

Université P. et M. Curie (Paris VI)
Deuxième semestre 2010/2011

date de mise à jour: 23/03/2011

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

Cinquième fascicule : 23/03/2011

3.5 Idéaux d'un corps de nombres

Petit aperçu historique

L'invention de la notion d'idéal provient des recherches au XIX^{ème} siècle sur le *dernier théorème de Fermat* : il s'agissait de démontrer qu'il n'y a pas d'entiers positifs $n \geq 3$, x , y et z satisfaisant $x^n + y^n = z^n$. En supposant n impair et en utilisant l'identité

$$x^n + y^n = (x + y)(x + \zeta y) \cdots (x + \zeta^{n-1}y), \quad \zeta = \zeta_n = e^{2i\pi/n}$$

Kummer a démontré en 1844 que l'énoncé de Fermat est vrai pour un exposant premier $n = p$ pour lequel l'anneau des entiers du corps $\mathbf{Q}(\zeta_p)$ est factoriel ; Dirichlet a alors remarqué que l'existence d'une décomposition en facteurs irréductibles est toujours vraie, mais que l'unicité n'est pas claire. C'est dès 1844 que Kummer a su qu'il n'y avait pas unicité de la décomposition en éléments irréductibles dans l'anneau $\mathbf{Z}[\zeta_{23}]$. Il l'a écrit à Liouville en 1847 (à la suite d'une note de G. Lamé à l'Académie des Sciences le 11 mars 1847), ajoutant qu'il avait trouvé un substitut qui étaient les "nombres idéaux". L'idée est la suivante.

Dans le corps $k = \mathbf{Q}(\sqrt{-5})$ la décomposition en facteurs irréductibles n'est pas unique

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}).$$

Kummer affirme qu'il existe des objets qu'il appelle *nombres idéaux* donnant une décomposition unique

$$(21) = \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3 \mathfrak{p}_4$$

qui explique la décomposition précédente :

$$\mathfrak{p}_1 \mathfrak{p}_2 = (3), \quad \mathfrak{p}_3 \mathfrak{p}_4 = (7), \quad \mathfrak{p}_1 \mathfrak{p}_3 = (1 + 2\sqrt{-5}), \quad \mathfrak{p}_2 \mathfrak{p}_4 = (1 - 2\sqrt{-5}).$$

Dedekind a précisé cette construction de nombres idéaux. Si \mathfrak{a} est un nombre idéal, on veut satisfaire les relations, pour a et b dans \mathbf{Z}_k ,

$$\text{si } \mathfrak{a}|a \text{ et } \mathfrak{a}|b \text{ alors pour tout } \lambda \in \mathbf{Z}_k \text{ et } \mu \in \mathbf{Z}_k \text{ on a } \mathfrak{a}|\lambda a + \mu b.$$

On veut aussi que \mathfrak{a} soit déterminé par $\{a \in \mathbf{Z}_k ; \mathfrak{a}|a\}$. L'idée est donc de considérer les sous-ensembles \mathfrak{a} de \mathbf{Z}_k qui vérifient la propriété

$$a \in \mathfrak{a}, b \in \mathfrak{a}, \lambda \in \mathbf{Z}_k, \mu \in \mathbf{Z}_k \Rightarrow \lambda a + \mu b \in \mathfrak{a}.$$

Ce sont donc les idéaux de \mathbf{Z}_k .

Dans l'exemple précédent on prend

$$\mathfrak{p}_1 = (3, 1 - \sqrt{-5}), \quad \mathfrak{p}_2 = (3, 1 + \sqrt{-5}), \quad \mathfrak{p}_3 = (7, 3 - \sqrt{-5}), \quad \mathfrak{p}_4 = (7, 3 + \sqrt{-5}).$$

Références: [9], [Pantchichkine], [Skoruppa].

3.5.1 Idéaux entiers

Soient K un corps de nombres de degré n sur \mathbf{Q} et \mathbf{Z}_K son anneau d'entiers.

Lemme 3.38. *Soit $\alpha \in \mathbf{Z}_K$, $\alpha \neq 0$. Alors $\mathbf{Z}_K/\alpha\mathbf{Z}_K$ a $|N_{K/\mathbf{Q}}(\alpha)|$ éléments.*

Démonstration. On utilise la proposition 3.1 : il existe une base $\{e_1, \dots, e_n\}$ de \mathbf{Z}_K et des entiers a_1, \dots, a_n tels que $\{a_1e_1, \dots, a_n e_n\}$ soit une base de l'idéal $\alpha\mathbf{Z}_K$. Soit u l'endomorphisme du \mathbf{Z} -module \mathbf{Z}_K qui envoie e_i sur $a_i e_i$. Son image est $\alpha\mathbf{Z}_K$ et sa matrice dans la base $\{e_1, \dots, e_n\}$ est la matrice diagonale $\text{diag}(a_1, \dots, a_n)$, dont le déterminant est $a_1 \cdots a_n$. Comme $\{\alpha e_1, \dots, \alpha e_n\}$ est aussi une base de $\alpha\mathbf{Z}_K$, il existe un automorphisme v du \mathbf{Z} -module $\alpha\mathbf{Z}_K$ tel que $v(a_i e_i) = \alpha e_i$ pour $1 \leq i \leq n$. Alors $\det v = \pm 1$. D'autre part les relations $v \circ u(e_i) = v(a_i e_i) = \alpha e_i$ pour $1 \leq i \leq n$ montrent que $v \circ u$ est la restriction de $[\alpha]$ à \mathbf{Z}_K , donc le déterminant de u est aussi égal à $\pm N_{K/\mathbf{Q}}(\alpha)$. \square

Soit \mathfrak{a} un idéal non nul de \mathbf{Z}_K , $\alpha \neq 0$ un élément de \mathfrak{a} . Alors $\mathbf{Z}_K \alpha \subset \mathfrak{a}$. Des propositions 3.15 et 3.1 on déduit que \mathfrak{a} est un \mathbf{Z} -module libre de rang $n = [K : \mathbf{Q}]$. Par conséquent il existe une base $\{e_1, \dots, e_n\}$ de \mathbf{Z}_K comme \mathbf{Z} -module et des entiers positifs a_1, \dots, a_n tels que $\{a_1 e_1, \dots, a_n e_n\}$ soit une base de \mathfrak{a} sur \mathbf{Z} et que a_i divise a_{i+1} dans \mathbf{Z} pour $1 \leq i < n$. On en déduit que le quotient $\mathbf{Z}_K/\mathfrak{a}$ est fini avec $a_1 \cdots a_n$ éléments. Le nombre d'éléments de $\mathbf{Z}_K/\mathfrak{a}$ est appelé *norme de \mathfrak{a}* et noté $N(\mathfrak{a})$.

Le lemme 3.38 montre que la norme d'un idéal principal est égale à la valeur absolue de la norme de K sur \mathbf{Q} d'un générateur.

Si \mathfrak{a} et \mathfrak{b} sont deux idéaux de \mathbf{Z}_K avec $\mathfrak{a} \subset \mathfrak{b}$, alors les surjections canoniques de \mathbf{Z}_K sur les quotients induisent une surjection de $\mathbf{Z}_K/\mathfrak{a}$ sur $\mathbf{Z}_K/\mathfrak{b}$, donc $N(\mathfrak{b})$ divise $N(\mathfrak{a})$.

Soient $n = [K : \mathbf{Q}]$ le degré de K et $\underline{\sigma} : K \rightarrow \mathbf{R}^n$ son plongement canonique. Comme $\underline{\sigma}(\mathfrak{a})$ est un sous réseau de $\underline{\sigma}(\mathbf{Z}_K)$ d'indice $N(\mathfrak{a})$, on obtient, comme au lemme 3.37 :

Lemme 3.39. *Soit \mathfrak{a} un idéal non nul de \mathbf{Z}_K . Alors $\underline{\sigma}(\mathfrak{a})$ est un réseau de \mathbf{R}^n de volume $2^{-r_2} |D_K|^{1/2} N(\mathfrak{a})$ et le discriminant de \mathfrak{a} est $D_K N(\mathfrak{a})^2$.*

Quand r_1 et r_2 sont deux entiers ≥ 0 avec $n = r_1 + 2r_2 \geq 1$ on définit la *constante de Minkowski* $M(r_1, r_2)$ par

$$M(r_1, r_2) = \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n}.$$

On écrit encore $M(K)$ au lieu de $M(r_1, r_2)$ quand K est un corps de nombres de degré n ayant r_1 plongements réels et $2r_2$ plongements imaginaires deux-à-deux conjugués.

Nous déduirons ultérieurement (§ 3.5.5) plusieurs conséquences du lemme suivant.

Théorème 3.40. *Soient K un corps de nombres et \mathfrak{a} un idéal non nul de \mathbf{Z}_K . Il existe $\alpha \in \mathfrak{a}$ tel que*

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

La démonstration (voir par exemple le § 4.2 de [9]) repose encore sur des arguments de géométrie des nombres, analogues à ceux de la démonstration du théorème 3.33 de Dirichlet.

3.5.2 Idéaux premiers

Soient K un corps de nombres, \mathbf{Z}_K son anneau d'entiers, \mathfrak{p} un idéal premier non nul de \mathbf{Z}_K . Si $\alpha \in \mathfrak{p}$ a pour polynôme minimal $X^m + a_1X^{m-1} + \cdots + a_m$ (avec $m = [\mathbf{Q}(\alpha) : \mathbf{Q}]$) alors a_m appartient $\mathfrak{p} \cap \mathbf{Z}$ donc cette intersection n'est pas réduite à 0.

L'injection de \mathbf{Z} dans \mathbf{Z}_K induit une injection de $\mathbf{Z}/\mathfrak{p} \cap \mathbf{Z}$ dans l'anneau $\mathbf{Z}_K/\mathfrak{p}$ qui est intègre, donc $\mathbf{Z}/\mathfrak{p} \cap \mathbf{Z}$ est intègre et l'idéal $\mathfrak{p} \cap \mathbf{Z}$ de \mathbf{Z} est premier non nul.

Rappelons le résultat élémentaire suivant :

Lemme 3.41. *Un anneau fini intègre est un corps.*

Démonstration. Si A est un anneau fini intègre, pour $x \in A \setminus \{0\}$ l'application $y \mapsto xy$ est une injection de A dans A , donc une bijection. \square

Si \mathfrak{p} est un idéal premier non nul de \mathbf{Z}_K , le corps fini $k = \mathbf{Z}_K/\mathfrak{p}$ est appelé *corps résiduel de \mathfrak{p}* . Dans ce cas $\mathbf{Z}/\mathfrak{p} \cap \mathbf{Z}$ est un sous-corps de k , donc le générateur positif de $\mathbf{Z} \cap \mathfrak{p}$ est un nombre premier p qui est appelé *la caractéristique du corps résiduel k* (on dit encore *la caractéristique résiduelle de \mathfrak{p}*). La norme de \mathfrak{p} (nombre d'éléments de $\mathbf{Z}_K/\mathfrak{p} = k$) est donc p^f où $f = [k : \mathbf{F}_p]$ est le *degré du corps résiduel*. Le schéma est

$$\begin{array}{ccc} \mathbf{Z}_K & \longrightarrow & \mathbf{Z}_K/\mathfrak{p} = k \\ \cup & & | f \\ \mathbf{Z} & \longrightarrow & \mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p \end{array}$$

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

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

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

Lemme 3.42. *Soient \mathfrak{a} et \mathfrak{b} deux idéaux non nuls de \mathbf{Z}_K . Si $\mathfrak{a} = \mathfrak{a}\mathfrak{b}$, alors $\mathfrak{b} = \mathbf{Z}_K$.*

Démonstration. Soit $\alpha_1, \dots, \alpha_n$ une base de l'idéal \mathfrak{a} comme \mathbf{Z} -module. Comme $\alpha_i \in \mathfrak{a}\mathfrak{b}$ pour $1 \leq i \leq n$, on peut écrire

$$\alpha_i = \sum_{j=1}^n \beta_{ij} \alpha_j \quad \text{pour } 1 \leq i \leq n,$$

avec des coefficients β_{ij} dans \mathfrak{b} . Alors la matrice $(\beta_{ij})_{1 \leq i, j \leq n} - I$ a un déterminant nul, d'où on déduit en développant $1 \in \mathfrak{b}$. \square

Soient A est un anneau, M un A -module et \mathfrak{a} un idéal de A différent de A . Alors $\mathfrak{a}M$ est un sous-module de M et le quotient $M/\mathfrak{a}M$ est un A -module. Montrons que $M/\mathfrak{a}M$ a une structure naturelle de A/\mathfrak{a} -module.

En effet, la structure de A -module du quotient $M/\mathfrak{a}M$ est donnée par un homomorphisme de A -modules

$$\begin{aligned} A &\rightarrow \text{Hom}_A(M/\mathfrak{a}M, M/\mathfrak{a}M) \\ a &\mapsto (x \mapsto ax) \end{aligned}$$

dont le noyau contient \mathfrak{a} . On en déduit un homomorphisme de A -modules

$$A/\mathfrak{a} \rightarrow \text{Hom}_A(M/\mathfrak{a}M, M/\mathfrak{a}M)$$

qui confère à $M/\mathfrak{a}M$ la structure de A/\mathfrak{a} -module annoncée.

En particulier si \mathfrak{a} est un idéal maximal \mathfrak{p} de A alors $M/\mathfrak{p}M$ a une structure naturelle d'espace vectoriel sur le corps A/\mathfrak{p} .

On applique ceci avec $A = \mathbf{Z}_K$.

Lemme 3.43. *Soit \mathfrak{a} un idéal non nul de \mathbf{Z}_K et soit \mathfrak{p} un idéal premier non nul de \mathbf{Z}_K . On désigne par k le corps résiduel $\mathbf{Z}_K/\mathfrak{p}$. Alors $\mathfrak{a}/\mathfrak{p}\mathfrak{a}$ est un k -espace vectoriel de dimension ≥ 1 .*

Démonstration. Le lemme 3.42 implique $\mathfrak{a} \neq \mathfrak{p}\mathfrak{a}$, donc la dimension de ce k -espace vectoriel est ≥ 1 . \square

En fait il va résulter de ce qui suit que la dimension de cet espace vectoriel est 1.

Soit \mathfrak{p} un idéal premier non nul de \mathbf{Z}_K . En utilisant au choix le lemme 3.42 ou bien le lemme 3.43, on obtient $\mathfrak{p}^m \neq \mathfrak{p}^{m+1}$ pour tout $m \geq 0$. La suite

$$\mathbf{Z}_K \supset \mathfrak{p} \supset \mathfrak{p}^2 \cdots \supset \mathfrak{p}^m \supset \cdots$$

est donc strictement décroissante. D'après le lemme 3.43 le quotient $\mathfrak{p}^m/\mathfrak{p}^{m+1}$ est isomorphe comme \mathbf{Z}_K -module à $\mathbf{Z}_K/\mathfrak{p}$; il en résulte que la norme de \mathfrak{p}^m est $N(\mathfrak{p})^m$.

L'intersection de tous les \mathfrak{p}^m est $\{0\}$: en effet, quand \mathfrak{b} est un idéal de \mathbf{Z}_K distinct de \mathbf{Z}_K et α est un élément non nul de \mathfrak{b} , le plus grand entier m tel que $\alpha \in \mathfrak{b}^m$ est borné par la condition que $N(\mathfrak{b})^m$ divise $N_{K/\mathbf{Q}}(\alpha)$.

Soit \mathfrak{a} un idéal non nul de \mathbf{Z}_K . L'ensemble des entiers $t \geq 0$ tels que $\mathfrak{a} \subset \mathfrak{p}^t$ est non vide (il contient 0) et fini. On désigne par $v_{\mathfrak{p}}(\mathfrak{a})$ le plus grand de ces entiers :

$$\mathfrak{a} \subset \mathfrak{p}^t \quad \text{pour } 0 \leq t \leq v_{\mathfrak{p}}(\mathfrak{a}) \quad \text{et} \quad \mathfrak{a} \not\subset \mathfrak{p}^t \quad \text{pour } t = v_{\mathfrak{p}}(\mathfrak{a}) + 1.$$

On a $v_{\mathfrak{p}}(\mathfrak{a}) > 0$ si et seulement si $\mathfrak{a} \subset \mathfrak{p}$. On a aussi $v_{\mathfrak{p}}(\mathfrak{a}\mathfrak{p}) = v_{\mathfrak{p}}(\mathfrak{a}) + 1$, donc $v_{\mathfrak{p}}(\mathfrak{p}^m) = m$ pour $m \geq 0$. Enfin $v_{\mathfrak{p}}(\mathfrak{p}') = 0$ si \mathfrak{p} et \mathfrak{p}' sont deux idéaux premiers distincts.

Théorème 3.44. *Soit \mathfrak{a} un idéal non nul de \mathbf{Z}_K . L'ensemble des idéaux premiers \mathfrak{p} de \mathbf{Z}_K qui contiennent \mathfrak{a} est fini et on a*

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})},$$

où le produit est étendu à l'ensemble des idéaux premiers non nuls de \mathbf{Z}_K .

De plus une telle décomposition est unique : si on a

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{a_{\mathfrak{p}}},$$

où les $a_{\mathfrak{p}}$ sont des entiers rationnels ≥ 0 tous nuls sauf un nombre fini, alors $a_{\mathfrak{p}} = v_{\mathfrak{p}}(\mathfrak{a})$ pour tout \mathfrak{p} .

Remarque. Le théorème 3.44 montre que, sous les hypothèses du lemme 3.43, $\mathfrak{a}/\mathfrak{ap}$ est de dimension 1 comme espace vectoriel sur $\mathbf{Z}_K/\mathfrak{p}$ car il n'y a pas d'idéal entre \mathfrak{ap} et \mathfrak{a} .

Pour une démonstration du théorème 3.44, voir par exemple [9].

3.5.3 Idéaux fractionnaires

Soit A un anneau, soit M un A -module et soient N_1 et N_2 deux sous- A -modules de M . On dit que M est *somme directe* de N_1 et N_2 , et on écrit $M = N_1 \oplus N_2$, si l'application $(x_1, x_2) \mapsto x_1 + x_2$ est un isomorphisme de A -modules de $N_1 \times N_2$ sur M . Cela revient à dire que l'on a $M = N_1 + N_2$ et $N_1 \cap N_2 = \{0\}$.

Si \mathfrak{A}_1 et \mathfrak{A}_2 sont deux idéaux d'un anneau A tels que $\mathfrak{A}_1 + \mathfrak{A}_2 = A$, alors $\mathfrak{A}_1 \cap \mathfrak{A}_2 = \mathfrak{A}_1 \mathfrak{A}_2$ et $A/\mathfrak{A}_1 \mathfrak{A}_2$ est isomorphe à $A/\mathfrak{A}_1 \times A/\mathfrak{A}_2$.

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

Proposition 3.45. Soient A un anneau et M un A -module. Les propriétés suivantes sont équivalentes :

- (i) Toute famille non vide de sous-modules de M admet un élément maximal.
- (ii) Toute suite croissante de sous-modules de M est stationnaire à partir d'un certain rang.
- (iii) Tout sous-module de M est de type fini.

Démonstration. Voir [9], § 1.4. □

Définition. Quand les conditions de la proposition 3.45 sont satisfaites on dit que M est un A -module *noethérien*. Un anneau est dit *noethérien* s'il est noethérien comme A -module, c'est-à-dire si toute suite croissante d'idéaux

$$\mathfrak{A}_1 \subset \mathfrak{A}_2 \subset \dots$$

est stationnaire.

De la condition (iii) de la proposition 3.45 il résulte qu'un anneau principal est noethérien.

Soient A un anneau intègre, K son corps des fractions. Un sous- A -module \mathfrak{a} **non nul** de K est un *idéal fractionnaire de K par rapport à A* s'il vérifie les propriétés équivalentes suivantes :

- (i) Il existe $\alpha \in A$, $\alpha \neq 0$ tel que $\alpha \mathfrak{a} \subset A$.
- (ii) Il existe $\beta \in K$, $\beta \neq 0$ tel que $\beta \mathfrak{a} \subset A$.

L'équivalence vient du fait que si $\beta \mathfrak{a} \subset A$ avec $\beta \in K^\times$, alors on peut écrire $\beta = \alpha/\gamma$ avec α et γ dans $A \setminus \{0\}$, d'où $\alpha \mathfrak{a} \subset A$.

On dira aussi que \mathfrak{a} est un *idéal fractionnaire de A* .

Lemme 3.46. Si \mathfrak{a}_1 et \mathfrak{a}_2 sont des idéaux fractionnaires de A , alors

$$\mathfrak{a}_1 + \mathfrak{a}_2, \quad \mathfrak{a}_1 \cap \mathfrak{a}_2, \quad \mathfrak{a}_1 \mathfrak{a}_2$$

et

$$(\mathfrak{a}_1 : \mathfrak{a}_2) := \{x \in K ; x \mathfrak{a}_2 \subset \mathfrak{a}_1\}$$

sont des idéaux fractionnaires de A .

Démonstration. Si α_1 et α_2 sont des éléments non nuls de $A \setminus \{0\}$ tels que $\mathfrak{a}_i \subset \alpha_i^{-1} A$ pour $i = 1$ et $i = 2$, alors $\mathfrak{a}_1 + \mathfrak{a}_2$, $\mathfrak{a}_1 \cap \mathfrak{a}_2$ et $\mathfrak{a}_1 \mathfrak{a}_2$ sont des sous- A -modules non nuls de K contenus dans $(\alpha_1 \alpha_2)^{-1} A$.

Si α_1 est un élément non nul de A tel que $\mathfrak{a}_1 \subset \alpha_1^{-1}A$ et si a_2 est un élément non nul de \mathfrak{a}_2 , alors pour tout $x \in (\mathfrak{a}_1 : \mathfrak{a}_2)$ on a

$$\alpha_1 a_2 x \in \alpha_1 x \mathfrak{a}_2 \subset \alpha_1 \mathfrak{a}_1 \subset A,$$

donc $\alpha_1 a_2 (\mathfrak{a}_1 : \mathfrak{a}_2) \subset A$.

Il reste à vérifier que le A -module $(\mathfrak{a}_1 : \mathfrak{a}_2)$ n'est pas nul. Si a_1 est un élément non nul de \mathfrak{a}_1 et α_2 un élément non nul de A tel que $\mathfrak{a}_2 \subset \alpha_2^{-1}A$, alors $a_1 \alpha_2$ est un élément non nul de $(\mathfrak{a}_1 : \mathfrak{a}_2)$:

$$a_1 \alpha_2 \mathfrak{a}_2 \subset a_1 A \subset \mathfrak{a}_1.$$

□

On déduit du lemme 3.46 que si \mathfrak{a} est un idéal fractionnaire de A , alors

$$(A : \mathfrak{a}) = \{x \in K ; x\mathfrak{a} \subset A\} \quad \text{et} \quad (\mathfrak{a} : \mathfrak{a}) = \{x \in K ; x\mathfrak{a} \subset \mathfrak{a}\}$$

sont des idéaux fractionnaires de A .

Tout sous- A -module de type fini de K non nul est un idéal fractionnaire.

Réciproquement, quand A est un anneau noethérien, tout idéal fractionnaire de A est de type fini : pour $\alpha \in A \setminus \{0\}$ les A -modules \mathfrak{a} et $\alpha\mathfrak{a}$ sont isomorphes. Donc, quand A est noethérien, un idéal fractionnaire n'est autre qu'un sous- A -module non nul de type fini de K . Si \mathfrak{a} admet $\{a_i\}$ comme partie génératrice et si \mathfrak{b} est engendré par $\{b_j\}$, alors $\mathfrak{a} + \mathfrak{b}$ est engendré par $\{a_i\} \cup \{b_j\}$ et $\mathfrak{a}\mathfrak{b}$ par $\{a_i b_j\}$.

Quand K est un corps de nombres, un idéal entier de K est un idéal de \mathbf{Z}_K , c'est-à-dire un idéal fractionnaire de \mathbf{Z}_K contenu dans \mathbf{Z}_K .

Proposition 3.47. Soit \mathfrak{p} un idéal premier non nul de \mathbf{Z}_K . Soit

$$\mathfrak{p}' = \{x \in K ; x\mathfrak{p} \subset \mathbf{Z}_K\}.$$

Alors \mathfrak{p}' est un idéal fractionnaire de \mathbf{Z}_K qui contient \mathbf{Z}_K et $\mathfrak{p}\mathfrak{p}' = \mathbf{Z}_K$.

Du théorème 3.44 on déduit que les idéaux fractionnaires de \mathbf{Z}_K forment un groupe abélien d'élément neutre $\mathbf{Z}_K = (1)$.

Théorème 3.48. Soit \mathfrak{a} un idéal fractionnaire de \mathbf{Z}_K . Il existe une décomposition unique

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{a_{\mathfrak{p}}},$$

où le produit est étendu à l'ensemble des idéaux premiers non nuls de \mathbf{Z}_K et les $a_{\mathfrak{p}}$ sont des entiers rationnels tels que $\{\mathfrak{p} ; a_{\mathfrak{p}} \neq 0\}$ soit fini.

Démonstration. Soit $\alpha \in \mathbf{Z}_K \setminus \{0\}$ tel que $\alpha\mathfrak{a} \subset \mathbf{Z}_K$. On décompose les idéaux entiers $\alpha\mathbf{Z}_K$ et $\alpha\mathfrak{a}$ en produit d'idéaux premiers, on multiplie par les inverses des idéaux premiers apparaissant dans la décomposition de $\alpha\mathbf{Z}_K$ et on trouve la décomposition annoncée de \mathfrak{a} . L'unicité résulte de ce qui précède.

□

Soit K un corps de nombres. Le théorème 3.44 montre que la propriété (3.4) de multiplicativité de la norme s'étend aux idéaux de \mathbf{Z}_K :

Corollaire 3.49. Soient \mathfrak{a} et \mathfrak{b} deux idéaux de \mathbf{Z}_K . Alors

$$N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b}). \quad (3.50)$$

Démonstration. Grâce au théorème 3.44 il suffit de vérifier la propriété (3.50) quand \mathfrak{b} est un idéal premier. Notons-le \mathfrak{p} .

L'homomorphisme canonique

$$\mathbf{Z}_K/\mathfrak{a}\mathfrak{p} \rightarrow \mathbf{Z}_K/\mathfrak{a}$$

est surjectif et a pour noyau $\mathfrak{a}/\mathfrak{a}\mathfrak{p}$. Le quotient $k = \mathbf{Z}_K/\mathfrak{p}$ est un corps fini (ayant $N(\mathfrak{p})$ éléments) et $\mathfrak{a}/\mathfrak{a}\mathfrak{p}$ est un k -espace vectoriel de dimension 1 (car \mathfrak{p} est maximal - cf lemme 3.43 et la remarque qui suit le théorème 3.44), donc est isomorphe à k . Ainsi $\mathfrak{a}/\mathfrak{a}\mathfrak{p}$ a $N(\mathfrak{p})$ éléments et par conséquent $\mathbf{Z}_K/\mathfrak{a}\mathfrak{p}$ en a $N(\mathfrak{a})N(\mathfrak{p})$. □

Remarque. Une autre démonstration, due à H.W. Lenstra, est donnée dans [1], Lemma 4.6.8.

Grâce au corollaire 3.49 on peut étendre la définition de la norme aux idéaux fractionnaires. Avec les notations du corollaire 3.48, on pose $v_{\mathfrak{p}}(\mathfrak{a}) = a_{\mathfrak{p}}$ et

$$N(\mathfrak{a}) = \prod_{\mathfrak{p}} N(\mathfrak{p})^{a_{\mathfrak{p}}}.$$

La norme d'un idéal fractionnaire principal de \mathbf{Z}_K est égale à la valeur absolue de la norme de K sur \mathbf{Q} d'un générateur : pour tout $\alpha \in K^\times$ on a $N(\alpha\mathbf{Z}_K) = |N_{K/\mathbf{Q}}(\alpha)|$.

Le lemme 3.47 signifie que les idéaux premiers non nuls sont inversibles dans le monoïde des idéaux fractionnaires de \mathbf{Z}_K . L'inverse \mathfrak{p}' de \mathfrak{p} est aussi noté \mathfrak{p}^{-1} :

$$\mathfrak{p}^{-1} = \{x \in K ; x\mathfrak{p} \subset \mathbf{Z}_K\}.$$

Exercice. Soient \mathfrak{a} un idéal non nul et \mathfrak{p} un idéal premier non nul de \mathbf{Z}_K .

1. Montrer qu'il existe $\alpha \in \mathfrak{a}$ tel que $\alpha \notin \mathfrak{a}\mathfrak{p}$.

Montrer qu'il existe un idéal \mathfrak{b} de \mathbf{Z}_K tel que $\mathfrak{a}\mathfrak{b} = \alpha\mathbf{Z}_K$.

Vérifier $\mathfrak{a} = \alpha\mathbf{Z}_K + \mathfrak{a}\mathfrak{p}$.

2. Soient a_1, \dots, a_N des représentants des classes de \mathbf{Z}_K modulo \mathfrak{a} , avec $N = N(\mathfrak{a})$, et soient b_1, \dots, b_M des représentants des classes de \mathbf{Z}_K modulo \mathfrak{p} , avec $M = N(\mathfrak{p})$. Vérifier que

$$\{a_i + \alpha b_j\}_{\substack{1 \leq i \leq N \\ 1 \leq j \leq M}}$$

est un système complet de représentants des classes de \mathbf{Z}_K modulo $\mathfrak{a}\mathfrak{p}$.

Du théorème 3.44 on déduit, pour \mathfrak{p} idéal premier de \mathbf{Z}_K et $\mathfrak{a}, \mathfrak{b}$ idéaux fractionnaires de \mathbf{Z}_K :

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

Soit \mathfrak{p} un idéal premier de \mathbf{Z}_K . On définit l'indice de ramification $e(\mathfrak{p})$ de \mathfrak{p} par $e(\mathfrak{p}) = v_{\mathfrak{p}}(p\mathbf{Z}_K)$ où p désigne la caractéristique résiduelle de \mathfrak{p} . Ainsi $e(\mathfrak{p}) \geq 1$.

Soit p un nombre premier et soit $p\mathbf{Z}_K$ l'idéal principal de \mathbf{Z}_K qu'il engendre. Le théorème 3.44 montre qu'il existe une décomposition, unique à l'ordre près des facteurs,

$$p\mathbf{Z}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}, \quad (3.51)$$

où g est un entier ≥ 1 , $\mathfrak{p}_1, \dots, \mathfrak{p}_g$ sont des idéaux premiers de \mathbf{Z}_K deux-à-deux distincts et $e_i \geq 1$ est l'indice de ramification de \mathfrak{p}_i ($1 \leq i \leq g$).

Les idéaux $\mathfrak{p}_1, \dots, \mathfrak{p}_g$ sont précisément les idéaux premiers \mathfrak{p} de \mathbf{Z}_K tels que $\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$. On dit que ce sont les *idéaux premiers de \mathbf{Z}_K au dessus de p* . De la décomposition (3.51) on déduit

$$\mathbf{Z}_K/p\mathbf{Z}_K \simeq \mathbf{Z}_K/\mathfrak{p}_1^{e_1} \cdots \mathbf{Z}_K/\mathfrak{p}_g^{e_g}.$$

En notant $n = [K : \mathbf{Q}]$, en désignant par f_i le degré du corps résiduel de \mathfrak{p}_i et en utilisant le corollaire 3.49, on obtient

$$p^n = N_{K/\mathbf{Q}}(p) = N(\mathfrak{p}_1)^{e_1} \cdots N(\mathfrak{p}_g)^{e_g} = p^{e_1 f_1 + \cdots + e_g f_g}.$$

Par conséquent

$$e_1 f_1 + \cdots + e_g f_g = n. \quad (3.52)$$

On dit que \mathfrak{p}_i est *ramifié au dessus de p* si l'exposant e_i est ≥ 2 . On dit que p est *ramifié dans K* si l'un des exposants e_i est ≥ 2 . On dit encore que p est

- *totalelement ramifié dans K* si $e_1 = n$: alors $g = 1$ et $f_1 = 1$
- *totalelement décomposé dans K* si $g = n$: alors $e_1 = \cdots = e_n = f_1 = \cdots = f_n = 1$
- *inerte dans K* si $f_1 = n$: alors $g = 1$ et $e_1 = 1$; cela revient à dire que $p\mathbf{Z}_K$ est un idéal premier.

Voici ce qui se passe pour les corps quadratiques

Proposition 3.53. *Soit d un entier sans facteur carré et soit p un nombre premier impair. Dans le corps $K = \mathbf{Q}(\sqrt{d})$, p se décompose de la façon suivante :*

(i) *Si p divise d , alors p est ramifié dans K :*

$$p\mathbf{Z}_K = \mathfrak{p}^2 \text{ avec } N(\mathfrak{p}) = p.$$

(ii) *Si $\left(\frac{d}{p}\right) = 1$, alors p est décomposé dans K :*

$$p\mathbf{Z}_K = \mathfrak{p}_1 \mathfrak{p}_2 \text{ avec } N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p.$$

(iii) *Si $\left(\frac{d}{p}\right) = -1$, alors p est inerte dans K :*

$$p\mathbf{Z}_K = \mathfrak{p}.$$

Démonstration. Si $d \equiv 2$ ou $3 \pmod{4}$, alors $\mathbf{Z}_K = \mathbf{Z}[\sqrt{d}]$. Si $d \equiv 1 \pmod{4}$, on a $\mathbf{Z}_K = \mathbf{Z}[(1 + \sqrt{d})/2]$, dans ce dernier cas comme p est un nombre premier impair on peut écrire $\mathbf{Z}_K = \mathbf{Z}[\sqrt{d}] + p\mathbf{Z}_K$. Par conséquent on a toujours

$$\mathbf{Z}_K/p\mathbf{Z}_K = \mathbf{Z}[\sqrt{d}]/p\mathbf{Z}[\sqrt{d}] \simeq \mathbf{Z}[X]/(p, X^2 - d) \simeq \mathbf{F}_p[X]/(X^2 - d).$$

- Le polynôme $X^2 - d$ a une racine double dans \mathbf{F}_p si et seulement si p divise d .

- Il se décompose en deux facteurs linéaires distincts si et seulement si $\left(\frac{d}{p}\right) = 1$.

- Il est irréductible si et seulement si $\left(\frac{d}{p}\right) = -1$. □

Exercice. Soit d un entier sans facteur carré et soit K le corps quadratique $\mathbf{Q}(\sqrt{d})$. Vérifier :

- (i) 2 est ramifié dans K si et seulement si $d \equiv 2$ ou $3 \pmod{4}$, c'est-à-dire si et seulement si le discriminant de K est pair.
- (ii) 2 est décomposé dans K si et seulement si $d \equiv 1 \pmod{8}$.
- (iii) 2 est inerte dans K si et seulement si $d \equiv 5 \pmod{8}$.

3.5.4 Discriminant et ramification

Nous admettrons l'énoncé suivant :

Théorème 3.54. *Soit K un corps de nombres. Les nombres premiers qui se ramifient dans K sont en nombre fini : ce sont les diviseurs premiers du discriminant D_K .*

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

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

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

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

et que l'indice résiduel f_i est égal au degré de T_i .

Référence. Voir [1], Théorème 4.8.13.

3.5.5 Classes d'idéaux - théorèmes de finitude

Soit K un corps de nombres. Les idéaux fractionnaires de \mathbf{Z}_K forment un groupe multiplicatif. Les idéaux fractionnaires principaux (c'est-à-dire monogènes) forment un sous-groupe, et le quotient est le *groupe* $\text{Cl}(K)$ *des classes d'idéaux de K* . Dire que deux idéaux fractionnaires \mathfrak{a} et \mathfrak{b} sont *équivalents* signifie qu'il existe $\alpha \in K$, $\alpha \neq 0$, tel que $\mathfrak{a} = \alpha\mathfrak{b}$.

Soit \mathfrak{a} un idéal fractionnaire et soit α un élément non nul de \mathbf{Z}_K tel que $\alpha\mathfrak{a}$ soit un idéal entier. Il résulte de la définition que \mathfrak{a} est équivalent à $\alpha\mathfrak{a}$. Donc toute classe d'équivalence contient un idéal entier.

Rappelons que $M(K)$ désigne la constante de Minkowski du corps K (théorème 3.40).

Proposition 3.55. *Toute classe d'idéaux contient un idéal entier \mathfrak{a} de norme $N(\mathfrak{a}) \leq M(K)|D_K|^{1/2}$.*

Démonstration. Si \mathfrak{a}_1 est un idéal dans la classe considérée, si α est un élément non nul de \mathbf{Z}_K tel que l'idéal $\mathfrak{a}_2 = \alpha\mathfrak{a}_1^{-1}$ soit entier, en appliquant le théorème 3.40 à \mathfrak{a}_2 on trouve un élément $\beta \in \mathfrak{a}_2$ vérifiant $|N_{K:\mathbf{Q}}(\beta)| \leq M(K)|D_K|^{1/2}N(\mathfrak{a}_2)$. Alors $\mathfrak{a} = \beta\mathfrak{a}_2^{-1}$ est équivalent à \mathfrak{a}_1 et vérifie la propriété requise. □

Théorème 3.56 (Minkowski). *Le groupe $\text{Cl}(K)$ des classes d'idéaux de K est fini.*

Le nombre d'éléments de $\text{Cl}(K)$ est le *nombre de classes* du corps K . On le note $h(K)$. Pour tout idéal fractionnaire \mathfrak{a} l'idéal $\mathfrak{a}^{h(K)}$ est principal.

Par conséquent l'anneau \mathbf{Z}_K est principal si et seulement si $h(K) = 1$.

Démonstration du théorème 3.56. La proposition 3.55 montre qu'il suffit de vérifier qu'il n'y a qu'un nombre fini d'idéaux entiers ayant une norme donnée. Soit donc N un entier non nul (seul l'idéal nul a pour norme 0). Soit \mathfrak{a} un idéal entier de norme N . Alors \mathfrak{a} est d'indice N dans \mathbf{Z}_K (lemme 3.38), donc \mathfrak{a} appartient à l'ensemble fini des idéaux de \mathbf{Z}_K qui contiennent N . □

Le théorème 3.40 donne une minoration du discriminant d'un corps de nombres : comme la norme de l'idéal $(1) = \mathbf{Z}_K$ vaut 1 on a

$$|D_K| \geq M(K)^{-2}. \quad (3.57)$$

On en déduit $|D_K| > 1$ pour $K \neq \mathbf{Q}$, donc il n'y a pas d'extension de \mathbf{Q} autre que \mathbf{Q} qui ne soit pas ramifiée.

La minoration (3.57) montre aussi que $|D_K|$ tend vers l'infini quand le degré n de K sur \mathbf{Q} tend vers l'infini. En voici une conséquence :

Corollaire 3.58 (*Hermite*). *Il n'y a qu'un nombre fini de sous-corps de \mathbf{C} de discriminant donné.*