Université P. et M. Curie (Paris VI),
Deuxième semestre 2006/2007

Michel Waldschmidt
date de mise à jour: 05/04/2007

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

Mention : Mathématiques et applications
MO11 : Théorie des nombres (12 ECTS)

Troisième partie : Arithmétique des Corps de Nombres

Fascicule 7 : section 3.5 (11 pages)

3.5 Idéaux d'un corps de nombres

Petit aperçu historique

L'invention de la notion d'idéal provient des recherches au XIXème 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 :

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

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 : [R], [P], Sk].`

3.5.1 Idéaux entiers

Soient K un corps de nombres, $\mathbf{Z}_K$ son anneau d'entiers.

Lemme 3.35. *Soit $\alpha \in \mathbf{Z}_K$. Alors $\mathbf{Z}_K/\alpha\mathbf{Z}_K$ a $|\mathrm{N}_{K/\mathbf{Q}}(\alpha)|$ éléments.*

Démonstration. On utilise la proposition 3.13 : il existe une base $\{e_1, \dots, e_n\}$ de $\mathbf{Z}_K$ et des entiers $a_1, \dots, a_n$ tels que $\{a_1e_1, \dots, a_ne_n\}$ 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_ie_i. Son image est $\alpha\mathbf{Z}_K$ et sa matrice dans la base $\{e_1, \dots, e_n\}$ est la matrice diagonale $\mathrm{diag}(a_1, \dots, a_n)$, dont le déterminant est $a_1 \cdots a_n = \mathrm{N}(\alpha\mathbf{Z}_K)$. 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 $v(a_ie_i) = \alpha e_i$. Alors $\det v = \pm 1$; comme $v \circ u$ est la restriction de $[\alpha]$ à $\mathbf{Z}_K$, le déterminant de u est aussi égal à $\pm\mathrm{N}_{K/\mathbf{Q}}(\alpha)$. □

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 3.11 et 3.13 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 $\{a_1e_1, \dots, a_ne_n\}$ 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 $\mathrm{N}(\mathfrak{a})$.

Le lemme 3.35 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 $\mathrm{N}(\mathfrak{b})$ divise $\mathrm{N}(\mathfrak{a})$.

Soient $n = [K : \mathbf{Q}]$ le degré de K et $\underline{\sigma} : K \to \mathbf{R}^n$ son plongement canonique.

Lemme 3.36. *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 $2^{-r_2}|D_K|^{1/2}\mathrm{N}(\mathfrak{a})$ et le discriminant de $\mathfrak{a}$ est $D_K\mathrm{N}(\mathfrak{a})^2$. .*

Démonstration. Le corollaire 3.27 donne le résultat quand $\mathfrak{a} = \mathbf{Z}_K$. Dans le cas général, $\mathfrak{a}$ est un sous-groupe d'indice fini $\mathrm{N}(\mathfrak{a})$ de $\mathbf{Z}_K$, donc $\underline{\sigma}(\mathfrak{a})$ est un sous-groupe d'indice fini $\mathrm{N}(\mathfrak{a})$ de $\underline{\sigma}(\mathbf{Z}_K)$. □

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 3.37. *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*

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

Démonstration. Nous renvoyons au livre de Samuel (§ 4.2) pour la démonstration. Le principe consiste à écrire les conditions que doit satisfaire un élément de $\mathfrak{a}$ pour que sa norme vérifie la majoration requise : cela définit dans $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ un *domaine symétrique convexe*. Pour assurer, en utilisant le théorème de Minkowski (corollaire 3.23), que ce domaine contient un élément non nul de l'image par le plongement logarithmique de l'idéal $\mathfrak{a}$, il reste à faire un petit calcul de volume. □

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 résuite 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 3.38. *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. □

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 $\mathfrak{p}$ est donc p^f où $f = [k : \mathbf{F}_p]$ est le *degré du corps résiduel*.

Lemme 3.39. *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 $\alpha_1, \ldots, \alpha_n$ 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

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

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

□

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

$$\begin{array}{ccc} A & \to & \mathrm{Hom}_A(M/\mathfrak{a}M, M/\mathfrak{a}M) \\ a & \mapsto & (x \mapsto ax) \end{array}$$

dont le noyau contient $\mathfrak{a}$. On en déduit un homomorphisme de A-modules de $A/\mathfrak{a}$ dans $\mathrm{Hom}_A(M/\mathfrak{a}M, M/\mathfrak{a}M)$ 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 3.40. *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 3.39 implique $\mathfrak{a} \neq \mathfrak{p}\mathfrak{a}$, donc la dimension de ce k-espace vectoriel est ≥ 1. □

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 3.39 ou bien le lemme 3.40, 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 3.40 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 $\mathrm{N}(\mathfrak{p})^m$.

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 $\mathrm{N}(\mathfrak{b})^m$ divise $\mathrm{N}_{K/\mathbf{Q}}(\alpha)$.

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 :

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

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 3.41. *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 3.41 montre que, sous les hypothèses du lemme 3.40, $\mathfrak{a}/\mathfrak{a}\mathfrak{p}$ est de dimension 1 comme espace vectoriel sur $\mathbf{Z}_K/\mathfrak{p}$ car il n'y a pas d'idéal entre $\mathfrak{a}\mathfrak{p}$ et $\mathfrak{a}$.

Pour une démonstration du théorème 3.41, voir par exemple le livre de Samuel.

3.5.3 Idéaux fractionnaires

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 3.42. *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 3.42 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 3.43. *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 3.41 on déduit que les idéaux fractionnaires de $\mathbf{Z}_K$ forment un groupe abélien d'élément neutre $\mathbf{Z}_K = (1)$.

Théorème 3.44. *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 3.41 montre que la propriété (3.1) de multiplicativité de la norme s'étend aux idéaux de $\mathbf{Z}_K$:

Corollaire 3.45. *Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux de $\mathbf{Z}_K$. Alors*

$$\mathrm{N}(\mathfrak{a}\mathfrak{b}) = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{b}). \tag{3.46}$$

Démonstration. Grâce au théorème 3.41 il suffit de vérifier la propriété (3.46) quand $\mathfrak{b}$ est un idéal premier. Notons-le $\mathfrak{p}$.

L'homomorphisme canonique

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

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 $\mathrm{N}(\mathfrak{p})$ éléments) et $\mathfrak{a}/\mathfrak{a}\mathfrak{p}$ est un k-espace vectoriel de dimension 1 (car $\mathfrak{p}$ est maximal - cf lemme 3.40 et la remarque qui suit le théorème 3.41), donc est isomorphe à k. Ainsi $\mathfrak{a}/\mathfrak{a}\mathfrak{p}$ a $\mathrm{N}(\mathfrak{p})$ éléments et par conséquent $\mathbf{Z}_K/\mathfrak{a}\mathfrak{p}$ en a $\mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{p})$.

□

Grâce au corollaire 3.45 on peut étendre la définition de la norme aux idéaux fractionnaires. Avec les notations du corollaire 3.44, on pose $v_\mathfrak{p}(\mathfrak{a}) = a_\mathfrak{p}$ et

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

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 $\mathrm{N}(\alpha\mathbf{Z}_K) = |\mathrm{N}_{K/\mathbf{Q}}(\alpha)|$.

Le lemme 3.43 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 $N = \mathrm{N}(\mathfrak{a})$, et soient $b_1, \dots, b_M$ des représentants des classes de $\mathbf{Z}_K$ modulo $\mathfrak{p}$, avec $M = \mathrm{N}(\mathfrak{p})$. Vérifier que

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

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

Du théorème 3.41 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 $e(\mathfrak{p}) \ge 1$.

Soit p un nombre premier et soit $p\mathbf{Z}_K$ l'idéal principal de $\mathbf{Z}_K$ qu'il engendre. Le théorème 3.41 montre qu'il existe une décomposition, unique à l'ordre près des facteurs,

$$p\mathbf{Z}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}, \tag{3.47}$$

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 $e_i \ge 1$ est l'indice de ramification de $\mathfrak{p}_i$ $(1 \le i \le g)$.

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 (3.47) 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 3.45, on obtient

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

Par conséquent

$$e_1 f_1 + \cdots + e_g f_g = n. \tag{3.48}$$

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
- *totalement ramifié dans* K si $e_1 = n$: alors $g = 1$ et $f_1 = 1$
- *totalement 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 3.49. *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 :

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

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

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

(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 3.50. *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.

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* $\mathrm{Cl}(K)$ *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 $\mathfrak{a} = \mathfrak{b} \cdot \alpha\mathbf{Z}_K$.

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 3.37).

Proposition 3.51. *Toute classe d'idéaux contient un idéal entier* $\mathfrak{a}$ *de norme* $\mathrm{N}(\mathfrak{a}) \leq M(K)|D_K|^{1/2}$.

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 3.37 à $\mathfrak{a}_2$ on trouve un élément $\beta \in \mathfrak{a}_2$ vérifiant $|\mathrm{N}_{K:\mathbf{Q}}(\beta)| \leq M(K)|D_K|^{1/2}\mathrm{N}(\mathfrak{a}_2)$. Alors $\mathfrak{a} = \beta\mathfrak{a}_2^{-1}$ est équivalent à $\mathfrak{a}_1$ et vérifie la propriété requise.

□

Théorème 3.52 (Minkowski). *Le groupe* $\mathrm{Cl}(K)$ *des classes d'idéaux de* K *est fini.*

Le nombre d'éléments de $\mathrm{Cl}(K)$ 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 3.52. La proposition 3.51 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 3.35), donc $\mathfrak{a}$ appartient à l'ensemble fini des idéaux de $\mathbf{Z}_K$ qui contiennent N.

□

Le théorème 3.37 donne une minoration du discriminant d'un corps de nombres : comme la norme de l'idéal $(1) = \mathbf{Z}_K$ vaut 1 on a

$$|D_K| \geq M(K)^{-2}. \tag{3.53}$$

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 (3.53) montre aussi que $|D_K|$ tend vers l'infini quand le degré n de K sur $\mathbf{Q}$ tend vers l'infini. Nous allons en déduire :

Corollaire 3.54 (*Hermite*). *Il n'y a qu'un nombre fini de sous-corps de* $\mathbf{C}$ *de discriminant donné.*

Démonstration. Il reste à vérifier qu'il n'y a qu'un nombre fini de corps de nombres de discriminant et de degré bornés.

Soit K un tel corps. Supposons pour commencer qu'il existe un plongement réel, c'est-à-dire $r_1 \geq 1$. Si A_0, A, B sont des nombres positifs, le volume du domaine convexe symétrique

$$|x_1| < A_0, \quad |x_i| < A \quad (2 \leq i \leq r_1), \quad |x_{r_1+i}| < B \quad (1 \leq i \leq r_2)$$

de $\mathbf{R}^{r_1} \times \mathbf{C}^{r_2}$ est $2^{r_1} A_0 A^{r_1-1} (\pi B^2)^{r_2}$. On prend $A = B = 1$ et on choisit A_0 de telle sorte que ce volume soit $> 2^{n-r_2} |D_K|^{1/2} = 2^n v\big(\underline{\sigma}(\mathbf{Z}_K)\big)$ (cf. Proposition 3.26). Par exemple $A_0 = 2^{n+1-r_1-r_2} \pi^{-r_2} |D_K|^{1/2}$. Alors le théorème de Minkowski (corollaire 3.23) montre qu'il existe un élément non nul α de $\mathbf{Z}_K$ tel que

$$|\sigma_1(\alpha)| < A_0 \text{ et } |\sigma_i(\alpha)| < 1 \text{ pour } 2 \leq i \leq n\ .$$

Comme α est entier sur $\mathbf{Z}$ et non nul sa norme est un entier de valeur absolue ≥ 1, donc $|\sigma_1(\alpha)| \geq 1 > |\sigma_i(\alpha)|$ pour $2 \leq i \leq n$. D'après le lemme 3.2 le polynôme caractéristique de α sur $\mathbf{Q}$ est la puissance $[K : \mathbf{Q}(\alpha)]$ du polynôme irréductible de α sur $\mathbf{Q}$. Le fait que $\sigma_1(\alpha)$ soit distinct des $\sigma_i(\alpha)$ pour $i \neq 1$ implique donc que α est un générateur de K sur $\mathbf{Q}$. Comme tous ses conjugués sont bornés en termes de n et de $|D_K|$, α appartient à un ensemble fini ne dépendant que de n et de $|D_K|$ (cela résulte de (3.24)).

Supposons maintenant qu'il n'existe pas de plongement de K dans $\mathbf{R}$, autrement dit $r_1 = 0$, $n = 2r_2$. Si A_0, A, B sont des nombres positifs, le volume du domaine convexe symétrique

$$|z_1 - \bar{z}_1| < A_0, \quad |z_1 + \bar{z}_1| < A \quad (2 \leq i \leq r_1), \quad |z_i| < B \quad (2 \leq i \leq r_2)$$

de $\mathbf{C}^{r_2}$ est $A_0 A(\pi B^2)^{r_2-1}$. On prend $A=2$, $B=1$ et on choisit A_0 de telle sorte que ce volume soit $> 2^{r_2}|D_K|^{1/2}$, disons $A_0 = 2(\pi/2)^{r_2-1}|D_K|^{1/2}$. Alors il existe $\alpha \in \mathbf{Z}_K \setminus \{0\}$ tel que $|\sigma_i(\alpha)| < 1$ pour $2 \leq i \leq r_2$, $|\Re\sigma_1(\alpha)| < 1$ et $|\Im\sigma_1(\alpha)| < A_0/2$. On a encore $|\sigma_1(\alpha)| = |\overline{\sigma}_1(\alpha)| \geq 1 > |\sigma_i(\alpha)|$ pour $2 \leq i \leq r_2$. De plus $\sigma_1(\alpha)$ n'est pas réel, donc $\sigma_1(\alpha) \neq \sigma_i(\alpha)$ pour $2 \leq i \leq n$. On en déduit de nouveau que α est un générateur de K qui appartient à un ensemble fini ne dépendant que de n et de $|D_K|$ □

3.5.6 Décomposition des idéaux premiers dans une extension

Soient k_1 un corps de nombres, k_2 une extension finie de k_1 de degré n, $\mathfrak{p}$ un idéal de $\mathbf{Z}_{k_1}$; on peut décomposer l'idéal engendré par $\mathfrak{p}$ dans $\mathbf{Z}_{k_2}$ sous la forme

$$\mathbf{Z}_{k_2}\mathfrak{p} = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$$

où $\mathfrak{P}_i$ sont des idéaux premiers deux-à-deux distincts de $\mathbf{Z}_{k_2}$ et $e_1, \ldots, e_g$ des entiers ≥ 1. Alors $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ sont les idéaux premiers de $\mathbf{Z}_{k_2}$ tels que $\mathfrak{P} \cap \mathbf{Z}_{k_1} = \mathfrak{p}$. L'entier e_i est *l'indice de ramification de* $\mathfrak{P}_i$ *sur* $\mathfrak{p}$. Si f_i désigne le *degré résiduel de* $\mathfrak{P}_i$ *sur* $\mathfrak{p}$, c'est-à-dire le degré de l'extension $[\mathbf{Z}_{k_2}/\mathfrak{P}_i : \mathbf{Z}_{k_1}/\mathfrak{p}]$, alors

$$\mathbf{Z}_{k_2}/\mathfrak{p}\mathbf{Z}_{k_2} \simeq \prod_{i=1}^{g} \mathbf{Z}_{k_2}/\mathfrak{P}_i^{e_i}.$$

Montrons que pour $1 \leq i \leq g$ le quotient $\mathbf{Z}_{k_2}/\mathfrak{P}_i^{e_i}$ est un $\mathbf{Z}_{k_1}/\mathfrak{p}$-espace vectoriel de dimension $e_i f_i$. Pour cela on considère la suite de $\mathbf{Z}_{k_1}/\mathfrak{p}$-espaces vectoriels

$$\mathbf{Z}_{k_2}/\mathfrak{P}_i^{e_i} \supset \mathbf{Z}_{k_2}/\mathfrak{P}_i^{e_i-1} \supset \cdots \supset \mathbf{Z}_{k_2}/\mathfrak{P}_i \supset \{0\}.$$

Le quotient de deux termes consécutifs est isomorphe $\mathfrak{P}_i^r/\mathfrak{P}_i^{r+1}$, qui est un $\mathbf{Z}_{k_2}/\mathfrak{P}_i$-espace vectoriel de dimension 1, donc un $\mathbf{Z}_{k_1}/\mathfrak{p}$-espace vectoriel de dimension f_i.

Montrons ensuite que $\mathbf{Z}_{k_2}/\mathfrak{p}\mathbf{Z}_{k_2}$ est un $\mathbf{Z}_{k_1}/\mathfrak{p}$ espace vectoriel de dimension n. Soit $\omega_1, \ldots, \omega_m$ une famille d'éléments de $\mathbf{Z}_{k_2}$ dont les classes $\bar{\omega}_1, \ldots, \bar{\omega}_m$ modulo $\mathfrak{p}\mathbf{Z}_{k_2}$ constituent une base du $\mathbf{Z}_{k_1}/\mathfrak{p}$-espace vectoriel $\mathbf{Z}_{k_2}/\mathfrak{p}\mathbf{Z}_{k_2}$. Il s'agit de vérifier que $\omega_1, \ldots, \omega_m$ est une base de k_2 sur k_1.

On commence par vérifier que $\{\omega_1, \ldots, \omega_m\}$ est une famille libre sur k_1. S'il y a une relation non triviale $a_1\omega_1 + \cdots + a_m\omega_m = 0$ avec des a_i dans $\mathbf{Z}_{k_1}$ non tous nuls, soit $\mathfrak{a}$ l'idéal de $\mathbf{Z}_{k_1}$ engendré par ces coefficients $a_1, \ldots, a_m$ et soit $\alpha \in \mathfrak{a}^{-1} \setminus \mathfrak{a}^{-1}\mathfrak{p}$. Alors $\alpha\mathfrak{a} \not\subset \mathfrak{p}$, donc $\alpha a_1, \ldots, \alpha a_m$ appartiennent à $\mathbf{Z}_{k_1}$ mais ne sont pas tous dans $\mathfrak{p}$, et la relation $\alpha a_1\omega_1 + \cdots + \alpha a_m\omega_m \equiv 0 \pmod{\mathfrak{p}}$ donne une contradiction avec l'hypothèse que $\{\bar{\omega}_1, \ldots, \bar{\omega}_m\}$ est une famille libre sur $\mathbf{Z}_{k_1}/\mathfrak{p}$.

Montrons enfin que la famille $\{\omega_1, \ldots, \omega_m\}$ engendre k_2 comme k_1-espace vectoriel. Soit $M = \mathbf{Z}_{k_1}\omega_1 + \cdots + \mathbf{Z}_{k_1}\omega_m$ et soit $N = \mathbf{Z}_{k_2}/M$. Par hypothèse $\{\bar{\omega}_1, \ldots, \bar{\omega}_m\}$ est une partie génératrice du $\mathbf{Z}_{k_1}/\mathfrak{p}$-espace vectoriel $\mathbf{Z}_{k_2}/\mathfrak{p}\mathbf{Z}_{k_2}$, donc $\mathbf{Z}_{k_2} = M + \mathfrak{p}\mathbf{Z}_{k_2}$. Alors $\mathfrak{p}N = N$. Le *Lemme de Nakayama* (voir 3.56) implique qu'il existe $\alpha \in 1 + \mathfrak{p}$ tel que $\alpha N = 0$. Alors $\alpha\mathbf{Z}_{k_2} \subset M$ et par conséquent $k_2 = k_1\omega_1 + \cdots + k_1\omega_m$. En particulier $m = n$.

De ceci on déduit une généralisation de (3.48) :

$$e_1 f_1 + \cdots + e_g f_g = n. \tag{3.55}$$

Lemme 3.56 (de Nakayama). *Soient A un anneau, $\mathfrak{a}$ un idéal de A et M un A-module de type fini. On suppose $\mathfrak{a}M = M$. Alors il existe un élément $\alpha \in 1 + \mathfrak{a}$ tel que $\alpha M = 0$.*

Démonstration. Soit $m_1, \ldots, m_n$ une famille génératrice du A-module M. Par hypothèse il existe des éléments x_{ij} dans $\mathfrak{a}$ $(1 \leq i, j \leq n)$ tels que

$$m_i = \sum_{j=1}^{n} x_{ij} m_j \quad (1 \leq i \leq n).$$

Soit M la matrice $\left(x_{ij}\right)_{1 \leq i,j \leq n}$ et soit α le déterminant de $I_n - M$. Alors α appartient à $1 + \mathfrak{a}$ et $\alpha M = 0$.

□

Dans le cas particulier où l'extension L/K est galoisienne le groupe de Galois agit transitivement sur les idéaux de L au dessus d'un idéal donné de K et il conserve les indices de ramification et des caractéristiques résiduelles : la formule (3.55) s'écrit alors simplement $efg = n$.

Définition. Un *anneau de Dedekind* est un anneau noethérien, intégralement clos, dans lequel tout idéal fractionnaire est inversible.

Théorème 3.57. *Soient A un anneau de Dedekind de caractéristique nulle, K son corps des fractions, L une extension finie de K. Alors la fermeture intégrale de A dans L est un anneau de Dedekind.*

En particulier ($A = \mathbf{Z}$, $K = \mathbf{Q}$) l'anneau des entiers d'un corps de nombres est un anneau de Dedekind.

Dans un anneau de Dedekind, tout idéal fractionnaire non nul s'écrit de manière unique

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

où $\mathfrak{p}$ décrit les idéaux premiers non nuls de A et où les $a_{\mathfrak{p}}$ sont des entiers rationnels tous nuls sauf un nombre fini.