ est inversible dans A. La notion de discriminant d'une base est par conséquent unique à multiplication par le carré d'un inversible de A près. L'idéal qu'il engendre dans A est donc indépendant du choix de la base de B ; venant justifier la légitimité de la définition suivante :

Définition 1.50. Sous les hypothèses de la définition 1.47, le *discriminant* de B/A est l'idéal principal de A engendré par le discriminant de n'importe quelle base de B sur A ; celui-ci est noté $\Delta(B/A)$.

Remarque 1.51. Cette notion est triviale quand il s'agit d'extensions de corps. Lorsque nous parlerons du discriminant d'un corps de nombres L, nous ferons allusion au discriminant de $\mathcal{O}_L/\mathbf{Z}$ (légitimé par la proposition 1.59). Puisque 1 est le seul carré inversible dans $\mathbf{Z}$, nous noterons l'unique générateur de $\Delta(\mathcal{O}_L/\mathbf{Z})$ par Δ_L.

Exemple 1.52. Soit $d \in \mathbf{Z}$ sans facteurs carrés tel que $d \equiv 2, 3 \bmod 4\mathbf{Z}$ et déterminons le discriminant de l'extension $\mathbf{Q}(\sqrt{d})/\mathbf{Z}$. De par nos conventions, il faut calculer le discriminant de $\mathbf{Z}[\sqrt{d}]/\mathbf{Z}$:

$$\Delta_{\mathbf{Q}(\sqrt{d})} = \mathrm{Disc}_{\mathbf{Z}[\sqrt{d}]/\mathbf{Z}}(1, \sqrt{d}) = \det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} = 4d.$$

Exemple 1.53. Soit $d \in \mathbf{Z}$ sans facteurs carrés tel que $d \equiv 1 \bmod 4\mathbf{Z}$ et déterminons le discriminant de l'extension $\mathbf{Q}(\sqrt{d})/\mathbf{Q}$. Cette fois-ci, l'anneau des entiers de $\mathbf{Q}(\sqrt{d})$ est $\mathbf{Z}[(1+\sqrt{d})/2]$ et donc :

$$\Delta_{\mathbf{Q}(\sqrt{d})} = \mathrm{Disc}_{\mathbf{Z}[(1+\sqrt{d})/2]/\mathbf{Z}}(1, (1+\sqrt{d})/2) = \det \begin{pmatrix} 2 & 1 \\ 1 & (d+1)/2 \end{pmatrix} = d.$$

Proposition 1.54. *Soient $A \subseteq B$ deux anneaux intègres dans lequel B est un A-module libre de rang m. Supposons que $\Delta(B/A)$ est non nul. La suite $(\gamma_1, \ldots, \gamma_m)$ est une base de B en tant que A-module si et seulement si*

$$(\mathrm{Disc}_{B/A}(\gamma_1, \ldots, \gamma_m)) = \Delta(B/A)$$

en tant qu'idéaux de A.

Démonstration. Soit $(\beta_1, \ldots, \beta_m)$ une base de B en tant que A-module et soient $\gamma_1, \ldots, \gamma_m$ des éléments de B. Notons chaque $\gamma_j = \sum a_{ji}\beta_i$ avec les coefficients $a_{ji} \in A$. Alors

$$\mathrm{Disc}_{B/A}(\gamma_1, \ldots, \gamma_m) = (\det(a_{ij})_{ij})^2 \ \mathrm{Disc}_{B/A}(\beta_1, \ldots, \beta_m),$$

et $(\gamma_1, \ldots, \gamma_m)$ une base de B si et seulement si $\det(a_{ij})_{ij}$ est inversible. □

Remarque 1.55. Avec $A = \mathbf{Z}$, les éléments $\gamma_1, \ldots, \gamma_m$ engendrent un sous-module N de B d'indice fini si et seulement si $\mathrm{Disc}(\gamma_1, \ldots, \gamma_m)$ est non nul, auquel cas

$$(\mathrm{Disc}(\gamma_1, \ldots, \gamma_m)) = (B : N)^2 \, \Delta(B/\mathbf{Z}).$$

Proposition 1.56. *Soit L/k une extension de corps séparable et finie de degré m et soit $\{\sigma_1, \ldots, \sigma_m\}$ l'ensemble des k-plongements de L dans une grande extension galoisienne Ω de L. Alors, pour toute base $(\beta_1, \ldots, \beta_m)$ de L/k :*

$$\mathrm{Disc}_{L/k}(\beta_1, \ldots, \beta_m) = \det(\sigma_i \beta_j)_{ij}^2 \neq 0.$$

Démonstration. En développant, nous obtenons que

$$\begin{aligned}\mathrm{Disc}_{L/k}(\beta_1, \ldots, \beta_m) = \det(\mathrm{Tr}(\beta_i\beta_j))_{ij} &\overset{1.43}{=} \det(\textstyle\sum_l \sigma_l(\beta_i\beta_j))_{ij} = \det(\sum_l \sigma_l(\beta_i)\sigma_l(\beta_j))_{ij} \\ &= \det(\sigma_l\beta_i)_{li} \cdot \det(\sigma_l\beta_j))_{lj} = \det(\sigma_l\beta_i)_{li}^2.\end{aligned}$$

Supposons finalement que $\det(\sigma_i\beta_j)_{ij}$ soit nul. Il existe dès lors des éléments $c_1, \ldots, c_m$ de Ω pour lesquels

$$\sum_{i=1}^{m} c_i \sigma_i(\beta_j) = 0 \quad \text{pour tout } j.$$

Par linéarité, il s'en suit que $\sum_{i=1}^m c_i\sigma_i(\beta) = 0$ pour tout $\beta \in L$ et ceci vient contredire le théorème sur l'indépendance des caractères [Mil21b, V, §4, thm.5.14]. □

Corollaire 1.57. *Soient K le corps des fractions d'un anneau intègre A et L/K une extension finie et séparable de degré m. Si la clôture intégrale B de A dans L est un A-module libre de rang m, alors $\Delta(B/A)$ est non nul.*

Démonstration. Si $(\beta_1, \ldots, \beta_m)$ est une base de B en tant que A-module, alors il s'agit également d'une base de L en tant que K-espace vectoriel. En effet, si

$$\sum_{i=1}^{m} c_i \beta_i = 0$$

où $c_1, \ldots, c_m \in K$, alors il existe $d_1, \ldots, d_m \in A^\times$ tels que chaque $d_i c_i$ appartient à B par la proposition 1.6. En posant d le produit des d_i, il s'en suit que

$$\sum_{i=1}^{m} d c_i \beta_i = 0$$

et donc que chaque $dc_i = 0$ car $(\beta_1, \ldots, \beta_m)$ est une base de B en tant que A-module. Comme d est non nul et A est intègre, chaque $a_i = 0$. Par conséquent, la quantité $\Delta(B/A)$ représente celle de $\Delta(L/K)$ et est non nulle par le résultat précédent. □

Remarque 1.58. La proposition précédente permet d'affirmer que la forme K-bilinéaire

$$L \times L \longrightarrow K \colon (\alpha, \beta) \longmapsto \mathrm{Tr}(\alpha\beta)$$

est non dégénérée ; son discriminant étant $\Delta(L/K)$.

1.6 L'anneau des entiers est de type fini

Dans cette sous-section, nous montrons que l'anneau des entiers $\mathcal{O}_L$ dans un corps de nombres L est de type fini en tant que $\mathbf{Z}$-module ; ayant pour conséquence qu'il s'agisse d'un anneau noethérien.

Proposition 1.59. *Soit A un anneau intégralement clos dont le corps des fractions est noté K et soit B la clôture intégrale de A dans une extension finie et séparable L/K de degré n. Alors il existe deux sous-A-modules libres M et M' de L tels que*

$$M \subseteq B \subseteq M'.$$

Par conséquent, B est de type fini en tant que A-module si A est noethérien, et il est libre de rang n si A est un anneau principal.

Démonstration. Soit $(\beta_1, \dots, \beta_m)$ une base de L sur K. Selon la proposition 1.6, il existe un $d \in A$ non nul tel que $d\beta_i \in B$ pour tout i. Alors $(d\beta_1, \dots, d\beta_m)$ est une base de L sur K et nous pouvons donc supposer que chaque $\beta_i \in B$. Comme l'application $(x, y) \mapsto \mathrm{Tr}(x, y)$ est non dégénérée, il existe une base duale $(\beta'_1, \dots, \beta'_m)$ de L sur K telle que $\mathrm{Tr}(\beta_i \beta'_j) = \delta_{ij}$ (via la remarque 6.34) ; alors

$$M := A\beta_1 + \cdots + A\beta_m \subseteq B \subseteq A\beta'_1 + \cdots + A\beta'_m =: M'.$$

La première inclusion résulte de la discussion débutant la preuve. Pour la seconde, soit $\beta \in B$; alors il peut s'écrire comme combinaison linéaire $\beta = \sum b_j \beta'_j$ des β'_j et à coefficients $b_j \in K$. Il reste à montrer que ces coefficients sont des éléments de A. Comme β_i et β sont dans B, leur produit l'est aussi et donc $\mathrm{Tr}(\beta\beta_i) \in A$ par le corollaire 1.46. Or,

$$\mathrm{Tr}(\beta\beta_i) = \mathrm{Tr}\left(\sum_{j=1}^m b_j \beta'_j \beta_i\right) = \sum_{j=1}^m b_j \,\mathrm{Tr}(\beta'_j \beta_i) = \sum_{j=1}^m b_j \delta_{ij} = b_i$$

et nous pouvons ainsi conclure que chaque b_i appartient à A.

Si A est noethérien, alors M' l'est aussi et donc $B \subseteq M'$ est de type fini en tant que A-module. Si A est principal, alors B est libre de rang au plus m puisqu'il est contenu dans un A-module libre de rang m [Sam97, I, §5, thm.1] et il est de rang au moins m puisqu'il contient un A-module libre de rang m. □

Remarque 1.60. En reprenant les notations de la proposition et de la preuve précédente, posons $M = A\beta_1 + \cdots + A\beta_m \subseteq B$ où $(\beta_1, \dots, \beta_m)$ est une base de L/K. Posons

$$M^* = \{\beta \in L \mid \forall \gamma \in M,\ \mathrm{Tr}(\beta\gamma) \in A\}.$$

Par linéarité, $\beta \in M^*$ si et seulement si $\mathrm{Tr}(\beta\beta_i) \in A$ pour tout $i = 1, \dots, m$. Il s'en suit que $M^* = A\beta'_1 + \cdots + A\beta'_m$ et dès lors

$$M = A\beta_1 + \cdots + A\beta_m \subseteq B \subseteq A\beta'_1 + \cdots + A\beta'_m = M^*.$$

Corollaire 1.61. *L'anneau des entiers $\mathcal{O}_L$ d'un corps de nombres L est le plus grand sous-anneau de L de type fini en tant que $\mathbf{Z}$-module. En particulier $\mathcal{O}_L$ est noethérien.*

Démonstration. Nous savons à présent que $\mathcal{O}_L$ est de type fini en tant que $\mathbf{Z}$-module. Soit B un autre sous-anneau de L de type fini en tant que $\mathbf{Z}$-module ; alors tout élément de B est entier sur $\mathbf{Z}$ et donc $B \subseteq \mathcal{O}_L$. □

Définition 1.62. Soit L un corps de nombres. Une base de $\mathcal{O}_L$ en tant que $\mathbf{Z}$-module est appelée *base entière* de L.

Exemple 1.63. Soit $K = \mathbf{Q}(\sqrt{d})$ un corps quadratique.

(*i*) Si $d \equiv 2, 3 \bmod 4\mathbf{Z}$, une base entière de K est donnée par $(1, \sqrt{d})$.

(*ii*) Si $d \equiv 1 \bmod 4\mathbf{Z}$, une base entière de K est donnée par $(1, (1 + \sqrt{d})/2)$.

2 Anneaux de Dedekind et Factorisation

2.1 Anneaux de valuation discrète

Définition 2.1. Un anneau principal A satisfaisant l'une des conditions équivalentes suivantes est appelé *anneau de valuation discrète* :

(*i*) A possède exactement un idéal premier non nul.

(*ii*) A possède un nombre premier, à inversible près.

(*iii*) A est un anneau local mais n'est pas un corps.

Exemple 2.2. Soit p un nombre premier. L'anneau $\mathbf{Z}_{(p)} := \{m/n \in \mathbf{Q} \mid (n,p) = 1\}$ est un anneau de valuation discrète dont l'unique idéal premier est (p). Les inversibles de $\mathbf{Z}_{(p)}$ sont exactement les éléments non nuls tels que $(mn,p) = 1$; dit autrement, $\mathbf{Z}_{(p)}^{\times} = \mathbf{Z}_{(p)} \smallsetminus (p)$. Les éléments premiers sont tous de la forme up où u est un inversible.

Exemple 2.3. L'anneau des entiers p-adiques $\mathbf{Z}_p$, où p est un nombre premier, est un anneau de valuation discrète. Son unique idéal premier est $(p) = p\mathbf{Z}_p$. L'ensemble de ses inversibles est $\mathbf{Z}_p^{\times} = \mathbf{Z}_p \smallsetminus p\mathbf{Z}_p$. Le seul élément premier de $\mathbf{Z}_p$ est p, à inversible près.

Remarque 2.4. Dans un anneau de valuation discrète A où π est l'élément premier, les éléments non nuls de A peuvent être décomposés de façon unique en $u\pi^m$ où u est un inversible et $m \geq 0$ (et même plus précisément $m > 0$, à moins que cet élément soit inversible). Tout idéal de A est donc de la forme (π^m) pour un unique $m \in \mathbf{N}$. Par conséquent, si $\mathfrak{a}$ est un idéal de A et si $\mathfrak{p}$ désigne l'(unique) idéal maximal de A, alors $\mathfrak{a} = \mathfrak{p}^m$ pour un certain $m \in \mathbf{N}$.

Rappel 2.5. L'annulateur d'un élément m appartenant à un module sur un anneau A est défini par

$$\mathrm{Ann}_A(m) = \{a \in A \mid am = 0\}$$

et il s'agit d'un idéal de A, distinct de A dès que m est non nul. Supposons que A soit un anneau de valuation discrète et soit c un élément non nul de A. Posons M le quotient $A/(c)$ et déterminons l'annulateur d'un élément non nul $b + (c) \in M$. Soit π l'élément premier de A et soient $c = u\pi^m$ et $b = v\pi^n$ dans lesquels u et v sont inversibles. Alors $n < m$, sinon $b + (c) = 0 \in M$ et

$$\mathrm{Ann}_A(b + (c)) = (\pi^{m-n}).$$

Dès lors, un élément b pour lequel $\mathrm{Ann}(b + (c))$ est maximal est de la forme $v\pi^{m-1}$ et pour ce choix $\mathrm{Ann}(b + (c))$ est l'idéal premier de A engendré par c/b.

Proposition 2.6. *Un anneau intègre A est de valuation discrète si et seulement si*

(i) A est noethérien,

(ii) A est intégralement clos, et

(iii) A possède exactement un idéal premier non nul.

Démonstration. Les conditions (*i*), (*ii*) et (*iii*) sont nécessaires de par la hiérarchie établie sur les anneaux. Ces conditions sont suffisantes : il suffit de s'assurer que A est un anneau principal. Dans un premier temps, nous allons nous concentrer sur les idéaux premiers non nuls. Noter que (*iii*) implique que A soit un anneau local.

Soit $c \in A$ non nul et non inversible, et considérons le A-module $M = A/(c)$. Pour tout élément $m \neq 0$ de M, $\mathrm{Ann}(m)$ est un idéal distinct de A. Puisque A est noethérien, il existe un m tel que $\mathrm{Ann}(m)$ est maximal parmi ces idéaux. Posons $m = b + (c)$ et $\mathfrak{p} = \mathrm{Ann}(b + (c))$. Noter que $c \in \mathfrak{p}$, donc $\mathfrak{p} \neq 0$, et que

$$\mathfrak{p} = \{a \in A \mid c \text{ divise } ab\}.$$

Alors $\mathfrak{p}$ est un idéal premier. En effet, si ce n'était pas le cas, il existerait $x, y \in A$ pour lesquels $xy \in \mathfrak{p}$ mais aucun de x et y ne seraient dans $\mathfrak{p}$. Alors $yb + (c)$ serait un élément non nul de M, vu que $y \notin \mathfrak{p}$. Considérons $\mathrm{Ann}(yb + (c))$, il contiendrait évidement $\mathfrak{p}$ et x, venant ainsi contredire la maximalité de $\mathfrak{p}$ parmi les idéaux de la forme $\mathrm{Ann}(m)$. Donc $\mathfrak{p}$ est premier. De plus, b/c n'est pas un élément de A, sinon $b = c \cdot b/c \in (c)$ et donc $m = 0$. En revanche, c/b est un élément de A et $\mathfrak{p} = (c/b)$. En effet, par définition $\mathfrak{p}b \subseteq (c)$ et donc $\mathfrak{p} \cdot b/c \subseteq A$ et est un idéal de A. Si $\mathfrak{p} \cdot b/c$ était contenu dans $\mathfrak{p}$, alors b/c serait entier sur A étant donné que $\mathfrak{p}$ est de type fini et donc b/c serait un élément de A par la condition (ii), ce qui est absurde car nous savons que $b/c \notin A$. Dès lors, $\mathfrak{p} \cdot b/c = A$ et cela implique que $\mathfrak{p} = (c/b)$.

Dans le cas général, nous posons $\pi = c/b$ de sorte que $\mathfrak{p} = (\pi)$. Soit $\mathfrak{a}$ un idéal propre de A et considérons la chaîne ascendante

$$\mathfrak{a} \subset \mathfrak{a}\pi^{-1} \subset \mathfrak{a}\pi^{-2} \subset \cdots .$$

Ces inclusions sont strictes : si $\mathfrak{a}\pi^{-r} = \mathfrak{a}\pi^{-r-1}$ pour un certain r, alors $\pi^{-1}(\mathfrak{a}\pi^{-r}) = \mathfrak{a}\pi^{-r}$, et π^{-1} est entier sur A et donc serait un élément de A, ce qui est impossible puisque π n'est pas inversible. Par conséquent, comme A est noethérien, cette chaîne strictement croissante ne peut pas être contenue dans A. Soit m le plus petit naturel tel que $\mathfrak{a}\pi^{-m} \subseteq A$ et $\mathfrak{a}\pi^{-m-1} \nsubseteq A$. Alors $\mathfrak{a}\pi^{-m} \nsubseteq \mathfrak{p}$ et donc $\mathfrak{a}\pi^{-m} = A$; ainsi $\mathfrak{a} = (\pi^m)$. □

Remarque 2.7. Une valuation discrète peut naturellement être munie à un anneau de valuation discrète A (justifiant ainsi l'appellation) en posant, pour π l'élément premier de A,

$$v \colon A \setminus \{0\} \longrightarrow \mathbf{Z} \colon a = u\pi^m \longmapsto m$$

et en étendant en 0 par $v(0) = \infty$. Réciproquement, la donnée d'un anneau intègre A muni d'une valuation discrète v est équivalente à la notion d'anneau de valuation discrète, en remarquant que

$$A = \{x \in \mathrm{Frac}(A) \mid v(x) \geq 0\}$$

est un anneau local, mais pas un corps. Cette discussion nous amène à une nouvelle reformulation de la définition 2.1 :

Définition 2.8. Un *anneau de valuation discrète* est un anneau intègre muni d'une valuation discrète.

2.2 Anneaux de Dedekind

Définition 2.9. Un *anneau de Dedekind* A est un anneau intègre tel que

- (i) A est noethérien,
- (ii) A est intégralement clos, et
- (iii) tout idéal premier non nul est maximal.

Remarque 2.10. La proposition 2.6 permet d'affirmer qu'un anneau local est de Dedekind si et seulement s'il s'agit d'un anneau de valuation discrète. En particulier, l'anneau des entiers p-adiques est de Dedekind.

Exemple 2.11. L'anneau $\mathbf{Z}$ est de Dedekind. Plus généralement, tout anneau d'entiers $\mathcal{O}_L$ d'un corps de nombres L est de Dedekind (voir remarque 2.56).

Lemme 2.12. *Soient A un anneau intègre et S un sous-ensemble multiplicatif de A.*

- *(i) Si A est noethérien, alors $S^{-1}A$ l'est aussi.*
- *(ii) Si A est intégralement clos, alors $S^{-1}A$ l'est aussi.*

Démonstration. (*i*) Soit $\mathfrak{a}$ un idéal de $S^{-1}A$; alors $\mathfrak{a} = S^{-1}(\mathfrak{a} \cap A)$ par 6.18 et donc $\mathfrak{a}$ est engendré par n'importe quel ensemble fini de générateurs de $\mathfrak{a} \cap A$.

(*ii*) Soit α un élément du corps des fractions de A. Noter qu'il s'agit du même corps que celui des fractions de $S^{-1}A$. Supposons que α soit entier sur $S^{-1}A$; alors

$$\alpha^m + a_1\alpha^{m-1} + \cdots + a_m = 0$$

pour certains $a_i \in S^{-1}A$. Pour tout i, il existe un $s_i \in S$ tel que $s_i a_i \in A$. Posons leur produit $s = \prod_i s_i \in S$ et multiplions l'équation précédente par s^m :

$$(s\alpha)^m + sa_1(s\alpha)^{m-1} + \cdots + s^m a_m = 0.$$

Cette équation nous apprend que $s\alpha$ est entier sur A et est donc un élément de A. Dès lors $\alpha = (s\alpha)/s \in S^{-1}A$. □

Proposition 2.13. *Soient A un anneau de Dedekind et S un sous-ensemble multiplicatif de A ; alors $S^{-1}A$ est un anneau de Dedekind.*

Démonstration. La condition (*iii*) signifie qu'il n'y a pas de relation d'inclusion entre les idéaux premiers non nuls de A. Si cette condition est vraie pour A, alors la proposition 6.19 affirme que c'est également vrai pour $S^{-1}A$. Les conditions (*i*) et (*ii*) résultent quant à elles du lemme précédent. □

Proposition 2.14. *Un anneau noethérien intègre A est un anneau de Dedekind si et seulement si la localisation $A_\mathfrak{p}$ en dehors de n'importe lequel de ses idéaux premiers non nul $\mathfrak{p}$ est un anneau de valuation discrète.*

Démonstration. La nécessité découle de l'observation que chaque localisé $A_\mathfrak{p}$ est un anneau local. La proposition précédente implique alors que chaque $A_\mathfrak{p}$ est de Dedekind et donc un anneau de valuation discrète.

Pour la suffisance, remarquons tout d'abord que $A = \bigcap_\mathfrak{p} A_\mathfrak{p}$. En effet, si $a/b \in \bigcap_\mathfrak{p} A_\mathfrak{p}$ avec a et b des éléments de A, alors

$$\mathfrak{a} = \{x \in A \mid xa \in bA\}$$

est un idéal non contenu dans chaque idéal premier de A : pour tout $\mathfrak{p}$, $a/b = c/s$ avec $c \in A$ et $s \notin \mathfrak{p}$, donc $sa = bc$ et ainsi $s \in \mathfrak{a} \smallsetminus \mathfrak{p}$. Par conséquent $\mathfrak{a}$ n'est contenu dans aucun idéal maximal de A et donc $\mathfrak{a} = A$. Ainsi $a = 1 \cdot a \in bA$, ou autrement dit $a/b \in A$.

Supposons désormais que les $A_\mathfrak{p}$ sont des anneaux de valuation discrète. Ils sont alors tous intégralement clos et, de ce fait, $A = \bigcap_\mathfrak{p} A_\mathfrak{p}$ l'est aussi. Finalement, la proposition 6.19 implique que chaque idéal premier $\mathfrak{p}$ de A est maximal car il l'est dans $A_\mathfrak{p}$. □

2.3 Factorisation unique des idéaux

Objectif. Lors de cette section, nous allons nous intéresser au principal résultat concernant les anneaux de Dedekind : tout idéal propre d'un anneau de Dedekind se décompose de façon unique en un produit d'idéaux premiers non nuls (voir théorème 2.21). Ce processus vient ainsi imiter la factorisation unique (à inversible près) des éléments de $\mathbf{Z}$ en un produit de nombres premiers.

Rappel 2.15. Soient $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ des idéaux d'un anneau A ; leur produit est défini par l'idéal de A :

$$\mathfrak{a}_1 \cdots \mathfrak{a}_n = \left\{ \textstyle\sum_{i=1}^m a_{1i} \cdots a_{ni} \;\middle|\; m \geq 0,\, a_{\ell i} \in \mathfrak{a}_\ell \right\}.$$

Lemme 2.16. *Tout idéal $\mathfrak{a}$ non nul d'un anneau noethérien A contient un produit d'idéaux premiers non nuls.*

Démonstration. Supposons que le lemme soit faux pour A, et considérons un contre-exemple maximal $\mathfrak{a}$. Alors $\mathfrak{a}$ n'est en particulier pas un idéal premier et donc il existe des éléments x et $y \in A$ tels que $xy \in \mathfrak{a}$ mais ni $x \in \mathfrak{a}$, ni $y \in \mathfrak{a}$. Les idéaux $\mathfrak{a} + (x)$ et $\mathfrak{a} + (y)$ contiennent strictement $\mathfrak{a}$, mais leur produit est contenu dans $\mathfrak{a}$. Comme $\mathfrak{a}$ a été choisi comme le contre-exemple maximal, chacun de $\mathfrak{a}+(x)$ et $\mathfrak{a} + (y)$ contient un produit d'idéaux premiers, et il s'en suit que $\mathfrak{a}$ contient un produit d'idéaux premiers. □

Lemme 2.17. *Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux comaximaux d'un anneau A ; alors pour tous m, $n \geq 1$, $\mathfrak{a}^m$ et $\mathfrak{b}^n$ sont comaximaux.*

Démonstration. Étant donné que $\mathfrak{a}$ et $\mathfrak{b}$ sont comaximaux, il existe un $a \in \mathfrak{a}$ et un $b \in \mathfrak{b}$ pour lesquels $a + b = 1$. Considérons

$$1 = (a+b)^r = a^r + \binom{r}{1} a^{r-1}b + \cdots + b^r.$$

Dès que $r \geq m+n-1$, le terme à droite est une somme d'un élément de $\mathfrak{a}^m$ avec un élément de $\mathfrak{b}^n$. □

Remarque 2.18. Si $\mathfrak{p}_1$ et $\mathfrak{p}_2$ sont des idéaux premiers distincts et non nuls d'un anneau de Dedekind, la condition (*iii*) de la définition implique que $\mathfrak{p}_1$ et $\mathfrak{p}_2$ sont comaximaux et le lemme précédent montre que $\mathfrak{p}_1^m$ et $\mathfrak{p}_2^n$ sont également comaximaux pour tous m, $n \geq 1$.

Lemme 2.19. *Soit $\mathfrak{p}$ un idéal maximal d'un anneau intègre A et soit $\mathfrak{q}$ l'idéal qu'il engendre dans $A_\mathfrak{p}$ ($\mathfrak{q} = \mathfrak{p}A_\mathfrak{p}$) ; l'application*

$$\begin{array}{ccc} A/\mathfrak{p}^m & \longrightarrow & A_\mathfrak{p}/\mathfrak{q}^m \\ a + \mathfrak{p}^m & \longmapsto & a + \mathfrak{q}^m \end{array}$$

est un isomorphisme pour tout $m \geq 1$.

Démonstration. Afin de vérifier que ce morphisme est injectif, nous montrons que $\mathfrak{q}^m \cap A = \mathfrak{p}^m$. Or, $\mathfrak{q}^m = S^{-1}\mathfrak{p}^m$ où $S = A \smallsetminus \mathfrak{p}$; ainsi il suffit de montrer que $\mathfrak{p}^m = (S^{-1}\mathfrak{p}^m) \cap A$. Un élément a de $(S^{-1}\mathfrak{p}^m) \cap A$ peut s'écrire comme $a = b/s$ avec $b \in \mathfrak{p}^m$ et $s \in S$; alors $sa \in \mathfrak{p}^m$ et donc $sa = 0$ dans $A/\mathfrak{p}^m$. Le seul idéal maximal contenant $\mathfrak{p}^m$ est $\mathfrak{p}$ et donc le seul idéal maximal de $A/\mathfrak{p}^m$ est $\mathfrak{p}/\mathfrak{p}^m$. En particulier, $A/\mathfrak{p}^m$ est un anneau local. Comme $s + \mathfrak{p}^m$ n'est pas dans $\mathfrak{p}/\mathfrak{p}^m$, il est inversible dans $A/\mathfrak{p}^m$ et donc $sa = 0 \in A/\mathfrak{p}^m$ implique que $a = 0 \in A/\mathfrak{p}^m$, autrement dit $a \in \mathfrak{p}^m$. L'inclusion réciproque est quant à elle triviale.

Pour la surjectivité, soit $a/s \in A_\mathfrak{p}$. Comme $s \notin \mathfrak{p}$ et $\mathfrak{p}$ est maximal, $(s) + \mathfrak{p} = A$, *i.e.* (s) et $\mathfrak{p}$ sont comaximaux. Par conséquent, (s) et $\mathfrak{p}^m$ sont comaximaux et donc il existe $b \in A$ et $q \in \mathfrak{p}^m$ tels que $bs + q = 1$. De par le fait que s soit inversible dans $A_\mathfrak{p}/\mathfrak{q}^m$, a/s est l'unique élément de cet anneau satisfaisant $s(a/s) = a$. Cependant, comme $s(ba) = a(1-q)$, l'image de ba dans $A_\mathfrak{p}$ satisfait également cette propriété et donc cette image est égale à a/s. □

Remarque 2.20. Nous avons ainsi montrer que $\mathfrak{a}^{ec} = \mathfrak{a}$ si $\mathfrak{a}$ est une puissance d'un idéal maximal $\mathfrak{p}$ et $S = S \smallsetminus \mathfrak{p}$.

Théorème 2.21 (Factorisation)**.** *Dans un anneau de Dedekind A, tout idéal propre $\mathfrak{a}$ se factorise de façon unique sous la forme*

$$\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n}$$

où les $\mathfrak{p}_i$ sont des idéaux premiers distincts et $r_i > 0$.

Démonstration. En appliquant le lemme 2.16 à l'anneau A, $\mathfrak{a}$ contient un produit d'idéaux premiers non nuls :

$$\mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_m^{r_m} = \mathfrak{b} \subseteq \mathfrak{a}$$

dans lequel nous supposons avoir agencé l'écriture de manière à ce que chaque $\mathfrak{p}_i$ soit distinct. Alors,

$$A/\mathfrak{b} \simeq A/\mathfrak{p}_1^{r_1} \times \cdots \times A/\mathfrak{p}_m^{r_m} \simeq A_{\mathfrak{p}_1}/\mathfrak{q}_1^{r_1} \times \cdots \times A_{\mathfrak{p}_m}/\mathfrak{q}_m^{r_m}$$

où $\mathfrak{q}_i = \mathfrak{p}_i A_{\mathfrak{p}_i}$ est l'idéal maximal de $A_{\mathfrak{p}_i}$. Le premier isomorphisme est donné par le théorème chinois et la remarque 2.18 ; le second est donné par le lemme 2.19. Sous cet isomorphisme, $\mathfrak{a}/\mathfrak{b}$ correspond à $\mathfrak{q}_1^{s_1}/\mathfrak{q}_1^{r_1} \times \cdots \times \mathfrak{q}_m^{s_m}/\mathfrak{q}_m^{r_m}$ avec $s_i \leq r_i$ puisque les $A_{\mathfrak{p}_i}$ sont de valuation discrète. Comme cet idéal est également l'image de $\mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m}$ sous cet isomorphisme :

$$\mathfrak{a} = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m} \quad \text{dans } A/\mathfrak{b}.$$

De par le fait que tous ces idéaux contiennent $\mathfrak{b}$ et en se remémorant l'existence d'une correspondance entre les idéaux de $A/\mathfrak{b}$ et les idéaux de A contenant $\mathfrak{b}$:

$$\mathfrak{a} = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m} \quad \text{dans } A.$$

Il ne reste plus qu'à montrer que cette factorisation est unique. Supposons que nous disposons de deux factorisations de l'idéal $\mathfrak{a}$. Après avoir ajouté les éventuels facteurs dont la puissance est nulle, nous pouvons supposer que les mêmes idéaux premiers sont sollicités dans chacune des deux factorisations et donc

$$\mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m} = \mathfrak{a} = \mathfrak{p}_1^{t_1} \cdots \mathfrak{p}_m^{t_m}.$$

Cependant, nous avons constaté que $\mathfrak{q}_i^{s_i} = \mathfrak{a} A_{\mathfrak{p}_i} = \mathfrak{q}_i^{t_i}$ où $\mathfrak{q}_i$ est l'idéal maximal de $A_{\mathfrak{p}_i}$. Par conséquent $s_i = t_i$ pour tout i et concluant la preuve. □

Remarque 2.22. En reprenant les notations de la preuve précédente,

$$s_i > 0 \quad \text{ssi} \quad \mathfrak{a} A_{\mathfrak{p}_i} \neq A_{\mathfrak{p}_i} \quad \text{ssi} \quad \mathfrak{a} \subseteq \mathfrak{p}_i.$$

Exemple 2.23. Considérons l'anneau $\mathbf{Z}$; ses idéaux premiers sont tous de la forme (p) où p est nombre premier. Soit (n) un idéal propre de $\mathbf{Z}$, le théorème 2.21 fournit l'existence d'une factorisation unique de (n) en

$$(n) = (p_1)^{r_1} \cdots (p_n)^{r_n}.$$

De cela, nous retrouvons la factorisation unique à inversible près des éléments n de $\mathbf{Z}$:

$$n = u p_1^{r_1} \cdots p_n^{r_n}, \quad u \in \mathbf{Z}^\times.$$

Remarque 2.24. Tout anneau factoriel n'est pas nécessairement un anneau de Dedekind pour autant. En effet, si k est un corps, $k[X_0, X_1, \dots] = \bigcup_{n \in \mathbf{N}} k[X_0, \dots, X_n]$ est factoriel puisque chaque élément de l'union l'est, cependant il ne s'agit pas d'un anneau noethérien, et donc pas non plus d'un anneau de Dedekind. Ce n'est en réalité pas le caractère factoriel de $\mathbf{Z}$ qui est à la source du fait qu'il soit de Dedekind : il s'agit d'une conséquence d'être principal (voir proposition 2.33).

Corollaire 2.25. *Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux propres de A ; alors*

$$\mathfrak{a} \subseteq \mathfrak{b} \quad \textit{ssi} \quad \textit{pour tout } \mathfrak{p} \textit{ premier non nul, } \mathfrak{a} A_{\mathfrak{p}} \subseteq \mathfrak{b} A_{\mathfrak{p}}$$

En particulier, $\mathfrak{a} = \mathfrak{b}$ si et seulement si $\mathfrak{a} A_{\mathfrak{p}} = \mathfrak{b} A_{\mathfrak{p}}$ pour tout $\mathfrak{p}$ premier non nul.

Démonstration. La condition nécessaire est claire. Réciproquement, les idéaux $\mathfrak{a}$ et $\mathfrak{b}$ se factorisent en

$$\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_m^{r_m} \quad \text{et} \quad \mathfrak{b} = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m}, \quad r_i,\, s_i \geq 0.$$

Alors, $\mathfrak{a} A_{\mathfrak{p}_i} \subseteq \mathfrak{b} A_{\mathfrak{p}_i}$ si et seulement si $r_i \geq s_i$: les $A_{\mathfrak{p}_i}$ sont des anneaux de valuation discrète. Dès lors, le fait que $r_i \geq s_i$ pour chaque i implique que $\mathfrak{a} \subseteq \mathfrak{b}$. □

Remarque 2.26. Soient $\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_m^{r_m}$ et $\mathfrak{b} = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m}$ avec $r_i,\, s_i \geq 0$; alors

$$\mathfrak{a} \mid \mathfrak{b} \quad \text{ssi} \quad \forall\, 1 \leq i \leq m,\ r_i \leq s_i \quad \text{ssi} \quad \forall i,\ \mathfrak{p}^{r_i} A_{\mathfrak{p}_i} \supseteq \mathfrak{p}^{s_i} A_{\mathfrak{p}_i} \quad \text{ssi} \quad \mathfrak{a} \supseteq \mathfrak{b}.$$

Corollaire 2.27. *Soit A un anneau intègre possédant un nombre fini d'idéaux premiers ; alors A est un anneau de Dedekind si et seulement s'il est principal.*

Démonstration. Supposons que A soit un anneau de Dedekind. D'après le théorème 2.21, afin de montrer que A est principal, il suffit de montrer que ses idéaux premiers sont principaux. Soient $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ ses idéaux premiers. Dès lors $\mathfrak{p}_1^2, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ sont deux-à-deux comaximaux. Considérons $x_1 \in \mathfrak{p}_1 \smallsetminus \mathfrak{p}_1^2$. Selon le théorème des restes chinois, il existe un élément $x \in A$ tel que

$$x \equiv x_1 \bmod \mathfrak{p}_1^2 \quad \text{et} \quad x \equiv 1 \bmod \mathfrak{p}_i,\ i = 2, \ldots, n.$$

En factorisant, nous devons avoir que $(x) = \mathfrak{p}_1$. En procédant de cette manière avec n'importe quel $\mathfrak{p}_i$, nous obtenons que chaque idéal premier est principal. Réciproquement, si A est principal, alors A est noethérien et est intégralement clos. De plus, il est facile de montrer que tout idéal premier d'un anneau principal est maximal. □

Corollaire 2.28. *Soient $\mathfrak{a} \supseteq \mathfrak{b}$ deux idéaux non nuls d'un anneau de Dedekind A ; alors $\mathfrak{a} = \mathfrak{b} + (a)$ pour un certain $a \in A$.*

Démonstration. Soient $\mathfrak{b} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_m^{r_m}$ et $\mathfrak{a} = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m}$ avec $r_i,\ s_i \geq 0$ leur décomposition. Comme $\mathfrak{b} \subseteq \mathfrak{a}$, les $s_i \leq r_i$. Pour tout $1 \leq i \leq m$, choisissons un $x_i \in A$ tel que $x_i \in \mathfrak{p}_i^{s_i} \smallsetminus \mathfrak{p}_i^{s_i+1}$. Par le théorème des restes chinois, il existe un $a \in A$ tel que

$$a \equiv x_i \bmod \mathfrak{p}_i^{r_i}, \qquad \text{pour tout } i.$$

Nous concluons que $\mathfrak{a} = \mathfrak{b} + (a)$ en regardant les idéaux qu'ils engendrent dans $A_\mathfrak{p}$, pour tout idéal premier $\mathfrak{p}$. □

Corollaire 2.29. *Soient $\mathfrak{a}$ un idéal d'un anneau de Dedekind et a l'un de ses éléments non nuls ; alors il existe un $b \in \mathfrak{a}$ tel que $\mathfrak{a} = (a, b)$.*

Démonstration. En appliquant le corollaire 2.28 aux idéaux $\mathfrak{a} \supseteq (a)$. □

Corollaire 2.30. *Soit $\mathfrak{a}$ un idéal non nul d'un anneau de Dedekind A ; alors il existe un idéal non nul $\mathfrak{a}^*$ de A tel que $\mathfrak{a}\mathfrak{a}^*$ est principal. De plus, $\mathfrak{a}^*$ peut être choisi comaximal à n'importe quel idéal non nul $\mathfrak{c}$, il peut également être choisi tel que $\mathfrak{a}\mathfrak{a}^* = (a)$ pour n'importe quel $a \in \mathfrak{a}$ non nul (mais potentiellement pas simultanément).*

Démonstration. Soit a un élément non nul de $\mathfrak{a}$; de ce fait $(a) \subseteq \mathfrak{a}$ et par conséquent

$$(a) = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_m^{r_m} \quad \text{et} \quad \mathfrak{a} = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m}, \quad s_i \leq r_i.$$

En considérant $\mathfrak{a}^* = \mathfrak{p}_1^{r_1 - s_1} \cdots \mathfrak{p}_m^{r_m - s_m}$, alors $\mathfrak{a}\mathfrak{a}^* = (a)$. Montrons désormais que $\mathfrak{a}^*$ peut être choisi comaximal à n'importe quel $\mathfrak{c}$. Comme $\mathfrak{a}\mathfrak{c} \subseteq \mathfrak{a}$, le corollaire 2.28 fournit l'existence d'un $a \in \mathfrak{a}$ tel que $\mathfrak{a} = \mathfrak{a}\mathfrak{c} + (a)$. Comme $(a) \subseteq \mathfrak{a}$, il s'en suit que $(a) = \mathfrak{a}\mathfrak{a}^*$ pour un certain idéal $\mathfrak{a}^*$ en utilisant l'argument précédent. Alors $\mathfrak{a}\mathfrak{c} + \mathfrak{a}\mathfrak{a}^* = \mathfrak{a}$ et donc $\mathfrak{c} + \mathfrak{a}^* = A$ (sinon $\mathfrak{c} + \mathfrak{a}^* \subseteq \mathfrak{p}$ pour un certain idéal premier $\mathfrak{p}$ et donc $\mathfrak{a}\mathfrak{c} + \mathfrak{a}\mathfrak{a}^* = \mathfrak{a}(\mathfrak{c} + \mathfrak{a}^*) \subseteq \mathfrak{a}\mathfrak{p} \subsetneq \mathfrak{a}$). □

Remarque 2.31. Tout anneau principal A est factoriel. En revanche, la réciproque est fausse en général, par exemple, soit k un corps, alors $k[X, Y]$ est factoriel mais l'idéal (X, Y) n'est pas principal. La réciproque est cependant vraie dans le cadre des anneaux de Dedekind.

Proposition 2.32. *Tout anneau de Dedekind et factoriel est un anneau principal.*

Démonstration. Rappelons que dans un anneau factoriel, un élément irréductible π divise un produit bc s'il divise b ou c ; cela signifie que (π) est premier.

Soit A un anneau de Dedekind et factoriel. Il suffit de montrer que chaque idéal premier (non nul) $\mathfrak{p}$ de A est principal. Soit a un élément non nul de $\mathfrak{p}$; alors a se factorise en un produit d'éléments irréductibles et, comme $\mathfrak{p}$ est premier, l'un de ces irréductibles π est dans $\mathfrak{p}$. Alors $(0) \subset (\pi) \subseteq \mathfrak{p}$ et comme (π) est premier dans un anneau de Dedekind, il est maximal, amenant l'égalité $(\pi) = \mathfrak{p}$. □

Proposition 2.33. *Tout anneau principal est de Dedekind.*

Démonstration. Soit A un anneau principal, alors A est noethérien et est intégralement clos. Il suffit de montrer que tout idéal premier non nul $\mathfrak{p}$ de A est maximal. Comme A est principal, il existe π premier et, donc irréductible, tel que $\mathfrak{p} = (\pi)$. Dès lors $\mathfrak{p} = (\pi)$ est maximal. □

Remarque 2.34. Ainsi, nous pouvons à nouveau enrichir la hiérarchie d'anneaux de la manière suivante :

$$\{\text{anneaux principaux}\} = \{\text{anneaux factoriels}\} \cap \{\text{anneaux de Dedekind}\}.$$

Exemple 2.35. Soit k un corps ; alors $k[X]$ est principal et est donc de Dedekind. En revanche $k[X, Y]$ est factoriel mais n'est pas principal ; il n'est donc pas de Dedekind.

2.4 Groupe des classes d'idéaux

Définition 2.36. Soit A un anneau de Dedekind dont le corps des fractions est K. Un *idéal fractionnaire* de A est un sous-A-module non nul $\mathfrak{f}$ de K tel que

$$d\mathfrak{f} := \{dx \mid x \in \mathfrak{f}\}$$

est contenu dans A pour un certain $d \in A$ (ou K) non nul.

Ainsi, un idéal fractionnaire est un sous-A-module non nul de K dont tous les éléments possèdent un dénominateur commun.

Remarque 2.37. Bien que tout idéal non nul de A soit fractionnaire, la réciproque est fausse en générale (à moins qu'il soit contenu dans A) ; afin de distinguer les idéaux de A, nous les désignerons par **idéaux entiers**.

Exemple 2.38. Soit $n\mathbf{Z}$ un idéal entier de $\mathbf{Z}$; alors pour tout $q \in \mathbf{Q}$ non nul, l'ensemble $qn\mathbf{Z} = \{qx \mid x \in n\mathbf{Z}\}$ est un idéal fractionnaire de $\mathbf{Z}$.

Remarque 2.39. Un idéal fractionnaire $\mathfrak{f}$ est un A-module de type fini : comme $d\mathfrak{f}$ est un idéal entier il est de type fini en tant que A-module et l'application $\mathfrak{f} \to d\mathfrak{f}\colon x \mapsto dx$ est un isomorphisme de A-modules. Réciproquement, tout sous-A-module non nul de K de type fini est un idéal fractionnaire : un dénominateur commun pour un système de générateurs est un dénominateur commun pour tous les éléments du module. Ainsi

$$\{\text{idéaux fractionnaires de } A\} = \{\text{sous-}A\text{-modules non nuls de } K \text{ de type fini}\}.$$

Définition 2.40. Tout élément non nul b de K définit un idéal fractionnaire, dit *principal*, par

$$(b) := bA = \{ba \mid a \in A\}.$$

Définition 2.41. Le *produit de deux idéaux fractionnaires* $\mathfrak{f}$, $\mathfrak{g}$ est définit de la même manière que le produit de deux idéaux (entiers) :

$$\mathfrak{f}\mathfrak{g} = \left\{\textstyle\sum_{i=1}^{n} x_i y_i \;\middle|\; n \geq 0,\, x_i \in \mathfrak{f},\, y_i \in \mathfrak{g}\right\}.$$

Remarque 2.42. Le produit de deux idéaux fractionnaires $\mathfrak{f}$, $\mathfrak{g}$ est à nouveau un idéal fractionnaire : il s'agit clairement d'un A-module et si $d\mathfrak{f}$ et $e\mathfrak{g}$ sont contenus dans A, alors $de\mathfrak{f}\mathfrak{g}$ l'est aussi. Noter que dans le cadre des idéaux fractionnaires principaux (a), (b), leur produit est $(a)(b) = (ab)$.

Exemple 2.43. Soit A un anneau de valuation discrète dont l'idéal maximal est $\mathfrak{p}$ et le corps des fractions est K. Soit π un générateur de $\mathfrak{p}$. Tout élément non nul de K peut s'écrire de façon unique sous la forme $a = u\pi^m$ avec u un inversible de A et $m \in \mathbf{Z}$. Soit $\mathfrak{a}$ un idéal fractionnaire de A ; alors $d\mathfrak{a} \subseteq A$ pour un certain $d \in A$, que nous supposer de la forme $d = \pi^n$. Par conséquent, $\pi^n\mathfrak{a}$ est un

idéal de A et donc il est de la forme (π^m) pour un certain $k \geq 0$. Clairement, $\mathfrak{a} = (\pi^{m-n})$. Dès lors, les idéaux fractionnaires de A sont de la forme (π^m), avec $m \in \mathbf{Z}$; ils forment un groupe abélien libre $\mathrm{Id}(A)$ de rang 1 et l'application

$$\mathbf{Z} \longrightarrow \mathrm{Id}(A) \colon m \longmapsto (\pi^m)$$

est un isomorphisme.

Théorème 2.44. *Soit A un anneau de Dedekind. L'ensemble $\mathrm{Id}(A)$ des idéaux fractionnaires de A est un groupe ; il s'agit du groupe abélien libre sur l'ensemble des idéaux premiers non nuls.*

Démonstration. Nous avons déjà constaté que le produit entre idéaux fractionnaires est stable et est clairement commutatif. Pour l'associativité,

$$(\mathfrak{fg})\mathfrak{h} = \left\{\textstyle\sum_{i=1}^n x_i y_i z_i \;\middle|\; n \geq 0,\, x_i \in \mathfrak{f},\, y_i \in \mathfrak{g},\, z_i \in \mathfrak{h}\right\} = \mathfrak{f}(\mathfrak{gh}).$$

Notons que l'anneau (et idéal) A joue le rôle de neutre : $\mathfrak{f}A = \mathfrak{f}$. Dans le but de montrer que $\mathrm{Id}(A)$ est un groupe, il reste à montrer que l'inverse existe.

Soit $\mathfrak{a}$ un idéal entier de A ; selon le corollaire 2.30, il existe un idéal $\mathfrak{a}^*$ et un élément $a \in A$ tels que $\mathfrak{a}\mathfrak{a}^* = (a)$. Clairement $\mathfrak{a}(a^{-1}\mathfrak{a}^*) = A$ et donc $a^{-1}\mathfrak{a}$ est l'inverse de $\mathfrak{a}$. Si $\mathfrak{f}$ est un idéal fractionnaire, alors $d\mathfrak{f}$ est un idéal entier pour un certain d et $d(d\mathfrak{f})^{-1}$ est l'inverse de $\mathfrak{f}$.

Il reste à montrer que le groupe $\mathrm{Id}(A)$ est engendré librement par les idéaux premiers, *i.e.* que chaque idéal fractionnaire peut-être exprimé de façon unique en un produit de puissance d'idéaux premiers. Soit $\mathfrak{f}$ un idéal fractionnaire ; alors $d\mathfrak{f}$ est un idéal entier pour un certain $d \in A$ et nous pouvons écrire, comme A est de Dedekind,

$$d\mathfrak{f} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_m^{r_m} \quad \text{et} \quad (d) = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m}.$$

Alors $\mathfrak{f} = \mathfrak{p}_1^{r_1 - s_1} \cdots \mathfrak{p}_m^{r_m - s_m}$. L'unicité de cette écriture provient de l'unicité de la factorisation des idéaux entiers. □

Remarque 2.45. Réciproquement, Emmy Noether a montré (thm. 4.6 de [Coh91]) que tout anneau intègre dont les idéaux fractionnaires forment un groupe pour le produit est de Dedekind.

Remarque 2.46. Soit S un sous-ensemble multiplicatif d'un anneau de Dedekind A, et notons $A_S := S^{-1}A$. Il s'agit d'un anneau intègre possédant le même corps de fractions que celui de A : $A \subseteq A_S \subseteq K$. Pour tout idéal fractionnaire $\mathfrak{f}$ de A,

$$S^{-1}\mathfrak{f} := \left\{\frac{x}{s} \;\middle|\; x \in \mathfrak{f},\, s \in S\right\}$$

est un idéal fractionnaire de A_S : il s'agit du A_S-module engendré par $\mathfrak{f}$. De plus, pour tous idéaux fractionnaires $\mathfrak{f}$ et $\mathfrak{g}$,

$$S^{-1}(\mathfrak{fg}) = (S^{-1}\mathfrak{f})(S^{-1}\mathfrak{g}) \quad \text{et} \quad S^{-1}\mathfrak{f}^{-1} = (\mathfrak{g}A_S)^{-1}.$$

Définition 2.47. Soit A un anneau de Dedekind. Le *groupe des classes d'idéaux* $\mathrm{Cl}(A)$ de A est le quotient $\mathrm{Id}(A)/\operatorname{Ppl}(A)$ de $\mathrm{Id}(A)$ par le sous-groupe des idéaux principaux. Le *nombre de classes* de A est l'ordre de $\mathrm{Cl}(A)$, lorsque celui-ci est fini.

Remarque 2.48. Lorsque A est l'anneau des entiers $\mathcal{O}_L$ d'un corps de nombres L, nous désignons par $\mathrm{Cl}(\mathcal{O}_L)$ le **groupe des classes d'idéaux** de L et son ordre h_L le **nombre de classes** de L. Nous prouverons par la suite (corollaire 3.13) que le nombre de classes h_L d'un corps de nombres L est systématiquement fini ; néanmoins celui-ci est difficile à calculer.

Remarque 2.49. Clairement, un anneau est principal si et seulement si son nombre de classes vaut 1. La notion de groupe de classes d'idéaux quantifie à quel point la factorisation unique échoue dans l'anneau des entiers d'un corps de nombres.

Exemple 2.50. Le nombre de classes de $\mathbf{Q}(\sqrt{-d})$, pour d un naturel sans facteurs carrés, vaut 1 si et seulement si $d = 1, 2, 3, 7, 11, 19, 43, 67, 163$: c'est seulement en 1954 que le mathématicien Heegner à montré qu'ils étaient les seuls. L'anneau $\mathbf{Z}[\sqrt{-5}]$ n'est pas principal puisque 6 admet deux décompositions : 2×3 et $(1 + \sqrt{-5}) \times (1 - \sqrt{-5})$. Dès lors, son nombre de classe ne vaut pas 1 – plus précisément celui-ci vaut 2.

Proposition 2.51. *Soient A un anneau de Dedekind et S un sous-ensemble multiplicatif de A ; l'application $\mathfrak{f} \mapsto S^{-1}\mathfrak{f}$ définit un isomorphisme du sous-groupe de* $\mathrm{Id}(A)$ *engendré par les idéaux premiers disjoints de S vers le groupe* $\mathrm{Id}(S^{-1}A)$.

Démonstration. Conséquence immédiate de la proposition 6.19 et du théorème 2.44. □

Remarque 2.52. Soit A un anneau de Dedekind dont le groupe des classes d'idéaux est fini. Il existe dans ce cas un nombre fini d'idéaux $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ formant un ensemble de représentants des classes d'idéaux ; ceux-ci peuvent être supposés entiers. Soit b un élément non nul de $\bigcap_{i=1}^{n} \mathfrak{a}_i$ et soit S l'ensemble multiplicatif engendré par b : $S = \{1, b, b^2, \ldots\}$. Alors $S^{-1}A$ est un anneau principal.

En effet, par hypothèse, tout idéal $\mathfrak{a}$ de A peut s'écrire sous la forme $\mathfrak{a} = (a)\mathfrak{a}_i$ pour un certain $a \in K^\times$ et un $1 \leq i \leq n$. Comme l'application $\mathfrak{b} \mapsto S^{-1}\mathfrak{b}$ est un morphisme, il s'en suit que $S^{-1}\mathfrak{a} = (a)S^{-1}\mathfrak{a}_i$ où (a) est l'idéal engendré par a dans $S^{-1}A$. Puisque $S^{-1}\mathfrak{a}_i$ possède un inversible, il s'agit de l'anneau au complet. Par conséquent, $S^{-1}\mathfrak{a} = (a)$ et ainsi nous constatons que tout idéal de $S^{-1}A$ de la forme $S^{-1}\mathfrak{a}$ est principal. Tous les idéaux de $S^{-1}A$ sont alors principaux par la proposition 6.18.

Remarque 2.53. Les conditions suivantes sur un anneau noethérien intègre A sont équivalentes :

(*i*) A est un anneau de Dedekind.

(*ii*) Le localisé en dehors n'importe quel premier $A_\mathfrak{p}$ est un anneau de valuation discrète.

(*iii*) Les idéaux fractionnaires de A forment un groupe.

(*iv*) Pour tout idéal fractionnaire $\mathfrak{a}$ de A, il existe un idéal $\mathfrak{b}$ tel que $\mathfrak{ab} = A$.

Démonstration. Nous avons vu que (*i*) implique (*ii*), (*iii*) et (*iv*) ; le même argument montre que (*ii*) implique (*iii*) et (*iv*). Les conditions (*iii*) et (*iv*) sont clairement équivalentes, et nous avons mentionné lors de la remarque 2.45 que (*iii*) implique (*i*). □

2.5 Clôture intégrale d'anneaux de Dedekind

Nous montrons que l'anneau des entiers $\mathcal{O}_L$ d'un corps de nombres L est un anneau de Dedekind ; ainsi tout idéal de $\mathcal{O}_L$ se factorise de façon unique en un produit d'idéaux premiers.

Lemme 2.54. *Tout anneau intègre B contenant un corps k et étant algébrique sur k est lui-même un corps.*

Démonstration. Soit β un élément non nul de B, nous montrons que β possède un inverse dans B. Comme β est algébrique sur k, l'anneau $k[\beta]$ est de dimension finie en tant que k-espace vectoriel et l'endomorphisme linéaire

$$k[\beta] \longrightarrow k[\beta] \colon x \longmapsto \beta x$$

est injectif (par intégrité de B). Par conséquent cette application est surjective ; ainsi il existe un élément β' de $k[\beta] \subseteq B$ satisfaisant $\beta'\beta = 1$. □

Théorème 2.55. *Soit A un anneau de Dedekind dont le corps des fractions est noté K et soit B la clôture intégrale de A dans une extension finie et séparable L/K ; alors B est un anneau de Dedekind.*

Démonstration. Selon la proposition 1.59, B est contenu dans un A-module de type fini. Il s'en suit que tous les idéaux de B sont de type fini lorsqu'ils sont vus en tant que A-modules. Comme $A \subseteq B$, ils sont à plus forte raison de type fini en tant que B-modules. Ainsi B est noethérien.

Via le corollaire 1.22, nous sommes en mesure de pouvoir affirmer que l'anneau B est intégralement clos.

Finalement, il reste à montrer que tout idéal premier non nul $\mathfrak{q}$ de B est maximal. Soit $\beta \in \mathfrak{q}$ non nul. Alors β est entier sur A et donc il satisfait une équation

$$\beta^n + a_1\beta^{n-1} + \cdots + a_n = 0, \quad a_i \in A,$$

que nous supposons de degré minimal ; ainsi, a_n est non nul. Comme $a_n \in \beta B \cap A$, nous obtenons que $\mathfrak{q} \cap A \neq (0)$. Or $\mathfrak{q} \cap A$ est un idéal premier de A et, comme A est de Dedekind, il s'agit même d'un idéal maximal $\mathfrak{p}$ de A ; autrement dit $A/\mathfrak{p}$ est un corps. Nous savons que $B/\mathfrak{q}$ est un anneau intègre et que l'application

$$\begin{array}{ccc} A/\mathfrak{p} & \longrightarrow & B/\mathfrak{q} \\ a+\mathfrak{p} & \longmapsto & a+\mathfrak{q} \end{array}$$

identifie $A/\mathfrak{p}$ à un sous-corps de $B/\mathfrak{q}$. Comme B est entier sur A, $B/\mathfrak{q}$ est algébrique sur $A/\mathfrak{p}$. Le lemme précédent nous permet de conclure que $B/\mathfrak{q}$ est un corps et donc que $\mathfrak{q}$ est maximal. □

Remarque 2.56. L'anneau des entiers $\mathcal{O}_L$ d'un corps de nombres L est un anneau de Dedekind puisque $\mathbf{Z}$ l'est.

2.6 Factorisation dans les extensions

Soit A un anneau de Dedekind dont le corps des fractions est noté K et soit B la clôture intégrale de A dans une extension finie et séparable L/K. Un idéal premier $\mathfrak{p}$ de A se factorise alors dans B en

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}, \quad e_i \geq 1. \tag{1}$$

Définition 2.57. L'exposant e_i apparaissant dans la factorisation (1) est appelé l'*indice de ramification* de $\mathfrak{P}_i$ sur $\mathfrak{p}$ et est parfois noté $e(\mathfrak{P}_i/\mathfrak{p})$. L'idéal premier $\mathfrak{p}$ de A *se ramifie* dans L lorsque l'un de ces indices de ramification est strictement plus grand que 1. Le degré $[B/\mathfrak{P}_i : A/\mathfrak{p}]$ est appelé *degré de la classe résiduelle* de $\mathfrak{P}_i$ sur $\mathfrak{p}$ et est noté f_i ou parfois $f(\mathfrak{P}_i/\mathfrak{p})$.

Définition 2.58. Un idéal premier $\mathfrak{P}$ de B *divise* $\mathfrak{p}$ lorsque celui-ci apparaît dans la factorisation (1) de $\mathfrak{p}$ dans B.

Exemple 2.59. Dans $\mathbf{Z}[i]$, l'idéal premier $2\mathbf{Z}$ de $\mathbf{Z}$ se factorise en $(2) = (1+i)^2$. Ainsi, $2\mathbf{Z}$ se ramifie dans $\mathbf{Q}(i)$ avec un indice de ramification de 2. De plus, $(1+i)$ divise (2) ; il s'agit de l'unique idéal premier de $\mathbf{Z}[i]$ qui le divise.

Définition 2.60. Un idéal premier $\mathfrak{p}$ se *décompose* (*complètement*) dans L lorsque chaque $e_i = f_i = 1$ pour tout i. Il est dit *inerte* dans L lorsque $\mathfrak{p}B$ est un idéal premier de B, auquel cas $g = 1 = e_1$.

Exemple 2.61. L'idéal premier $3\mathbf{Z}$ de $\mathbf{Z}$ est inerte dans $\mathbf{Q}(i)$. Ce n'est en revanche pas le cas de l'idéal premier $5\mathbf{Z}$ de $\mathbf{Z}$. Par contre, ce dernier se décompose complètement dans $\mathbf{Q}(i)$ en $(5) = (2+i)(2-i)$. Dès lors, les idéaux $(2+i)$ et $(2-i)$ sont les uniques diviseurs premiers de (5) dans $\mathbf{Z}[i]$.

Lemme 2.62. *Un idéal premier $\mathfrak{P}$ de B divise $\mathfrak{p}$ si et seulement si $\mathfrak{p} = \mathfrak{P} \cap K$.*

Démonstration. Il est clair que $\mathfrak{p} \subseteq \mathfrak{P} \cap K$ et que $\mathfrak{P} \cap K$ est un idéal distinct de A. La maximalité de $\mathfrak{p}$ implique l'égalité, établissant la nécessité. Réciproquement, $\mathfrak{p} \subseteq \mathfrak{P}$ implique que $\mathfrak{p}B \subseteq \mathfrak{P}$ et il s'en suit de la remarque 2.26 que $\mathfrak{P}$ apparaît dans la factorisation de $\mathfrak{p}B$. □

Théorème 2.63. *Soit m le degré de L/K et soient $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ les diviseurs premiers de $\mathfrak{p}$ dans B ; alors*

$$\sum_{i=1}^{g} e_i f_i = m. \tag{2}$$

Lorsque L/K est une extension galoisienne, les indices de ramification e_i sont tous égaux, ainsi que tous les degrés de classe résiduelle f_i. En particulier,

$$g \times e \times f = m.$$

Démonstration. Dans le but de prouver (2), nous allons montrer que les deux membres de l'égalité sont égaux au degré $[B/\mathfrak{p}B : A/\mathfrak{p}]$.

Pour le membre de droite, notons qu'il suffit de vérifier que chaque $[B/\mathfrak{P}_i^{e_i} : A/\mathfrak{p}] = e_i f_i$ car le théorème chinois des restes implique que

$$B/\mathfrak{p}B \;=\; B/\prod_{i=1}^{g}\mathfrak{P}_i^{e_i} \;\simeq\; \prod_{i=1}^{g} B/\mathfrak{P}_i^{e_i}.$$

Par définition $f_i = [B/\mathfrak{P}_i : A/\mathfrak{p}]$. De plus, $\mathfrak{P}_i^{r_i}/\mathfrak{P}_i^{r_i+1}$ est un $B/\mathfrak{P}_i$-module pour tout r_i et, puisqu'il n'y aucun idéal entre $\mathfrak{P}_i^{r_i}$ et $\mathfrak{P}_i^{r_i+1}$, ce quotient est de dimension 1 en tant que $B/\mathfrak{P}_i$-espace vectoriel et donc de dimension f_i en tant que $A/\mathfrak{p}$-espace vectoriel. Ainsi, la dimension de $B/\mathfrak{P}_i^{e_i}$ sur $A/\mathfrak{p}$ est $e_i f_i$.

Le cas du second membre est facile à traiter lorsque B est un A-module libre. En particulier, lorsque A est un idéal principal, l'isomorphisme de A-modules $A^n \to B$ donne lieu à un isomorphisme $K^n \to L$ en tensorisant par K et donc $n = m$; ainsi qu'à un isomorphisme $(A/\mathfrak{p})^n \to B/\mathfrak{p}B$ en tensorisant par $A/\mathfrak{p}$ montrant que $n = [B/\mathfrak{p}B : A/\mathfrak{p}]$.

Considérons à présent S un sous-ensemble multiplicatif de A, disjoint de $\mathfrak{p}$ et tel que $S^{-1}A$ est principal (*e.g.* $S = A \smallsetminus \mathfrak{p}$). Notons $B' = S^{-1}B$ et $A' = S^{-1}A$; il s'en suit de la proposition 1.9 que B' est la clôture intégrale de A' dans L et de la proposition 2.51 que $\mathfrak{p}B' = \prod_{i=1}^{g}(\mathfrak{P}B')^{e_i}$. Par conséquent $\sum_{i=1}^{g} e_i f_i = [B'/\mathfrak{p}B' : A/\mathfrak{p}A']$, or A' est principal, et donc $[B'/\mathfrak{p}B' : A'/\mathfrak{p}A'] = m$. Cette discussion vient vérifier (2).

Supposons désormais que L/K est une extension galoisienne. Un élément $\sigma \in \mathrm{Gal}(L/K)$ envoie B sur lui-même ; en particulier, si $\mathfrak{P}$ est un idéal premier de B, alors $\sigma\mathfrak{P}$ l'est aussi. Le lemme 2.62 nous apprend que si $\mathfrak{P}$ divise $\mathfrak{p}$ alors $\sigma\mathfrak{P}$ divise également $\mathfrak{p}$. Clairement $e(\sigma\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{p})$ et $f(\sigma\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{p})$ et donc il ne reste qu'à montrer que $\mathrm{Gal}(L/K)$ agit transitivement sur les idéaux premiers de B divisant $\mathfrak{p}$.

Supposons que $\mathfrak{P}$ et $\mathfrak{Q}$ divisent tous deux $\mathfrak{p}$ mais que $\mathfrak{Q}$ n'est pas conjugué à $\mathfrak{P}$, *i.e.* il n'existe aucun $\sigma \in \mathrm{Gal}(L/K)$ tel que $\sigma\mathfrak{P} = \mathfrak{Q}$. Selon le théorème chinois des restes, nous pouvons trouver un élément $\beta \in \mathfrak{Q}$ n'appartenant à aucun des $\sigma\mathfrak{P}$. Posons b l'élément $b := \mathrm{Nm}(\beta) = \prod \sigma\beta$. Alors $b \in A$ et, comme $\beta \in \mathfrak{Q}$, nous avons que $b \in \mathfrak{Q} \cap A = \mathfrak{p}$. D'autre part, pour tout $\sigma \in \mathrm{Gal}(L/K)$, $\beta \notin \sigma^{-1}\mathfrak{P}$ et donc $\sigma\beta \notin \mathfrak{P}$. Le fait que $b = \prod \sigma\beta \in \mathfrak{p} \subseteq \mathfrak{P}$ vient alors contredire la primalité de $\mathfrak{P}$. □

2.7 Caractérisation des idéaux premiers se ramifiant

Lemme 2.64. *Soient $A \subseteq B$ deux anneaux dans lequel B est un A-module libre de rang n et dont une base est $(e_1, \ldots, e_n)$. Pour tout idéal $\mathfrak{a}$ de A, $(\bar{e}_1, \ldots, \bar{e}_n)$ est une base de $B/\mathfrak{a}B$ en tant que $A/\mathfrak{a}$-module et*

$$\mathrm{Disc}_{(B/\mathfrak{a}B)/(A/\mathfrak{a})}(\bar{e}_1, \ldots, \bar{e}_n) \equiv \mathrm{Disc}_{B/A}(e_1, \ldots, e_n) \bmod \mathfrak{a}$$

où $\bar{e}_i$ désigne $e_i \bmod \mathfrak{a}$ pour tout i.

Démonstration. Via le même argument que lors de la preuve du théorème précédent, l'isomorphisme

$$A^m \longrightarrow B\colon (a_1, \ldots, a_n) \longmapsto \textstyle\sum_{i=1}^{n} a_i e_i$$

donne lieu, en tensorisant avec $A/\mathfrak{a}$, à un isomorphisme

$$(A/\mathfrak{a})^m \longrightarrow B/\mathfrak{a}\colon (a_1, \ldots, a_n) \longmapsto \textstyle\sum_{i=1}^{n} a_i \bar{e}_i$$

montrant ainsi que $(\bar{e}_1, \ldots, \bar{e}_n)$ est une $A/\mathfrak{a}$-base de $B/\mathfrak{a}B$. La seconde assertion résulte directement des définitions. □

Lemme 2.65. *Soit A un anneau et soient $B_1, \ldots, B_n$ des anneaux contenants A et libres de rang fini en tant que A-modules ; alors*

$$\Delta((\prod_{i=1}^n B_i)/A) = \prod_{i=1}^n \Delta(B_i/A).$$

Démonstration. En choisissant une A-base ε_i pour tous les B_i et en calculant le discriminant de $\prod_{i=1}^n B/A$ avec la base $\bigcup_{i=1}^n \varepsilon_i$. □

Définition 2.66. Un élément α d'un anneau est *nilpotent* lorsqu'il existe un $m > 1$ pour lequel $\alpha^m = 0$. Quand il n'existe aucun élément non nul nilpotent dans un anneau, celui-ci est dit **réduit**.

Exemple 2.67. Tout anneau intègre est réduit ; sinon α et α^{m-1} sont des diviseurs de zéro. En particulier, l'anneau des entiers $\mathcal{O}_L$ d'un corps de nombres L est un anneau réduit. En revanche, tout anneau réduit n'est pas nécessairement intègre : c'est le cas de $\mathbf{Z}/m\mathbf{Z}$ où $m > 1$ n'est pas un nombre premier.

Exemple 2.68. Soit p un nombre premier ; alors p est nilpotent dans $\mathbf{Z}/p^n\mathbf{Z}$ pour $n > 1$. En particulier $\mathbf{Z}/p^n\mathbf{Z}$ n'est pas réduit.

Remarque 2.69. Le produit d'anneaux intègres n'est jamais intègre ; par contre ceci devient vrai en remplaçant intègre par réduit : le produit d'anneaux $A_1 \times \cdots \times A_n$ est réduit si et seulement si chaque A_i l'est.

Rappel 2.70. Un corps est **parfait** lorsque toutes ses extensions finies sont séparables.

Remarque 2.71. Tout corps de caractéristique 0 est parfait. Un corps k de caractéristique $p \neq 0$ est parfait si et seulement si tout élément de k est une puissance p-ième ; en particulier, un corps fini k de caractéristique p est parfait car l'application $k \to k \colon x \mapsto x^p$ est injective, et donc surjective.

Lemme 2.72. *Soit B une algèbre de dimension finie sur un corps parfait k. Alors B est réduit si et seulement si $\Delta(B/k) \neq 0$.*

Démonstration. Supposons l'existence d'un élément nilpotent non nul β de B et choisissons une k-base $(e_1, \ldots, e_n)$ de B en prenant soin d'avoir $e_1 = \beta$. L'élément βe_i est nilpotent pour tout i et donc l'endomorphisme k-linéaire

$$m_{\beta e_i} \colon B \longrightarrow B \colon x \longmapsto \beta e_i x$$

est nilpotent. Ainsi, la matrice associée à $m_{\beta e_i}$ est nilpotente et de telles matrices ont une trace nulle (le polynôme minimal est de la forme X^r). Par conséquent, la première colonne de la matrice $(\mathrm{Tr}(e_i e_j))_{ij}$ est nulle et donc le déterminant aussi.

Réciproquement, supposons que B soit réduit. Nous montrons tout d'abord que l'intersection $\mathfrak{N}$ des idéaux premiers de B est nulle. Soit $b \neq 0$ un élément de B et soit Σ l'ensemble des idéaux de B ne comprenant pas de puissances de b. De par le fait que b ne soit pas nilpotent, Σ contient l'idéal nul et est donc non vide. Comme B est noethérien, Σ possède un élément maximal $\mathfrak{p}$. Nous allons montrer que $\mathfrak{p}$ est premier. Comme $b \notin \mathfrak{p}$, cela montrera que $b \notin \mathfrak{N}$, et cela pour tout b non nul.

Soient x, y deux éléments de B n'appartenant pas à $\mathfrak{p}$. Alors $\mathfrak{p}+(x)$ et $\mathfrak{p}+(y)$ contiennent strictement $\mathfrak{p}$ et, par maximalité de $\mathfrak{p}$ dans Σ,

$$b^m \in \mathfrak{p} + (x) \quad \text{et} \quad b^n \in \mathfrak{p} + (y)$$

pour certains m et n. Disons $b^m = p + cx$ et $b^n = p' + c'y$ où p, $p' \in \mathfrak{p}$ et c, $c' \in B$. Il est alors facile de voir que leur produit b^{m+n} est dans $\mathfrak{p} + (xy)$ et donc que $\mathfrak{p} + (xy)$ n'est pas dans Σ. En particulier $\mathfrak{p} + (xy) \neq \mathfrak{p}$ et $xy \notin \mathfrak{p}$. Par conséquent $\mathfrak{p}$ est premier.

Finalement, soit $\mathfrak{p}$ un idéal premier de B. Alors $B/\mathfrak{p}$ est intègre, algébrique sur k par finitude et est donc un corps par le lemme 2.54. Par conséquent $\mathfrak{p}$ est maximal. Soient $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ des idéaux premiers

de B. Puisqu'ils sont tous maximaux, ils sont deux-à-deux comaximaux. Le théorème chinois des restes implique que

$$B/\bigcap_{i=1}^{n} \mathfrak{p}_i \ \simeq \ \prod_{i=1}^{n} B/\mathfrak{p}_i. \tag{3}$$

Notons également que

$$[B : k] \geq [B/\textstyle\bigcap_{i=1}^{n} \mathfrak{p}_i : k] = \displaystyle\sum_{i=1}^{n} [B/\mathfrak{p}_i : k] \geq n.$$

Par conséquent B possède un nombre fini d'idéaux premiers, disons $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$, sous la contrainte $m \leq [B : k]$ et $\bigcap_{i=1}^{m} \mathfrak{p}_i = 0$. En prenant $n = m$ dans (3), nous trouvons

$$B \simeq \prod_{i=1}^{m} B/\mathfrak{p}_i.$$

Pour tout i, $B/\mathfrak{p}_i$ est un corps et est une extension finie et séparable (car k est parfait) de k. En appliquant la proposition 1.56, nous déduisions que $\Delta((B/\mathfrak{p}_i)/k) \neq 0$ et du lemme précédent nous obtenons que $\Delta(B/k) \neq 0$. □

Théorème 2.73. *Soient L une extension finie d'un corps de nombres K, A un anneau de Dedekind dont le corps des fractions est K (e.g. $A = \mathcal{O}_K$) et B la clôture intégrale de A dans L. Supposons que B soit un A-module libre. Un idéal premier $\mathfrak{p}$ de A se ramifie dans L si et seulement si $\mathfrak{p}$ divise $\Delta(B/A)$; en particulier seul un nombre fini d'idéaux premiers se ramifient.*

Démonstration. Du lemme 2.64, nous pouvons affirmer que

$$\Delta((B/\mathfrak{p}B)/(A/\mathfrak{p})) = \Delta(B/A) \bmod \mathfrak{p},$$

et nous savons du lemme 2.72 que $\Delta((B/\mathfrak{p}B)/(A/\mathfrak{p})) = 0$ est équivalent à ce que $B/\mathfrak{p}B$ ne soit pas réduit. Soit $\mathfrak{p}B = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$ sa factorisation dans l'anneau B. Le théorème chinois des restes implique que $B/\mathfrak{p}B \simeq \prod_{i=1}^{g} B/\mathfrak{P}_i^{e_i}$. Donc $\prod_{i=1}^{g} B/\mathfrak{P}_i^{e_i}$ est réduit si et seulement si chaque $B/\mathfrak{P}_i^{e_i}$ l'est (voir remarque 2.69), ou encore si et seulement si chaque $e_i = 1$. □

Exemple 2.74. Soit $K = \mathbf{Q}(\sqrt{d})$ un corps quadratique. Lorsque $d \equiv 2, 3 \bmod 4\mathbf{Z}$, le discriminant de K est $\Delta_K = 4d$ (voir exemple 1.52) ; dès lors les nombres premiers de $\mathbf{Z}$ qui se ramifient dans K sont 2 et les diviseurs (premiers) de d. Sinon $d \equiv 1 \bmod 4\mathbf{Z}$ et dans ce cas là $\Delta_K = d$ (voir exemple 1.53). Par conséquent les nombres premiers de $\mathbf{Z}$ qui se ramifient dans K sont les diviseurs (premiers) de d.

2.8 Détermination de la factorisation

Soit A un anneau de Dedekind dont le corps des fractions est noté K et soit B la clôture intégrale de A dans une extension finie et séparable L/K.

Théorème 2.75. *Supposons que $B = A[\alpha]$. Soient $f(X)$ le polynôme minimal de α sur K et $\mathfrak{p}$ un idéal premier de A. Soient $g_1(X), \ldots, g_n(X) \in A[X]$ des polynômes distincts et irréductibles modulo $\mathfrak{p}$, vérifiant $f(X) \equiv \prod_{i=1}^{n} g_i(X)^{e_i} \bmod \mathfrak{p}$. Alors*

$$\mathfrak{p}B = \prod_{i=1}^{n} (\mathfrak{p}, g_i(\alpha))^{e_i}$$

est la factorisation de $\mathfrak{p}B$ en un produit de puissances d'idéaux premiers distincts. De plus, $B/(\mathfrak{p}, g_i(\alpha)) \simeq (A/\mathfrak{p})[X]/(\bar{g}_i)$ et donc le degré de la classe résiduelle f_i vaut le degré de g_i.

Démonstration. La retranscription de l'hypothèse amène l'existence d'un isomorphisme donné par

$$\mathrm{ev}_\alpha \colon A[X]/(f(X)) \longrightarrow B \colon X \longmapsto \alpha.$$

En quotientant par $\mathfrak{p}$ et en notant $k = A/\mathfrak{p}$, cet isomorphisme donne lieu à un nouvel isomorphisme

$$\overline{\mathrm{ev}}_\alpha \colon k[X]/(\bar{f}(X)) \longrightarrow B/\mathfrak{p}B \colon X \longmapsto \alpha.$$

L'anneau $k[X]/(\bar{f})$ a pour idéaux maximaux $(\bar{g}_1), \ldots, (\bar{g}_n)$ et remarquons que $\prod_{i=1}^n (\bar{g}_i)^{e_i} = 0$ dans $k[X]/(\bar{f})$ mais aucun autre produit avec des puissances plus petites est nul.

L'idéal $(\bar{g}_i)$ de $k[X]/(\bar{f})$ correspond à l'idéal $(g_i(\alpha)) + \mathfrak{p}B$ de $B/\mathfrak{p}B$, qui lui-même correspond à $\mathfrak{P}_i := (\mathfrak{p}, g_i(\alpha))$ dans B. Par conséquent, $\mathfrak{P}_1, \ldots, \mathfrak{P}_n$ est l'ensemble des idéaux premiers contenant $\mathfrak{p}B$ et il s'agit de l'ensemble des diviseurs premiers de $\mathfrak{p}$ selon la remarque 2.22. Lorsque nous notons $\mathfrak{p}B = \prod_{i=1}^n \mathfrak{P}_i^{e_i}$, les quantités e_i sont caractérisées par le fait que $\mathfrak{p}B$ contienne $\prod_{i=1}^n \mathfrak{P}_i^{e_i}$; cependant il ne contient pas un tel produit lorsque l'un des e_i est remplacé par une plus petite valeur. Alors e_i est l'exposant de $\bar{g}_i$ occurrant dans la factorisation de $\bar{f}$. □

Remarque 2.76. Quand il s'applique, le dernier résultat peut être utilisé afin de prouver les théorèmes 2.63 et 2.73. Par exemple, lorsque $m = \deg(f)$, l'équation $m = \sum_{i=1}^g e_i f_i$ est simplifiée en $\deg(f) = \sum_{i=1}^g e_i \deg(g_i)$.

Remarque 2.77. La conclusion du théorème est valable pour n'importe quel idéal premier $\mathfrak{p}$ de A sous l'hypothèse plus faible : $(\mathrm{Disc}(1, \alpha_1, \ldots, \alpha_{n-1})) = \mathfrak{a}\Delta(B/A)$ avec $\mathfrak{a}$ un idéal de A non divisible par $\mathfrak{p}$. Afin de le prouver, il faut rendre inversible les éléments de $\mathfrak{a}$ ne se trouvant pas dans $\mathfrak{p}$ et d'ensuite appliquer le théorème sur ce nouvel anneau et sa clôture intégrale.

Exemple 2.78. Soit $K = \mathbf{Q}(\sqrt{d})$ un corps quadratique ; étudions le comportement dans $\mathcal{O}_K$ de $p \in \mathbf{Z}$ un nombre premier. Nous avons précédemment montré que $\mathcal{O}_K = \mathbf{Z}[\sqrt{d}]$ ou $\mathbf{Z}[(1+\sqrt{d})/2]$. Dans les deux cas, nous pouvons utiliser l'ensemble $\{1, \sqrt{d}\}$ afin de déterminer la factorisation de p (par la remarque 2.77). Comme l'extension est quadratique, le théorème 2.63 permet seulement trois factorisations possibles de (p) dans $\mathcal{O}_K$, à savoir :

- $(p) = \mathfrak{p}^2$ et donc (p) se ramifie dans $\mathcal{O}_K$ avec $e = 2$, $f = 1$ et $g = 1$, ou
- $(p) = \mathfrak{p}$ et donc (p) est inerte dans $\mathcal{O}_K$ (reste premier) avec $e = 1$, $f = 2$ et $g = 1$, ou
- $(p) = \mathfrak{p}_1\mathfrak{p}_2$ et donc (p) se décompose dans $\mathcal{O}_K$ avec $e_i = 1$, $f_i = 1$ et $g = 2$.

Remarque 2.79. L'exemple précédant peut être approfondi afin d'obtenir que

(*i*) soit p divise Δ_K, et donc (p) se ramifie dans $\mathcal{O}_K$,

(*ii*) soit p est impair et ne divise pas d, auquel cas (p) est le produit de deux idéaux distincts si et seulement si m est un carré modulo $p\mathbf{Z}$, et (p) est inerte $\mathcal{O}_K$ si et seulement si d n'est pas un carré modulo $p\mathbf{Z}$,

(*iii*) soit $p = 2$, avec $d \equiv 1 \bmod 4\mathbf{Z}$, auquel cas (2) est le produit de deux idéaux distincts si et seulement si $d \equiv 1 \bmod 8\mathbf{Z}$, et (2) est inerte $\mathcal{O}_K$ si et seulement si $d \equiv 5 \bmod 8\mathbf{Z}$.

Exemple 2.80. L'anneau $\mathbf{Z}[i\sqrt{5}]$ n'est pas factoriel : $6 = 2 \times 3$ et $(1 + i\sqrt{5}) \times (1 - i\sqrt{5})$ et ces irréductibles sont deux-à-deux non associés. Puisque la factorisation des idéaux est unique, il suffit d'exprimer (2) et (3) en un produit d'idéaux premiers dans $\mathbf{Z}[i\sqrt{5}]$. Sur base du théorème 2.75, avec $f(X) = X^2 + 5$ le polynôme minimal de $i\sqrt{5}$ sur $\mathbf{Q}$:

- $(2) = (2, 1 - i\sqrt{5})^2 =: \mathfrak{p}^2$ puisque $f(X) \equiv (X-1)^2 \bmod 2\mathbf{Z}$, et
- $(3) = (3, 1 - i\sqrt{5})(3, 1 + i\sqrt{5}) =: \mathfrak{q}_1\mathfrak{q}_2$ puisque $f(X) \equiv (X-1)(X+1) \bmod 3\mathbf{Z}$.

Dès lors, $(6) = \mathfrak{p}^2\mathfrak{q}_1\mathfrak{q}_2$ dans $\mathbf{Z}[i\sqrt{5}]$. En particulier $2\mathbf{Z}$ se ramifie dans $K = \mathbf{Q}(i\sqrt{5})$, ce qui n'est pas étonnant puisqu'il divise $\Delta_K = -20$.

2.9 Extensions d'Eisenstein

Dans cette sous-section, nous raffinons le critère d'Eisenstein d'irréductibilité des polynômes sur un anneau de Dedekind.

Rappel 2.81 (Critère d'Eisenstein)**.** Un polynôme $X^n + a_1X^{n-1} + \cdots + a_n \in \mathbf{Z}[X]$ est irréductible dans $\mathbf{Q}[X]$ dès qu'il existe un nombre premier $p \in \mathbf{Z}$ divisant tous les a_i et tel que p^2 ne divise pas a_n.

Ce critère peut également être généralisé à n'importe quel anneau factoriel, donnant lieu au résultat suivant :

Rappel 2.82 (Critère d'Eisenstein)**.** Soit A un anneau factoriel dont le corps des fractions est noté K. Un polynôme $X^n + a_1X^{n-1} + \cdots + a_n \in A[X]$ est irréductible dans $K[X]$ dès qu'il existe un élément premier $\pi \in A$ divisant tous les a_i et tel que π^2 ne divise pas a_n.

Soit A un anneau de Dedekind et soit B sa clôture intégrale dans une extension finie L de son corps des fractions K.

Remarque 2.83. Tout anneau de Dedekind induit une valuation discrète sur son corps des fractions : pour un idéal premier $\mathfrak{p}$ fixé, la valuation $\mathrm{ord}_\mathfrak{p}$ d'un élément non nul x du corps des fractions est la puissance de $\mathfrak{p}$ dans la factorisation de (x).

Remarque 2.84. Soit $\mathfrak{p}$ un idéal premier de A et soit $\mathfrak{P}$ un idéal premier de B divisant $\mathfrak{p}$, disons $\mathfrak{p}B = \mathfrak{P}^e \cdots$. Considérons la valuation discrète $\mathrm{ord}_\mathfrak{p}$ (resp. $\mathrm{ord}_\mathfrak{P}$) sur K (resp. L) induite par $\mathfrak{p}$ (resp. $\mathfrak{P}$) ; alors

$$\mathrm{ord}_\mathfrak{P} \restriction_K = e \cdot \mathrm{ord}_\mathfrak{p}$$

puisque, si $(a) = \mathfrak{p}^m \cdots$ dans A, alors $(a) = \mathfrak{P}^{me} \cdots$ dans B.

Lemme 2.85. *Si $a_1 + \cdots + a_n = 0$, alors la valeur minimale de $\mathrm{ord}(a_i)$ est atteinte pour au moins deux i.*

Démonstration. Si ce n'était pas le cas, disons que $\mathrm{ord}(a_1) < \mathrm{ord}(a_i)$ pour tout $i > 1$. Dès lors, comme $-a_1 = \sum_{i=2}^n a_i$, il s'en suit que

$$\mathrm{ord}(a_1) = \mathrm{ord}\left(\textstyle\sum_{i=2}^n a_i\right) \geq \min_{2 \leq i \leq n} \mathrm{ord}(a_i),$$

menant à une contradiction. □

Définition 2.86. Soient A un anneau de Dedekind et $\mathfrak{p}$ un idéal premier de A. Un polynôme $X^n + a_1X^{n-1} + \cdots + a_n \in A[X]$ est dit d'*Eisenstein en* $\mathfrak{p}$ si

$$\mathrm{ord}_\mathfrak{p}(a_i) > 0, \quad \cdots, \quad \mathrm{ord}_\mathfrak{p}(a_{n-1}) > 0 \quad \text{et} \quad \mathrm{ord}_\mathfrak{p}(a_n) = 1.$$

Proposition 2.87 (Critère d'Eisenstein)**.** *Soit $f(X) \in A[X]$ un polynôme d'Eisenstein en un idéal premier $\mathfrak{p}$ de A ; alors $f(X)$ est irréductible dans $K[X]$. Si α est une racine de $f(X)$, alors $\mathfrak{p}$ est totalement ramifié dans $K(\alpha)$: $\mathfrak{p}B = \mathfrak{P}^m$ avec $\mathfrak{P} = (\mathfrak{p}, \alpha)$ et $m = \deg(f)$.*

Démonstration. Soit α une racine de $f(X)$ et considérons $K(\alpha)$; alors $[K(\alpha) : K] \leq m := \deg(f)$. Soit $\mathfrak{P}$ un idéal premier divisant $\mathfrak{p}$, avec pour indice de ramification e. Considérons l'équation

$$\alpha^m + a_1\alpha^{m-1} + \cdots + a_m = 0.$$

Comme $f(X)$ est d'Eisenstein,

$$\mathrm{ord}_\mathfrak{P}(\alpha^m) = m \cdot \mathrm{ord}_\mathfrak{P}(\alpha), \quad \mathrm{ord}_\mathfrak{P}(a_i\alpha^{m-i}) \geq (m-i) \cdot \mathrm{ord}_\mathfrak{P}(\alpha) + e, \quad \mathrm{ord}_\mathfrak{P}(a_m) = e.$$

Si $\mathrm{ord}_{\mathfrak{P}}(\alpha) = 0$, alors il n'y a qu'une seule valeur minimale de $\mathrm{ord}_{\mathfrak{P}}$ atteinte par α^m, venant contredire le lemme 2.85. Dès lors $\mathrm{ord}_{\mathfrak{P}}(\alpha) \geq 1$ et $\mathrm{ord}_{\mathfrak{P}}(a_i\alpha^{m-i}) > \mathrm{ord}_{\mathfrak{P}}(a_m) = e$ pour $i = 1, \ldots, m-1$. En ayant recours une nouvelle fois au lemme 2.85, nous obtenons que $m \cdot \mathrm{ord}_{\mathfrak{P}}(\alpha) = e$; donc

$$m \cdot \mathrm{ord}_{\mathfrak{P}}(\alpha) = e \leq [K(\alpha) : K] \leq m$$

forçant ainsi $\mathrm{ord}_{\mathfrak{P}}(\alpha)$ à valoir 1 et donc $[K(\alpha) : K] = m = e$. En particulier, $f(X)$ est le polynôme minimal de α sur K et est donc irréductible. □

3 La finitude du nombre de classes

Lors de cette section, nous prouvons l'un des résultats principaux de ce document : le nombre de classes d'un corps de nombres est fini.

3.1 Norme et norme numérique d'un idéal

Soit A un anneau de Dedekind de corps des fractions K et soit B la clôture intégrale de A dans une extension finie et séparable L/K. Nous souhaitons définir un morphisme $\mathscr{N}\colon \mathrm{Id}(B) \to \mathrm{Id}(A)$ compatible avec la notion de norme d'un élément, *i.e.* tel que le diagramme suivant commute :

$$\begin{array}{ccc} L^\times & \xrightarrow{b\mapsto(b)} & \mathrm{Id}(B) \\ \downarrow{\scriptstyle \mathrm{Nm}} & & \downarrow{\scriptstyle \mathscr{N}} \\ K^\times & \xrightarrow{a\mapsto(a)} & \mathrm{Id}(A). \end{array} \tag{4}$$

Comme $\mathrm{Id}(B)$ est le groupe abélien libre sur l'ensemble des idéaux premiers, il nous suffit de définir $\mathscr{N}(\mathfrak{P})$ pour tout idéal premier $\mathfrak{P}$. Dès lors, soit $\mathfrak{p}$ un idéal premier de A et considérons sa factorisation dans B : $\mathfrak{p}B = \prod_{i=1}^g \mathfrak{P}_i^{e_i}$. Si $\mathfrak{p} = (\pi)$ est principal, alors le comportement naturel de $\mathscr{N}$ doit être le suivant :

$$\mathscr{N}(\mathfrak{p}B) = \mathscr{N}(\pi B) = \mathrm{Nm}(\pi)A = (\pi^m) = \mathfrak{p}^m, \quad m = [L:K].$$

De plus, comme $\mathscr{N}\colon \mathrm{Id}(B) \to \mathrm{Id}(A)$ se veut d'être un morphisme de groupe, il faut également s'assurer que

$$\mathscr{N}(\mathfrak{p}B) = \mathscr{N}(\textstyle\prod_{i=1}^g \mathfrak{P}_i^{e_i}) = \prod_{i=1}^g \mathscr{N}(\mathfrak{P}_i)^{e_i}.$$

En comparant ces deux développements et en se remémorant l'égalité $m = \sum_{i=1}^g e_i f_i$ du théorème 2.63, nous constatons qu'il faut poser $\mathscr{N}(\mathfrak{P}_i) = \mathfrak{p}^{f_i}$.

Définition 3.1. La *norme* d'un idéal premier $\mathfrak{P}$ de B est la quantité

$$\mathscr{N}_{L/K}(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})}, \quad \text{avec } \mathfrak{p} = \mathfrak{P} \cap A.$$

Remarque 3.2. La norme $\mathscr{N}\colon \mathrm{Id}(B) \to \mathrm{Id}(A)$ est (par construction) un morphisme de groupe. Dès lors, pour tout $\mathfrak{a} = \mathfrak{P}_1^{s_1} \cdots \mathfrak{P}_n^{s_n}$, la norme de $\mathfrak{a}$ est $\mathscr{N}(\mathfrak{a}) = \mathfrak{p}_1^{s_1 f_1} \cdots \mathfrak{p}_n^{s_n f_n}$.

Proposition 3.3 (Transitivité de la norme)**.** *Soit $K \subseteq L \subseteq M$ une tour d'extensions de corps ; alors pour tout idéal $\mathfrak{a}$ de M,*

$$\mathscr{N}_{L/K} \circ \mathscr{N}_{M/L}(\mathfrak{a}) = \mathscr{N}_{M/K}(\mathfrak{a}).$$

Démonstration. En notant respectivement $A \subseteq B \subseteq C$ la clôture intégrale de A dans K, L et M, nous avons par multiplicativité des degrés que $[C/\mathfrak{Q} : B/\mathfrak{P}] \cdot [B/\mathfrak{P} : A/\mathfrak{p}] = [C/\mathfrak{Q} : A/\mathfrak{p}]$, autrement dit que $f(\mathfrak{Q}/\mathfrak{P}) \cdot f(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{Q}/\mathfrak{p})$. □

Proposition 3.4. *Soit A un anneau de Dedekind dont le corps des fractions est noté K et soit B la clôture intégrale de A dans une extension finie et séparable L/K.*

(i) Pour tout idéal non nul $\mathfrak{a}$ de A, $\mathscr{N}_{L/K}(\mathfrak{a}B) = \mathfrak{a}^m$ où $m = [L:K]$.

(ii) Supposons que L soit galoisienne sur K. Soit $\mathfrak{P}$ un idéal premier non nul de B et posons $\mathfrak{p} = \mathfrak{P} \cap A$. Comme en 2.63, notons $\mathfrak{p}B = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e$. Alors

$$\mathscr{N}(\mathfrak{P})B = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^{ef} = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma\mathfrak{P}.$$

(iii) Pour tout élément non nul $\beta \in B$, $\mathrm{Nm}(\beta)A = \mathscr{N}(\beta B)$, autrement dit (4) commute.

Démonstration. (i) Il suffit de le vérifier sur un idéal premier $\mathfrak{p}$ quelconque : pour un tel idéal, nous avons

$$\mathscr{N}(\mathfrak{p}B) = \mathscr{N}(\textstyle\prod_{i=1}^{g} \mathfrak{P}_i^{e_i}) = \mathfrak{p}^{\sum_{i=1}^{g} e_i f_i} = \mathfrak{p}^m \quad \text{par le théorème 2.63.}$$

(ii) La première égalité découle de l'observation que $\mathscr{N}\mathfrak{P}_i = \mathfrak{p}^f$ pour tout i. Lors de la preuve du théorème 2.63, nous avons constaté que $\mathrm{Gal}(L/K)$ agissait transitivement sur l'ensemble $\{\mathfrak{P}_1, \dots, \mathfrak{P}_g\}$; il s'en suit que chaque $\mathfrak{P}_i$ apparaît exactement $m/g = ef$ fois dans la famille $(\sigma\mathfrak{P} \mid \sigma \in \mathrm{Gal}(L/K))$.

(iii) Commençons par supposer que L est galoisienne sur K et notons $\mathfrak{b} := \beta B$. L'application $\mathrm{Id}(A) \to \mathrm{Id}(B)\colon \mathfrak{a} \mapsto \mathfrak{a}B$ est injective (ce sont les groupes abéliens libres sur l'ensemble de leurs idéaux premiers) et donc il suffit de montrer que $\mathrm{Nm}(\beta)B = \mathscr{N}(\mathfrak{b})B$. C'est le cas :

$$\mathscr{N}(\mathfrak{b})B \overset{(ii)}{=} \prod \sigma\mathfrak{b} = \prod(\sigma\beta B) = (\prod \sigma\beta)B = \mathrm{Nm}(\beta)B.$$

Dans le cas général, soit E une extension galoisienne finie de K contenant L et notons $d = [E : L]$. Soit C la clôture intégrale de B dans E. Du point (i), du cas galoisien précédent et de la transitivité des normes, nous obtenons

$$\mathscr{N}_{L/K}(\beta B)^d = \mathscr{N}_{E/K}(\beta C) = \mathrm{Nm}_{E/K}(\beta)A = \mathrm{Nm}_{L/K}(\beta)^d A$$

et comme le groupe $\mathrm{Id}(A)$ est sans torsion, cela implique que $\mathscr{N}(\beta B) = \mathrm{Nm}(\beta)A$. □

Exemple 3.5. Le point (iii) de la proposition 3.4 fournit un moyen rapide et efficace afin de calculer la norme d'idéaux principaux. Par exemple la norme de l'idéal $(1 + i)$ de $\mathbf{Z}[i]$ est

$$\mathscr{N}_{\mathbf{Q}(i)/\mathbf{Q}}((1 + i)) = (\mathrm{Nm}_{\mathbf{Q}(i)/\mathbf{Q}}(1 + i)) = 2\mathbf{Z}.$$

Noter qu'elle envoie un idéal premier de $\mathbf{Z}[i]$ sur un idéal premier de $\mathbf{Z}$.

Soit $\mathfrak{a}$ un idéal non nul de l'anneau des entiers $\mathcal{O}_K$ d'un corps de nombres L ; alors $\mathfrak{a}$ est d'indice fini dans $\mathcal{O}_K$, légitimant ainsi la définition suivante :

Définition 3.6. La *norme numérique* (parfois *norme absolue*) d'un idéal non nul $\mathfrak{a}$ de $\mathcal{O}_K$ est la quantité

$$\mathbb{N}_{K/\mathbf{Q}}(\mathfrak{a}) = (\mathcal{O}_K : \mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|.$$

Propriété 3.7. *Soient $\mathfrak{a} \subseteq \mathfrak{b}$ deux idéaux tels que $\mathbb{N}(\mathfrak{a}) = \mathbb{N}(\mathfrak{b})$; alors $\mathfrak{a} = \mathfrak{b}$.*

Exemple 3.8. Déterminons la norme numérique de $(1 + i)$ dans $\mathbf{Z}[i]$. Tout d'abord remarquons que $\mathbf{Z}[i]/(1 + i) \simeq \mathbf{Z}/2\mathbf{Z}$. En effet, la division euclidienne dans $\mathbf{Z}[i]$ implique que $a + bi = q(1 + i) + r$ avec $\mathrm{Nm}(r) < \mathrm{Nm}(1 + i) = 2$, réduisant les valeurs de r à 0, 1 et i. Il suffit ensuite de constater que $1 \equiv i \bmod (1 + i)$. De cette manière, nous obtenons que

$$\mathbb{N}_{\mathbf{Q}(i)/\mathbf{Q}}((1 + i)) = 2 = |\mathrm{Nm}_{\mathbf{Q}(i)/\mathbf{Q}}1 + i)|.$$

Cette constatation est un cas particulier de la propriété 3.10.

Proposition 3.9. *Soit $\mathcal{O}_K$ l'anneau des entiers d'un corps de nombres K.*

(i) Pour tout idéal $\mathfrak{a}$ de $\mathcal{O}_K$, $\mathscr{N}_{K/\mathbf{Q}}(\mathfrak{a}) = (\mathbb{N}(\mathfrak{a}))$; en particulier $\mathbb{N}(\mathfrak{ab}) = \mathbb{N}(\mathfrak{a})\mathbb{N}(\mathfrak{b})$.

(ii) Soient $\mathfrak{g} \subseteq \mathfrak{f}$ deux idéaux fractionnaires de K ; alors $(\mathfrak{f} : \mathfrak{g}) = \mathbb{N}(\mathfrak{f}^{-1}\mathfrak{g})$.

Démonstration. (i) Notons $\mathfrak{a} = \prod_{i=1}^{n} \mathfrak{p}_i^{r_i}$ sa factorisation dans $\mathcal{O}_K$ et posons $f_i := f(\mathfrak{p}_i/p_i)$ avec $(p_i) = \mathbf{Z} \cap \mathfrak{p}_i$; alors $\mathscr{N}(\mathfrak{p}_i) = (p_i)^{f_i}$. Via le théorème chinois des restes $\mathcal{O}_K/\mathfrak{a} \simeq \prod_{i=1}^{n} \mathcal{O}_K/\mathfrak{p}_i^{r_i}$ et donc $(\mathcal{O}_K : \mathfrak{a}) = \prod_{i=1}^{n}(\mathcal{O}_K : \mathfrak{p}_i^{r_i})$. Au cours de la preuve du théorème 2.63, nous avons constaté que $(\mathcal{O}_K : \mathfrak{p}_i^{r_i}) = p_i^{f_i r_i}$. Dès lors, nous pouvons conclure que

$$((\mathcal{O}_K : \mathfrak{a})) = \prod_{i=1}^{n}(p_i^{f_i r_i}) = \mathscr{N}_{K/\mathbf{Q}}(\mathfrak{a}).$$

En identifiant l'ensemble des idéaux de $\mathbf{Z}$ par celui des naturels, la norme $\mathscr{N}$ s'identifie à la norme numérique $\mathbb{N}$. Par conséquent, $\mathbb{N}$ hérite de l'aspect multiplicatif de $\mathscr{N}$.

(ii) Pour tout élément $d \in K$ non nul, l'application $K \to K : x \mapsto dx$ est un isomorphisme de groupe additif et donc $(d\mathfrak{f} : d\mathfrak{g}) = (\mathfrak{f} : \mathfrak{g})$. En vertu de l'égalité $(d\mathfrak{f})(d\mathfrak{g})^{-1} = \mathfrak{f}\mathfrak{g}^{-1}$, nous pouvons supposer que $\mathfrak{f}$ et $\mathfrak{g}$ sont des idéaux entiers. La formule découle alors du point (i) ainsi que des égalités suivantes :

$$(\mathcal{O}_K : \mathfrak{f})(\mathfrak{f} : \mathfrak{g}) = (\mathcal{O}_K : \mathfrak{g}) \quad \text{et} \quad \mathbb{N}(\mathfrak{f})\mathbb{N}(\mathfrak{f}^{-1}\mathfrak{g}) = \mathbb{N}(\mathfrak{g}).$$

□

Propriété 3.10. *Si $\mathfrak{a} = (a)$ est un idéal principal de $\mathcal{O}_K$, alors $\mathbb{N}_{K/\mathbf{Q}}(\mathfrak{a}) = |\operatorname{Nm}_{K/\mathbf{Q}}(a)|$. En particulier, ceci vient justifier l'appellation de norme absolue.*

Démonstration. Par la proposition 3.9 et la commutativité du diagramme (4). □

3.2 Enoncé du théorème principal et ses conséquences

Théorème 3.11. *Soit K une extension finie de $\mathbf{Q}$, de degré n et soit $2s$ le nombre de plongements strictement complexes de K ; il existe un ensemble de représentants du groupe des classes d'idéaux de K constitué des idéaux entiers $\mathfrak{a}$ satisfaisant*

$$\mathbb{N}(\mathfrak{a}) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s |\Delta_K|^{\frac{1}{2}}.$$

Remarque 3.12. Cette borne supérieure porte le nom de **borne de Minkowski** ; elle est parfois notée B_K. Le facteur précédant $|\Delta_K|^{\frac{1}{2}}$ porte le nom de **constante de Minkowski** et est parfois noté C_K.

Corollaire 3.13. *Soit K une extension finie de degré n de $\mathbf{Q}$; alors le nombre de classes h_K de K est fini.*

Démonstration. Il suffit de montrer qu'il n'existe qu'un nombre fini d'idéaux entiers $\mathfrak{a}$ de $\mathcal{O}_K$ tels que $\mathbb{N}(\mathfrak{a})$ soit inférieur à la borne de Minkowski – nous allons même faire mieux : il n'existe qu'un nombre fini d'idéaux entiers $\mathfrak{a}$ satisfaisant $\mathbb{N}(\mathfrak{a}) < M$ pour tout naturel M. Si $\mathfrak{a}$ se factorise en $\prod_{i=1}^n \mathfrak{p}_i^{r_i}$, alors $\mathbb{N}(\mathfrak{a}) = \prod_{i=1}^n p_i^{r_i f_i}$ où $(p_i) = \mathfrak{p}_i \cap \mathbf{Z}$. Étant donné que $\mathbb{N}(\mathfrak{a}) < M$, les possibilités de p_i (et donc de $\mathfrak{p}_i$) sont contraintes à être finies, de même pour les exposants r_i. □

Exemple 3.14. Soit $K = \mathbf{Q}(i)$. Rappelons que via l'exemple 1.52, $\Delta_K = -4$. La condition du théorème 3.11 devient

$$\mathbb{N}(\mathfrak{a}) \leq \frac{2}{4}\frac{4}{\pi}2 < 1.27.$$

Il n'y a (hormis $\mathbf{Z}[i]$) aucun idéal satisfaisant cette contrainte. Nous trouvons donc que $h_K = 1$, montrant en particulier que $\mathbf{Z}[i]$ est un anneau principal. En raisonnant sur l'inégalité précédente, les mêmes conclusions s'appliquent lorsque $B_K < 2$, *i.e.* lorsque $K = \mathbf{Q}(\sqrt{d})$ avec $d = -7, -3, -2, -1, 2, 3, 5, 13$.

Exemple 3.15. Soit $K = \mathbf{Q}(\sqrt{-5})$. Cette fois-ci $\Delta_K = -20$ et donc la contrainte du théorème 3.11 devient

$$\mathbb{N}(\mathfrak{a}) \leq \frac{2}{4}\frac{4}{\pi}\sqrt{20} < 3.$$

Dès lors, tout idéal satisfaisant cette inégalité doit diviser (2). En réalité, $(2) = \mathfrak{p}^2$ dans lequel $\mathfrak{p} = (2, 1 + \sqrt{-5})$ et notons que $\mathbb{N}(\mathfrak{p}^2) = \mathbb{N}(2) = 4$; donc $\mathbb{N}(\mathfrak{p}) = 2$. Les idéaux $\mathcal{O}_K$ et $\mathfrak{p}$ forment ainsi un ensemble de représentants de $\mathrm{Cl}(\mathbf{Z}[\sqrt{-5}])$. L'idéal $\mathfrak{p}$ ne peut-être principal puisqu'il n'existe aucun élément $\alpha = m + n\sqrt{-5}$ tel que $\operatorname{Nm}(\alpha) = m^2 + 5n^2 = 2$ et donc $h_K = 2$. En particulier $\mathbf{Z}[\sqrt{-5}]$ n'est pas un anneau principal.

Définition 3.16. Une extension L d'un corps de nombres K est *non ramifiée sur* K si aucun des idéaux premiers de $\mathcal{O}_K$ ne se ramifie dans $\mathcal{O}_L$.

Corollaire 3.17. *Il n'existe pas d'extension non ramifiée de* $\mathbf{Q}$.

Démonstration. Soit K une extension finie de $\mathbf{Q}$. Étant donné qu'un ensemble de représentants pour le groupe des classes d'idéaux doit au moins posséder un élément et que celui-ci doit avoir une norme numérique supérieure (au sens large) à 1, le théorème 3.11 implique que

$$|\Delta_K|^{\frac{1}{2}} \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^s \geq \frac{n^n}{n!}\left(\frac{\pi}{4}\right)^{\frac{n}{2}}.$$

Posons a_n le membre de droite. Alors $a_2 > 1$ et $a_{n+1}/a_n = \sqrt{\pi/4}(1+1/n)^n > 1$; la suite $(a_n)_n$ est strictement croissante. Ainsi, le discriminant de K est de valeur absolue strictement supérieure à 1 et nous savons du théorème 2.73 que tout idéal premier divisant le discriminant se ramifie. □

3.3 Réseaux

Définition 3.18. Soit V un espace vectoriel de dimension n sur $\mathbf{R}$. Un *réseau* Λ de V est un sous-groupe de V de la forme

$$\Lambda = \mathbf{Z}e_1 + \cdots + \mathbf{Z}e_m$$

où la suite $(e_1, \ldots, e_m)$ d'éléments de V est libre. Un réseau est dit *complet* lorsque $m = n$.

Remarque 3.19. Par conséquent, un réseau n'est rien d'autre que le sous-groupe abélien libre de V engendré par les éléments $e_1, \ldots, e_m$ de V, linéairement indépendants sur $\mathbf{R}$.

Exemple 3.20. Pour tout espace vectoriel V de dimension n sur $\mathbf{R}$ et pour tout $m \in \mathbf{Z}$ non nul, $m\mathbf{Z}$ est un réseau de V. Il s'agit là de l'exemple trivial où la suite d'éléments est de longueur 1 et est donc libre si et seulement l'élément est non nul. En particulier, $\mathbf{Z}$ est un réseau de n'importe quel $\mathbf{R}$-espace vectoriel de dimension finie.

Exemple 3.21. Le corps $\mathbf{C}$ peut être vu comme un $\mathbf{R}$-espace vectoriel de dimension 2 ; le sous-anneau $\mathbf{Z}[i] = \mathbf{Z} + \mathbf{Z}i$ est un réseau complet de $\mathbf{C}$.

Exemple 3.22. Le sous-groupe $\mathbf{Z} + \mathbf{Z}\sqrt{2}$ de $\mathbf{R}$ est un groupe abélien libre de rang 2 (car $\sqrt{2}$ n'est pas un rationnel) mais il ne s'agit pas pour autant d'un réseau de $\mathbf{R}$: les éléments 1 et $\sqrt{2}$ ne sont pas linéairement indépendants sur $\mathbf{R}$.

Objectif. Fixons V un espace vectoriel de dimension n sur $\mathbf{R}$. Nous allons donner un critère afin qu'un sous-groupe Λ de V soit un réseau. Le choix d'une base de V détermine un isomorphisme entre V et $\mathbf{R}^n$, et par conséquent une topologie sur V ; cette topologie est indépendante de la base puisque tout automorphisme linéaire de $\mathbf{R}^n$ est un homéomorphisme.

Définition 3.23. Un sous-groupe Λ de V est *discret* lorsque la topologie induite par V sur Λ est discrète.

Remarque 3.24. Autrement dit, un sous-groupe Λ est discret si et seulement si tout point α de Λ possède un voisinage U dans V tel que $U \cap \Lambda = \{\alpha\}$.

Lemme 3.25. *Les conditions suivantes sur un sous-groupe* Λ *d'un espace vectoriel réel de dimension finie sont équivalentes :*

(i) Λ *est un sous-groupe discret.*

(ii) Il existe un ouvert U *de* V *tel que* $U \cap \Lambda = \{0\}$.

(iii) Tout sous-ensemble compact de V *intersecté avec* Λ *est un ensemble fini.*

(iv) Tout sous-ensemble borné de V *intersecté avec* Λ *est un ensemble fini.*

Démonstration. $(i) \Leftrightarrow (ii)$ Il est évident que (i) implique (ii). Réciproquement, notons que la translation $V \to V : x \mapsto \alpha + x$ est un homéomorphisme pour tout $\alpha \in V$. Ainsi, si U est un voisinage de 0 tel que $U \cap \Lambda = \{0\}$, alors $\alpha + U$ est un voisinage de α tel que $(\alpha + U) \cap \Lambda = \{\alpha\}$.

$(i) \Rightarrow (iii)$ Le point (i) affirme que Λ est un espace discret pour la topologie induite. Dès lors, si C est compact, alors $C \cap \Lambda$ est discret et compact. Il se doit, par conséquent, d'être fini.

$(iii) \Rightarrow (iv)$ La fermeture d'un sous-ensemble borné de $\mathbf{R}^n$ (et donc de V) est compact, et donc par le même argument qu'avant, nous concluons.

$(iv) \Rightarrow (ii)$ Soit U un voisinage de 0 ouvert et borné. Alors $S := U \cap \Lambda \smallsetminus \{0\}$ est fini et est dès lors fermé dans V. Il s'en suit que $U \smallsetminus S$ est un voisinage de 0 ouvert et satisfait $(U \smallsetminus S) \cap \Lambda = \{0\}$. □

Proposition 3.26. *Un sous-groupe Λ de V est un réseau si et seulement s'il est discret.*

Démonstration. Tout réseau est clairement un groupe discret. Réciproquement, soit Λ un sous-groupe discret de V et considérons une suite libre $(e_1, \dots, e_m)$ de Λ de longueur maximale. Procédons par induction sur m.

Si $m = 0$, il n'y a dans ce cas rien à prouver.

Si $m = 1$, alors $\Lambda \subseteq \mathbf{R}e_1$. Comme Λ est discret, pour tout $M > 0$, l'ensemble

$$\{ae_1 \mid |a| < M\} \cap \Lambda$$

est fini et donc il existe un $f \in \Lambda$ qui est tel que lorsque nous écrivons $f = ae_1$, a atteint sa valeur minimale > 0. Alors $\Lambda = \mathbf{Z}f$; sinon il existerait $\alpha \in \Lambda \smallsetminus \mathbf{Z}f$ s'écrivant sous la forme $(n + b)f$ avec un certain $n \in \mathbf{Z}$ et un certain $0 < b < 1$. Dans ce cas $(\alpha - nf) = bf = abe_1$, avec $0 < ab < a$, contredisant la minimalité de f.

Si $m > 1$, posons $\Lambda' := \Lambda \cap (\mathbf{R}e_1 + \cdots + \mathbf{R}e_{m-1})$. Il s'agit clairement d'un sous-groupe discret de l'espace vectoriel $V' := \mathbf{R}e_1 + \cdots + \mathbf{R}e_{m-1}$ et donc, par notre hypothèse d'induction, $\Lambda' = \mathbf{Z}f_1 + \cdots + \mathbf{Z}f_{m-1}$ pour certains f_i linéairement indépendants sur $\mathbf{R}$ (ils forment également une base de V'). Tout élément $\alpha \in \Lambda$ peut s'écrire de façon unique sous la forme

$$\alpha = a_1 f_1 + \cdots + a_{m-1} f_{m-1} + ae_m, \quad a_i, a \in \mathbf{R}.$$

Considérons alors l'application $\phi : \Lambda \to \mathbf{R} : \alpha \mapsto a$ dont nous notons Λ'' son image ; remarquons que a est également atteint par

$$(a_1 - [a_1])f_1 + \cdots + (a_{r-1} - [a_{m-1}])f_{m-1} + ae_m$$

où $[-]$ est la partie entière. Dès lors, tout élément $a \in \Lambda''$ appartenant à un ensemble borné (disons $0 \leq |a| < M$) est l'image d'un élément de Λ dans un ensemble borné

$$0 \leq a_i < 1, \quad i = 1, \cdots, m-1 \quad \text{et} \quad |a| < M.$$

Selon le lemme précédent, il n'existe alors qu'un nombre fini de a et donc Λ'' est un réseau de $\mathbf{R}$; disons que $\Lambda'' = \mathbf{Z}\phi(f_m)$ pour un certain $f_m \in \Lambda$.

Soit $\alpha \in \Lambda$; alors $\phi(\alpha) = a\phi(f_m)$ pour un certain $a \in \mathbf{Z}$ et $\phi(\alpha - af_m) = 0$. Il s'en suit que $\alpha - af_m \in \Lambda'$ et donc que

$$\alpha - af_m = a_1 f_1 + \cdots + a_{m-1} f_{m-1}, \quad a_i \in \mathbf{Z}$$

montrant que $\Lambda = \mathbf{Z}f_1 + \cdots + \mathbf{Z}f_m$. □

Définition 3.27. Soit V un $\mathbf{R}$-espace vectoriel de dimension n et soit Λ un réseau complet de V, dont une base est $(e_1, \dots, e_n)$. Un *parallélépipède fondamental* de Λ est un ensemble

$$D = \left\{ \lambda_0 + \textstyle\sum_{i=1}^n a_i e_i \;\middle|\; 0 \leq a_i < 1 \right\}.$$

pour un certain $\lambda_0 \in \Lambda$ fixé.

Remarque 3.28. La forme des parallélépipèdes fondamentaux dépend du choix de la base $(e_1, \dots, e_n)$. Une fois celle-ci fixée, et en faisant varier $\lambda_0 \in \Lambda$, les parallélépipèdes fondamentaux recouvrent tout $\mathbf{R}^n$ sans chevauchement.

Exemple 3.29. Dans $\mathbf{Z}[i]$, en utilisant la base $(1, i)$, chaque maillage (*i.e.* chaque zone délimitée par le carré formé à partir des sommets z, $z+1$ et $z+i$, pour $z \in \mathbf{Z}[i]$) constitue un parallélépipède fondamental (voir Figure 1).

Remarque 3.30. Considérons un parallélépipède fondamental D d'un réseau complet $\Lambda = \mathbf{Z}e_1 + \cdots + \mathbf{Z}e_n$ de $\mathbf{R}^n$, le **volume** de D est

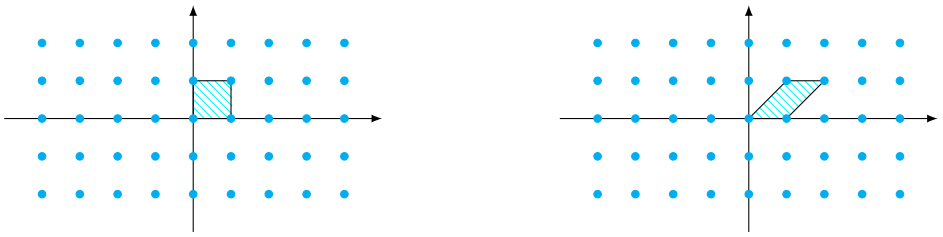
$$\mu(D) = |\det(e_1, \dots, e_n)|.$$

De plus, si $\Lambda = \mathbf{Z}e'_1 + \cdots + \mathbf{Z}e'_n$, alors le déterminant de la matrice des e_i est ± 1 celui de la matrice des e'_i. Par conséquent, le volume d'un parallélépipède fondamental ne dépend pas du choix de la base de Λ.

Remarque 3.31. Lorsque $\Lambda' \subseteq \Lambda$ sont deux réseaux complets de $\mathbf{R}^n$, nous pouvons choisir $(f_1, \dots, f_n)$ et $(e_1, \dots, e_n)$ pour Λ' et Λ telles que $f_i = m_i e_i$ avec m_i un naturel non nul. Avec ce choix de bases, le parallélépipède fondamental D' de Λ' est une union disjointe de $(\Lambda : \Lambda')$ parallélépipèdes fondamentaux D de Λ ; ainsi

$$\frac{\mu(D')}{\mu(D)} = (\Lambda : \Lambda'). \tag{5}$$

Comme précédemment remarqué, le choix d'une base de V détermine un isomorphisme $V \simeq \mathbf{R}^n$ et ainsi une mesure μ sur V. Cette mesure est invariante par translation (puisque la mesure de Lebesgue sur $\mathbf{R}^n$ l'est) et est bien définie à multiplication près par une constante non nulle (dépendant du choix de la base). Le ratio des mesures entre deux ensembles est dès lors bien défini et l'équation (5) est valide pour deux réseaux complets $\Lambda' \subseteq \Lambda$ de V.



(a) dans la base $(1, i)$ (b) dans la base $(1, 1+i)$

FIGURE 1 – Parallélépipède fondamental dans différentes bases de $\mathbf{Z}[i]$.

Théorème 3.32. *Soit D_0 un parallélépipède fondamental d'un réseau complet Λ de V et soit S un sous-ensemble mesurable de V. Si $\mu(S) > \mu(D_0)$, alors S possède deux points distincts α et β tels que $\alpha - \beta \in \Lambda$.*

Démonstration. L'ensemble $S \cap D$ est mesurable pour tout parallélépipède fondamental D et

$$\mu(S) = \sum \mu(S \cap D)$$

où la somme porte sur les translatés de D_0 par les éléments de Λ. Pour tout D, un unique translaté de $S \cap D$ par un élément de Λ est un sous-ensemble de D_0. Comme $\mu(S) > \mu(D_0)$, au moins deux de ces ensembles se chevauchent, *i.e.* il existe deux éléments α, $\beta \in S$ tels que

$$\alpha - \lambda = \beta - \lambda'$$

pour certains λ et $\lambda' \in \Lambda$. Ainsi $\alpha - \beta \in \Lambda$. □

Rappel 3.33. Un ensemble T est **convexe** si il contient le segment joignant n'importe quelle paire des points de T. Un ensemble T est **symétrique en l'origine** si $\alpha \in T$ implique que $-\alpha \in T$.

Remarque 3.34. Soit T un ensemble satisfaisant l'implication

$$\alpha, \beta \in T \quad \Longrightarrow \quad \frac{1}{2}(\alpha - \beta) \in T, \tag{6}$$

et soit $S = 1/2T$. Alors T possède la différence de n'importe quelle paire de points de S et donc T possède un point de Λ autre que l'origine (*i.e.* de 0) dès que

$$\mu(D) < \mu(1/2T) = 2^{-n}\mu(T)$$

autrement dit, dès que

$$\mu(T) > 2^n \mu(D).$$

Il s'en suit que tout ensemble convexe et symétrique en l'origine satisfait l'implication (6) et donc possède un point de $\Lambda \smallsetminus \{0\}$ dès que son volume est strictement supérieur à $2^n\mu(D)$.

Théorème 3.35 (Minkowski)**.** *Soit T un sous-ensemble de V compact, convexe et symétrique en l'origine. Si*

$$\mu(T) \geq 2^n \mu(D)$$

alors T possède un point du réseau autre que l'origine.

Démonstration. Remplaçons T par $(1+\varepsilon)T$, avec $\varepsilon > 0$. Remarquons que $(1+\varepsilon)T$ reste compact, convexe et symétrique en l'origine. De plus

$$\mu((1+\varepsilon)T) = (1+\varepsilon)^n \mu(T) > 2^n \mu(D)$$

et donc $(1+\varepsilon)T$ possède un point de Λ autre que l'origine via la remarque 3.34. Il ne peut posséder qu'un nombre fini de tels points étant donné que Λ est discret et que $(1+\varepsilon)T$ est compact. Puisque T est fermé,

$$T = \bigcap_{\varepsilon > 0} (1+\varepsilon)T.$$

Si aucun de ces points appartenant $\Lambda \cap (1+\varepsilon)T$ et autre que l'origine est dans T, nous sommes capable de rétrécir $(1+\varepsilon)T$ en conservant un $\varepsilon > 0$ de manière à ce qu'il ne possède aucun tel point de Λ, amenant à une contradiction. □

3.4 Detour analytique

Considérons le $\mathbf{R}$-espace vectoriel $V = \mathbf{R}^r \times \mathbf{C}^s$ de dimension $n = r + 2s$ et munissons-le d'une norme :

$$\|\mathbf{x}\| = \sum_{i=1}^{r} |x_i| + 2 \sum_{i=r+1}^{r+s} |z_i|$$

pour $\mathbf{x} = (x_1, \ldots, x_r, z_{r+1}, \ldots, z_{r+s}) \in V$.

Rappel 3.36. La fonction Γ, satisfaisant $\Gamma(n) = (n-1)!$ pour tout naturel non nul n est définie par

$$\Gamma(x) = \int_{0^+}^{\infty} e^{-t} t^{x-1} \, \mathrm{d}t.$$

Lemme 3.37. *Pour tout $a_i > 0$ réel, posons*

$$I(a_1, \ldots, a_m, t) = \int_{Z(t)} x_1^{a_1} \cdots x_m^{a_m} \, dx_1 \cdots dx_m,$$

où $Z(t) = \{\mathbf{x} \in \mathbf{R}^m \mid x_i \geq 0 : \sum_{i=1}^m x_i \leq t\}$; alors

$$I(a_1, \ldots, a_m, t) = t^{\sum a_i + m} \, \frac{\Gamma(a_1+1) \cdots \Gamma(a_m+1)}{\Gamma(a_1 + \cdots + a_m + m + 1)}.$$

Démonstration. En effectuant le changement de variables $x_i' = tx_i$ dans I, nous constatons que

$$I(a_1, \dots, a_m, t) = t^{\sum a_i + m} I(a_1, \dots, a_m, 1).$$

Par conséquent, il suffit de prouver la formule pour $t = 1$. Procédons par induction sur m. Premièrement,

$$I(a_1, 1) = \int_0^1 x_1^{a_1} \, \mathrm{d}x_1 = \frac{1}{a_1 + 1} = \frac{\Gamma(a_1 + 1)}{\Gamma(a_1 + 2)}.$$

Pour le cas général, posons $Z(x_m)' = \{\mathbf{x} \in \mathbf{R}^{m-1} \mid x_i \geq 0, \ \sum_{i=1}^{m-1} x_i \leq 1 - x_m\}$; alors

$$\begin{aligned} I(a_1, \dots, a_m, 1) &= \int_0^1 x_m^{a_m} \left(\int_{Z(x_m)'} x_1^{a_1} \cdots x_{m-1}^{a_{m_1}} \, \mathrm{d}x_1 \cdots \mathrm{d}x_{m-1} \right) \mathrm{d}x_m \\ &= \int_0^1 x_m^{a_m} I(a_1, \dots, a_{m-1}, 1 - x_m) \, \mathrm{d}x_m \\ &= I(a_1, \dots, a_{m-1}, 1) \int_0^1 x_m^{a_m} (1 - x_m)^{\sum a_i + m - 1} \, \mathrm{d}x_m \\ &= I(a_1, \dots, a_{m-1}, 1) \frac{\Gamma(a_m + 1)\Gamma(a_1 + \cdots + a_{m-1} + m)}{\Gamma(a_1 + \cdots + a_m + m + 1)}. \end{aligned}$$

La dernière étape découle de la formule suivante :

$$\int_0^1 x^{m-1}(1 - x)^{n-1} \mathrm{d}x = \mathcal{B}(m, n) = \frac{\Gamma(m)\Gamma(n)}{\Gamma(m + n)}.$$

□

Lemme 3.38. *Pour tout réel $t > 0$, posons $X(t) := \{\mathbf{x} \in V \mid \|\mathbf{x}\| \leq t\}$; alors*

$$\mu(X(t)) = 2^r \left(\frac{\pi}{2}\right)^s \frac{t^n}{n!}.$$

Démonstration. Comme $X(t)$ est symétrique pour les r axes réels, il s'en suit que

$$\mu(X(t)) = 2^r \mu(Y(t))$$

avec $Y(t) := \{\mathbf{x} \mid \|\mathbf{x}\| \leq t : x_1, \dots, x_r \geq 0\}$. Pour les variables complexes, nous procédons à un changement de variable :

$$z_j = x_j + iy_j = \frac{1}{2}\rho_j(\cos\theta_j + i \sin\theta_j).$$

Le jacobien relatif à ce changement de variable est $\rho_j/4$. Après intégration sur les θ_j où $0 \leq \theta_j \leq 2\pi$, nous trouvons que

$$\mu(X(t)) = 2^r \, 4^{-s} \, (2\pi)^s \int_Z \rho_{r+1} \cdots \rho_{r+s} \, \mathrm{d}x_1 \cdots \mathrm{d}x_r \mathrm{d}\rho_{r+1} \cdots \mathrm{d}\rho_{r+s},$$

dans lequel Z désigne l'espace

$$Z = \left\{(\mathbf{x}, \rho) \in \mathbf{R}^{r+s} \;\middle|\; x_i, \rho_i \geq 0, \ \sum_{i=1}^{r} x_i + \sum_{i=r+1}^{r+s} \rho_i \leq t\right\}.$$

Le résultat suit alors du lemme précédant, en prenant $m = r + s$, $a_i = 0$ pour $1 \leq i \leq r$ et $a_i = 1$ pour $r + 1 \leq i \leq m$. □

Exemple 3.39. Lorsque $r = 2$ et $s = 0$, alors $X(t)$ est défini comme l'ensemble des couples (x, y) tels que $|x| + |y| \leq t$. Il s'agit d'un carré de coté de longueur $\sqrt{2}t$. Ainsi $\mu(X(t)) = 2t^2$. Si maintenant $r = 0$ et $s = 1$, alors $X(t)$ est un cercle de rayon $t/2$, dont l'aire est $\pi t^2/4$. Noter que ces volumes coïncident avec les résultats élémentaires de calcul de volume.

Lemme 3.40. *La moyenne géométrique d'un ensemble fini de réels positifs est majorée par leur moyenne arithmétique : soient $a_1, \ldots, a_n$ des réels strictement positifs, alors*

$$\left(\prod_{i=1}^{n} a_i\right)^{\frac{1}{n}} \leq \frac{1}{n}\sum_{i=1}^{n} a_i.$$

Démonstration. En consultant [AmGm]. □

3.5 Finitude du nombre de classes

Soit K un corps de nombres, de degré n sur $\mathbf{Q}$. Supposons qu'il possède r plongements réels $\sigma_1, \ldots, \sigma_r$ ainsi que $2s$ plongements complexes $\sigma_{r+1}, \overline{\sigma}_{r+1}, \ldots, \sigma_{r+s}, \overline{\sigma}_{r+s}$, de sorte que $n = r + 2s$. Nous obtenons un plongement $K \to \mathbf{R}^r \times \mathbf{C}^s$ en définissant :

$$\sigma\colon \begin{cases} K & \hookrightarrow & \mathbf{R}^r \times \mathbf{C}^s \\ \alpha & \longmapsto & (\sigma_1\alpha, \ldots, \sigma_{r+s}\alpha). \end{cases} \tag{7}$$

Nous identifions $V := \mathbf{R}^r \times \mathbf{C}^s$ à $\mathbf{R}^n$ en utilisant la base $(1, i)$ pour $\mathbf{C}$.

Proposition 3.41. *Soit $\mathfrak{a}$ un idéal non nul de $\mathcal{O}_K$; alors $\sigma(\mathfrak{a})$ est un réseau complet de V et le volume d'un parallélépipède fondamental de $\sigma(\mathfrak{a})$ vaut $2^{-s}\mathbb{N}(\mathfrak{a})|\Delta_K|^{\frac{1}{2}}$.*

Démonstration. En véhiculant un argument similaire à celui de la fin de preuve de la proposition 1.59, $\mathfrak{a}$ est un $\mathbf{Z}$-module libre de rang n ; soit $(\alpha_1, \ldots, \alpha_n)$ l'une de ses bases. Afin de montrer que $\sigma(\mathfrak{a})$ est un réseau, nous vérifions que les vecteurs $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$ sont linéairement indépendants. Pour ce faire, nous montrons que la matrice A dont la i-ième ligne est

$$\begin{bmatrix} \sigma_1\alpha_i & \cdots & \sigma_r\alpha_i & \Re(\sigma_{r+1}\alpha_i) & \Im(\sigma_{r+1}\alpha_i) & \cdots & \Re(\sigma_{r+s}\alpha_i) & \Im(\sigma_{r+s}\alpha_i) \end{bmatrix}$$

a un déterminant non nul. Tout d'abord considérons la matrice B dont la i-ième ligne est donnée par

$$\begin{bmatrix} \sigma_1\alpha_i & \cdots & \sigma_r\alpha_i & \sigma_{r+1}\alpha_i & \overline{\sigma}_{r+1}\alpha_i & \cdots & \sigma_{r+s}\alpha_i & \overline{\sigma}_{r+s}\alpha_i \end{bmatrix}$$

Nous avons vu lors de la proposition 1.56 que $\det(B)^2 = \mathrm{Disc}(\alpha_1, \ldots, \alpha_n) \neq 0$. Remarquons que la matrice A s'obtient à partir de B de la manière suivante : ajouter la $r+2$-ième colonne dans B à la $r+1$-ième colonne, ensuite soustraire la moitié de la $r+1$-ième colonne de la $r+2$-ième colonne. Cela donne $2\Re(\sigma_{r+1}(\alpha_i))$ en colonne $r+1$ et $-i\Im(\sigma_{r+1}(\alpha_i))$ en colonne $r+2$. Il suffit ensuite de répéter ce processus à chaque autre paire de colonnes. Ces opérations élémentaires viennent perturber le déterminant de A par un facteur de $(-2i)^s$, donc

$$\det(B) = (-2i)^s \ \det(A)$$

et ainsi

$$\det(A) = (-2i)^{-s} \ \det(B) = \pm(-2i)^{-s} \ \mathrm{Disc}(\alpha_1, \ldots, \alpha_n)^{\frac{1}{2}} \neq 0.$$

Par conséquent $\sigma(\mathfrak{a})$ est un réseau complet de V.

Comme $\sigma(\mathfrak{a}) = \mathbf{Z}\sigma(\alpha_1) + \cdots + \mathbf{Z}\sigma(\alpha_n)$, le volume d'un parallélépipède fondamental D de $\sigma(\mathfrak{a})$ vaut $|\det(A)|$ et nous savons de la remarque 1.55 que

$$|\mathrm{Disc}(\alpha_1, \ldots, \alpha_n)| = (\mathcal{O}_K : \mathfrak{a})^2 \ |\Delta_K|.$$

Dès lors,

$$\mu(D) = |\det(A)| = 2^{-s} \ |\mathrm{Disc}(\alpha_1, \ldots, \alpha_n)| = 2^{-s} \ \mathbb{N}(\mathfrak{a}) \ |\Delta_K|^{\frac{1}{2}}.$$

□

Proposition 3.42. *Soit $\mathfrak{a}$ un idéal non nul de $\mathcal{O}_K$; alors $\mathfrak{a}$ possède un élément α de $K^\times$ satisfaisant*

$$|\operatorname{Nm}(\alpha)| \leq \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\, \mathbb{N}(\mathfrak{a})\, |\Delta_K|^{\frac{1}{2}}.$$

Démonstration. Soit $X(t)$ défini comme en 3.38 et soit D un parallélépipède fondamental de $\sigma(\mathfrak{a})$. L'ensemble $X(t)$ est compact, convexe et symétrique en l'origine ; dès lors, pour un t suffisamment grand afin que $\mu(X(t)) \geq 2^n \mu(D)$, le théorème de Minkowski implique que $X(t)$ possède un point $\sigma(\alpha) \in \sigma(\mathfrak{a})$ non nul. Pour cet $\alpha \in \mathfrak{a}$,

$$\begin{aligned} |\operatorname{Nm}(\alpha)| &= |\sigma_1(\alpha)| \cdots |\sigma_r(\alpha)||\sigma_{r+1}(\alpha)|^2 \cdots |\sigma_{r+s}(\alpha)|^2 \\ &\overset{3.40}{\leq} \left(\textstyle\sum_{i=1}^{r} |\sigma_i(\alpha)| + \sum_{i=r+1}^{r+s} 2|\sigma_i(\alpha)|\right)^n / n^n \\ &\leq t^n / n^n. \end{aligned}$$

Afin d'obtenir $\mu(X(t)) \geq 2^n \mu(D)$, il faut que (voir 3.38 et 3.41) :

$$2^r \left(\frac{\pi}{2}\right)^s \frac{t^n}{n!} \geq 2^n\, 2^{-s}\, \mathbb{N}(\mathfrak{a})\, |\Delta_K|^{\frac{1}{2}}$$

ou dit autrement, il faut que :

$$t^n \geq n!\, \frac{2^{n-r}}{\pi^s}\, \mathbb{N}(\mathfrak{a})\, |\Delta_K|^{\frac{1}{2}}.$$

En prenant t^n égal au membre droit, nous trouvons que

$$|\operatorname{Nm}(\alpha)| \leq \frac{n!}{n^n}\, \frac{2^{n-r}}{\pi^s}\, \mathbb{N}(\mathfrak{a})\, |\Delta_K|^{\frac{1}{2}}$$

et comme $n - r = 2s$, nous concluons la preuve. □

Remarque 3.43. La proposition 3.42 peut s'avérer d'une grande utilité afin de déterminer si un idéal entier est principal.

Démonstration du théorème 3.11. Soit $\mathfrak{f}$ un idéal fractionnaire de K ; il nous faut alors montrer que la classe de $\mathfrak{f}$ dans le groupe des classes d'idéaux est représentée par un idéal entier $\mathfrak{a}$ satisfaisant

$$\mathbb{N}(\mathfrak{a}) \leq B_K := \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s |\Delta_K|^{\frac{1}{2}}.$$

Pour un certain $d \in K^\times$, $d\mathfrak{f}^{-1}$ est un idéal entier, disons que $(d) \cdot \mathfrak{f}^{-1} = \mathfrak{b}$. Selon le résultat précédent, il existe un $\beta \in \mathfrak{b}$ non nul tel que

$$|\operatorname{Nm}(\beta)| \leq B_K\, \mathbb{N}(\mathfrak{b}).$$

Comme $\beta\mathcal{O}_K \subseteq \mathfrak{b}$, il s'en suit que $\beta\mathcal{O}_K = \mathfrak{a}\mathfrak{b}$ pour un certain idéal entier $\mathfrak{a}$. De plus, la propriété 3.10 implique que

$$\mathbb{N}(\mathfrak{a})\, \mathbb{N}(\mathfrak{b}) = |\operatorname{Nm}(\beta)| \leq B_K\, \mathbb{N}(\mathfrak{b}).$$

En divisant par $\mathbb{N}(\mathfrak{b})$ dans chaque membre, nous obtenons que $\mathbb{N}(\mathfrak{a}) \leq B_K$. □

4 Le théorème des unités

Nous prouvons au cours de cette section le deuxième résultat principal de ce document : le théorème des unités (théorème 4.4). Celui-ci fournit un dévissage du groupe des unités d'un corps de nombres.

4.1 Énoncé du théorème

Soit K un corps de nombres, de degré n sur $\mathbf{Q}$ et reprenons nos notations précédentes : r désigne le nombre de plongements réels de K et $2s$ celui de ses plongements complexes.

Définition 4.1. Une *unité* de K est un élément inversible dans l'anneau des entiers $\mathcal{O}_K$ de K. Ces unités forment un groupe multiplicatif, noté U_K.

Exemple 4.2. Selon la proposition 1.32, les éléments 1, i, -1 et $-i$ sont les seules unités de $\mathbf{Q}(i)$. Il s'agit également des racines quatrièmes de l'unité. Attention, l'appellation *unité* a deux sens dans ce chapitre : celui défini précédemment et celui d'être racine de 1. Toutefois, la clarté du contexte permettra de distinguer aisément ces deux notions.

Remarque 4.3. La partie de torsion de U_K est le groupe $(U_K)_{\text{tors}} = \mu(K)$ des racines de l'unité comprise dans K.

Théorème 4.4 (des unités)**.** *Le groupe des unités de K se dévisse en*

$$U_K \simeq \mu(K) \times \mathbf{Z}^{r+s-1}. \tag{8}$$

Remarque 4.5. Par la suite, nous désignerons par rang de U_K l'exposant de $\mathbf{Z}$ (*i.e.* le rang du groupe abélien libre) apparaissant dans l'isomorphisme (8).

Exemple 4.6. Il s'en suit que si K est un corps quadratique réel, $r+s-1 = 1$ et donc $U_K \simeq \mu(K) \times \mathbf{Z}$. En revanche, lorsqu'il s'agit d'un corps quadratique complexe, $r+s-1 = 0$ et donc $U_K = \mu(K)$; c'est notamment le cas des inversibles de $\mathbf{Z}[i]$. Nous reviendrons plus en détails sur cet exemple lors d'une prochaine section dédiée aux corps quadratiques.

Définition 4.7. Une suite d'unités $(u_1, \dots, u_{r+s-1})$ de K est un *système fondamental d'unités* s'il s'agit d'une base de U_K modulo la torsion, *i.e.* si toute unité $u \in U_K$ peut s'écrire de façon unique sous la forme

$$u = \zeta u_1^{m_1} \cdots u_{r+s-1}^{m_{r+s-1}}, \quad \zeta \in \mu(K),\ m_i \in \mathbf{Z}.$$

Remarque 4.8. Le théorème 4.4 implique que $\mu(K)$ est fini (et donc cyclique). Une autre manière de le voir est en ayant recourt à la théorie des corps : si ζ_m est une racine primitive m-ième de l'unité, alors $\mathbf{Q}(\zeta_m)$ est une extension galoisienne de $\mathbf{Q}$, dont le groupe de galois est isomorphe à $(\mathbf{Z}/m\mathbf{Z})^\times$ et dont l'ordre est $\varphi(m)$. Dès lors, $\varphi(m)$ divise $[K : \mathbf{Q}]$ dès que $\zeta_m \in K$; montrant que K ne peut posséder qu'un nombre fini de racines de l'unité.

Lemme 4.9. *Soit α un élément de K ; alors α est une unité de K si et seulement si $\alpha \in \mathcal{O}_K$ et* $\mathrm{Nm}_{K/\mathbf{Q}}(\alpha) = \pm 1$.

Démonstration. Si α est une unité de K, alors $\alpha\beta = 1$ pour un certain $\beta \in \mathcal{O}_K$. Dès lors, comme $\mathbf{Z}$ est intégralement clos, $\mathrm{Nm}(\alpha)$ et $\mathrm{Nm}(\beta)$ sont des éléments de $\mathbf{Z}$ et $1 = \mathrm{Nm}(\alpha\beta)$ implique que $\mathrm{Nm}(\alpha) \in \mathbf{Z}^\times = \{\pm 1\}$. Réciproquement, α satisfait une équation de la forme

$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_{n-1}\alpha \pm 1 = 0, \quad a_i \in \mathbf{Z}$$

et donc $\pm(\alpha^{n-1} + \cdots + a_{n-1})$ est l'inverse de α et est un entier de K ; ainsi α est une unité de K. □

4.2 Preuve que U_K est de type fini

Proposition 4.10. *Pour tous m et $M \in \mathbf{Z}$, l'ensemble des éléments entiers $\alpha \in K$ satisfaisant*

(i) le degré du polynôme minimal de α est inférieur (au sens large) à m, et

(ii) $|\alpha'| < M$ pour tous les conjugués α' de α

est fini.

Démonstration. La première condition nous apprend que α est racine d'un polynôme monique irréductible de degré inférieur à m et la seconde implique que les coefficients de ce polynôme sont bornés suivant M. Étant donné qu'ils s'agit de coefficients dans $\mathbf{Z}$, il n'existe qu'un nombre fini de tels polynômes, et donc un nombre fini de α. □

Corollaire 4.11. *Tout $\alpha \in \mathcal{O}_K$ dont les conjugués dans $\mathbf{C}$ sont de module 1 est une racine de l'unité.*

Démonstration. Selon la proposition précédente, l'ensemble $\{1, \alpha, \alpha^2, \ldots\}$ est fini ; il s'en suit que α est une racine de l'unité. □

Remarque 4.12. Dans le corollaire précédent, il est crucial que α soit entier : $\alpha = (3+4i)/5$ et ses conjugués sont de module 1, tout comme leurs puissances, mais $\{1, \alpha, \alpha^2, \ldots\}$ n'est pas fini.

À partir du plongement $K \to \mathbf{R}^r \times \mathbf{C}^s$ donné en (7), nous construisons un morphisme de groupe multiplicatif vers un groupe additif (en ayant recours au logarithme réel) :

$$L\colon \left\{ \begin{array}{ccc} K^\times & \longrightarrow & \mathbf{R}^{r+s} \\ \alpha & \longmapsto & (\ln|\sigma_1\alpha|, \ldots, \ln|\sigma_r\alpha|, \ln|\sigma_{r+1}\alpha|, \ldots, \ln|\sigma_{r+s}\alpha|). \end{array} \right.$$

Une simple vérification montre que $L\colon K^\times \to \mathbf{R}^{r+s}$ est bel et bien un morphisme. Lorsque u est une unité de K, elle satisfait $\mathrm{Nm}(u) = \pm 1$ et donc

$$|\sigma_1 u| \cdots |\sigma_r u||\sigma_{r+1} u|^2 \cdots |\sigma_{r+s} u|^2 = 1.$$

En appliquant les logarithmes, nous constatons que $L(u)$ appartient à l'hyperplan

$$H \equiv x_1 + \cdots + x_r + 2x_{r+1} + \cdots + 2x_{r+s} = 0.$$

L'abandon de la dernière coordonnée définit un isomorphisme $H \simeq \mathbf{R}^{r+s-1}$.

Proposition 4.13. *L'image de $L\colon U_K \to H$ est un réseau de H ; le noyau de L est un groupe fini et vaut $\mu(K)$.*

Démonstration. Soit C un sous-ensemble borné de H comprenant 0, disons $C \subseteq \{\mathbf{x} \in H \mid |x_i| \leq M\}$. Si $L(u) \in C$, alors chaque $|\sigma_i u| \leq e^M$ et la proposition 4.10 nous permet d'affirmer qu'il n'y a qu'un nombre fini de tels u. Par conséquent $L(U_K) \cap C$ est fini, impliquant que $L(U_K)$ est un réseau de H (proposition 3.26). Si α est dans le noyau de L, alors chaque $|\sigma_i \alpha| = 1$ et donc, à nouveau par 4.10, le noyau de L est fini. □

Remarque 4.14. Comme le noyau de L est fini, $\mathrm{rang}(U_K) = \mathrm{rang}(L(U_K)) \leq \dim H = r + s - 1$.

4.3 Calcul du rang de U_K

Lemme 4.15. *Soit $(a_{ij})_{ij}$ une matrice de taille $m \times m$ à coefficients dans $\mathbf{R}$ vérifiant*

(i) pour tout $i \neq j$, $a_{ij} < 0$, et

(ii) pour tout $i = 1, \ldots, m$, $\sum_{j=1}^m a_{ij} > 0$.

Alors la matrice $(a_{ij})_{ij}$ est inversible.

Démonstration. Si ce n'était pas le cas, le système formé des m équations

$$\sum_{j=1}^{m} a_{ij}x_j = 0, \quad i = 1, \dots, m$$

posséderait une solution non triviale (notons-là $x_1, \dots, x_m$) et soit i^* tel que $|x_{i^*}| = \max |x_i|$. Nous pouvons adapter la solution de manière à avoir $x_{i^*} = 1$. Alors $|x_j| \leq 1$ pour $j \neq i^*$, et la i^*-ième équation amène à une contradiction :

$$0 \;=\; \sum_{j=1}^{m} a_{i^*j}x_j \;=\; a_{i^*}x_{i_0} + \sum_{j\neq i^*} a_{i^*j}x_j \;\geq\; a_{i^*}x_{i^*} + \sum_{j\neq i^*} a_{i^*j} \;>\; 0. \qquad \square$$

Théorème 4.16. *Le réseau $L(U_K)$ de H est complet ; ainsi U_K est de rang $r + s - 1$.*

Démonstration. Afin de prouver ce théorème, nous avons besoin d'expliciter une manière de construire les unités. Nous considérons à nouveau le plongement $\sigma\colon K \to \mathbf{R}^r \times \mathbf{C}^s$ donné en (7), en voyant cette fois-ci les éléments de $\mathbf{R}^r \times \mathbf{C}^s$ comme des éléments de $\mathbf{R}^{r+2s}$. Pour $\mathbf{x} = (x_1, \dots, x_r, x_{r+1}, \dots, x_{r+s}) \in \mathbf{R}^r \times \mathbf{C}^s$, nous définissons

$$\mathrm{Nm}(\mathbf{x}) = x_1 \cdots x_r \cdot (x_{r+1} \cdot \overline{x}_{r+1}) \cdots (x_{r+s} \cdot \overline{x}_{r+s})$$

et nous notons $\mathrm{Nm}(\alpha) \coloneqq \mathrm{Nm}(\sigma(\alpha))$ pour tout $\alpha \in K$. Profitons également de l'instant afin de remarquer que $|\mathrm{Nm}(\mathbf{x})| = |x_1| \cdots |x_r||x_{r+1}|^2 \cdots |x_{r+s}|^2$.

Rappelons de la proposition 3.41 que $\sigma(\mathcal{O}_K)$ est un réseau complet de $\mathbf{R}^r \times \mathbf{C}^s$ et que le volume d'un parallélépipède fondamental vaut $2^{-s}|\Delta_K|^{\frac{1}{2}}$; plus précisément, si $(\alpha_1, \dots, \alpha_n)$ est une base entière de K, nous avons alors montré que la valeur absolue du déterminant de la matrice dont la i-ième ligne est

$$\begin{bmatrix} \sigma_1\alpha_i & \cdots & \sigma_r\alpha_i & \Re(\sigma_{r+1}\alpha_i) & \Im(\sigma_{r+1}\alpha_i) & \cdots & \Re(\sigma_{r+s}\alpha_i) & \Im(\sigma_{r+s}\alpha_i) \end{bmatrix}$$

vaut $2^{-s}|\Delta_K|^{\frac{1}{2}}$. Cette matrice peut s'obtenir via des opérations élémentaires depuis la matrice dont la i-ième ligne est

$$\begin{bmatrix} \sigma_1\alpha_i & \cdots & \sigma_r\alpha_i & \sigma_{r+1}\alpha_i & \overline{\sigma}_{r+1}\alpha_i & \cdots & \sigma_{r+s}\alpha_i & \overline{\sigma}_{r+s}\alpha_i \end{bmatrix}.$$

Ces opérations élémentaires ne font que multiplier la valeur absolue du déterminant par 2^{-s} et nous savons que le déterminant de cette seconde matrice vaut $\pm|\Delta_K|^{\frac{1}{2}}$.

Pour le reste de la preuve, $\mathbf{x}$ est un point de $\mathbf{R}^r \times \mathbf{C}^s$ satisfaisant $1/2 \leq |\mathrm{Nm}(\mathbf{x})| \leq 1$. Posons

$$\mathbf{x} \cdot \sigma(\mathcal{O}_K) \coloneqq \{\mathbf{x} \cdot \sigma(\alpha) \mid \alpha \in \mathcal{O}_K\}.$$

Noter que cette multiplication a un sens puisque $\mathbf{R}^r \times \mathbf{C}^s$ est un anneau. Il s'agit à nouveau d'un réseau de $\mathbf{R}^r \times \mathbf{C}^s$, dont le volume d'un parallélépipède fondamental est donné par le déterminant de la matrice dont la i-ième ligne est

$$\begin{bmatrix} x_1\sigma_1(\alpha_i) & \cdots & x_r\sigma_r(\alpha_i) & \Re(x_{r+1}\sigma_{r+1}(\alpha_i)) & \Im(x_{r+1}\sigma_{r+s}(\alpha_i)) & \cdots \end{bmatrix}$$

Comme précédemment, la valeur absolue du déterminant de cette matrice est 2^{-s} fois celui de la matrice dont la i-ième ligne est

$$\begin{bmatrix} x_1\sigma_1(\alpha_i) & \cdots & x_r\sigma_r(\alpha_i) & x_{r+1}\sigma_{r+1}(\alpha_i) & \overline{x}_{r+1}\overline{\sigma}_{r+1}(\alpha_i) & \cdots \end{bmatrix}$$

valant $|\Delta_K|^{\frac{1}{2}}|\mathrm{Nm}(\mathbf{x})|$. Par conséquent $\mathbf{x} \cdot \sigma(\mathcal{O}_K)$ est un réseau dont le volume d'un parallélépipède fondamental vaut $2^{-s}|\Delta_K|^{\frac{1}{2}}|\mathrm{Nm}(\mathbf{x})|$. Noter que puisque $1/2 \leq |\mathrm{Nm}(\mathbf{x})| \leq 1$, ces volumes sont bornés.

Soit T un sous-ensemble compact et convexe de $\mathbf{R}^r \times \mathbf{C}^s$, étant également symétrique en l'origine et dont le volume est suffisamment grand afin que, pour tout $\mathbf{x}$, le théorème de Minkowski (3.35) fournisse

l'existence d'un point $\gamma \in \mathcal{O}_K$ non nul tel que $\mathbf{x} \cdot \sigma(\gamma) \in T$. Les points de T ont alors des coordonnées bornées et donc une norme bornée ; ainsi

$$\mathbf{x} \cdot \sigma(\gamma) \in T \quad \Longrightarrow \quad |\operatorname{Nm}(\mathbf{x} \cdot \sigma(\gamma))| \leq M$$

pour un certain $M \in \mathbf{Z}$ (dépendant de T). Par conséquent, $|\operatorname{Nm}(\gamma)| \leq M/\operatorname{Nm}(\mathbf{x}) \leq 2M$. Considérons l'ensemble des idéaux principaux $\gamma\mathcal{O}_K$ où γ parcourt les éléments γ de $\mathcal{O}_K$ tels que $\mathbf{x} \cdot \sigma(\gamma)$ appartient à T pour un certain $\mathbf{x}$. La norme numérique d'un tel idéal est bornée par $2M$; il ne peut donc y avoir qu'un nombre fini de tels idéaux, disons $\gamma_1\mathcal{O}_K, \ldots, \gamma_t\mathcal{O}_K$. Si γ est n'importe quel élément de $\mathcal{O}_K$ satisfaisant $\mathbf{x} \cdot \sigma(\gamma) \in T$ pour un certain $\mathbf{x}$, alors $\gamma\mathcal{O}_K = \gamma_i\mathcal{O}_K$ pour un certain i et donc il existe une unité u de K telle que $\gamma = u\gamma_i$. Alors $\mathbf{x} \cdot \sigma(u) \in \sigma(\gamma_i)^{-1} \cdot T$. L'ensemble

$$T' := \bigcup_{i=1}^{t} \sigma(\gamma_i)^{-1} \cdot T$$

est borné et donc nous avons montré qu'en tout point $\mathbf{x}$, il existe une unité u de K telle que les coordonnées de $\mathbf{x} \cdot \sigma(u)$ sont uniformément bornées en $\mathbf{x}$ (l'ensemble T' est indépendant de $\mathbf{x}$).

Montrons désormais que $L(U)$ est un réseau complet de H. Si $r + s - 1 = 0$, il n'y a rien à prouver et donc supposons que $r + s - 1 \geq 1$. Pour tout $1 \leq i \leq r + s$, choisissons un $\mathbf{x}$ dans notre ensemble dont toutes ses coordonnées (appart x_i) sont suffisamment grandes comparées à T' et que x_i est suffisamment petite de manière à avoir $|\operatorname{Nm}(\mathbf{x})| = 1$. Nous savons qu'il existe une unité u_i de K telle que $\mathbf{x} \cdot \sigma(u_i)$ possède des coordonnées bornées ; nous en déduisons donc que $|\sigma_j(u_j)| < 1$ pour tout $j \neq i$ et ainsi que $\ln|\sigma_j(u_j)| < 0$.

La suite de vecteurs $(L(u_1), \ldots, L(u_{r+s-1}))$ est libre dans le réseau $L(U)$. En effet, pour l'affirmer il suffit de montrer que la matrice dont la i-ième ligne est

$$\begin{bmatrix} \ell_1(u_i) & \cdots & \ell_r(u_i) & 2\ell_{r+1}(u_i) & \cdots & 2\ell_{r+s-1}(u_i) \end{bmatrix}, \quad \ell_i(u) = \ln|\sigma_i(u)|$$

est inversible. Les éléments de cette matrice, exceptés ceux de la diagonale principale, sont strictement négatifs, mais la somme

$$\ell_1(u_i) + \cdots + \ell_r(u_i) + 2\ell_{r+1}(u_i) + \cdots + 2\ell_{r+s-1}(u_i) = -2\ell_{r+s}(u_i) > 0.$$

Le lemme 4.15 nous permet alors de conclure la preuve. □

4.4 Exemple : les corps quadratiques

Rappel 4.17. Soit K un corps quadratique imaginaire ; le théorème des unités implique que les seules unités de K sont les racines de l'unité présentes dans K (car $r+s-1 = 0$). Celles-ci forment un groupe cyclique fini, plus précisément :

Proposition 4.18. *Si K est un corps quadratique imaginaire, le groupe des unités de K est formé de ± 1, sauf dans les deux cas suivants :*

(i) Si $K = \mathbf{Q}(i)$, alors U_K est formé des racines quatrièmes de l'unité.

(ii) Si $K = \mathbf{Q}(\sqrt{-3})$, alors U_K est formé des racines sixièmes de l'unité.

Démonstration. Soit $K = \mathbf{Q}(\sqrt{-d})$ où d est un naturel non nul sans facteurs carrés. Rappelons que les unités de K sont les entiers de norme ± 1 (lemme 4.9). Lorsque $d \equiv 1, 2 \bmod 4\mathbf{Z}$, l'anneau des entiers de K est $\mathbf{Z}[\sqrt{-d}]$. La norme d'un élément $x = a + b\sqrt{-d}$ de $\mathbf{Z}[\sqrt{-d}]$ est donc

$$\operatorname{Nm}(x) = a^2 + b^2 d \geq 0.$$

Ainsi, pour que x soit une unité, il est nécessaire et suffisant que $a^2 + b^2 d = 1$. Si $d \geq 2$, ceci implique que $b = 0$ et $a = \pm 1$, d'où $x = \pm 1$. En revanche si $d = 1$, outre les solutions $x = \pm 1$, il y a également les solutions $a = 0$, $b = \pm 1$ et donc $x = \pm i$.

Lorsque $d \equiv 3 \bmod 4\mathbf{Z}$, l'anneau des entiers de K est $\mathbf{Z}[(1+\sqrt{-d})/2]$. La norme d'un de ses éléments $x = a + b(1+\sqrt{-d})/2$ est alors

$$\mathrm{Nm}(x) = \left(a + \frac{b}{2}\right)^2 + \frac{b^2 d}{4}.$$

Dès lors, pour que x soit une unité, il faut et il suffit que $(2a+b)^2 + b^2 d = 4$. Si $d \geq 7$, ceci implique que $b = 0$, d'où $(2a)^2 = 4$; $a = \pm 1$ et donc $x = \pm 1$. Si $d = 3$, nous obtenons à nouveau les solutions $x = \pm 1$, ainsi que les solutions $b = \pm 1$, d'où $(2a \pm 1)^2 = \pm 1$, c'est-à-dire $x = (\pm 1 \pm \sqrt{-3})/2$. □

Rappel 4.19. Supposons désormais que K est un corps quadratique réel ; le théorème des unités implique que U_K se dévisse en $\mu(K) \times \mathbf{Z}$ (car $r + s - 1 = 1$). Puisque K admet un plongement dans $\mathbf{R}$, les seules racines de l'unité (toujours) présentes dans K sont nécessairement ± 1 et donc $\mu(K) = \langle -1 \rangle$.

Proposition 4.20. *Les unités positives d'un corps quadratique réel K forment un groupe multiplicatif isomorphe à $\mathbf{Z}$.*

Remarque 4.21. Ainsi, U_K admet un seul générateur strictement supérieur à 1 ; appelé **unité fondamentale** de K.

Démonstration. Soit $K = \mathbf{Q}(\sqrt{d})$ où $d \geq 2$ est un naturel sans facteurs carrés. Notons que si u est une unité de K, alors $-u$, u^{-1} et $-u^{-1}$ le sont aussi.

Supposons d'abord que $d \equiv 2, 3 \bmod 4\mathbf{Z}$. Les entiers de K sont de la forme $x = a + b\sqrt{d}$ avec a, $b \in \mathbf{Z}$; ainsi, pour que x soit une unité, il est nécessaire et suffisant de satisfaire $\mathrm{Nm}(x) = a^2 - b^2 d = \pm 1$ (lemme 4.9). Si $x = a + b\sqrt{d}$ est une solution, alors les quatre nombres $\pm a \pm b\sqrt{d}$ sont x, $-x$, x^{-1} et $-x^{-1}$ (à l'ordre près). Pour $x \neq \pm 1$, l'un de ces quatre nombres est strictement plus grand que 1 ; celui où a et b sont positifs. L'unité fondamentale (qui est la plus petite unité strictement supérieure à 1) peut être déterminée de la manière suivante : calculer $b^2 d$ pour $b = 1, 2, 3, \ldots$ et s'arrêter à la première valeur de $b_1^2 d$ qui diffère d'un carré a_1^2 de ± 1. Alors $a_1 + b_1\sqrt{d}$ est l'unité fondamentale.

Supposons que $d \equiv 1 \bmod 4\mathbf{Z}$. Les entiers de K sont de la forme $x = a + b(1+\sqrt{d})/2$ avec a, $b \in \mathbf{Z}$. Puisque que la norme de x est $a^2 + ab - (b^2 d - b^2)/4$, x est une unité si et seulement si $(2a+b)^2 - b^2 d = \pm 4$. Réciproquement, toute solution à cette équation détermine un entier et donc une unité de K. L'unité fondamentale est alors déterminée de la manière suivante : calculer $b^2 d$ pour $b = 1, 2, 3, \ldots$ et s'arrêter à la première valeur de $b_1^2 d$ qui diffère d'un $(2a_1 + b_1)^2$ de ± 4. Alors $a_1 + b_1(1+\sqrt{d})/2$ est l'unité fondamentale. □

4.5 Exemple : les corps CM

Définition 4.22. Un corps de nombres est *totalement réel* lorsque tous ses plongements dans $\mathbf{C}$ sont à valeur dans $\mathbf{R}$.

Exemple 4.23. Le corps $K = \mathbf{Q}(\alpha) \simeq \mathbf{Q}[X]/(f)$ est totalement réel si toutes les racines de f sont réelles. En particulier, tout corps quadratique réel est totalement réel.

Définition 4.24. Un corps de nombres est *totalement imaginaire* lorsqu'aucun de ses plongements dans $\mathbf{C}$ n'est à valeur dans $\mathbf{R}$.

Exemple 4.25. Le corps $K = \mathbf{Q}(\alpha) \simeq \mathbf{Q}[X]/(f)$ est totalement imaginaire si aucune des racines de f n'est réelle. En particulier, tout corps quadratique complexe est totalement imaginaire.

Définition 4.26. Un *corps CM* est une extension quadratique totalement imaginaire d'un corps totalement réel.

Remarque 4.27. Tout corps CM peut être obtenu en adjoignant à un corps totalement réel la racine carré d'un élément dont tous les conjugués réels sont négatifs.

Exemple 4.28. Tout corps quadratique complexe est un corps CM ; de corps totalement réel $\mathbf{Q}$.

Exemple 4.29. Pour tout $n \geq 1$, le corps cyclotomique $\mathbf{Q}(\zeta_n)$ est un corps CM ; il s'agit de l'extension quadratique totalement imaginaire de $\mathbf{Q}(\zeta_n + \zeta_n^{-1})$. Il est obtenu en adjoignant à ce dernier corps la racine carré de $\zeta_n^2 + \zeta_n^{-2} - 2 = (\zeta_n - \zeta_n^{-1})^2$.

Remarque 4.30. Soit K un corps CM, étant l'extension quadratique du corps totalement réel K^+ et notons $2n = [K : \mathbf{Q}]$; alors K possède $2n$ plongements complexes et K^+ possède n plongements réels ; dès lors

$$\operatorname{rang}(U_K) = n - 1 = \operatorname{rang}(U_{K^+}).$$

Par conséquent, U_{K^+} est d'indice fini dans U_K. Il est même possible d'en montrer d'avantage :

Proposition 4.31. *L'indice de $\mu(K) \cdot U_{K^+}$ dans U_K est soit 1, soit 2.*

Démonstration. Soit $a \mapsto \overline{a}$ l'automorphisme non trivial de K fixant K^+. Alors celui-ci commute avec n'importe quel morphisme $K \to \mathbf{C}$; en particulier, pour tout $a \in U_K$, tous les conjugués de $a/\overline{a}$ dans $\mathbf{C}$ sont de module 1 et donc $a/\overline{a} \in \mu(K)$ par le corollaire 4.11. Considérons le morphisme

$$\phi\colon \left\{ \begin{array}{ccc} U_K & \longrightarrow & \mu(K)/\mu(K)^2 \\ a & \longmapsto & a/\overline{a} \bmod \mu(K)^2. \end{array} \right.$$

Soit u un élément du noyau de $\phi : u/\overline{u} = \zeta^2$ pour un $\zeta \in \mu(K)$. Alors $(u\overline{\zeta})/(\overline{u}\zeta) = 1$ et donc $u\overline{\zeta} \in K^+$ (puisqu'il est fixe). Il s'en suit que $u \in \mu(K) \cdot U_{K^+}$. Réciproquement, si $u = \zeta u^+ \in \mu(K) \cdot U_{K^+}$, alors $u/\overline{u} = \zeta^2 \in \operatorname{Ker}(\phi)$. Nous avons par conséquent montré que $\operatorname{Ker}(\phi) = \mu(K) \cdot U_{K^+}$. Comme $\mu(K)/\mu(K)^2$ est d'ordre 2, ceci termine la preuve. □

4.6 Les S-unités

Objectif. Soit S un ensemble fini d'idéaux premiers de K. Nous généralisons le théorème des unités (4.4) pour la notion de S-unités.

Définition 4.32. L'anneau des *S-entiers* est une extension de $\mathcal{O}_K$ défini par

$$\mathcal{O}_K(S) := \bigcap_{\mathfrak{p} \notin S} \mathcal{O}_\mathfrak{p} = \{\alpha \in K \mid \forall\, \mathfrak{p} \notin S,\, \operatorname{ord}_\mathfrak{p}(\alpha) \geq 0\}.$$

Remarque 4.33. De façon générale $\mathcal{O}_K$ est contenu dans $\mathcal{O}_K(S)$, avec égalité lorsque l'ensemble S est vide.

Définition 4.34. Le groupe des unités U_K s'étend en le groupe des *S-unités*, défini par

$$U_K(S) := \mathcal{O}_K(S)^\times = \{\alpha \in K \mid \forall\, \mathfrak{p} \notin S,\, \operatorname{ord}_\mathfrak{p}(\alpha) = 0\}.$$

Remarque 4.35. De façon générale, U_K est contenu dans $U_K(S)$, à nouveau avec égalité lorsque l'ensemble S est vide. Il est également clair que la partie de torsion de $U_K(S)$ reste $(U_K(S))_{\text{tors}} = \mu(K)$.

Théorème 4.36 (des S-unités)**.** *Le groupe des S-unités de K se dévisse en*

$$U_K(S) \simeq \mu(K) \times \mathbf{Z}^{r+s+(\#S-1)}.$$

Démonstration. Soient $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ les idéaux premiers collectés dans S. Le morphisme

$$U_K(S) \longrightarrow \mathbf{Z}^t\colon u \longmapsto (\operatorname{ord}_{\mathfrak{p}_1}(u), \ldots, \operatorname{ord}_{\mathfrak{p}_t}(u))$$

a pour noyau U_K. Afin de terminer la preuve, il suffit de montrer que l'image de $U_K(S)$ dans $\mathbf{Z}^t$ est de rang t. Soit h le nombre de classes de K ; alors $\mathfrak{p}_i^h$ est principal, disons $\mathfrak{p}_i^h = (\pi_i)$ où π_i est une S-unité avec pour image $(0, \ldots, h, \ldots, 0)$ (h en i-ième position). Il est alors clair que $(\mathfrak{p}_1^h, \ldots, \mathfrak{p}_t^h)$ engendre un sous-groupe de rang t. □

Exemple 4.37. Soient $K = \mathbf{Q}$ et $S = \{(2), (3), (5)\}$, il s'en suit que l'ensemble des S-unités de K est $U_K(S) = \{\pm 2^\ell 3^m 5^n \mid \ell, m, n \in \mathbf{Z}\}$. Le résultat nous fournit que $U_K(S) \simeq \{\pm 1\} \times \mathbf{Z}^3$.

5 Les extensions cyclotomiques

Cette section se concentre sur les extensions cyclotomiques, *i.e.* les extensions de $\mathbf{Q}$ engendrées par une racine de l'unité. L'étude de ces extensions s'avèrent d'un grand intérêt afin de prouver le dernier théorème de Fermat.

5.1 Résultats élémentaires

Définition 5.1. Un élément ζ d'un corps K est une *racine primitive* n-ième de l'unité si ζ est d'ordre n dans $K^\times$.

Exemple 5.2. Les racines n-ième de l'unité dans $\mathbf{C}$ sont les éléments $\zeta_n^m := e^{2i\pi m/n}$ où m varie de 0 à $n-1$. Le lemme suivant donne une condition nécessaire et suffisante afin qu'une racine ζ_n^m soit primitive.

Lemme 5.3. *Soit ζ une racine primitive n-ième de l'unité ; alors ζ^m est une racine primitive n-ième de l'unité si et seulement si n et m sont copremiers.*

Démonstration. Il s'agit d'une conséquence d'un résultat bien connu : si x est d'ordre n dans un groupe, alors x^m est d'ordre n si et seulement si n et m sont copremiers. □

Corollaire 5.4. *Une racine n-ième de l'unité ζ_n^m dans $\mathbf{C}$ est primitive si et seulement n et m sont copremiers.*

Remarque 5.5. Soit K le corps obtenu en adjoignant à $\mathbf{Q}$ une racine primitive n-ième de l'unité ζ. Alors K est le corps de décomposition de $X^n - 1$; il s'agit ainsi d'une extension galoisienne de $\mathbf{Q}$. Notons G le groupe de Galois associé à cette extension ; il permute l'ensemble des racines primitives n-ième de l'unité dans K et donc, pour tout $\sigma \in G$, $\sigma(\zeta) = \zeta^m$ pour un certain m copremier à n. L'exposant m est de plus bien défini modulo n et l'application $\sigma \mapsto [m]$ est un morphisme injectif $G \to (\mathbb{Z}/n\mathbb{Z})^\times$. Il s'agit même d'un isomorphisme et donc :

$$[K : \mathbf{Q}] = \varphi(n) = |(\mathbf{Z}/n\mathbf{Z})^\times|.$$

Nous fournirons plus tard une autre preuve de ce résultat.

Définition 5.6. Soit ζ une racine primitive n-ième de l'unité ; le *n-ième polynôme cyclotomique* Φ_n est défini par

$$\Phi_n(X) = \prod_{\substack{m=0 \\ (n,m)=1}}^{n-1} (X - \zeta^m).$$

Remarque 5.7. De façon équivalente, $\Phi_n(X) = \prod(X - \zeta')$ où ζ' parcourt les racines primitives n-ième de l'unité. Comme G permute les ζ', $\Phi_n(X)$ est à coefficients dans $\mathbf{Q}$ et clairement $\Phi_n(\zeta) = 0$. Par conséquent, il faut et il suffit que $\Phi_n(X)$ soit irréductible afin qu'il s'agisse du polynôme minimal de ζ sur $\mathbf{Q}$; auquel cas $[K : \mathbf{Q}] = \varphi(n)$ et l'application $G \to (\mathbb{Z}/n\mathbb{Z})^\times$ est un isomorphisme. Il s'en suit alors que :

Proposition 5.8. *Les assertions suivantes sont équivalentes :*

(i) L'application $\mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$ *est un isomorphisme.*

(ii) L'extension $\mathbf{Q}(\zeta)/\mathbf{Q}$ *est de degré* $\varphi(n)$.

(iii) $\Phi_n(X)$ *est irréductible sur* $\mathbf{Q}$ *; donc* $\Phi_n(X)$ *est le polynôme minimal de* ζ *sur* $\mathbf{Q}$.

(iv) Le groupe $\mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$ *agit transitivement sur l'ensemble des racines primitives n-ième de l'unité.*

Remarque 5.9. Nous verrons par la suite que toutes ces assertions sont vraies.

Remarque 5.10. Notons que toute racine n-ième de l'unité est une racine primitive d-ième de l'unité pour exactement les diviseurs d de n ; ainsi

$$X^n - 1 = \prod_{d|n} \Phi_d(X) = (X-1) \cdots \Phi_n(X). \tag{9}$$

Nous allons tout d'abord nous intéresser au cas des extensions cyclotomiques où n est une puissance d'un nombre premier.

Proposition 5.11. *Soit ζ une racine primitive p^r-ième de l'unité et posons $K = \mathbf{Q}(\zeta)$.*

(i) Le corps $\mathbf{Q}(\zeta)$ est de degré $\varphi(p^r) = p^{r-1}(p-1)$ sur $\mathbf{Q}$.

(ii) L'élément $\pi := 1 - \zeta$ est premier dans $\mathcal{O}_K$; de plus $(p) = (\pi)^e$ où $e = \varphi(p^r)$.

Démonstration. (i) Puisque ζ est entier sur $\mathbf{Z}$, l'anneau $\mathbf{Z}[\zeta]$ est contenu dans $\mathcal{O}_K$. Si ζ' est une autre racine primitive p^r-ième de l'unité, alors celles-ci sont liées : $\zeta' = \zeta^s$ et $\zeta = \zeta'^t$ pour deux entiers s et t non divisibles par p ; ainsi $\mathbf{Z}[\zeta'] = \mathbf{Z}[\zeta]$ et $\mathbf{Q}(\zeta') = \mathbf{Q}(\zeta)$. Il s'en suit également que

$$\frac{1-\zeta'}{1-\zeta} = 1 + \zeta + \cdots + \zeta^{s-1} \in \mathbf{Z}[\zeta].$$

De façon analogue, $(1-\zeta)/(1-\zeta') \in \mathbf{Z}[\zeta]$; dès lors $(1-\zeta')/(1-\zeta)$ est inversible dans $\mathbf{Z}[\zeta]$ et par conséquent dans $\mathcal{O}_K$. Notons que par (9) :

$$\Phi_{p^r}(X) = \frac{X^{p^r}-1}{X^{p^{r-1}}-1} = \frac{Y^p - 1}{Y-1} = 1 + Y + \cdots + Y^{p-1} \quad \text{avec } Y = X^{p^{r-1}}$$

et donc $\Phi_{p^r}(1) = p$. De par sa définition,

$$\Phi_{p^r}(1) = \prod (1-\zeta') = \prod \frac{1-\zeta'}{1-\zeta}(1-\zeta) = u(1-\zeta)^{\varphi(p^r)}$$

pour une certaine unité u de K appartenant à $\mathbf{Z}[\zeta]$. En combinant ces deux informations, nous obtenons une égalité au niveau des idéaux de $\mathcal{O}_K$:

$$(p) = (\pi)^e \quad \text{où } \pi := 1 - \zeta \text{ et avec } e = \varphi(p^r).$$

Dès lors (p) possède au moins $\varphi(p^r)$ facteurs premiers dans $\mathcal{O}_K$; le théorème 2.63 implique alors que $[\mathbf{Q}(\zeta) : \mathbf{Q}] \geq \varphi(p^r)$. Étant donné que nous savions déjà que $[\mathbf{Q}(\zeta) : \mathbf{Q}] \leq \varphi(p^r)$, nous en déduisons le premier point.

(ii) L'élément π est alors contraint d'engendrer un idéal premier dans $\mathcal{O}_K$, sinon (p) se factoriserait à nouveau. □

Remarque 5.12. Ainsi, p se ramifie dans $\mathbf{Q}(\zeta)$ avec $e = \varphi(p^r)$ et $f = 1$. La valeur du degré de la classe résiduelle résulte du théorème 2.63.

Proposition 5.13. *Soit ζ une racine primitive p^r-ième de l'unité et posons $K = \mathbf{Q}(\zeta)$. Le discriminant de K vaut $\pm p^c$, dans lequel $c = p^{r-1}(pr - r - 1)$.*

Démonstration. Pour la suite, fixons les notations suivantes dans $\mathcal{O}_K$: $(p) = \mathfrak{p}^{\varphi(p^r)}$ où $\mathfrak{p} = (\pi)$ et avec $f(\mathfrak{p}/p\mathbf{Z}) = 1$; donnant lieu à un isomorphisme $\mathbf{Z}/p\mathbf{Z} \to \mathcal{O}_K/(\pi)$. Nous montrons qu'au signe près $\Delta(\mathbf{Z}[\zeta]/\mathbf{Z})$ est une puissance de p. Ainsi, l'égalité

$$\Delta_K \, (\mathcal{O}_K : \mathbf{Z}[\zeta])^2 = \Delta(\mathbf{Z}[\zeta]/\mathbf{Z})$$

impliquera que Δ_K et $(\mathcal{O}_K : \mathbf{Z}[\zeta])$ sont également des puissances de p et que dès lors $p^M \mathcal{O}_K \subseteq \mathbf{Z}[\zeta]$ pour un certain M. Afin de calculer $\Delta(\mathbf{Z}[\zeta]/\mathbf{Z})$, nous utilisons la formule (non prouvée) suivante :

$$\Delta(\mathbf{Z}[\zeta]/\mathbf{Z}) = \pm \operatorname{Nm}_{K/\mathbf{Q}}(\Phi'_{p^r}(\zeta)).$$

En dérivant l'équation $(X^{p^{r-1}}-1)\Phi_{p^r}(X) = X^{p^r}-1$ et en évaluant en ζ, il en résulte que $\Phi'_{p^r}(\zeta) = p^r\zeta^{p^r-1}/(\zeta^{p^{r-1}}-1)$. Clairement, $\operatorname{Nm}\zeta = \pm 1$ et $\operatorname{Nm} p^r = p^{r\varphi(p^r)}$. Nous allons montrer que

$$\operatorname{Nm}_{K/\mathbf{Q}}(1-\zeta^{p^s}) = \pm p^{p^s}, \quad 0 \leq s < r$$

et donc

$$\operatorname{Nm}_{K/\mathbf{Q}} \Phi'_{p^r}(\zeta) = \pm p^c \quad \text{avec } c = p^{r-1}(pr-r-1).$$

Tout d'abord calculons $\operatorname{Nm}(1-\zeta)$: le polynôme minimale de $1-\zeta$ sur $\mathbf{Q}$ est $\Phi_{p^r}(1-X)$ et le terme indépendant vaut $\Phi_{p^r}(1) = p$; donc $\operatorname{Nm}(1-\zeta) = \pm p$. Ensuite nous calculons $\operatorname{Nm}(1-\zeta^{p^s})$ un certain $s < r$: comme ζ^{p^s} est une racine primitive p^{r-s}-ième de l'unité, nous obtenons similairement que

$$\operatorname{Nm}_{\mathbf{Q}[\zeta^{p^s}]/\mathbf{Q}}(1-\zeta^{p^s}) = \pm p.$$

En utilisant la transitivité des normes et le fait que $\operatorname{Nm}_{M/L}(\alpha) = \alpha^{[M:L]}$ lorsque $\alpha \in L$, il s'en suit que

$$\operatorname{Nm}_{K/\mathbf{Q}}(1-\zeta^{p^s}) = \pm p^a \quad \text{où } a = \left[\mathbf{Q}[\zeta] : \mathbf{Q}[\zeta^{p^s}]\right] = p^s.$$

□

Remarque 5.14. En particulier, p est le seul nombre premier se ramifiant dans $\mathbf{Q}(\zeta)$.

Proposition 5.15. *Soit ζ une racine primitive p^r-ième de l'unité et posons $K = \mathbf{Q}(\zeta)$. L'anneau des entiers de $\mathbf{Q}(\zeta)$ est $\mathbf{Z}[\zeta]$.*

Démonstration. Comme observé précédemment, l'inclusion $\mathbf{Z} \to \mathcal{O}_K$ induit un isomorphisme $\mathbf{Z}/(p) \to \mathcal{O}_K/(\pi)$. En d'autres termes $\mathcal{O}_K = \mathbf{Z} + \pi\mathcal{O}_K$ et par conséquent $\mathcal{O}_K = \mathbf{Z}[\zeta] + \pi\mathcal{O}_K$. En multipliant de part et d'autre par π :

$$\mathcal{O}_K = \mathbf{Z}[\zeta] + \pi\mathbf{Z}[\zeta] + \pi^2\mathcal{O}_K = \mathbf{Z}[\zeta] + \pi^2\mathcal{O}_K.$$

En itérant cet argument, nous obtenons que $\mathcal{O}_K = \mathbf{Z}[\zeta] + \pi^m\mathcal{O}_K$ pour tout $m \geq 1$. Comme $\pi^{\varphi(p^r)} = up$ où u est une unité de K, il s'en suit que $\mathcal{O}_K = \mathbf{Z}[\zeta] + p^m\mathcal{O}_K$ pour n'importe quel $m \geq 1$. Toutefois, pour un M suffisamment grand, nous savons (via la preuve précédente) que $p^M\mathcal{O}_K \subseteq \mathbf{Z}[\zeta]$ et donc $\mathbf{Z}[\zeta] = \mathcal{O}_K$. □

Remarque 5.16. Soit ζ (resp. ζ') une racine primitive p^r-ième (resp. ℓ^s-ième) de l'unité. Si p et ℓ sont deux nombres premiers distincts, alors

$$\mathbf{Q}(\zeta) \cap \mathbf{Q}(\zeta') = \mathbf{Q}$$

puisque si $K \subseteq \mathbf{Q}(\zeta)$, alors p se ramifie totalement dans K mais pas ℓ et si $K \subseteq \mathbf{Q}(\zeta')$, alors ℓ se ramifie totalement dans K mais pas p, amenant à une contradiction à moins que $K = \mathbf{Q}$.

Lemme 5.17. *Soient K et L deux extensions finies de $\mathbf{Q}$ dont le compositum est tel que $[KL : \mathbf{Q}] = [K : \mathbf{Q}] \cdot [L : \mathbf{Q}]$ et soit d le plus grand diviseur commun de Δ_K et Δ_L ; alors*

$$\mathcal{O}_{KL} \subseteq d^{-1}\mathcal{O}_K \cdot \mathcal{O}_L.$$

Démonstration. Soient $(\alpha_1, \ldots, \alpha_m)$ et $(\beta_1, \ldots, \beta_n)$ deux bases entières de K et L respectivement. Alors les $\alpha_i\beta_j$ constituent une base entière de KL ; par conséquent, tout élément $\gamma \in \mathcal{O}_{KL}$ peut s'écrire sous la forme

$$\gamma = \sum_{ij} \frac{a_{ij}}{r}\alpha_i\beta_j, \quad a_{ij} \in \mathbf{Z},\ r \in \mathbf{Z}$$

avec les coefficients a_{ij}/r déterminés de façon unique. Une fois ces fractions misent sous leur forme irréductible, il ne reste plus qu'à montrer que r divise d.

Tout plongement σ de K dans $\mathbf{C}$ s'étend de façon unique en un L-plongement de KL dans $\mathbf{C}$. En appliquant un tel σ à l'équation précédente, nous obtenons

$$\sigma(\gamma) = \sum_{ij} \frac{a_{ij}}{r} \sigma(\alpha_i)\beta_j.$$

Posons $x_i := \sum_j (a_{ij}/r)\beta_j$ et considérons $\sigma_1, \ldots, \sigma_m$ les plongements distincts de K dans $\mathbf{C}$. Nous obtenons un système de m équations

$$\sum_i \sigma_k(\alpha_i)x_i = \sigma_k(\gamma), \quad k = 1, \ldots, m,$$

et la règle de Cramer nous fournit que $Dx_i = D_i$ où $D = \det(\sigma_j(\alpha_i))$ et D_i est un déterminant similaire. Selon la proposition 1.56, $D^2 = \Delta_K$ et donc

$$\Delta_K x_i = DD_i.$$

Par construction, les éléments D et D_i sont entiers sur $\mathbf{Z}$ et donc $\Delta_K x_i$ l'est aussi. Cependant, $\Delta_K x_i = \sum_j (\Delta_K a_{ij})/r\beta_j$ et les β_j forment une base entière de L. Donc $\Delta_K a_{ij}/r \in \mathbf{Z}$ et ainsi r divise $\Delta_K a_{ij}$ pour tous i, j. De notre hypothèse envers r et les a_{ij}, nous concluons que r divise Δ_K.

Similairement, r divise Δ_L et donc divise le plus grand diviseur commun de Δ_K et Δ_L. □

Théorème 5.18. *Soit ζ une racine primitive n-ième de l'unité.*

(i) Le corps $\mathbf{Q}(\zeta)$ est de degré $\varphi(n)$ sur $\mathbf{Q}$.

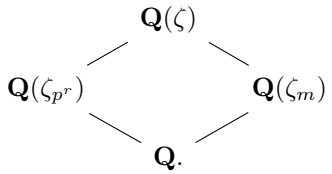
(ii) L'anneau des entiers de $\mathbf{Q}(\zeta)$ est $\mathbf{Z}[\zeta]$; ainsi $(1, \zeta, \ldots, \zeta^{\varphi(n)-1})$ est une base entière de $\mathbf{Q}(\zeta)$.

(iii) Si p se ramifie dans $\mathbf{Q}(\zeta)$, alors p divise n ; plus précisément, si $n = p^r m$ avec m copremier à p, alors

$$(p) = (\mathfrak{P}_1 \cdots \mathfrak{P}_s)^{\varphi(p^r)}$$

dans $\mathbf{Q}(\zeta)$, où les $\mathfrak{P}_i$ sont des idéaux premiers distincts de $\mathbf{Q}(\zeta)$.

Démonstration. Procédons par induction sur le nombre de diviseurs premiers de n. Supposons que p divise n et notons $n = p^r m$ avec $(p, m) = 1$. Nous supposons que le théorème est vrai pour m. Remarquons que $\zeta_{p^r} := \zeta^m$ est une racine p^r-ième de l'unité, que $\zeta_m := \zeta^{p^r}$ est une racine primitive m-ième de l'unité et que $\mathbf{Q}(\zeta)$ résulte du compositum de $\mathbf{Q}(\zeta_{p^r})$ et $\mathbf{Q}(\zeta_m)$. Considérons le diagramme suivant :



Selon la proposition 5.13, (p) se ramifie totalement dans $\mathbf{Q}(\zeta_{p^r})$, disons $(p) = \mathfrak{p}^{\varphi(p^r)}$, mais p ne se ramifie pas dans $\mathbf{Q}(\zeta_m)$, disons que $(p) = \mathfrak{p}_1 \cdots \mathfrak{p}_s$ où les $\mathfrak{p}_i$ sont des idéaux premiers distincts. Comme $\mathbf{Q}(\zeta)$ est obtenu en adjoignant ζ_{p^r} à $\mathbf{Q}(\zeta_m)$, son degré sur $\mathbf{Q}(\zeta_m)$ est au plus $\varphi(p^r)$. Il résulte du théorème 2.63 que $\mathfrak{p}_1 \cdots \mathfrak{p}_s$ devient une $\varphi(p^r)$ puissance dans $\mathbf{Q}(\zeta)$ si et seulement si $[\mathbf{Q}(\zeta) : \mathbf{Q}(\zeta_m)] = \varphi(p^r)$ et si chaque idéal premier $\mathfrak{p}_i$ se ramifie totalement dans $\mathbf{Q}(\zeta)$, disons $\mathfrak{p}_i \mathcal{O}_{\mathbf{Q}(\zeta)} = \mathfrak{P}_i^{\varphi(p^r)}$. Par conséquent,

$$[\mathbf{Q}(\zeta) : \mathbf{Q}] = \varphi(p^r)\, \varphi(m) = \varphi(n).$$

Afin de terminer la preuve, il reste à montrer que $\mathcal{O}_{\mathbf{Q}(\zeta)} = \mathbf{Z}[\zeta_{p^r}, \zeta_m] = \mathbf{Z}[\zeta]$. Ceci découle du lemme 5.17 puisque les seuls idéaux premiers divisant le discriminant de $\mathcal{O}_{\mathbf{Q}(\zeta_m)}/\mathbf{Z}$ sont les diviseurs de m : par induction et par le théorème 2.73. □

Remarque 5.19. Le point (*iii*) du théorème montre que si p divise n, alors p se ramifie (à moins que $\varphi(p^r) = 1$). Comme $\varphi(p^r) = p^{r-1}(p-1)$, cela se produit seulement lorsque $p^r = 2$. Par conséquent, si p divise n, alors p se ramifie dans $\mathbf{Q}(\zeta_n)$ excepté quand $p = 2$ et $n = 2o$ où o est un nombre impair.

Remarque 5.20. Soit $m > 1$ un naturel ; alors $\varphi(mn) > \varphi(n)$ excepté lorsque n est impair et $m = 2$. Par conséquent, $\mu(\mathbf{Q}(\zeta_n))$ est cyclique d'ordre n (engendré par ζ_n) excepté lorsque n est impair, auquel cas il est cyclique d'ordre $2n$ (engendré par $-\zeta_n$).

Remarque 5.21. Dans la situation du lemme précédent, l'égalité

$$\Delta_{KL} = \Delta_K^{[L:\mathbf{Q}]} \Delta_L^{[K:\mathbf{Q}]} \tag{10}$$

fournit que $\mathcal{O}_{KL} = \mathcal{O}_K \cdot \mathcal{O}_L$. Ceci se prouve via des calculs élémentaires sur le déterminant. En utilisant ceci, nous pouvons montrer que pour toute racine primitive n-ième de l'unité ζ_n,

$$\Delta_{\mathbf{Q}(\zeta_n)} = \frac{(-1)^{\varphi(n)/2} n^{\varphi(n)}}{\prod_{p|n} p^{\varphi(n)/(p-1)}}.$$

Le cas de $\mathbf{Q}(i, \sqrt{5}) = \mathbf{Q}(i)\mathbf{Q}(\sqrt{-5})$ montre que la condition sur l'anneau des entiers est nécessaire pour avoir 10 : les extensions $\mathbf{Q}(i)$ et $\mathbf{Q}(\sqrt{-5})$ ont respectivement pour discriminant 4 et 20, mais $\mathbf{Q}(i, \sqrt{5})$ a pour discriminant $4^2 5^2 = 4^2 20^2 / 4^2$.

5.2 Discussion : nombre de classes d'un corps cyclotomique

Soit ζ une racine primitive p-ième de l'unité, où p est un nombre premier impair.

Remarque 5.22. Il s'avère que le nombre de classes de $\mathbf{Q}(\zeta)$ augmente (rapidement) avec p ; il vaut 1 si et seulement si $p \leq 19$.

Exemple 5.23. Considérons le cas où $p = 23$. Le groupe de Galois de $\mathbf{Q}(\zeta)/\mathbf{Q}$ est cyclique d'ordre 22 ; il possède donc un unique sous-groupe d'indice 2. Ainsi $\mathbf{Q}(\zeta)$ contient une unique extension quadratique K de $\mathbf{Q}$. Puisque 23 est le seul nombre premier se ramifiant dans $\mathbf{Q}(\zeta)$, il est également le seul à se ramifier dans K, impliquant que $K = \mathbf{Q}(\sqrt{-23})$.

Nous pouvons vérifier que (2) se décompose dans $\mathbf{Q}(\sqrt{-23})$: disons que $(2) = \mathfrak{pq}$, tel que $\mathfrak{p}$ n'est pas principal et $\mathfrak{p}^3$ est principal. Soit $\mathfrak{P}$ un idéal premier de $\mathbf{Z}[\zeta]$ contenant $\mathfrak{p}$. Alors $\mathscr{N}(\mathfrak{P}) = \mathfrak{p}^f$, où f désigne le degré de la classe résiduelle. Comme f divise le degré $[\mathbf{Q}(\zeta) : \mathbf{Q}(\sqrt{-23})] = 11$, il ne peut valoir que 1 ou 11 (en réalité $f = 11$). Dans tous les cas, $\mathfrak{p}^f$ n'est pas principal et cela implique que $\mathfrak{P}$ ne le soit pas non plus : la norme d'un idéal principal est un idéal principal.

5.3 Unités d'un corps cyclotomique

Soit ζ une racine primitive n-ième de l'unité où $n > 2$ est un naturel et posons

$$\mathbf{Q}(\zeta)^+ := \mathbf{Q}(\zeta + \zeta^{-1}).$$

Par exemple, si $\zeta = e^{2\pi i/n}$, alors $\zeta + \zeta^{-1} = 2\cos(2\pi/n)$ et donc $\mathbf{Q}(\zeta)^+ = \mathbf{Q}(\cos(2\pi/n))$. Remarquons que tout plongement de $\mathbf{Q}(\zeta)$ dans $\mathbf{C}$ envoie ζ^{-1} sur le conjugué complexe de ζ et par conséquent l'image de $\mathbf{Q}(\zeta)^+$ est fixée par la conjugaison complexe et est un sous-corps de $\mathbf{R}$. Dès lors, $\mathbf{Q}(\zeta)$ est un corps CM ayant pour sous-corps totalement réel $\mathbf{Q}(\zeta)^+$. Selon la proposition 4.31, l'indice de $\mu(\mathbf{Q}(\zeta)) \cdot U_{\mathbf{Q}(\zeta)}$ vaut soit 1, soit 2. Il s'avère que celui-ci est contraint de valoir 1 lorsque n est une puissance d'un nombre premier.

Proposition 5.24. *Si n est une puissance d'un nombre premier, alors toute unité u de $\mathbf{Q}(\zeta)$ peut s'écrire sous la forme*

$$u = \zeta' v$$

où ζ' est une racine de l'unité et v est une unité de $\mathbf{Q}(\zeta)^+$.

Démonstration. Posons $K = \mathbf{Q}(\zeta)$. Nous n'énonçons la preuve que dans le cadre où p est impair. Si ce n'était pas le cas, le morphisme

$$\begin{array}{rcl} U_K & \longrightarrow & \mu(K)/\mu(K)^2 \\ u & \longmapsto & u/\overline{u} \bmod \mu(K)^2 \end{array}$$

donné lors de la preuve de la proposition 4.31 serait surjectif ; il existerait donc une unité u de K telle que $\overline{u} = \zeta' u$ avec ζ' une racine de l'unité n'étant pas un carré. Rappelons de la remarque 5.20 que $\mu(K) = \{\pm 1\} \cdot \langle \zeta \rangle$ (car n est impair) et donc $\mu(K)^2 = \langle \zeta \rangle$. Par conséquent, $\zeta' = -\zeta^m$ pour un certain entier m. Notons

$$u = a_0 + \cdots + a_{\varphi(n)-1}\zeta^{\varphi(n)-1}, \quad a_i \in \mathbf{Z}.$$

Alors $\overline{u} = a_0 + \cdots + a_{\varphi(n)-1}\overline{\zeta}^{\varphi(n)-1}$ et modulo l'idéal premier $\mathfrak{p} = (1-\zeta) = (1-\overline{\zeta})$ de $\mathbf{Z}[\zeta]$, nous obtenons que

$$u \equiv a_0 + \cdots + a_{\varphi(n)-1} \equiv \overline{u}.$$

De ce fait, $u \equiv -\zeta^m u \equiv -u \bmod \mathfrak{p}$ et donc $2u \in \mathfrak{p}$; amenant une contradiction puisque $\mathfrak{p}$ est premier mais ni $2 \in \mathfrak{p}$, ni $u \in \mathfrak{p}$. □

5.4 Premier cas du dernier théorème de Fermat

Objectif. Nous prouvons une version plus faible du dernier théorème de Fermat ; connue sous le nom de premier cas du dernier théorème de Fermat.

Théorème 5.25 (Fermat)**.** *Soit ζ une racine primitive p-ième de l'unité où p est un nombre premier impair. Si le nombre de classes de $\mathbf{Q}(\zeta)$ n'est pas divisible par p, alors il n'existe aucune solution x, y, $z \in \mathbf{Z}$ à l'équation*

$$X^p + Y^p = Z^p$$

où p est copremier à xyz.

Démonstration. Nous montrons que l'existence d'entiers x, y, z tels que $x^p + y^p = z^p$ et $p \nmid xyz$ mène à une contradiction. Une fois les facteurs communs retirés, nous pouvons supposer que $\operatorname{pgcd}(x, y, z) = 1$.

Traitons tout d'abord le cas où $p = 3$. Les seuls cubes modulo $9\mathbf{Z}$ sont -1, 0 et 1 ; ainsi

$$x^3 + y^3 \equiv -2, 0, 2 \bmod 9\mathbf{Z} \quad \text{et} \quad z^3 \equiv -1, 1 \bmod 9\mathbf{Z}$$

puisque $p \nmid xyz$, ce qui est contradictoire. De façon similaire, nous pouvons éliminer le cas où $p = 5$ en regardant modulo $25\mathbf{Z}$. Nous supposons donc que $p > 5$.

Si $x \equiv y \equiv -z \bmod p\mathbf{Z}$, alors $-2z^p \equiv z^p$ et donc $p \mid 3z$, venant contredire les hypothèses. Ainsi, l'une des congruences est fausse et, quitte à écrire $x^p + (-z)^p = (-y)^p$ si nécessaire, nous pouvons supposer que $p \nmid x - y$. Les racines dans $\mathbf{C}$ de $X^p + 1$ sont -1, $-\zeta$, …, $-\zeta^{p-1}$ et donc

$$X^p + 1 = \prod_{i=0}^{p-1} (X + \zeta^i).$$

Ainsi,

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

Il s'en suit que $\prod_{i=0}^{p-1}(x + \zeta^i y) = z^p$. L'idée est ensuite de raisonner sur cette factorisation ainsi que sur des propriétés de $\mathbf{Q}(\zeta)$ afin d'obtenir une contradiction.

Soit $\mathfrak{p}$ l'unique idéal premier de $\mathbf{Z}[\zeta]$ divisant (p) ; dès lors $\mathfrak{p} = (1 - \zeta^i)$ où i peut être choisi parmi n'importe quel naturel $1 \leq i < p$ par la proposition 5.11.

Lemme 5.26. *Soient $i \neq j$; les éléments $x + \zeta^i y$ et $x + \zeta^i y$ de $\mathbf{Z}[\zeta]$ sont copremiers.*

Démonstration. Supposons au contraire qu'il existe un idéal premier $\mathfrak{q}$ divisant à la fois $(x + \zeta^i y)$ et $(x + \zeta^j y)$ pour $i \neq j$. La remarque 2.26 fournit alors que

$$\mathfrak{q} \supseteq ((\zeta^i - \zeta^j)y) = \mathfrak{p}y \quad \text{et} \quad \mathfrak{q} \supseteq ((\zeta^j - \zeta^i)x) = \mathfrak{p}x$$

et elle permet d'affirmer que $\mathfrak{q} \mid \mathfrak{p}y$ et $\mathfrak{q} \mid \mathfrak{p}x$; comme x et y sont supposés copremiers, $\mathfrak{q} = \mathfrak{p}$. Ainsi $x+y \equiv x+\zeta^i y \equiv 0 \bmod \mathfrak{p}$ et donc $x+y \in \mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$. Toutefois, la congruence $z^p = x^p + y^p \equiv x + y \equiv 0 \bmod p\mathbf{Z}$ amène à $p \mid z$, contredisant les hypothèses. □

Lemme 5.27. *Si $\alpha \in \mathbf{Z}[\zeta]$, alors $\alpha^p \in \mathbf{Z} + p\mathbf{Z}[\zeta]$.*

Démonstration. En notant $\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$ avec les $a_i \in \mathbf{Z}$, il s'en suit que

$$\alpha^p \equiv a_0^p + a_1^p + \cdots + a_{p-2}^p \bmod p\mathbf{Z}[\zeta]$$

est un élément de $\mathbf{Z}$. □

Lemme 5.28. *Soit $\alpha = a_0 + a_1\zeta + \cdots + a_{p-1}\zeta^{p-1}$ avec les $a_i \in \mathbf{Z}$ et au moins l'un des a_i est nul. Si α est divisible par un entier n (i.e. $\alpha \in n\mathbf{Z}[\zeta]$), alors chaque a_i est divisible par n.*

Démonstration. Comme $1+\zeta+\cdots+\zeta^{p-1} = 0$, tout sous-ensemble de $\{1, \zeta, \ldots, \zeta^{p-1}\}$ à $p-1$ éléments est une $\mathbf{Z}$-base de $\mathbf{Z}[\zeta]$. Le résultat s'en suit. □

Démonstration. Reprenons et achevons la preuve du théorème 5.25. Considérons l'égalité d'idéaux de $\mathbf{Z}[\zeta]$:

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

Comme les facteurs de gauche sont deux-à-deux copremiers, ceux-ci doivent être des puissances p-ième d'idéaux, disons $(x + \zeta^i y) = \mathfrak{a}_i^p$ pour certains idéaux $\mathfrak{a}_i$ de $\mathbf{Z}[\zeta]$. Ainsi l'ordre des $\mathfrak{a}_i$ divise p dans le groupe des classes ; toutefois nous faisons l'hypothèse que l'ordre du groupe des classes de $\mathbf{Z}[\zeta]$ est copremier à p, impliquant que les $\mathfrak{a}_i$ soient principaux, disons $\mathfrak{a}_i = (\alpha_i)$.

Considérons $i = 1$ et omettons l'indiçage sur α_1. Alors $x + \zeta y = u\alpha^p$ pour une certaine unité $u \in \mathbf{Z}[\zeta]$. En appliquant la proposition 5.24, nous pouvons noter $u = \zeta^r v$ avec $\overline{v} = v$. Selon le lemme 5.27, il existe un $a \in \mathbf{Z}$ tel que $\alpha^p \equiv a \bmod p\mathbf{Z}[\zeta]$. Par conséquent :

$$x + \zeta y = \zeta^r v\alpha^p \equiv \zeta^r va \bmod p\mathbf{Z}[\zeta] \quad \text{et} \quad x + \bar{\zeta} y = \zeta^{-r} v\overline{\alpha}^p \equiv \zeta^{-r} va \bmod p\mathbf{Z}[\zeta].$$

En combinant ces deux assertions, nous obtenons que

$$\zeta^{-r}(x + \zeta y) \equiv \zeta^r(x + \zeta^{-1} y) \bmod p\mathbf{Z}[\zeta]$$

ou, de façon équivalente,

$$x + \zeta y - \zeta^{2r} x - \zeta^{2r-1} y \equiv 0 \bmod p\mathbf{Z}[\zeta]. \tag{11}$$

Si 1, ζ, ζ^{2r-1} et ζ^{2r} sont tous distincts, alors le lemme 5.28 implique (car $p > 5$) que p divise x et y, venant contredire nos hypothèses. Les seuls cas restants sont alors :

(*i*) $1 = \zeta^{2r}$: mais alors (11) implique que $\zeta y - \zeta^{-1} y \equiv 0 \bmod p\mathbf{Z}[\zeta]$ et le lemme 5.28 fournit que p divise y, contredisant les hypothèses.

(*ii*) $1 = \zeta^{2r-1}$: donc $\zeta = \zeta^{2r}$ et (11) implique que $(x - y) - (x - y)\zeta \equiv 0 \bmod p\mathbf{Z}[\zeta]$. À nouveau, le lemme 5.28 amène à une contradiction : p divise $x - y$, contredisant le choix fait sur x et y.

(*iii*) $\zeta = \zeta^{2r-1}$: mais alors (11) fournit que $x - \zeta^2 x \equiv 0 \bmod p\mathbf{Z}[\zeta]$ et le lemme 5.28 implique que p divise x, contredisant les hypothèses. □

6 Annexe : compléments d'algèbre commutative

6.1 Algèbre sur un anneau

Définition 6.1. Soit A un anneau. Une *A-algèbre* est la donnée d'un anneau B muni d'un morphisme d'anneau $A \to B$.

Exemple 6.2. Cette terminologie est majoritairement utilisée dans le contexte où A est un sous-anneau de B ; dans ce cas le morphisme associé est l'inclusion $a \mapsto a$. En l'occurrence, toute extension d'anneau B de A est une A-algèbre.

Remarque 6.3. Si $\beta_1, \dots, \beta_n$ sont des éléments de B, nous désignons par $A[\beta_1, \dots, \beta_n]$ le plus petit sous-anneau de B contenant A ainsi que chacun des β_i. Explicitement, il s'agit de l'ensemble des polynômes en les β_i et à coefficients dans A, *i.e.* l'ensemble des éléments de la forme

$$\sum a_{i_1,\dots,i_n} \beta_1^{i_1} \dots \beta_n^{i_n}, \quad a_{i_1,\dots,i_m} \in A.$$

Cet ensemble est parfois désigné par la sous-A-algèbre de B engendrée par les β_i. De plus, lorsque $B = A[\beta_1, \dots, \beta_n]$, nous disons que les β_i engendrent B en tant que A-algèbre.

Exemple 6.4. Soit k un corps, l'anneau $k[X_1, \dots, X_n]$ est engendré par $(X_1, \dots, X_n)$ en tant que k-algèbre : il s'agit d'une k-algèbre de type fini. En revanche, $k[X_1, X_2, \dots]$ n'est pas de type fini en tant que k-algèbre.

6.2 Idéaux d'un produit d'anneaux

Lemme 6.5. *Un produit d'anneau $A \times B$ est intègre si et seulement si l'un d'entre eux est nul et l'autre est intègre.*

Démonstration. En procédant par l'absurde et en explicitant les différentes situations. □

Proposition 6.6. *Soit $A \times B$ un produit d'anneau. Si $\mathfrak{a}$ et $\mathfrak{b}$ sont des idéaux respectifs de A et de B, alors $\mathfrak{a} \times \mathfrak{b}$ est un idéal de $A \times B$. De plus, tout idéal de $A \times B$ est de cette forme.*

Démonstration. Soit $\mathfrak{c}$ un idéal de $A \times B$ et posons

$$\mathfrak{a} = \{a \in A \mid (a, 0) \in \mathfrak{c}\} \quad \text{et} \quad \mathfrak{b} = \{b \in B \mid (0, b) \in \mathfrak{c}\}.$$

Il est alors clair que $\mathfrak{a} \times \mathfrak{b}$ est contenu dans $\mathfrak{c}$. Réciproquement, tout $(a, b) \in \mathfrak{c}$ est un élément de $\mathfrak{a} \times \mathfrak{b}$ en remarquant que $(a, 0) = (a, b) \cdot (1, 0) \in \mathfrak{c}$ et $(0, b) = (a, b) \cdot (0, 1) \in \mathfrak{c}$. □

Proposition 6.7. *Soit $A \times B$ un produit d'anneau. Les idéaux premiers de $A \times B$ sont les idéaux de la forme $\mathfrak{p} \times B$ (pour $\mathfrak{p}$ un idéal premier de B) et $A \times \mathfrak{p}$ (pour $\mathfrak{p}$ un idéal premier de A).*

Démonstration. Tout idéal $\mathfrak{c}$ de C est premier si et seulement si $C/\mathfrak{c}$ est intègre. La projection naturelle

$$\begin{cases} A \times B & \longrightarrow\!\!\!\!\!\rightarrow & A/\mathfrak{a} \times B/\mathfrak{b} \\ (a, b) & \longmapsto & (a + \mathfrak{a}, b + \mathfrak{b}) \end{cases}$$

a pour noyau $\mathfrak{a} \times \mathfrak{b}$, elle se factorise donc en un isomorphisme canonique

$$(A \times B)/(\mathfrak{a} \times \mathfrak{b}) \simeq A/\mathfrak{a} \times B/\mathfrak{b}$$

et le lemme 6.5 nous permet de conclure. □

Remarque 6.8. Les résultats précédents s'étendent au cas d'un produit fini d'anneaux : les idéaux de $A_1 \times \dots \times A_m$ sont de la forme $\mathfrak{a}_1 \times \dots \times \mathfrak{a}_m$ où chaque $\mathfrak{a}_i$ est un idéal de A_i et ils sont tous de cette forme. En outre $\mathfrak{a}_1 \times \dots \times \mathfrak{a}_m$ est premier si et seulement s'il existe un j pour lequel $\mathfrak{a}_j$ est premier dans A_j et les autres sont tels que $\mathfrak{a}_i = A_i$, pour $i \neq j$.

6.3 Anneaux noethériens

Proposition 6.9. *Tout élément non nul et non inversible d'un anneau noethérien intègre se décompose en un produit d'éléments irréductibles.*

Démonstration. Supposons au contraire qu'il existe un élément a d'un anneau noethérien intègre A venant contredire la proposition et qui est tel que (a) soit maximal parmi les idéaux générés par ces éléments ; un tel idéal existe étant donné que A est noethérien. Comme a ne peut être écrit comme un produit d'éléments irréductibles, il n'en est lui même pas un et dès lors $a = bc$ pour b et c deux non inversibles. Clairement $(a) \subset (b)$ et cette inclusion est stricte sinon c serait inversible. De par la maximalité de (a), nous en déduisons que b peut s'écrire sous la forme d'un produit d'éléments irréductibles. La même conclusion peut être tirée envers c et donc a est un produit d'éléments irréductibles. □

6.4 Localisation et corps des fractions

Définition 6.10. Le *corps des fractions* d'un anneau intègre A est le plus petit corps $K \supseteq A$, dont tous les éléments $c \in K$ s'écrivent sous la forme $c = a/b$ avec a, $b \in A$ et $b \neq 0$. Celui-ci peut être construit en quotientant $A \times (A \smallsetminus \{0\})$ par la relation d'équivalence : $(a, b) \sim (c, d)$ si $ad = cb$.

Exemple 6.11. Le corps $\mathbf{Q}$ est le corps des fractions de $\mathbf{Z}$, le corps $k(X)$ est celui de $k[X]$ où k est un corps. Pour tout nombre premier $p \in \mathbf{Z}$, $\mathbf{Q}_p$ est le corps des fractions des entiers p-adiques $\mathbf{Z}_p$.

Proposition 6.12. *Soit Ω un corps algébriquement clos contenant $\mathbf{Q}$ et soit $\alpha \in \Omega$ un élément algébrique sur $\mathbf{Q}$. Le corps des fractions de $\mathbf{Z}[\alpha]$ est $\mathbf{Q}(\alpha)$.*

Démonstration. D'une part, $\operatorname{Frac} \mathbf{Z}[\alpha]$ est contenu dans $\mathbf{Q}(\alpha)$ puisqu'il s'agit du plus petit corps contenant $\mathbf{Z}[\alpha]$ et

$$\mathbf{Z}[\alpha] \subseteq \mathbf{Q}[\alpha] = \mathbf{Q}(\alpha)$$

qui est un corps. D'autre part, $\mathbf{Q} \subseteq \operatorname{Frac} \mathbf{Z}[\alpha]$ et $\alpha \in \operatorname{Frac} \mathbf{Z}[\alpha]$ ce qui permet d'affirmer que le plus petit corps contenant $\mathbf{Q}$ et α (à savoir $\mathbf{Q}(\alpha)$) est contenu dans $\operatorname{Frac} \mathbf{Z}[\alpha]$. □

Exemple 6.13. La proposition précédente offre une multitude d'exemples. En particulier, le corps des fractions de $\mathbf{Z}[i]$ est $\mathbf{Q}(i)$, celui de $\mathbf{Z}[\sqrt{5}]$ est $\mathbf{Q}(\sqrt{5})$ et, pour tout p premier, le corps des fractions de $\mathbf{Z}[\zeta_p]$ est $\mathbf{Q}(\zeta_p)$.

Définition 6.14. Soit A un anneau intègre dont le corps des fractions est K. Un sous-ensemble S de A est dit *multiplicatif* si $0 \notin S$, $1 \in S$ et S est stable pour la multiplication. Si S est un sous-ensemble multiplicatif, nous posons

$$S^{-1}A := \{a/s \in K \mid a \in A,\, s \in S\}.$$

Il s'agit d'un sous-anneau de K, étant donné que S est multiplicatif, contenant A.

Remarque 6.15. Lorsque $A \smallsetminus \{0\}$ est pris comme ensemble multiplicatif, l'anneau $S^{-1}A$ est précisément le corps des fractions de A.

Exemple 6.16. Soit t un élément non nul de A, alors

$$S_t := \{1, t, t^2, \ldots\}$$

est un sous-ensemble multiplicatif de A et nous notons (lorsque le contexte est clair) A_t pour désigner $S_t^{-1}A$. Cet anneau est appelé **localisé de A en t**. Dans le cas où $A = \mathbf{Z}$ et où d est un entier non nul, $\mathbf{Z}_d$ est constitué des éléments de $\mathbf{Q}$ dont le dénominateur est une puissance de d :

$$\mathbf{Z}_d = \{a/d^n \in \mathbf{Q} \mid n \geq 0\}.$$

Exemple 6.17. Si $\mathfrak{p}$ est un idéal premier, alors $S_\mathfrak{p} = A \smallsetminus \mathfrak{p}$ est un ensemble multiplicatif : si ni a, ni b appartient à $\mathfrak{p}$, alors ab n'appartient pas $\mathfrak{p}$. Nous notons $A_\mathfrak{p}$ pour désigner $S_\mathfrak{p}^{-1}A$. Cet anneau est appelé **localisé de A en dehors de $\mathfrak{p}$**. Par exemple,

$$\mathbf{Z}_{(p)} = \{m/n \in \mathbf{Q} \mid n \notin (p)\}, \quad p \text{ premier.}$$

Proposition 6.18. *Soient A un anneau intègre et S un sous-ensemble multiplicatif de A. Pour tout idéal $\mathfrak{a}$ de A, nous notons $\mathfrak{a}^e$ l'idéal qu'il engendre dans $S^{-1}A$ (extension) ; pour tout idéal $\mathfrak{a}$ de $S^{-1}A$, nous notons $\mathfrak{a}^c$ pour l'idéal $\mathfrak{a} \cap A$ (contraction). Alors*

$$\mathfrak{a}^{ce} = \mathfrak{a} \quad \textit{pour tout idéal } \mathfrak{a} \textit{ de } S^{-1}\mathfrak{a}$$
$$\mathfrak{a}^{ec} = \mathfrak{a} \quad \textit{si } \mathfrak{a} \textit{ est un idéal premier de } A \textit{ disjoint de } S.$$

Démonstration. Soit $\mathfrak{a}$ un idéal de l'anneau $S^{-1}A$. Étant donné que $\mathfrak{a} \cap A \subseteq \mathfrak{a}$ et que $\mathfrak{a}$ est un idéal de $S^{-1}A$, nous avons clairement que $(\mathfrak{a} \cap A)^e \subseteq \mathfrak{a}$. Réciproquement, tout élément $b \in \mathfrak{a}$ s'écrit sous la forme $b = a/s$ avec $a \in A$ et $s \in S$. Par conséquent $a = s(a/s)$ est un élément de $\mathfrak{a} \cap A$ puisque $\mathfrak{a}$ est un idéal de $S^{-1}A$ et ainsi $b = a/s = (s(a/s))/s \in (\mathfrak{a} \cap A)^e$.

Soit $\mathfrak{p}$ un idéal premier de A disjoint de S. Il est clair que $(S^{-1}\mathfrak{p}) \cap A$ est contenu dans $\mathfrak{p}$. Nous avons l'égalité : soit $a/s \in (S^{-1}\mathfrak{p}) \cap A$, où $a \in \mathfrak{p}$ et $s \in S$. Comme $(a/s)s = a \in \mathfrak{p}$ et a/s, s sont tous deux des éléments de A, nous avons par primalité de $\mathfrak{p}$ qu'au moins a/s ou s est dans $\mathfrak{p}$; le deuxième cas n'arrive jamais par hypothèse et donc $a/s \in \mathfrak{p}$. □

Proposition 6.19. *Soit A un anneau intègre et soit S un sous-ensemble multiplicatif de A. L'application $\mathfrak{p} \mapsto \mathfrak{p}^e = \mathfrak{p}S^{-1}A$ est une bijection de l'ensemble des idéaux premiers de A tels que $\mathfrak{p}$ est disjoint de S vers l'ensemble des idéaux premiers de $S^{-1}A$; l'application inverse est donnée par $\mathfrak{p} \mapsto \mathfrak{p} \cap A$.*

Démonstration. Si $\mathfrak{p}$ est un idéal premier de A disjoint de S, alors $\mathfrak{p}^e$ est un idéal premier de $S^{-1}A$. En effet, $(a_1a_2)/(s_1s_2) \in S^{-1}A$ implique que $(s_1s_2)(a_1a_2)/(s_1s_2) = a_1a_2 \in \mathfrak{p}S^{-1}A \cap A$ puisque $S^{-1}A$ est un idéal. Or $\mathfrak{p}S^{-1}A \cap A = \mathfrak{p}$ car $\mathfrak{p}$ est disjoint de S et donc l'un des $a_i \in \mathfrak{p}$ et cela permet d'affirmer que l'un des $a_i/s_i \in S^{-1}A$. De plus, si $\mathfrak{p}$ est un idéal premier de $S^{-1}A$, alors $\mathfrak{p} \cap A$ est un idéal premier de A disjoint de S : soient a, $b \in A$, si $ab \in \mathfrak{p} \cap A$, alors en particulier $ab \in \mathfrak{p}$ et donc $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$. Ainsi $a \in \mathfrak{p} \cap A$ ou $b \in \mathfrak{p} \cap A$. La proposition 6.18 montre que ces deux applications sont inverses l'une de l'autre. □

Proposition 6.20. *Soient A un anneau et $\mathfrak{p}$ l'un de ses idéaux premiers. La localisation de A en dehors de $\mathfrak{p}$ est un anneau local ; d'unique idéal maximal $\mathfrak{p}A_\mathfrak{p}$.*

Démonstration. Soit $\mathfrak{a}$ un idéal de $A_\mathfrak{p}$ non contenu dans $\mathfrak{p}A_\mathfrak{p}$. Alors il existe un $a/b \in \mathfrak{a}$ tels que a et $b \notin \mathfrak{p}$. Dès lors b/a est un élément de $A_\mathfrak{p}$ et ainsi l'idéal $\mathfrak{a}$ comprend $1 = (a/b)(b/c)$, impliquant que $\mathfrak{a} = A$. □

Exemple 6.21. Nous listons ci-après les idéaux premiers de quelques anneaux :

$$\begin{aligned}
\mathbf{Z} &: \ (0), (2), (3), (5), (7), (11,), \ldots \\
\mathbf{Z}_2 &: \ (0), (3), (5), (7), (11), \ldots \\
\mathbf{Z}_{(2)} &: \ (0), (2) \\
\mathbf{Z}_{42} &: \ (0), (5), (11), (13), \ldots \\
\mathbf{Z}/42\mathbf{Z} &: \ (2), (3), (7).
\end{aligned}$$

En général, pour t un élément non nul d'un anneau intègre, il y a une correspondance entre les ensembles suivants :

$$\begin{aligned}
\{\text{idéaux premiers de } A_t\} \quad &\leftrightarrow \quad \{\text{idéaux premiers de } A \text{ ne comprenant pas } t\} \\
\{\text{idéaux premiers de } A/(t)\} \quad &\leftrightarrow \quad \{\text{idéaux premiers de } A \text{ comprenant } t\}
\end{aligned}$$

6.5 Bases des A-modules

Remarque 6.22. Au même titre que les espaces vectoriels sur un corps, la notion de base peut être définie sur certains A-modules. Dans ceux-ci, tout élément s'écrit de façon unique comme combinaison linéaire des éléments de la base. Sauf mention contraire, nous considérons des modules de type fini mais cette notion s'étend aux modules de type quelconque.

Définition 6.23. Soit M un A-module de type fini. Une suite d'éléments $(e_1, \dots, e_n)$ de M est une *base de M* si les deux conditions suivantes sont satisfaites :

(*i*) la suite $(e_1, \dots, e_n)$ est *libre* : si $\sum_{i=1}^n a_i e_i = 0$ pour $a_i \in A$ alors $a_i = 0$ pour tout i, et

(*ii*) la suite $(e_1, \dots, e_n)$ est *génératrice de M* : $\langle e_1, \dots, e_n \rangle_{A\text{-mod}} = M$.

Remarque 6.24. Soit $(e_1, \dots, e_n)$ une base de M et soit $(\varepsilon_1, \dots, \varepsilon_n)$ une deuxième suite de n éléments de M. Alors, pour tout i, $\varepsilon_i = \sum a_{ij} e_j$ pour certains $a_{ij} \in A$ et la suite $(\varepsilon_1, \dots, \varepsilon_n)$ est une base si et seulement si la matrice $(a_{ij})_{ij}$ est inversible dans l'anneau $\mathrm{M}_n(A)$. De plus, $(a_{ij})_{ij}$ est inversible dans $\mathrm{M}_n(A)$ si et seulement si sont déterminant est inversible dans A, et dans ce cas, l'inverse est donné par

$$(a_{ij})_{ij}^{-1} = \mathrm{adj}(a_{ij})_{ij} \cdot \det(a_{ij})_{ij}^{-1}.$$

Dans le cas où l'anneau $A = \mathbf{Z}$, l'**indice** de $N := \mathbf{Z}\varepsilon_1 + \mathbf{Z}\varepsilon_2 + \cdots + \mathbf{Z}\varepsilon_n$ dans M est $|\det(a_{ij})|$ en supposant qu'il soit non nul. Afin de prouver ceci, il est utile de se remémorer que l'on peut choisir une base $(e'_1, \dots, e'_n)$ pour M et une base $(\varepsilon'_1, \dots, \varepsilon'_n)$ pour N tels que $\varepsilon'_i = m_i e'_i$, où $m_i \in \mathbf{N} \smallsetminus \{0\}$. Si $(e'_i)_i = U \cdot (e_i)_i$ et $(\varepsilon'_i)_i = V \cdot (\varepsilon_i)_i$, alors $(\varepsilon_i)_i = V^{-1} D U (e_i)_i$ dans laquelle D désigne la matrice diagonale $\mathrm{diag}(m_1, \dots, m_n)$ et

$$\det(V^{-1}DU) = \det(V^{-1}) \cdot \det(D) \cdot \det(U) = \prod_{i=1}^n m_i = (M : N).$$

Définition 6.25 (équivalente)**.** Soit M un A-module de type fini. La suite $(e_1, \dots, e_n)$ d'éléments de M est une *base de M* si tout élément de M peut être exprimé de façon unique comme une combinaison linéaire à coefficients dans A des e_i. Alors l'application

$$\begin{array}{ccc} A^m & \xrightarrow{\sim} & M \\ (a_i)_{i=1}^m & \longmapsto & \sum a_i e_i \end{array}$$

est un isomorphisme de A-module, et M est dit *A-module libre de rang m*.

Exemple 6.26. Tout anneau A est un A-module libre de rang 1. Plus généralement, pour n un naturel non nul, la somme directe $A^n := A \oplus \cdots \oplus A$ (pris n fois) est un A-module libre de rang n.

Exemple 6.27. Le $\mathbf{Z}$-module $\mathbf{Q}$ n'est pas de type fini. Il ne possède pas non plus de base, car pour q et $q' \in \mathbf{Q}^\times$, il est possible de trouver deux entiers non nuls n et m tels que $nq + mq' = 0$: typiquement, si $q = a/b$ et $q' = c/d$, alors $n = cb$ et $m = -ad$ satisfont cette propriété.

Rappel 6.28. Le lemme de Zorn implique que tout espace vectoriel (y compris de type quelconque) sur un corps possède une base.

6.6 Formes bilinéaires

Définition 6.29. Soit V un k-espace vectoriel de dimension finie. Une *forme bilinéaire* sur V est une application k-bilinéaire

$$\psi \colon V \times V \longrightarrow k.$$

Une telle forme est dite *symétrique* lorsque $\psi(x, y) = \psi(y, x)$ pour tous x, $y \in V$.

Exemple 6.30. Tout produit scalaire sur un $\mathbf{R}$-espace vectoriel V est une forme bilinéaire symétrique sur V. En revanche, un produit scalaire sur un $\mathbf{C}$-espace vectoriel V (forme hermitienne) n'est pas une forme bilinéaire à cause de l'anti-linéarité à droite ; il s'agit plus précisément d'une forme *sesquilinéaire* sur V.

Définition 6.31. Soit V un k-espace vectoriel de dimension finie. Le *discriminant* d'une forme bilinéaire ψ relative à une base $(e_1, \dots, e_n)$ de V est le déterminant de la matrice $(\psi(e_i, e_j))_{ij}$.

Remarque 6.32. La notion de discriminant est unique à carré d'élément de A près. En effet, si $(\varepsilon_1, \dots, \varepsilon_{n'})$ est une suite d'éléments de V et en écrivant $\varepsilon_j = \sum a_{ij} e_i$ pour tout j, alors

$$\psi(\varepsilon_\ell, \varepsilon_m) = \sum_{i,j} \psi(a_{\ell i} e_i, a_{mj} e_j) = \sum_{i,j} a_{\ell i} \cdot \psi(e_i, e_j) \cdot a_{mj}.$$

Dès lors, en posant A la matrice $(a_{ij})_{ij}$, nous obtenons que

$$(\psi(\varepsilon_\ell, \varepsilon_m))_{\ell m} = A \cdot (\psi(e_i, e_j))_{ij} \cdot A^{\intercal}$$

et par conséquent,

$$\det(\psi(\varepsilon_\ell, \varepsilon_m))_{\ell m} = \det(A)^2 \ \det(\psi(e_i, e_j))_{ij}.$$

Définition 6.33. Soit V un k-espace vectoriel de dimension finie. Une forme bilinéaire $\psi \colon V \times V \to k$ est dite *non dégénérée* si elle satisfait l'une des conditions équivalentes suivantes :

(*i*) ψ possède un discriminant non nul relativement à une (et donc toute) base de V.

(*ii*) Le noyau gauche de $\psi = \{v \in V \mid \forall x \in V,\ \psi(v, x) = 0\}$ est réduit à 0.

(*iii*) Le noyau droit de ψ est réduit à 0.

Remarque 6.34. Si ψ est une forme bilinéaire non dégénérée, l'application

$$\begin{array}{ccc} V & \xrightarrow{\sim} & V^\star \\ v & \longmapsto & \psi_v \colon \left\{ \begin{array}{ccc} V & \longrightarrow & k \\ x & \longmapsto & \psi(v, x) \end{array} \right. \end{array}$$

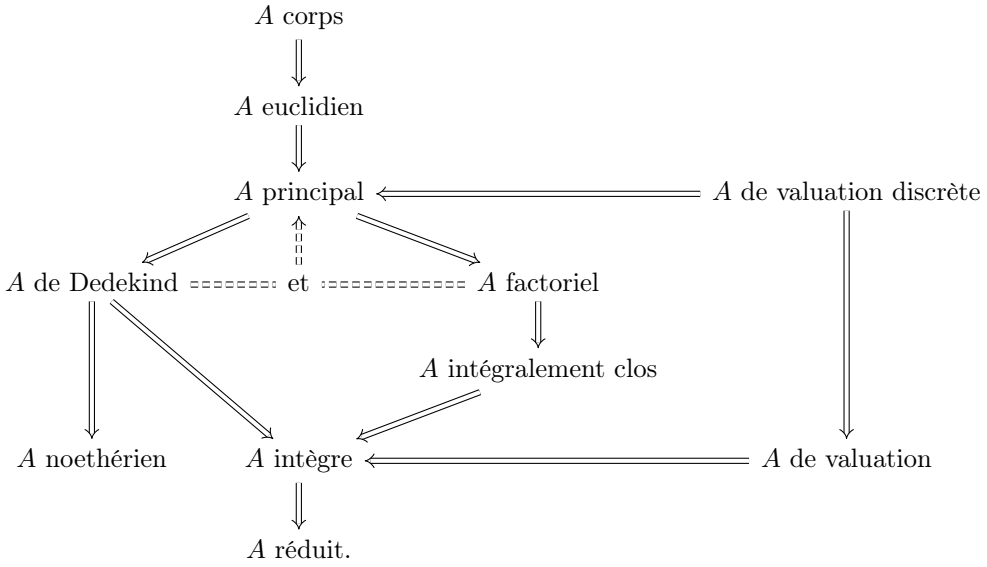
est un isomorphisme (non canonique). Soit $(e_1, \dots, e_m)$ une base de V et soit $(\varepsilon_1, \dots, \varepsilon_m)$ la base duale de $V^\star$. Nous pouvons utiliser l'isomorphisme afin de transférer $(\varepsilon_1, \dots, \varepsilon_m)$ en une base $(e'_1, \dots, e'_m)$ de V, ayant la propriété que

$$\forall i, j, \quad \psi(e'_i, e_j) = \delta_{ij}$$

où δ_{ij} désigne le symbole de Kronecker.

7 Annexe : hiérarchie partielle des anneaux commutatifs

Soit A un anneau commutatif non nul ; alors



Références

[AmGm] Inequality of arithmetic and geometric means, depuis Wikipédia.

[AM69] Atiyah and MacDonald (1969), *Introduction to Commutative Algebra*, Addison-Wesley publishing Co., Inc.

[Coh91] Cohn, Paul M. (1991), *Algebraic numbers and algebraic functions*, Chapman and Hall Mathematics Series, Chapman & Hall, London.

[Con] Conrad, Keith *Trace and Norm, II*, depuis `kconrad.math.uconn.edu`.

[Jar14] Jarvis, Frazer (2014), *Algebraic Number Theory*, Springer New York.

[Lan02] Lang, Serge (2002), *Algebra* (revised third edition), Springer New York.

[Mil21a] Milne, James S. (2021), *Algebraic Number Theory* (v3.08), depuis `www.jmilne.org/math/`.

[Mil21b] Milne, James S. (2021), *Fields and Galois Theory* (v5.00), depuis `www.jmilne.org/math/`.

[Neu99] Neukirch, Jürgen (1999), *Algebraic number theory*, Springer New York.

[Sam97] Samuel, Pierre (1997), *Théorie algébrique des nombres*. Hermann, Paris.

[Wil] Wilson's theorem, depuis Wikipédia.