

Notes de lecture: J. Neukirch, Algebraic Number Theory

A~Z / Justin Carel

Last updated December 15, 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 $p \equiv 3 \pmod{4}$, donc α ou α est inversible.

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

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

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 troisième type. □

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

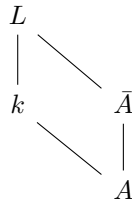
Preuve. Soit $z = x + iy \in \mathbb{Q}(i)$ une racine de $X^2 - aX + b$. On a d'une part $z + \bar{z} = a \in \mathbb{Z}[i]$ donc $2x \in \mathbb{Z}$ et d'autre part $b = x^2 + y^2$ donc $2y \in \mathbb{Z}$. Désormais $(2x)^2 + (2y)^2 = 4b \equiv 0 \pmod{4}$, soit $4 \mid 4x^2$ et $4 \mid 4y^2$: $x,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

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 $k = \text{Frac } A$, 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 $\psi_\alpha \in A[X]$ annihilant 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 A .*

Preuve. Soit $c \in C$, et $b_0 + b_1c + \dots + c^n = 0$. 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 $k = \text{Frac } A$.*

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

Proposition 1.3. *Si A est factoriel, il est intégralement clos¹.*

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

$$c_0b^d + c_1ab^{d-1} + \dots + a^d = 0.$$

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 $\bar{A} \cap k = A$.

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

Proposition 1.4. Si A est int gralement clos, les  l ments de L sont de la forme b/a o  $b \in \bar{A}$ et $a \in A$. En particulier, $L = \text{Frac } \bar{A}$.

Preuve. Soit $\alpha \in L$. Comme L est alg brique, on trouve un polyn me $f \in A[X]$ tel que

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

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 int gralement clos, un  l ment $\alpha \in L$ est entier si et seulement si son polyn me minimal μ_α est   coefficients dans A .

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

D finition 1.2. Si $\alpha \in L$, on appelle sa **norme** $\mathcal{N}(\alpha)$ et sa **trace** $\text{Tr } \alpha$ le d terminant et la trace respectivement de l'application lin aire induite par la multiplication par α . Autrement dit, $\mathcal{N}(\alpha) = \det[\alpha]$ et $\text{Tr } \alpha = \text{Tr}[\alpha]$.

Lemme 1.2. Pour tout α de L , si ψ_α est le polyn me caract ristique de α alors $\psi_\alpha = \mu_\alpha^d$ o  $d = [L : k(\alpha)]$.

Preuve. Consid rons la base $(1, \alpha, \dots, \alpha^{m-1})$ 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 d compose en

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

On en d duit alors

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

Th or me 1.3. Si L/k est s parable et $G = \text{hom}_k(L, \bar{k})$, alors pour tout $\alpha \in L$ on a

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

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

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

On en d duit

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

Les deux derniers points sont donn s par l' galit  suivante, d montr e dans n'importe quel bon cours d'alg bre lin aire:

$$\psi_\alpha = X^n - \text{Tr } \alpha X^{n-1} + \dots + (-1)^n \mathcal{N}(\alpha). \quad \square$$

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

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

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

On partitionne $G = \mathrm{hom}_k(M, \bar{k})$ 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

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

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 $\mathrm{hom}_k(L, \bar{k})$. 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 $\mathcal{B} = (1, \alpha, \dots, \alpha^{n-1})$ alors

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

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

Lemme 1.5. Si $\mathcal{B} = (\alpha_i)$ est une base de L constituée d'éléments entières 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 $d\alpha = \sum_i da_i \alpha_i \in \sum_i \alpha_i A$. □

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 $d = \Delta(\mathcal{B})$. 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, $[L : k] = \text{rg } \bar{A} \leq \text{rg } M \leq \text{rg } N = [L : k]$ d'où $\text{rg } M = [L : k]$. \square

On regarde le cas particulier d'un corps de nombres $\mathbb{Q} \subseteq k \subseteq \bar{\mathbb{Q}}$, 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

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

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 \mathbb{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 algèbre 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. \square

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.

Lemme 1.6. *Soit $\mathfrak{a} \subseteq \mathcal{O}_k$. Il existe des idéaux premiers \mathfrak{p}_i vérifiant*

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.