Notes de lecture: J. Neukirch, Algebraic Number Theory

A∼Z / Justin Carel

Last updated December 24, 2022

Ci-après mes notes de lectures de l'excellent *Algebraic Number Theory* de Neukirch [Neu99]. Elles seront mises à jour au fur et à mesure de mes avancées dans le livre, ou si je tombe sur d'autres résultats qui s'insèrent bien dedans, ou si j'ai envie d'écrire un truc intéressant tangentiellement en lien.

1 Chapitre 1: Entiers algébriques

1.1 Entiers Gaussiens

Proposition 1.1. *$\mathbb{Z}[i]$ est euclidien.*

Preuve. Soit $0 \neq \alpha, \beta \in \mathbb{Z}[i]$. $\mathbb{Z}[i]$ forme une grille dans $\mathbb{C}$ où tout complexe est à distance plus petite que 1 d'un point entier. En particulier, il existe $\gamma \in \mathbb{Z}[i]$ tel que

$$\left|\frac{\alpha}{\beta} - \gamma\right| < 1,$$

soit $\alpha - \beta\gamma = r$ avec $N(r) < N(\beta)$. □

Lemme 1.1. *On trouve $a, b \in \mathbb{Z}$ tq $p = a^2 + b^2$ si et seulement si $p \not\equiv 3 \pmod 4$.*

Preuve. Le sens direct est trivial. Pour le sens réciproque, considérons a une racine de -1 modulo p. On a $p \mid a^2 + 1$ par définition, mais pas $p \mid a + i$ ni $p \mid a - i$, donc p n'est pas premier dans $\mathbb{Z}[i]$. Ainsi, on le décompose de manière non-triviale $p = \alpha\beta$, ce qui donne $N(\alpha) \mid N(p) = p^2$ puis $p = N(\alpha) = a^2 + b^2$. □

Théorème 1.1. *À association près, les premiers de $\mathbb{Z}[i]$ sont les éléments suivants:*

- $\pi = 1 + i$.
- $\pi = a + ib$, *où* $N(\pi) = p \equiv 1 \pmod 4$.
- $\pi = p \equiv 3 \pmod 4$.

Preuve. Posons $\pi = \alpha\alpha$. Les éléments des deux premières formes sont bien premiers: $N(\alpha)N(\alpha) = N(\pi) = p$, donc α ou α est inversible. Les éléments de la dernière forme sont premiers: $N(\alpha)N(\alpha) = N(\pi) = p^2$, donc $N(\alpha) \in \{1, p, p^2\}$. On ne peut pas avoir $N(\alpha) = p$ car $p = 3 \pmod 4$, donc α ou α est inversible.

Réciproquement, montrons que tout premier est associé à l'une de ces formes. On décompose $N(\pi)$ en

$$N(\pi) = \pi \cdot \overline{\pi} = \prod_{i=1}^{n} p_i,$$

ce qui donne $\pi \mid p_i =: p$ pour un certain i. Ainsi $N(\pi) \mid N(p) = p^2$, soit $N(\pi) \in \{p, p^2\}$. Si $N(\pi) = p$, alors π est du premier ou second type suivant la parité de p. Si $N(\pi) = p^2$ alors $N(p/\pi) = 1$ soit $\pi \sim p$, donc π est du troisème type. □

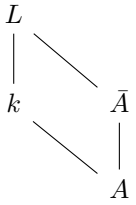
Proposition 1.2. *$\mathbb{Z}[i]$ est intégralement clos.*

Preuve. Soit $z = x + iy \in \mathbb{Q}(i)$ une racine de $X^2 - aX + b$. On a d'une part $z + \bar{z} = a \in \mathbb{Z}[i]$ donc $2x \in \mathbb{Z}$ et d'autre part $b = x^2 + y^2$ donc $2y \in \mathbb{Z}$. Désormais $(2x)^2 + (2y)^2 = 4b \equiv 0 \pmod 4$, soit $4 \mid 4x^2$ et $4 \mid 4y^2$: $x, y \in \mathbb{Z}$. □

Preuve alternative, se basant sur un résultat de la section suivante:
Preuve. Il est euclidien, donc principal, donc factoriel, donc intégralement clos. □

1.2 Intégralité

On va désormais considérer le schéma suivant jusqu'à la fin de nos jours, où $k = \operatorname{Frac} A$, L/k est une extension finie, et $\bar{A}$ est l'ensemble des entiers sur A.



Afin de nous munir d'outils puissants, un premier but va être de transférer à B/A les résultats de la théorie de Galois élémentaire qu'on peut employer pour étudier L/k. Sans surprise, nous allons tout d'abord donner un analogue à "α algébrique sur k ssi $k[\alpha]$ est de degré fini" puis l'employer pour montrer que B est un anneau.

Théorème 1.2. *Un élément α est entier sur A si et seulement si il existe un A-module de type fini $M \subseteq L$ tel que $\alpha M \subseteq M$.*

Voir [Mil20] pour une démonstration élémentaire mais abominablement calculatoire et peu intuitive.

Preuve.

⇒) Si $g(\alpha) \in A[\alpha]$ et $f(\alpha) = 0$ avec f unitaire, on peut écrire $g = fh + r$ avec $r \in A[X]$ et $\deg r < \deg f$. On a donc $g(\alpha) = r(\alpha)$, soit $A[\alpha]$ est généré par $(1, \alpha, \dots, \alpha^{d-1})$ où $d = \deg \alpha = \deg f$.

⇐) Soit M un tel module. La multiplication par α étant un endomorphisme de M, le théorème de Cayley-Hamilton donne un polynôme unitaire $\psi_\alpha \in A[X]$ annulant α. □

Corollaire. *$\bar{A}$ est un anneau. On l'appelle l'anneau des entiers de L sur A, ou la clôture intégrale de A dans L.*

Preuve. Si $\alpha, \beta \in \bar{A}$, considérons des modules $M, N \subseteq L$ tels que $\alpha M \subseteq M$ et $\beta N \subseteq N$. On obtient alors $(\alpha\beta)MN \subseteq MN$ et $(\alpha + \beta)MN \subseteq MN$. □

Corollaire 1.1. *Si C est entier sur B et B est entier sur A, alors C est entier sur B.*

Preuve. Soit $c \in C$, et $b_0 + b_1 c + \dots + c^n = 0$. Alors par récurrence $A[(b_i)]$ est un A-module de type fini. Comme c est entier sur $A[(b_i)]$, $A[(b_i), c]$ est de type fini sur $A[(b_i)]$ donc sur A. Ainsi c est entier sur A. □

Définition 1.1. *On dit que A est **intégralement clos** dans L si $\bar{A} = A$. On dit que A est intégralement clos tout court s'il est intégralement clos dans $k = \operatorname{Frac} A$.*

Corollaire 1.2. *La clôture intégrale de A dans L est intégralement close.*

Proposition 1.3. *Si A est factoriel, il est intégralement clos*[1].

Preuve. Soit $f(X) \in A[X]$ un polynôme unitaire annulant $\alpha = a/b \in k$. La factorialité permet de supposer a et b premiers entre eux. En posant (c_i) les coefficients de f, on écrit

$$c_0 b^d + c_1 a b^{d-1} + \dots + a^d = 0.$$

Ainsi tout diviseur premier de b est un diviseur premier de a, soit b est inversible et $\alpha \in A$. □

On remarque que si A est intégralement clos, alors $\bar{A} \cap k = A$.

[1] Quand le surcorps n'est pas précisé, on travaille dans le corps des fractions.

Proposition 1.4. *Si A est intégralement clos, les éléments de L sont de la forme b/a où $b \in \bar{A}$ et $a \in A$. En particulier, $L = \operatorname{Frac} \bar{A}$.*

Preuve. Soit $\alpha \in L$. Comme L est algébrique, on trouve un polynôme $f \in A[X]$ tel que

$$f(\alpha) = a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0.$$

En multipliant le tout par a_n^{n-1}, on obtient $g \in A[X]$ unitaire tel que $g(a_n\alpha) = 0$. □

Proposition 1.5. *Si A est intégralement clos, un élément $\alpha \in L$ est entier si et seulement si son polynôme minimal μ_α est à coefficients dans A.*

Preuve. Le sens réciproque est trivial. Pour le sens direct, remarquons que les conjugués de α sont eux aussi entiers ($\mu_\alpha \mid f$ pour tout $f \in A[X]$ annulant α). Les coefficients du polynômes minimal sont alors entiers sur A, donc dans A. □

Définition 1.2. *Si $\alpha \in L$, on appelle sa **norme** $\mathcal{N}(\alpha)$ et sa **trace** $\operatorname{Tr}\alpha$ le déterminant et la trace respectivement de l'application linéaire induite par la multiplication par α. Autrement dit, $\mathcal{N}(\alpha) = \det[\alpha]$ et $\operatorname{Tr}\alpha = \operatorname{Tr}[\alpha]$.*

Lemme 1.2. *Pour tout α de L, si ψ_α est le polynôme caractéristique de α alors $\psi_\alpha = \mu_\alpha^d$ où $d = [L : k(\alpha)]$.*

Preuve. Considérons la base $(1, \alpha, \ldots, \alpha^{m-1})$ de $k(\alpha)/k$ ainsi qu'une base (β_i) de $L/k(\alpha)$. La famille $(\alpha^i\beta_j)$ formant une base de L/k, la matrice $[\alpha]_{L/k}$ de la multiplication par α dans cette base se décompose en

$$[\alpha]_{L/k} = \bigoplus_{j=1}^{d} [\alpha]_{k(\alpha)/k}.$$

On en déduit alors

$$\psi_{\alpha,L/k} = \prod_{j=1}^{d} \psi_{\alpha,k(\alpha)/k} = \mu_\alpha^d.$$ □

Théorème 1.3. *Si L/k est séparable et $G = \hom_k(L, \bar{k})$, alors pour tout $\alpha \in L$ on a*

$$\psi_\alpha = \prod_{\sigma\in G} (X - \sigma\alpha), \quad \operatorname{Tr}\alpha = \sum_{\sigma\in G} \sigma\alpha, \quad \mathcal{N}(\alpha) = \prod_{\sigma\in G} \sigma\alpha.$$

Preuve. On partitionne G par $\sigma \sim \tau \iff \sigma\alpha = \tau\alpha$ en classes de $d = [L : k(\alpha)]$ éléments chacune. Si on choisit une famille (σ_i) de représentants, on obtient donc

$$\mu_\alpha = \prod_{i=1}^{m} (X - \sigma_i\alpha) \text{ avec } m = \deg\alpha.$$

On en déduit

$$\psi_\alpha = \mu_\alpha^d = \prod_{\sigma\in G} (X - \sigma\alpha).$$

Les deux derniers points sont donnés par l'égalité suivante, démontrée dans n'importe quel bon cours d'algèbre linéaire:

$$\psi_\alpha = X^n - \operatorname{Tr}\alpha X^{n-1} + \ldots + (-1)^n\mathcal{N}(\alpha).$$ □

Lemme 1.3. *Si $L/K/k$ est une tour d'extensions finies, alors*

$$\mathrm{Tr}_{L/k} = \mathrm{Tr}_{K/k} \circ \mathrm{Tr}_{L/K} \quad \text{et } \mathcal{N}_{L/k} = \mathcal{N}_{K/k} \circ \mathcal{N}_{L/K}.$$

Preuve. On montre le résultat uniquement dans le cas séparable, avec la même idée de preuve.

On partitionne $G = \hom_k(M, \bar{k})$ par $\sigma \sim \tau \iff \sigma_{|K} = \tau_{|K}$ en $m = [K : k]$ classes de $d = [L/K]$ éléments. Si (σ_i) est une famille de représentants, alors

$$\mathrm{Tr}_{K/k} \mathrm{Tr}_{L/K} \alpha = \sum_{i=0}^{m} \sigma_i \mathrm{Tr}_{L/K} \alpha = \sum_{i=0}^{m} \mathrm{Tr}_{\sigma_i L/\sigma_i K}(\sigma_i \alpha) = \sum_{i=0}^{m} \sum_{\sigma \sim \sigma_i} \sigma\alpha = \mathrm{Tr}_{L/k}.$$

La preuve pour la norme est exactement la même. □

Définition 1.3. *Soit $\mathcal{B} = (\alpha_i)_{1 \leq i \leq n}$ une base de L/k, et (σ_j) une énumération de $\hom_k(L, \bar{k})$. On définit le* ***discriminant*** *de $\mathcal{B}$ par*

$$\Delta(\mathcal{B}) = \Delta(\alpha_i) = \det[\sigma_j \alpha_i]^2.$$

On suppose désormais que L est séparable, et que A est intégralement clos. Si $a \in \bar{A}$ est entier, alors tous ses conjugués le sont. Comme d'autre part $\bar{A} \cap k = A$, on obtient $\mathrm{Tr}\, a \in A$ et $\mathcal{N}(a) \in A$. De plus, $a \in \bar{A}^\times$ si et seulement si $\mathcal{N}(a) \in A^\times$.

Lemme 1.4. $\Delta(\mathcal{B}) = \det[\mathrm{Tr}]_{\mathcal{B}}$, *où $[\mathrm{Tr}]_{\mathcal{B}}$ est la matrice de l'application bilinéaire induite par la trace.*

Preuve. Pour tout i, j, $\mathrm{Tr}(\alpha_i \alpha_j) = \sum_{\sigma \in G} (\sigma\alpha_i)(\sigma\alpha_j)$. Autrement dit, $[\mathrm{Tr}]_{\mathcal{B}} = [\sigma_j \alpha_i]^t \cdot [\sigma_j \alpha_i]$. □

Proposition 1.6. *La trace est non dégénérée, et le discriminant d'une base est non nul.*

Preuve. Si on considère la base $\mathcal{B} = (1, \alpha, \ldots, \alpha^{n-1})$ alors

$$\det[Tr]_{\mathcal{B}} = \Delta(\mathcal{B}) = \prod_{i<j} (\sigma_i \alpha - \sigma_j \alpha)^2 \neq 0,$$

où (σ_i) est une énumération de $\hom_k(L, \bar{k})$. Le second point suit trivialement du premier. □

Lemme 1.5. *Si $\mathcal{B} = (\alpha_i)$ est une base de L constituée d'éléments intègres et $d = \Delta(\mathcal{B})$, alors*

$$d\bar{A} \subseteq \bigoplus_i \alpha_i A.$$

Preuve. Soit $\alpha = \sum_i a_i \alpha_i$ entier avec $a_j \in k$. Alors pour tout i, $\mathrm{Tr}(\alpha_i \alpha) = \sum_j \mathrm{Tr}(\alpha_i \alpha_j) a_j$. Autrement dit,

$$[\mathrm{Tr}(\alpha_i \alpha)]_i = [\mathrm{Tr}]_{\mathcal{B}} \cdot [a_i]_i.$$

En multipliant par l'adjoint, on obtient

$$d[a_i]_i = \det[\mathrm{Tr}]_{\mathcal{B}} \cdot [a_i]_i = \mathrm{adj}[\mathrm{Tr}]_{\mathcal{B}} \cdot [\mathrm{Tr}(\alpha_i \alpha)]_i \in A^n.$$

Ainsi $d\alpha = \sum_i d a_i \alpha_i \in \sum_i \alpha_i A$. □

Définition 1.4. *Quand $\bar{A}$ est un A-module libre, on appelle une base de $\bar{A}/A$ une* ***base intégrale****. Une telle famille formant aussi une base de L/k, on a alors* $\mathrm{rg}\, \bar{A} = [L : k]$.

Théorème 1.4. *Si A est principal, alors tout $\bar{A}$-module $M \subseteq L$ de type fini est un A-module libre de rang $[L : k]$. En particulier, il existe une base intégrale.*

Preuve. Soit $\mathcal{B} = (\alpha_i)$ une base de L contenue dans $\bar{A}$, et soit $d = \Delta(B)$. Si maintenant M est de type fini sur $\bar{A}$, on trouve $a \in A$ tq $aM \subseteq \bar{A}$, soit

$$M \hookrightarrow daM \subseteq d\bar{A} \subseteq \bigoplus_i \alpha_i A = N.$$

Or A est principal, donc M est libre. De plus, $[L : k] = \operatorname{rg} \bar{A} \leq \operatorname{rg} M \leq \operatorname{rg} N = [L : k]$ d'où $\operatorname{rg} M = [L : k]$. □

On regarde le cas particulier d'un corps de nombres $\mathbb{Q} \subseteq k \subseteq \overline{\mathbb{Q}}$, dans lequel on note $\mathcal{O}_k$ l'anneau des entiers algébriques. Tout $\mathcal{O}_k$-module $\mathfrak{a} \subseteq k$ est libre de degré $[k : \mathbb{Q}]$ sur $\mathbb{Z}$. Si $\mathcal{B}$ et $\mathcal{B}'$ sont deux $\mathbb{Z}$-bases de $\mathfrak{a}$, alors $\Delta(\mathcal{B}) = \det P^2 \cdot \Delta(\mathcal{B}') = \Delta(\mathcal{B})$ où P est la matrice de passage. On note donc $\Delta(\mathfrak{a}) = \Delta(\mathcal{B})$. De plus, on écrit $\Delta_k = \Delta(\mathcal{O}_k)$ le discriminant du corps de nombres.

Proposition 1.7. *Si $\mathfrak{a} \subseteq \mathfrak{b}$ sont deux $\mathcal{O}_k$-modules de type fini, alors l'index est fini et*

$$\Delta(\mathfrak{a}) = [\mathfrak{b} : \mathfrak{a}]^2 \cdot \Delta(\mathfrak{b}).$$

Preuve. $\mathfrak{a}$ et $\mathfrak{b}$ sont tous deux libres de rang $n = [k : \mathbb{Q}]$. Soit (a_i) et (b_j) des bases de $\mathfrak{a}$ et $\mathfrak{b}$ respectivement. On peut écrire $[\mathfrak{b} : \mathfrak{a}] = |\det P|$, où P est la matrice de passage de (b_j) à (a_i). Ainsi

$$\Delta(\mathfrak{a}) = \Delta(a_i) = |\det P|^2 \cdot \Delta(b_j) = [\mathfrak{b} : \mathfrak{a}]^2 \cdot \Delta(\mathfrak{b}).$$ □

1.3 Idéaux

Théorème 1.5. *Si A est un PID, sa clôture intégrale $\bar{A}$ est Noethérienne, intégralement close, et tous ses idéaux premiers non nuls sont maximaux.*

Preuve. Si $\mathfrak{a} \subseteq \bar{A}$ est un idéal, alors il est libre en tant que sous-module d'un Z-module libre. En particulier, il est finiment généré. La clôture intégrale est intégralement close. Soit $\mathfrak{p} \subseteq \bar{A}$ un idéal premier. Alors $(p) = \mathfrak{p} \cap \mathbb{Z}$ est un idéal premier non-nul de $\mathbb{Z}$, et $\bar{A}/\mathfrak{p}$ est une $\mathbb{Z}/p\mathbb{Z}$-algèbre. Mais tout élément de $\bar{A}$ est entier sur $\mathbb{Z}$, ce qui se traduit après passage au quotient en algébrique sur $\mathbb{Z}/p\mathbb{Z}$. Ainsi $\bar{A}/\mathfrak{p}$ est une extension de corps de $\mathbb{Z}/p\mathbb{Z}$, et en particulier un corps. □

Définition 1.5. *Un domaine est dit de Dedekind s'il est Noethérien, intégralement clos, et que tous ses idéaux premiers sont maximaux.*

Dans ce nouveau langage, $\mathcal{O}_k$ est un domaine de Dedekind pour tout corps de nombre k. Cette notion est très proche de celle d'un domaine principal; en effet, un UFD est un PID si et seulement si ses idéaux premiers sont maximaux. La condition de Noetherianité implique l'existence d'une factorisation en irréductibles: il ne manque plus que les irréductibles soient premiers pour qu'un anneau de Dedekind devienne principal.

Un anneau de Dedekind réunit les conditions qui permettent aux idéaux de se factoriser de manière unique en un produit de premier. Nous étudierons un anneau de Dedekind arbitraire $\mathcal{O}$, et poserons K son corps des fractions.

Lemme 1.6. *Soit $\mathfrak{a} \subseteq \mathcal{O}$ un idéal non nul. Il existe des idéaux premiers $\mathfrak{p}_i$ vérifiant $\prod_i \mathfrak{p}_i \subseteq \mathfrak{a}$.*

Preuve. Soit $\mathfrak{a}$ un idéal maximal parmi ceux ne vérifiant pas la propriété. Comme $\mathfrak{a}$ n'est pas premier, il existe $a, b \notin \mathfrak{a}$ tels que $ab \in \mathfrak{a}$. Par maximalité, $\mathfrak{a} + (a)$ et $\mathfrak{a} + (b)$ possèdent respectivement des premiers $\mathfrak{p}_i$ et $\mathfrak{q}_i$ vérifiant $\prod \mathfrak{p}_i \subseteq \mathfrak{a} + (a)$ et $\prod \mathfrak{q}_i \subseteq \mathfrak{a} + (b)$. On obtient alors l'absurdité suivante:

$$\prod \mathfrak{p}_i \cdot \prod \mathfrak{q}_i \subseteq \big(\mathfrak{a} + (a)\big)\big(\mathfrak{b} + (a)\big) \subseteq \mathfrak{a}.$$ □

Lemme 1.7. *Soit $\mathfrak{p} \subseteq \mathcal{O}$ un premier. On définit son* ***inverse*** *par*

$$\mathfrak{p}^{-1} = \{x \in K \mid x\mathfrak{p} \subseteq O\}.$$

Alors pour tout idéal non nul $\mathfrak{a}$ de $\mathcal{O}$, $\mathfrak{a}\mathfrak{p}^{-1} \neq \mathfrak{a}$.

Preuve. Montrons tout d'abord que $p^{-1} \neq \mathcal{O}$. Considérons pour cela un élément non-nul $a \in \mathfrak{p}$ et le r minimal tel que

$$\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r \subseteq (a) \subseteq p,$$

pour certains premiers $\mathfrak{p}_i$. Alors spdg $\mathfrak{p}_1 \subseteq p$, d'où $\mathfrak{p}_1 = \mathfrak{p}$ par maximalité. Maintenant $\mathfrak{b} = \mathfrak{p}_2 \cdots \mathfrak{p}_r$ n'est pas contenu dans (a) par minimalité de r, donc on trouve $b \in \mathfrak{b}$ avec $b \notin (a)$. Autrement dit, on a $a^{-1}b \notin \mathcal{O}$ d'une part, et $b\mathfrak{p} \subseteq \mathfrak{a}$ soit $a^{-1}b \in \mathfrak{p}^{-1}$ d'autre part. Ainsi $\mathfrak{p}^{-1} \neq \mathcal{O}$.

Posons désormais $\mathfrak{a}$ un idéal non-nul de $\mathcal{O}$, généré un nombre fini de α_i. Nous allons montrer que si $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$, alors $\mathfrak{p}^{-1} = \mathcal{O}$. Si $x \in \mathfrak{p}^{-1}$, alors

$$\alpha_i x = \sum_{j=1}^{n} a_{ij}\alpha_j \quad \forall\, 1 \leq i \leq n.$$

La matrice $A = xI - [a_{ij}]_{i,j}$ vérifie $A(a_i)_i = 0$, soit $\psi(x) = \det A = 0$ où ψ est le polynôme caractéristique de $[a_{ij}]_{i,j}$. Ainsi x est intègre sur $\mathcal{O}$, soit $x \in \mathcal{O}$. On en déduit $\mathfrak{p}^{-1} = \mathcal{O}$, absurde. □

Lemme 1.8. *Si $\mathfrak{p}$ est premier, alors $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$.*

Preuve. D'après le lemme précédent, $\mathfrak{p} \subsetneq pp^{-1} \subseteq \mathcal{O}$. De plus $\mathfrak{p}\mathfrak{p}^{-1}$ est un sous-$\mathcal{O}$-module de $\mathcal{O}$ donc un idéal, soit $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$ par maximalité de $\mathfrak{p}$. □

Théorème 1.6. *Tout idéal non-nul $\mathfrak{a}$ d'un anneau de Dedekind $\mathcal{O}$ se décompose de manière unique en produit de premiers, ie*

$$\mathfrak{a} = \prod_i \mathfrak{p}_i^{\nu_i}$$

où les $\mathfrak{p}_i$ sont des premiers distincts et tout autre décomposition est donnée par les mêmes premiers à la même puissance.

Preuve. Soit $\mathfrak{a} \neq 0$ un idéal maximal parmi ceux ne vérifiant pas l'existence de la factorisation. Alors $\mathfrak{a}$ est contenu dans un idéal maximal $\mathfrak{p}$, soit

$$\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}.$$

La maximalité de $\mathfrak{a}$ garantit l'existence d'une factorisation $\mathfrak{a}\mathfrak{p}^{-1} = \prod \mathfrak{p}_i$, et $\mathfrak{a} = \mathfrak{p}\prod \mathfrak{p}_i$ est une factorisation pour $\mathfrak{a}$. L'unicité est donnée par une récurrence évidente, une fois remarqué que si

$$\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{a} = \mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_s,$$

alors $\mathfrak{p}_1 = \mathfrak{q}_1$ à réindexation près. □

L'emploi de $\mathfrak{p}^{-1}$ dans les preuves précédentes motive l'introduction d'une généralisation des idéaux de $\mathcal{O}$, qui permettra entre autres de donner un inverse à la multiplication.

Définition 1.6. *Un* ***idéal fractionnel*** *de K est un $\mathcal{O}$-module non-nul $\mathfrak{a} \subseteq K$ de type fini.*

Proposition 1.8. *L'ensemble J_K des idéaux fractionnels de K forme un groupe d'unité $(1) = \mathcal{O}$ et d'inverse*

$$\mathfrak{a}^{-1} = \{z \in K \mid z\mathfrak{a} \subseteq \mathcal{O}\}.$$

Preuve. Soit $\mathfrak{a}$ un idéal fractionnel. Alors $\mathcal{O}\mathfrak{a} = \mathfrak{a}\mathcal{O} = \mathfrak{a}$ trivialement. En mettant au même dénominateur les générateurs de $\mathfrak{a}$, on l'écrit $\mathfrak{a} = c^{-1}\mathfrak{b}$ où $\mathfrak{b}$ est un idéal de $\mathcal{O}$. On a donc $\mathfrak{b} = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r$ où les $\mathfrak{p}_i$ sont premiers. On pose $\mathfrak{b}' = \mathfrak{p}_1^{-1}\mathfrak{p}_2^{-1} \cdots \mathfrak{p}_r^{-1}$ et $\mathfrak{a}' = c\mathfrak{b}'$. On obtient $\mathfrak{a}\mathfrak{a}' = \mathcal{O}$, donc $\mathfrak{a}'$ est l'inverse et $\mathfrak{a}' \subseteq \mathfrak{a}^{-1}$. Réciproquement, si $z\mathfrak{a} \subseteq \mathcal{O}$ alors $z \in (z) = z\mathfrak{a}\mathfrak{a}' \subseteq \mathcal{O}\mathfrak{a}' = \mathfrak{a}'$, d'où $\mathfrak{a}^{-1} = \mathfrak{a}'$ est l'inverse de $\mathfrak{a}$. □

Corollaire 1.3. *Tout idéal fractionnel $\mathfrak{a}$ se factorise de manière unique en*

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

où les $\nu_\mathfrak{p} \in \mathbb{Z}$ sont presque tous nuls. Ainsi, J_K est le groupe abélien libre sur les idéaux premiers de $\mathcal{O}$.

Définition 1.7. *On appelle $Cl_K = J_K/K^*$ le* ***groupe de classe*** *de K. On obtient alors la suite exacte suivante:*

$$0 \longrightarrow \mathcal{O}^* \longrightarrow K^* \longrightarrow J_K \longrightarrow Cl_K \longrightarrow 0.$$

Dans cette suite, les flèches $K^* \to J_K \to Cl_K$ mesurent la dilatation obtenue en passant des éléments aux idéaux, ou en d'autres termes à quel point $\mathcal{O}$ n'est pas factoriel. Inversement, les flèches $\mathcal{O}^* \to K^* \to J_K$ mesurent la compression dans la même opération. Il est donc important de comprendre les groupes $\mathcal{O}^*$ et Cl_K.

1.3.1 Exercices

Proposition (Ex.4). *Un anneau de Dedekind $\mathcal{O}$ possédant un nombre fini d'idéaux premiers $\mathfrak{p}_i$ est principal.*

Preuve. Soit $\pi \in \mathfrak{p}_1 \setminus \mathfrak{p}_1^2$. D'après le CRT on peut trouver $x \in R$ vérifiant $x - \pi \in \mathfrak{p}_1^2$ et $x - 1 \in \mathfrak{p}_i$ pour tout $i \neq 1$. Il s'ensuit que la factorisation de (x) est donnée par $(x) = \mathfrak{p}_1$. Tous les idéaux premiers sont principaux, donc tous les idéaux sont principaux. □

Proposition (Ex.5). *Si $\mathfrak{a}$ est un idéal non-nul d'un domaine de Dedekind $\mathcal{O}$, alors $\mathcal{O}/\mathfrak{a}$ est un anneau principal.*

Preuve. Il suffit de démontrer le résultat pour $\mathfrak{a} = \mathfrak{p}^n$, le CRT donnant la principalité dans le cas $\mathfrak{a} = \mathfrak{p}_1^{\nu_1}\mathfrak{p}_2^{\nu_2}\cdots\mathfrak{p}_r^{\nu_r}$. Alors $\mathcal{O}/\mathfrak{p}^n\mathcal{O} \cong \mathcal{O}_\mathfrak{p}/\mathfrak{p}^n\mathcal{O}_\mathfrak{p}$ qui est principal. □

Preuve. On prend $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. Alors $(\pi^k) = \mathfrak{p}^k\mathfrak{b}$, où $\mathfrak{b}$ est premier avec $\mathfrak{p}$. Ainsi, il existe $(u, v) \in \mathfrak{b} \times \mathfrak{p}^{n-k}$ tel que $u + v = 1$. Si $x \in \mathfrak{p}^k$, on obtient $x = xu + xv \in (\pi^k) + \mathfrak{p}^n$, d'où $\mathfrak{p}^k = (\pi^k) + \mathfrak{p}^n$. On en déduit que $\mathfrak{p}^k/\mathfrak{p}^n = \pi^k\mathcal{O}/\mathfrak{p}^n$ est principal. □

Corollaire (Ex.6). *Tout idéal $\mathfrak{a}$ d'un domaine de Dedekind $\mathcal{O}$ peut être généré par deux éléments.*

Preuve. Soit $0 \neq a \in \mathfrak{a}$. Comme $\mathfrak{a}/(a)$ est principal, $\mathfrak{a} = (a) + (b)$ pour un certain b par le théorème de correspondance. □

1.4 Lattices

References

[Mil20] J.S. Milne. *Algebraic Number Theory*. https://www.jmilne.org/math/CourseNotes/ant.html. Version v3.08. 2020.

[Neu99] Jürgen Neukirch. *Algebraic number theory. Transl. from the German by Norbert Schappacher*. English. Vol. 322. Grundlehren Math. Wiss. Berlin: Springer, 1999. ISBN: 3-540-65399-6.