Leçon 127 : Exemples de nombres remarquables. Exemples d'anneaux de nombres remarquables. Applications.

Mémoire de M2

Préparation à l'agrégation 2025-2026

Tristan Roy

ens rennes | école normale supérieure

Université de Rennes

Table des matières

Introduction

Les premiers nombres que l'on rencontre à l'école sont les nombres entiers. Mais la discipline mathématique qui s'y intéresse, la théorie des nombres, fait très souvent intervenir d'autres types de nombres, qui élargissent le champ des possibles. Par exemple, le théorème des deux carrés étudie la possibilité d'écrire un nombre entier comme somme de deux carrés d'entiers. C'est un problème faisant intervenir uniquement des nombres entiers mais une façon de le résoudre est d'étudier l'anneau $\mathbb{Z}[i]$. On touche alors à la théorie algébrique des nombres : elle s'intéresse à une "notion plus générale" d'entiers, les entiers algébriques, qui peuvent être utilisés pour résoudre des problèmes concernant les entiers relatifs.

Dans ce mémoire, on s'intéresse d'abord aux ensembles classiques de nombres : les entiers, parmi lesquels les nombres premiers jouent un rôle particulier, puis les nombres rationnels et réels.

Il est ensuite nécessaire de faire un peu de théorie des corps pour introduire un autre type de nombres remarquables : les nombres algébriques. On verra en particulier que ceux-ci forment la clôture algébrique (complexe) de $\mathbb{Q}$. Les complexes qui ne sont pas algébriques sont les mystérieux nombres transcendants, dont on donnera quelques exemples. Nous nous intéresserons ensuite à la classe de nombres mentionnée ci-dessus, les entiers algébriques. Leur étude est complexe, c'est pourquoi nous nous limiterons à étudier les entiers algébriques contenus dans certains corps plutôt simples, les corps quadratiques (*i.e.* qui sont des $\mathbb{Q}$-espaces vectoriels de dimension 2).

Enfin, nous nous intéresserons aux racines complexes de l'unité, qui engendrent des extensions de $\mathbb{Q}$ très importantes, les corps cyclotomiques. Une raison pour laquelle ces extensions sont intéressantes est le théorème de Kronecker-Weber, qui stipule que toute extension finie abélienne de $\mathbb{Q}$ est contenue dans un corps cyclotomique. Nous concluerons ce mémoire par la preuve de ce théorème dans un cadre très restreint : encore une fois celui des corps quadratiques, qui sont en particulier des extensions finies abéliennes de $\mathbb{Q}$.

Les développements choisis sont :

- l'étude du caractère euclidien et principal des anneaux d'entiers quadratiques (propositions 42 et 45)
- le théorème de Kronecker-Weber faible (théorème 59).

I Nombres remarquables

I.1 Entiers

Dans l'ensemble des entiers relatifs $\mathbb{Z}$ il existe une division euclidienne, ce qui lui donne une structure intéressante.

Proposition 1. $\mathbb{Z}$ est euclidien, donc principal, donc factoriel.

Définition 2 (Nombre premier)**.** On appelle nombre premier un élément irréductible positif de $\mathbb{Z}$. Autrement dit, $p \in \mathbb{Z}$ est premier si et seulement si $p > 1$ et ses seuls diviseurs positifs sont 1 et lui-même.

Proposition 3 (Décomposition en produit de nombres premiers)**.** Pour tout $n \in \mathbb{Z}$, il existe $\varepsilon \in \{\pm 1\}$, $r \geq 1$, $p_1, \ldots, p_r$ des nombres premiers et $\alpha_1, \ldots, \alpha_r \in \mathbb{N}^*$ tels que :

$$n = \varepsilon \prod_{i=1}^{r} p_i^{\alpha_i}$$

et cette factorisation est unique.

Démonstration. C'est simplement une reformulation de la factorialité de $\mathbb{Z}$, en utilisant la définition des nombres premiers, qui sont (au signe près) les éléments irréductibles. □

Proposition 4. Il existe une infinité de nombres premiers.

Les nombres premiers apparaissent dans de nombreux contextes. On peut par exemple les utiliser pour montrer que des relations ne peuvent avoir lieu dans $\mathbb{Z}$ en les réduisant modulo p et en obtenant une contradiction, ce qui est souvent plus simple car $\mathbb{Z}/p\mathbb{Z}$ est un corps, qui est de plus fini.

Exemple 5. Pour $n \in \mathbb{N}, 4n^2 + 17n - 31$ est divisible par 5 ssi $n \equiv 1 \mod 5$.

Un autre exemple d'utilisation des nombres premiers est le critère d'Eisenstein, qui est un critère d'irréductibilité de polynômes à coefficients entiers.

Proposition 6 (Critère d'Eisenstein)**.** Soit $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ de degré n. S'il existe p premier tel que :

- p divise $a_0, \ldots, a_{n-1}$
- p ne divise pas a_n
- p^2 ne divise pas a_0,

alors P est irréductible dans $\mathbb{Q}[X]$.

Exemple 7. Le polynôme $\Phi_p = \sum_{i=0}^{p-1} X^i$ est irréductible dans $\mathbb{Q}[X]$ pour tout p premier.

Pour le montrer, on applique le critère d'Eisenstein à $\Phi_p(X+1)$ avec le nombre premier p. On obtient l'irréductibilité de $\Phi_p(X+1)$ et par conséquent celle de Φ_p.

I.2 Réels

Définition 8 (Nombre rationnel)**.** L'ensemble des nombres rationnels est $\mathbb{Q} = \mathrm{Frac}(\mathbb{Z}) = \{\frac{p}{q}; (p,q) \in \mathbb{Z} \times \mathbb{N}^*\}$.

Définition 9 (Nombre réel)**.** L'ensemble des nombres réels $\mathbb{R}$ peut être défini comme le complété de $\mathbb{Q}$ pour la distance donnée par la valeur absolue.

Exemple 10. Il existe des réels non rationnels : $\sqrt[n]{2}, e, \pi$ sont irrationnels.

Proposition 11 (Décomposition en base b)**.** Soit $b \geq 2$ un entier naturel. Tout réel $x \in [0,1[$ s'écrit de manière unique sous la forme

$$x = \sum_{i=1}^{\infty} \frac{a_i}{b^i}$$

avec $a_i \in [\![0, b-1]\!]$ pour tout $i \geq 1$ et $a_i \leq b-2$ pour une infinité d'entiers i.

Autrement dit, en notant S_b le sous-ensemble de $[\![0, b-1]\!]^{\mathbb{N}^*}$ constitué des suites non ultimement

stationnaires à $b-1$, on a une bijection

$$f_b : \left| \begin{array}{ccc} S_b & \longrightarrow & [0,1[\\ (a_i)_{i\in\mathbb{N}^*} & \longmapsto & \sum_{i=1}^{\infty} \frac{a_i}{b^i} \end{array} \right. .$$

Remarque 12. L'écriture obtenue s'appelle l'écriture en base b de x. On peut définir l'écriture en base b de tout $y \geq 0$ en écrivant $y = \lfloor y \rfloor + (y - \lfloor y \rfloor)$ et en développant $y - \lfloor y \rfloor \in [0,1[$ en base b.

Proposition 13. Soit $b \geq 2$ un entier naturel et $x \geq 0$. Alors x est rationnel si et seulement si son développement en base b est périodique à partir d'un certain rang (*i.e.* s'il existe deux entiers $N, k > 0$ tels que $\forall n \geq N, a_{n+k} = a_n$).

Corollaire 14. $\alpha \in \mathbb{R}$ est rationnel si et seulement si la suite de ses décimales est périodique à partir d'un certain rang.

II Extensions de corps, nombres algébriques

II.1 Généralités

Ici $\mathbb{K}$ désigne un sous-corps de $\mathbb{C}$.

Proposition 15. Si $\alpha \in \mathbb{C}$, on a un morphisme de $\mathbb{K}$-algèbres $ev_\alpha : \mathbb{K}[X] \to \mathbb{C}, P \mapsto P(\alpha)$. Son noyau est un idéal de $\mathbb{K}[X]$ donc nul ou de la forme $(\mu_{\alpha,\mathbb{K}})$ pour un unique $\mu_{\alpha,\mathbb{K}}$ unitaire.

On définit alors deux classes de nombres :

Définition 16 (Nombre transcendant, nombre algébrique, polynôme minimal, degré)**.** Soit $\alpha \in \mathbb{C}$.

- si ev_α est injective, α est dit transcendant sur $\mathbb{K}$.
- sinon, $\ker ev_\alpha$ est non nul donc s'écrit $(\mu_{\alpha,\mathbb{K}})$ pour un unique μ_α unitaire. α est alors dit algébrique sur $\mathbb{K}$ et $\mu_{\alpha,\mathbb{K}}$ est appelé polynôme minimal de α. On définit également le degré d'un nombre algébrique comme le degré de son polynôme minimal.

On a directement la caractérisation utile suivante :

Proposition 17. Si $\alpha \in \mathbb{C}$,

$$\alpha \text{ algébrique sur } \mathbb{K} \iff \exists P \in \mathbb{K}[X] \setminus \{0\}, P(\alpha) = 0.$$

Proposition 18. Pour tout $\alpha \in \mathbb{C}$, $\mu_{\alpha,\mathbb{K}}$ est irréductible dans $\mathbb{K}[X]$.

Démonstration. Cela découle de l'intégrité de $\mathbb{C}$: si $\mu_{\alpha,\mathbb{K}} = PQ$, en évaluant en α on obtient $0 = P(\alpha)Q(\alpha)$ donc P ou Q annule α et la minimalité de $\mu_{\alpha,\mathbb{K}}$ permet de conclure. □

On va maintenant étudier l'anneau $\mathbb{K}[\alpha]$ et le corps $\mathbb{K}(\alpha)$.

Regardons d'abord les propriétés de la $\mathbb{K}$-algèbre $\mathbb{K}[\alpha]$ dans les deux cas précédents (algébrique et transcendant).

Proposition 19. Soit $\alpha \in \mathbb{C}$.

(i) Si α est transcendant sur $\mathbb{K}$, $\mathbb{K}[\alpha]$ est isomorphe (en tant que $\mathbb{K}$-algèbre) à $\mathbb{K}[X]$.

(ii) Si α est algébrique sur $\mathbb{K}$, on a un isomorphisme de $\mathbb{K}$-algèbres $\mathbb{K}[X]/(\mu_{\alpha,\mathbb{K}}) \simeq \mathbb{K}[\alpha]$ et en notant $d = \deg(\mu_{\alpha,\mathbb{K}})$, la famille $(1, \alpha, \ldots, \alpha^{d-1})$ est une $\mathbb{K}$-base de $\mathbb{K}[\alpha]$.

En particulier, $\dim \mathbb{K}[\alpha] = d$.

Démonstration. Les isomorphismes de $\mathbb{K}$-algèbres s'obtiennent en appliquant le premier théorème d'isomorphisme à ev_α.

Dans le cas algébrique, la famille évoquée est une base car : elle est génératrice (par un argument de division euclidienne) et libre (par minimalité du polynôme minimal). □

Exemple 20. Le complexe i est algébrique sur $\mathbb{Q}$ de degré 2 (car non rationnel et annulé par X^2+1), donc $\mathbb{Q}[i] = \{a+ib; (a,b) \in \mathbb{Q}^2\}$.

Corollaire 21. Il y a équivalence entre :

(i) α est algébrique sur $\mathbb{K}$

(ii) $[\mathbb{K}[\alpha] : \mathbb{K}] < \infty$

(iii) $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$.

Démonstration. Montrons (ii) $\Longrightarrow$ (iii), qui illustre l'utilité des techniques vectorielles pour étudier les extensions de corps.

Comme $\mathbb{K}(\alpha)$ est le plus petit corps contenant $\mathbb{K}$ et α, il suffit de montrer que $\mathbb{K}[\alpha]$ est un corps. Soit $x \in \mathbb{K}[\alpha]$ non nul. L'application de multiplication par x

$$m_x : \left| \begin{array}{ccc} \mathbb{K}[\alpha] & \longrightarrow & \mathbb{K}[\alpha] \\ y & \longmapsto & xy \end{array} \right.$$

est :

- bien définie car $\mathbb{K}[\alpha]$ est stable par multiplication
- $\mathbb{K}$-linéaire
- injective : son noyau est réduit à $\{0\}$ par intégrité de $\mathbb{C}$ (x est non nul).

Ainsi m_x est un endomorphisme injectif du $\mathbb{K}$-espace vectoriel $\mathbb{K}[\alpha]$, qui est de dimension finie puisqu'on a (ii). Il est alors nécessairement surjectif. Il existe donc $y \in \mathbb{K}[\alpha]$ tel que $m_x(y) = 1$ *i.e.* $xy = 1$.

On a donc $y = x^{-1} \in \mathbb{K}[\alpha]$. □

Avec les deux résultats précédents, on connaît la structure de $\mathbb{K}(\alpha)$, l'extension de $\mathbb{K}$ engendrée par α.

Corollaire 22. Soit $\alpha \in \mathbb{C}$.

(i) Si α est transcendant sur $\mathbb{K}$, il y a un isomorphisme (de corps et même de $\mathbb{K}$-algèbres) entre $\mathbb{K}(\alpha)$ et $\mathbb{K}(X)$.

(ii) Si α est algébrique sur $\mathbb{K}$ de degré d, le corps $\mathbb{K}(\alpha)$ est $\mathbb{K}[\alpha]$, la $\mathbb{K}$-algèbre de dimension finie dont une base est $(1, \alpha, \ldots, \alpha^{d-1})$.

Démonstration. Le premier point découle du fait que l'isomorphisme entre $\mathbb{K}[\alpha]$ et $\mathbb{K}[X]$ de la proposition 19 donne par passage au corps des fractions un isomorphisme entre $\mathbb{K}(\alpha)$ et $\mathbb{K}(X)$.

Le deuxième point découle directement des deux résultats précédents. □

Le plus souvent, on est dans le cas $\mathbb{K} = \mathbb{Q}$ et on ne précise pas que le corps $\mathbb{K}$ est $\mathbb{Q}$. On parle ainsi de nombre algébrique, et le polynôme minimal d'un nombre algébrique (sur $\mathbb{Q}$, donc) est noté μ_α.

On va donc maintenant étudier l'ensemble des nombres algébriques (sous-entendu algébriques sur $\mathbb{Q}$).

Exemple 23. $\sqrt[n]{2}$ est irrationnel mais algébrique pour tout $n \geq 2$. Son polynôme minimal est $X^n - 2$ (il annule $\sqrt[n]{2}$ et est irréductible d'après le critère d'Eisenstein). Ainsi il existe des éléments irréductibles de tout degré.

Théorème 24. L'ensemble des nombres algébriques est un sous-corps de $\mathbb{C}$.

Démonstration. Tout d'abord, $\mathbb{Q}$ est inclus dans l'ensemble des nombres algébriques puisque si q est un rationnel, $X - q \in \mathbb{Q}[X]$ est un polynôme annulateur (non nul) de q, et q est donc algébrique. En particulier, 1 est algébrique. Soient maintenant $x, y \in \mathbb{C}$ des nombres algébriques avec y non nul. On veut montrer que $x - y, xy$ et $\frac{1}{y}$ sont algébriques. Tous ces nombres sont dans l'extension $\mathbb{Q}(x,y) =$

$\mathbb{Q}(x)(y)$ de $\mathbb{Q}$. De plus, d'après la formule de multiplicativité des degrés, comme $\mathbb{Q} \subset \mathbb{Q}(x) \subset \mathbb{Q}(x,y)$, on a :

$$[\mathbb{Q}(x,y) : \mathbb{Q}] = [\mathbb{Q}(x)(y) : \mathbb{Q}(x)] \cdot [\mathbb{Q}(x) : \mathbb{Q}]. \tag{1}$$

Comme x est algébrique (sur $\mathbb{Q}$), $[\mathbb{Q}(x) : \mathbb{Q}] < \infty$. De plus, y est algébrique sur $\mathbb{Q}$ et donc sur $\mathbb{Q}(x)$ (son polynôme minimal sur $\mathbb{Q}$ est en particulier un polynôme annulateur sur $\mathbb{Q}(x)$). Ainsi, $[\mathbb{Q}(x)(y) : \mathbb{Q}(x)] < \infty$ d'après le corollaire 21. Ces deux résultats de finitude impliquent, au vu de (1), que l'extension $\mathbb{Q}(x,y)$ de $\mathbb{Q}$ est finie.

Si $\alpha \in \mathbb{Q}(x,y)$, $\mathbb{Q}(\alpha)$ est inclus dans $\mathbb{Q}(x,y)$ et c'est donc un sous-espace vectoriel d'un $\mathbb{Q}$-espace vectoriel de dimension finie. Ainsi $\mathbb{Q}(\alpha)$ est de dimension finie sur $\mathbb{Q}$ et d'après le corollaire 21, α est algébrique sur $\mathbb{Q}$. En particulier, $x - y, xy, \frac{1}{y}$ sont algébriques sur $\mathbb{Q}$ et l'ensemble des nombres algébriques est un corps. □

Ce corps est très particulier comme le montre le théorème suivant.

Théorème 25. Le corps des nombres algébriques est la clôture algébrique de $\mathbb{Q}$. En particulier, il est algébriquement clos.

Démonstration. On a montré dans le théorème précédent que l'ensemble des nombres algébriques, qu'on note pour l'instant A, est un sous-corps de $\mathbb{C}$ qui contient $\mathbb{Q}$. Par définition, tous ses éléments sont algébriques sur $\mathbb{Q}$. Pour montrer que c'est la clôture algébrique de $\mathbb{Q}$, il reste donc à vérifier que c'est un corps algébriquement clos.

Soit alors $P \in A[X]$. Montrons que P admet une racine dans A. Comme $\mathbb{C}$ est algébriquement clos, il existe α une racine complexe de P. Montrons que $\alpha \in A$. On écrit

$$P = \sum_{i=0}^{d} a_i X^i$$

avec $a_0, \dots, a_d \in A$. On va s'intéresser à l'extension $\mathbb{Q}(a_0, \dots, a_d)$ de $\mathbb{Q}$. Celle-ci finie. En effet, on a vu dans la preuve précédente que l'extension de $\mathbb{Q}$ engendrée par deux éléments algébriques est finie et on montre ensuite par récurrence que l'extension de $\mathbb{Q}$ engendrée par un nombre fini d'éléments algébriques est finie. P étant un polynôme annulateur de α à coefficients dans $\mathbb{Q}(a_0, \dots, a_d)$, α est algébrique sur $\mathbb{Q}(a_0, \dots, a_d)$. D'après le corollaire 21, $[\mathbb{Q}(a_0, \dots, a_d)(\alpha) : \mathbb{Q}(a_0, \dots, a_d)] < \infty$. Par mutiplicativité des degrés,

$$[\mathbb{Q}(a_0, \dots, a_d, \alpha) : \mathbb{Q}] = [\mathbb{Q}(a_0, \dots, a_d)(\alpha) : \mathbb{Q}(a_0, \dots, a_d)] \cdot [\mathbb{Q}(a_0, \dots, a_d) : \mathbb{Q}]$$

et comme on vient de montrer que les deux termes de droites sont finis, celui de gauche l'est également. Enfin, $\mathbb{Q}(\alpha) \subset \mathbb{Q}(a_0, \dots, a_d, \alpha)$ donc $[\mathbb{Q}(\alpha) : \mathbb{Q}] < \infty$. Toujours d'après le corollaire 21, α est algébrique sur $\mathbb{Q}$, *i.e.* $\alpha \in A$. C'est ce qu'on voulait montrer. □

Comme on note généralement $\overline{\mathbb{K}}$ "la" clôture algébrique d'un corps $\mathbb{K}$, on note $\overline{\mathbb{Q}}$ l'ensemble des nombres algébriques.

Proposition 26. L'ensemble des nombres algébriques est dénombrable. Par conséquent, il existe des nombres complexes transcendants.

Cette preuve de l'existence de nombres transcendants par un argument de cardinalité montre qu'il existe une infinité indénombrable de nombres transcendants mais n'en donne aucun. On va en construire des exemples dans la sous-section suivante.

II.2 Approximation diophantienne et nombres de Liouville

Proposition 27. Si $a \in \mathbb{R} \setminus \mathbb{Q}$ est algébrique de degré $n \geq 2$, alors il existe $C > 0$ tel que

$$\forall (p,q) \in \mathbb{Z} \times \mathbb{N}^*, \left| a - \frac{p}{q} \right| \geq \frac{C}{q^n}.$$

Application 28. Soit $b \in \mathbb{N}, b \geq 2$. Le nombre $a = \sum_{n=0}^{+\infty} \frac{1}{b^{n!}}$ est transcendant.

II.3 Entiers algébriques

Définition 29 (Entier algébrique)**.** Un nombre $z \in \mathbb{C}$ est un entier algébrique s'il admet un polynôme annulateur unitaire à coefficients entiers.

Remarque 30. Notons $\mathcal{O}$ l'ensemble des entiers algébriques. On a

$$\mathbb{Z} \subset \mathcal{O} \subset \overline{\mathbb{Q}} \subset \mathbb{C},$$

la première inclusion venant du fait que si a est un entier, il est annulé par $X - a$ qui est unitaire à coefficients entiers.

De plus ces inclusions sont strictes ; le nombre $\sqrt{2}$ est annulé par $X^2 - 2$ donc est un entier algébrique mais n'est pas entier ; $\frac{1}{2}$ est dans $\overline{\mathbb{Q}}$ mais pas dans $\mathcal{O}$ comme on le verra bientôt ; et on a vu précédemment que la dernière inclusion est également stricte.

Proposition 31. Un nombre complexe α est un entier algébrique si et seulement si son polynôme minimal est à coefficients entiers.

Démonstration. Le sens réciproque est évident au vu de la définition d'un entier algébrique, car le polynôme minimal est unitaire. Montrons le sens direct. Soit α un entier algébrique. Il existe alors $P \in \mathbb{Z}[X]$ unitaire tel que $P(\alpha) = 0$. En particulier P est un polynôme annulateur de α dans $\mathbb{Q}[X]$. Ainsi μ_α divise P : il existe $Q \in \mathbb{Q}[X]$ tel que

$$P = Q\mu_\alpha.$$

On va montrer que cela implique que μ_α est à coefficients entiers.

Tout d'abord, en examinant les coefficients dominants, comme P et μ_α sont unitaires, Q est nécessairement unitaire.

Soit $r \in \mathbb{Q}^*$ (resp. $s \in \mathbb{Q}^*$) tel que rQ (resp. $s\mu_\alpha$) soit à coefficients entiers et primitif. On a donc

$$rsP = (rQ)(s\mu_\alpha) \in \mathbb{Z}[X].$$

Le coefficient dominant de rQ, qui est à coefficients entiers, est r (car Q est unitaire), donc r est entier. De même, s est entier et donc rs est entier. On peut alors prendre le contenu dans l'égalité précédente. Celui-ci étant multiplicatif (d'après le lemme de Gauss), on a :

$$rs \cdot c(P) = c(rQ)c(s\mu_\alpha).$$

De plus P est primitif (car unitaire) et rQ et $s\mu_\alpha$ sont primitifs donc on obtient :

$$rs = 1.$$

Ainsi r et s sont des entiers inversibles : $r = s = \pm 1$.

On a donc $s\mu_\alpha = \pm\mu_\alpha \in \mathbb{Z}[X]$ donc $\mu_\alpha \in \mathbb{Z}[X]$.

□

Corollaire 32. Les seuls rationnels qui soient des entiers algébriques sont les nombres entiers.

Démonstration. Le polynôme minimal d'un rationnel q étant $X - q$, ce dernier est à coefficients entiers si et seulement si q est entier. □

Ainsi, on obtient le fait annoncé en remarque 30 : $\frac{1}{2}$ est algébrique car rationnel mais n'est pas un entier algébrique.

Lemme 33. Soit $\alpha \in \mathbb{C}$. Il y a équivalence entre :

(i) α est un entier algébrique

(ii) le groupe additif $\mathbb{Z}[\alpha]$ est de type fini

(iii) il existe un sous-anneau B de $\mathbb{C}$ contenant α qui soit un groupe abélien (additif) de type fini.

Démonstration. Montrons l'équivalence de manière circulaire.

- (i) $\Longrightarrow$ (ii) : Si α est un entier algébrique, il existe $P \in \mathbb{Z}[X]$ unitaire tel que $P(\alpha) = 0$. Notons $d \in \mathbb{N}^*$ son degré. On va montrer que $\mathbb{Z}[\alpha]$ est de type fini et plus précisément engendré par $1, \alpha, \dots, \alpha^{d-1}$. Soit $\beta = Q(\alpha)$ un élément de $\mathbb{Z}[\alpha]$ (avec $Q \in \mathbb{Z}[X]$). Comme P est unitaire, on peut effectuer la division euclidienne de Q par P dans $\mathbb{Z}[X]$: on écrit

$$Q = AP + R \tag{2}$$

avec $A, R \in \mathbb{Z}[X]$ et $\deg R < d$. On peut alors écrire

$$R(X) = \sum_{i=0}^{d-1} a_i X^i$$

avec $a_i \in \mathbb{Z}$. En évaluant la relation de division euclidienne (2) en α, on obtient ainsi :

$$\beta = R(\alpha) = \sum_{i=0}^{d-1} a_i \alpha^i,$$

ce qui montre que β est dans le groupe additif engendré par $1, \dots, \alpha^{d-1}$. Finalement, le groupe additif $\mathbb{Z}[\alpha]$ est engendré par les d éléments $1, \dots, \alpha^{d-1}$.

- (ii) $\Longrightarrow$ (iii) : Il suffit de prendre $B = \mathbb{Z}[\alpha]$.

- (iii) $\Longrightarrow$ (i) : Soit B un sous-anneau de $\mathbb{C}$ contenant α et de type fini, engendré par n éléments $b_1, \dots, b_n$ (en tant que groupe additif). Pour tout $i \in [\![1, n]\!]$, αb_i est dans B puisque B est un anneau contenant α et b_i. Il existe donc $a_{i,1}, \dots, a_{i,n} \in \mathbb{Z}$ tels que

$$\alpha b_i = a_{i,1} b_1 + \cdots + a_{i,n} b_n.$$

On obtient ainsi n équations qui peuvent se réécrire matriciellement. Posons

$$\overrightarrow{b} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \text{ et } A = (a_{i,j})_{1 \leq i,j \leq n}.$$

Dans $\mathbb{C}^n$, on a alors :

$$\alpha \overrightarrow{b} = A \overrightarrow{b},$$

ce qui signifie que $\overrightarrow{b}$ est un vecteur propre de A associé à la valeur propre α. Ainsi α est racine du polynôme caractéristique $\chi_A(X) = \det(XI_n - A)$ de A, qui est un polynôme unitaire (de degré n). De plus, $XI_n - A$ est à coefficients dans $\mathbb{Z}[X]$ (car les $a_{i,j}$ sont des entiers) et comme le déterminant est polynomial, χ_A est dans $\mathbb{Z}[X]$. On a donc un polynôme annulateur de α unitaire à coefficients entiers, donc α est un entier algébrique.

□

Proposition 34. L'ensemble des entiers algébriques $\mathcal{O}$ est un sous-anneau de $\mathbb{C}$.

Il y a ici un fort parallèle avec le théorème 24 et la preuve est similaire. Ici la clé de la démonstration n'est pas la finitude de la dimension d'une certaine extension de corps mais le fait qu'un certain groupe additif soit de type fini. On va en effet se baser sur le lemme 33 ci-dessus, qui est l'analogue du corollaire 21 (pour les deux premiers points).

Démonstration. Tout d'abord, on a vu dans la remarque 30 ci-dessus que $\mathcal{O}$ contient $\mathbb{Z}$. Soient $x, y \in \mathcal{O}$. On veut montrer que $x - y$ et xy sont des entiers algébriques. D'après le lemme 33 précédent, il suffit de montrer que $x - y$ et xy sont dans un sous-anneau de $\mathbb{C}$ qui soit un groupe abélien de type fini. De manière similaire à la preuve du théorème 24, notre candidat sera $\mathbb{Z}[x, y]$.

$\mathbb{Z}[x,y]$ est engendré en tant que groupe additif par les $x^i y^j$ pour $i,j \in \mathbb{N}$. D'après le lemme, comme x est un entier algébrique, il existe $x_1,\dots,x_n \in \mathbb{Z}[x]$ qui engendrent $\mathbb{Z}[x]$ en tant que groupe abélien. De même, il existe $y_1,\dots,y_m$ qui engendrent $\mathbb{Z}[y]$.

Soit $i,j \in \mathbb{N}$. On a $x^i \in \mathbb{Z}[x]$ et $y^j \in \mathbb{Z}[y]$ donc il existe des entiers $a_1,\dots,a_n$ et $b_1,\dots,b_m$ tels que :

$$x^i = \sum_{k=1}^{n} a_k x_k \text{ et } y^j = \sum_{l=1}^{m} b_l y_l.$$

On a alors

$$x^i y^j = \sum_{k,l} a_k b_l x_k y_l.$$

Ainsi pour tout $i,j \in \mathbb{N}$, $x^i y^j$ est dans le groupe additif de type fini engendré par les nm éléments $x_k y_l$ pour $1 \le k \le n$ et $1 \le l \le m$, qu'on note Γ. Les éléments $x^i y^j$ engendrant $\mathbb{Z}[x,y]$ en tant que groupe additif, on a donc $\mathbb{Z}[x,y] \subset \Gamma$. Mais comme $x_k \in \mathbb{Z}[x] \subset \mathbb{Z}[x,y]$ et $y_l \in \mathbb{Z}[y] \subset \mathbb{Z}[x,y]$, on a aussi l'inclusion réciproque.

Ainsi $\mathbb{Z}[x,y] = \Gamma$ est un groupe additif de type fini et un anneau contenant xy et $x-y$. Cela montre que $x-y$ et xy sont des entiers algébriques. □

Définition 35 (Entiers d'un corps de nombres)**.** Si $\mathbb{K} \subset \mathbb{C}$ est un corps de nombres (*i.e.* une extension finie de $\mathbb{Q}$), on définit son anneau d'entiers $\mathcal{O}_\mathbb{K}$ comme

$$\mathcal{O}_\mathbb{K} := \mathbb{K} \cap \mathcal{O}.$$

Avant de nous intéresser à l'anneau des entiers de certains corps de nombres, on introduit un dernier outil qui sera utile dans cette étude.

Si $\mathbb{L}$ est une extension de $\mathbb{Q}$ et $\alpha \in \mathbb{L}$, la multiplication par α

$$m_\alpha : \left| \begin{array}{ccc} \mathbb{L} & \longrightarrow & \mathbb{L} \\ x & \longmapsto & \alpha x \end{array} \right.$$

est un endomorphisme linéaire du $\mathbb{Q}$-espace vectoriel $\mathbb{L}$.

Définition 36 (Norme et trace)**.** Soit $\mathbb{L}$ un corps de nombres. Pour tout $\alpha \in \mathbb{L}$, on définit :

(i) sa norme $\mathrm{N}_\mathbb{L}(\alpha) = \det_\mathbb{Q}(m_\alpha)$

(ii) sa trace $\mathrm{Tr}_\mathbb{L}(\alpha) = \mathrm{Tr}_\mathbb{Q}(m_\alpha)$.

Avec les propriétés basiques du déterminant et de la trace, on a :

Proposition 37. Pour tous $x,y \in \mathbb{L}$,

(i) $\mathrm{N}_\mathbb{L}(x)$ et $\mathrm{Tr}_\mathbb{L}(x)$ sont des éléments de $\mathbb{Q}$

(ii) $\mathrm{N}_\mathbb{L}(xy) = \mathrm{N}_\mathbb{L}(x)\,\mathrm{N}_\mathbb{L}(y)$

(iii) $\mathrm{Tr}_\mathbb{L}(x+y) = \mathrm{Tr}_\mathbb{L}(x) + \mathrm{Tr}_\mathbb{L}(y)$

II.4 Entiers des corps quadratiques

On s'intéresse aux extensions quadratiques de $\mathbb{Q}$ (*i.e.* de degré 2). D'abord, voici leur forme :

Proposition 38. Les extensions quadratiques de $\mathbb{Q}$ sont les $\mathbb{Q}(\sqrt{d})$ où $d \in \mathbb{Z} \setminus \{0,1\}$ est un entier sans facteurs carrés.

Si $d < 0$, $\sqrt{d}$ désigne dans la suite $i\sqrt{-d}$ pour fixer les choses mais on pourrait tout aussi bien choisir $-i\sqrt{-d}$.

Démonstration. • Vérifions que ces extensions sont quadratiques. $X^2 - d \in \mathbb{Q}[X]$ est un polynôme annulateur de $\sqrt{d}$, donc d est de degré au plus 2 sur $\mathbb{Q}$. Il suffit alors de montrer que d est irrationnel pour avoir que son degré est exactement 2. Si $d < 0$, $\sqrt{d}$ est un imaginaire pur donc

le résultat est clair. Supposons alors $d > 0$ et $\sqrt{d}$ rationnel. On écrit $\sqrt{d} = \frac{a}{b}$ avec $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ et $a \wedge b = 1$. On a donc

$$a^2 = db^2.$$

Soit p un facteur premier de d. Comme d divise a^2, c'est aussi un facteur premier de a^2 et donc de a. Ainsi p^2 divise a^2. Avec la relation ci-dessus, on a donc $p^2 | db^2$. Mais comme $a \wedge b = 1$ et que p est un facteur premier de a, p n'est pas un facteur premier de b. Donc p^2 et b sont premiers entre eux. Avec le lemme de Gauss, on obtient $p^2 | d$, ce qui est impossible puisque d est sans facteurs carrés (et différent de 1).

Ainsi $\sqrt{d}$ n'est pas rationnel. Il est donc de degré 2 sur $\mathbb{Q}$ et d'après la proposition 19, $[\mathbb{Q}(\sqrt{d} : \mathbb{Q}] = 2$.

- Soit maintenant $\mathbb{K}$ une extension de $\mathbb{Q}$ de degré 2. On a *a fortiori* $\mathbb{K} \neq \mathbb{Q}$. Soit alors $x \in \mathbb{K} \setminus \mathbb{Q}$. On considère $\mu_x \in \mathbb{Q}[X]$ son polynôme minimal et $r = \deg(\mu_x) = [\mathbb{Q}(x) : \mathbb{Q}]$. Comme $x \notin \mathbb{Q}$, $r \geq 2$. Mais $\mathbb{Q}(x)$ est également un sous-$\mathbb{Q}$-espace vectoriel de $\mathbb{K}$, qui est de dimension 2 sur $\mathbb{Q}$. Nécessairement, $r = 2$. Ainsi on a l'inclusion $\mathbb{Q}(x) \subset \mathbb{K}$ et l'égalité de leurs dimensions (finies) en tant que $\mathbb{Q}$-espaces vectoriels, donc $\mathbb{Q}(x) = \mathbb{K} = \{\alpha + \beta x; (\alpha, \beta) \in \mathbb{Q}^2\}$.

  Comme $r = 2$, on peut écrire $\mu_x = X^2 + bX + c$ avec $b, c \in \mathbb{Q}$. On sait alors que

$$x = \frac{-b \pm \sqrt{\Delta}}{2}$$

  où $\Delta = b^2 - 4c \in \mathbb{Q}$ et $\sqrt{\Delta}$ est l'une des racines carrées de Δ dans $\mathbb{C}$. On a donc $\mathbb{K} = \mathbb{Q}(x) = \mathbb{Q}(\sqrt{\Delta})$. Si $\Delta = \frac{p}{q}$ avec $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$, $\sqrt{\Delta} = \sqrt{\frac{p}{q}} = \frac{1}{q}\sqrt{pq}$ donc $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{pq})$. Ainsi, on peut écrire $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ avec $d \in \mathbb{Z}$. On peut même supposer d sans facteur carré, car si jamais d a des facteurs carrés on peut l'écrire $d = d'\alpha^2$ avec $d' \in \mathbb{Z}$ sans facteurs carrés et $\alpha \in \mathbb{N}^*$, et alors $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\alpha\sqrt{d'}) = \mathbb{Q}(\sqrt{d'})$.

  Ainsi $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ avec $d \in \mathbb{Z}$ sans facteurs carrés.

□

On va maintenant étudier l'anneau des entiers (algébriques) des extensions quadratiques.

Proposition 39. Soit $\mathbb{Q}(\sqrt{d})$ une extension quadratique de $\mathbb{Q}$. On a les propriétés suivantes :

(i) pour tout $x = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, $\mathrm{Tr}_{\mathbb{Q}(\sqrt{d})}(x) = 2a$ et $\mathrm{N}_{\mathbb{Q}(\sqrt{d})}(x) = a^2 - db^2$

(ii) x est un élément de $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ si et seulement si $\mathrm{N}_{\mathbb{Q}(\sqrt{d})}(x)$ et $\mathrm{Tr}_{\mathbb{Q}(\sqrt{d})}(x)$ sont entiers.

Corollaire 40. Soit $d \in \mathbb{Z} \setminus \{0, 1\}$ un entier sans facteurs carrés. Alors

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{si } d \equiv 2, 3 \mod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{si } d \equiv 1 \mod 4 \end{cases}$$

Le cas $d \equiv 0 \mod 4$ ne se produit pas car d est sans facteurs carrés.

On va maintenant se restreindre au cas $d < 0$, *i.e.* s'intéresser aux corps $\mathbb{Q}(i\sqrt{d})$ pour $d > 0$. Ce cas est le moins compliqué à étudier car $\mathcal{O}_{\mathbb{Q}(i\sqrt{d})}$ est un réseau du plan donc on peut le visualiser aisément et utiliser des arguments géométriques. Au contraire, $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ pour $d > 0$ est dense dans $\mathbb{R}$ donc plus compliqué à appréhender.

On note alors $\mathcal{O}_d$ l'anneau des entiers de $\mathbb{Q}(i\sqrt{d})$. Avec ces nouvelles notations, le corollaire précédent se réécrit :

$$\mathcal{O}_d = \begin{cases} \mathbb{Z}[i\sqrt{d}] & \text{si } d \equiv 1, 2 \mod 4 \\ \mathbb{Z}[\frac{1+i\sqrt{d}}{2}] & \text{si } d \equiv 3 \mod 4. \end{cases}$$

On va aussi omettre l'indice $\mathbb{Q}(i\sqrt{d})$ dans la trace et la norme, car il n'y aura pas d'ambiguité, c'est toujours dans ce corps que l'on considérera la trace et la norme.

Remarque 41. Dans ce cas, la norme de $x = a + ib\sqrt{d} \in \mathbb{Q}(i\sqrt{d})$ est $\mathrm{N}(x) = a^2 + db^2$, qui n'est autre que le module de x au carré.

Dans le cas de $\mathbb{Z}[i]$ (*i.e.* cas $d = -1$), on sait que l'anneau est euclidien, et le stathme n'est autre que la norme. On peut alors se demander si cela est vrai pour tous les anneaux d'entiers quadratiques. En fait, c'est loin d'être le cas :

Proposition 42. Soit $d \in \mathbb{N}^*$ sans facteurs carrés.

(i) si $d \equiv 1, 2 \mod 4$, alors $\mathcal{O}_d$ est euclidien pour la norme N si et seulement si $d = 1$ ou $d = 2$

(ii) si $d \equiv 3 \mod 4$, alors $\mathcal{O}_d$ est euclidien pour la norme N si et seulement si $d \in \{3, 7, 11\}$.

Pour le démontrer, on utilise le lemme suivant :

Lemme 43. N est un stathme euclidien sur $\mathcal{O}_d$ si et seulement si :

$$\forall z \in \mathbb{Q}(i\sqrt{d}), \exists \gamma \in \mathcal{O}_d, \mathrm{N}(z - \gamma) < 1.$$

Démonstration.

- Supposons d'abord que pour tout $z \in \mathbb{Q}(i\sqrt{d})$, il existe un entier $\gamma \in \mathcal{O}_d$ tel que $\mathrm{N}(z-\gamma) < 1$. On va montrer que N est un stathme euclidien. D'abord, N est bien définie sur $\mathcal{O}_d$ et à valeurs dans $\mathbb{Z}$ d'après la proposition 39. Elle est même à valeurs dans $\mathbb{N}^*$ puisque c'est le carré du module.

  Soit $z_1, z_2 \in \mathcal{O}_d$ avec $z_2 \neq 0$. Alors $\frac{z_1}{z_2} \in \mathbb{Q}(i\sqrt{d})$. Par hypothèse, il existe $\gamma \in \mathcal{O}_d$ tel que $\mathrm{N}\left(\frac{z_1}{z_2} - \gamma\right) < 1$. On a alors la décomposition dans $\mathcal{O}_d$:

  $$z_1 = \gamma z_2 + (z_1 - \gamma z_2)$$

  avec, en utilisant la multiplicativité de N établie en proposition 37 :

  $$\mathrm{N}(z_1 - \gamma z_2) = \mathrm{N}\left(z_2\left(\frac{z_1}{z_2} - \gamma\right)\right) = \mathrm{N}(z_2)\,\mathrm{N}\left(\frac{z_1}{z_2} - \gamma\right) < \mathrm{N}(z_2).$$

  Cela montre que N est un stathme euclidien sur $\mathcal{O}_d$.

- Réciproquement, supposons que N est un stathme sur $\mathcal{O}_d$. Soit $z \in \mathbb{Q}(i\sqrt{d}) = \{a+ib\sqrt{d}; a, b \in \mathbb{Q}\}$. On peut écrire $z = \frac{k+il\sqrt{d}}{m}$ avec $k, l, m \in \mathbb{Z}$ et m non nul. Quelle que soit la valeur de d modulo 4, on a $\mathbb{Z}[i\sqrt{d}] \subset \mathcal{O}_d$ donc $k + il\sqrt{d} \in \mathcal{O}_d$, et bien sûr m est aussi dans $\mathcal{O}_d$. Comme $m \neq 0$ et que N est un stathme, il existe $\gamma, \delta \in \mathcal{O}_d$ tels que :

  $$\begin{cases} k + il\sqrt{d} = m\gamma + \delta \\ \mathrm{N}(\delta) < \mathrm{N}(m). \end{cases}$$

  On a alors

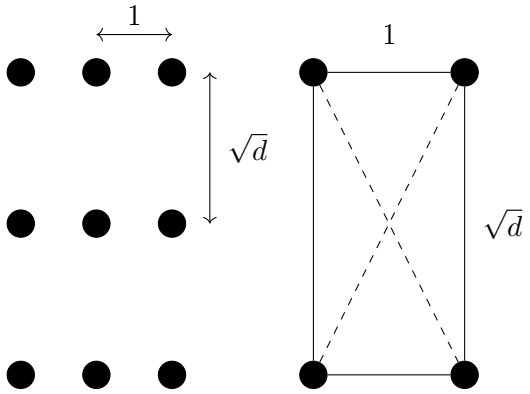
  $$\mathrm{N}(z - \gamma) = \mathrm{N}\left(\frac{k + il\sqrt{d}}{m} - \gamma\right) = \mathrm{N}\left(\frac{\delta}{m}\right) = \frac{\mathrm{N}(\delta)}{\mathrm{N}(m)} < 1,$$

  donc γ est un entier algébrique qui vérifie ce qu'on voulait.

□

On peut maintenant démontrer la proposition :

Démonstration. (i) On considère d'abord le cas $d \equiv 1, 2 \mod 4$. L'anneau des entiers $\mathbb{Z}[i\sqrt{d}]$ est un réseau de $\mathbb{C}$.

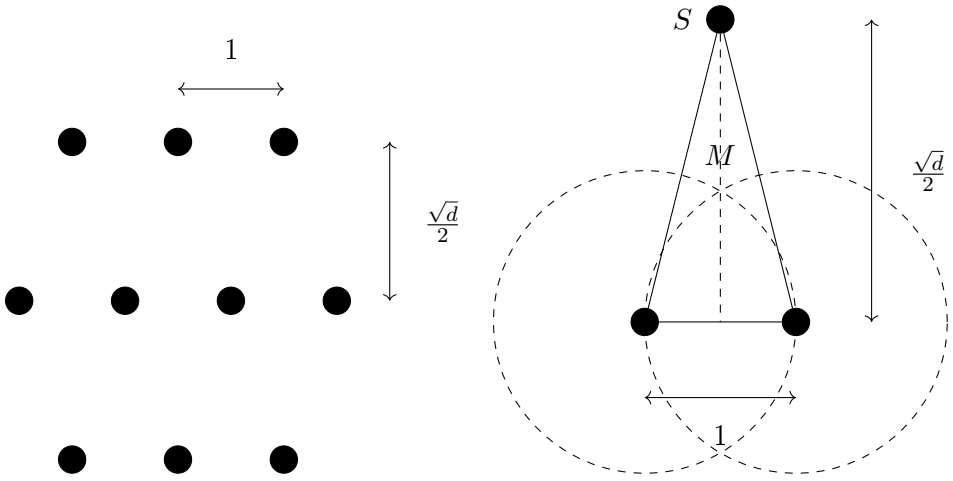


L'affixe du centre d'un rectangle est de la forme $k + \frac{1}{2} + (l + \frac{1}{2})i\sqrt{d}$ donc ce centre est dans $\mathbb{Q}(i\sqrt{d})$. D'après le lemme, N est un stathme si et seulement si tout point de $\mathbb{Q}(i\sqrt{d})$ est à distance strictement inférieure à 1 d'un point de $\mathbb{Z}[i\sqrt{d}]$ et on voit bien que cela se ramène à vérifier que le centre d'une maille est à distance strictement inférieure à 1 de ses sommets (car le centre est le point le plus éloigné de l'ensemble constitué par les sommets). Or le carré de la distance du centre à n'importe quel sommet est

$$\left(\frac{\sqrt{d}}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1+d}{4}.$$

Ainsi N est un stathme si et seulement si $\frac{1+d}{4} < 1$ *i.e.* $d < 3$.

(ii) Dans le cas $d \equiv 3 \mod 4$, $\mathcal{O}_d$ est un réseau dont les mailles sont des losanges.



En utilisant le lemme et la géométrie de $\mathbb{Q}(i\sqrt{d})$ et de $\mathcal{O}_d$, on voit que N est un stathme si et seulement si tout point de $\mathbb{Q}(i\sqrt{d})$ contenu dans un triangle "élémentaire" (dessiné à droite) est à distance strictement inférieure à 1 d'un des sommets.

On s'intéresse au point d'intersection de l'axe de symétrie du triangle isocèle et des deux cercles de rayon 1 et de centre les sommets de la base, qu'on note M. Tout point de $\mathbb{Q}(i\sqrt{d})$ contenu dans le triangle est à distance strictement inférieure à 1 d'un des sommets si et seulement si M est à distance inférieure ou égale à 1 de S. Ainsi N est un stathme si et seulement si $MS \leq 1$. De plus,

$$MS = \frac{\sqrt{d}}{2} - \frac{\sqrt{3}}{2},$$

d'où

$$MS \leq 1 \Leftrightarrow d \leq 7 + 4\sqrt{3}$$

et comme $7 + 4\sqrt{3} \simeq 13,9$, on en déduit que N est un stathme euclidien sur $\mathcal{O}_d$ dans le cas $d \equiv 3 \mod 4$ si et seulement si d est égal à $3, 7$ ou 11. □

Remarque 44. On peut montrer (mais c'est plus long) que ces 5 cas $d \in \{1, 2, 3, 7, 11\}$ sont même les seuls cas dans lesquels $\mathcal{O}_d$ est euclidien. On va tout de même montrer de manière élémentaire que dans la plupart des autres cas, $\mathcal{O}_d$ n'est pas principal.

Proposition 45. Soit $d \in \mathbb{N}^*$ tel que $d \notin \{1, 2, 3, 7, 11\}$.

(i) si $d \equiv 1, 2 \mod 4$, $\mathcal{O}_d$ n'est pas principal,

(ii) si $d \equiv 7 \mod 8$, $\mathcal{O}_d$ n'est pas principal.

Ainsi, il ne resterait que le cas $d \equiv 3 \mod 8$ à traiter pour savoir quels anneaux $\mathcal{O}_d$ sont principaux ou euclidiens. En fait, dans le cas $d \equiv 3 \mod 8$, $\mathcal{O}_d$ est principal (mais non euclidien) dans les cas $d = 19, 43, 67, 163$.

Pour la preuve, on va utiliser un petit lemme :

Lemme 46. Soit $d \geq 5$. Si I est un idéal principal non nul de $\mathcal{O}_d$:

(i) il existe un élément non nul de norme minimale

(ii) tout élément non nul de norme minimale engendre I.

Démonstration. Comme sur $\mathcal{O}_d$ la norme est à valeurs entières, positive et nulle seulement en 0, $\{\mathrm{N}(x); x \in I \setminus \{0\}\}$ est une partie non vide de $\mathbb{N}^*$ donc elle admet un minimum. Cela donne l'existence d'un élément non nul de norme minimale.

Comme I est principal, on écrit $I = (a)$. Soit $x \in I$ un élément non nul de norme minimale. On peut écrire $x = az$ avec $z \in \mathcal{O}_d$ puisque $I = (a)$. Par multiplicativité de la norme,

$$\mathrm{N}(x) = \mathrm{N}(a)\,\mathrm{N}(z)$$

avec $\mathrm{N}(z) \in \mathbb{N}^*$. Ainsi $\mathrm{N}(x) \geq \mathrm{N}(a)$ et par minimalité de la norme de x, $\mathrm{N}(x) = \mathrm{N}(a)$. Cela implique $\mathrm{N}(z) = 1$. Quelle que soit la valeur de d, on peut écrire $z = \frac{a}{2} + i\sqrt{d}\frac{b}{2}$ avec $a, b \in \mathbb{Z}$. Ainsi on obtient $\mathrm{N}(z) = \frac{a^2+db^2}{4} = 1$, ou encore

$$a^2 + db^2 = 4.$$

Comme $d \geq 5$, nécessairement $b = 0$ et donc $a = \pm 2$, d'où $z = \pm 1$, qui est clairement inversible. Ainsi a et x sont associés, donc $I = (x)$. □

Montrons maintenant la proposition :

Démonstration. (i) On considère d'abord le cas $d \equiv 1, 2 \mod 4$ et donc $d \geq 5$. On est dans le cas où $\mathcal{O}_d = \mathbb{Z}[i\sqrt{d}]$. On va chercher un idéal de $\mathcal{O}_d$ non principal. Notre candidat sera :

- $I_1 = (1 + i\sqrt{d}, 1 - i\sqrt{d})$ si $d \equiv 1 \mod 4$,
- $I_2 = (2, i\sqrt{d})$ si $d \equiv 2 \mod 4$.

Pour $k \in \{1, 2\}$, I_k contient 2, qui est de norme 4. Si $z = a + ib\sqrt{d}$ est un élément de $\mathcal{O}_d$ (avec $a, b \in \mathbb{Z}$), $\mathrm{N}(z) = a^2 + b^2 d$ qui est supérieur ou égal à 5 dès que $b \neq 0$. Ainsi un élément non nul de norme minimale de I est réel et vérifie $a^2 \leq 4$. C'est donc ± 1 ou ± 2.

- Si ± 2 est de norme minimale, d'après le lemme $I_k = (2)$. C'est impossible car $i\sqrt{d}$ ou $1+i\sqrt{d}$ est dans I_k mais pas dans $(2) = \{a + ib\sqrt{d}; a, b \in 2\mathbb{Z}\}$.
- Sinon, $1 \in I_k$. On distingue les valeurs de k :
  - Si $k = 1$: $1 \in (1 + i\sqrt{d}, 1 - i\sqrt{d})$. On a donc $a, b, a', b' \in \mathbb{Z}$ tels que

$$1 = (a + ib\sqrt{d})(1 + i\sqrt{d}) + (a' + ib'\sqrt{d})(1 - i\sqrt{d})$$

et en identifiant partie réelle et partie imaginaire, on obtient :

$$\begin{cases} 1 = a - bd + a' + b'd \\ 0 = a + b + b' - a' \end{cases}$$

puis en sommant :

$$1 = 2a - b(d-1) + b'(d+1),$$

ce qui est absurde car le terme de droite est pair (d est impair donc $d-1$ et $d+1$ sont pairs).

– Si $k = 2$: $1 \in (2, i\sqrt{d})$. On a donc $a, b, a', b' \in \mathbb{Z}$ tels que

$$1 = (a + ib\sqrt{d})2 + (a' + ib'\sqrt{d})i\sqrt{d}$$

et en prenant la partie réelle on obtient

$$1 = 2a - db',$$

ce qui est absurde car le terme de droite est pair (d est ici pair).

Ainsi dans les deux cas on a trouvé un idéal non principal.

(ii) Considérons maintenant le cas $d \equiv 7 \mod 8$, avec $d \neq 7$ donc $d \geq 15$. On est maintenant dans le cas où $\mathcal{O}_d = \mathbb{Z}[\omega_d]$ avec $\omega_d = \frac{1+i\sqrt{d}}{2}$. On va montrer que $I = (2, \omega_d)$ n'est pas principal. Si $z = a + b\omega_d$ est un élément de $\mathcal{O}_d$ (avec $a, b \in \mathbb{Z}$) tel que $b \neq 0$, $\mathrm{N}(z) = \left(a + \frac{b}{2}\right)^2 + \frac{b^2 d}{4} \geq \frac{1+d}{4} \geq 4$. Donc comme dans le cas précédent, 2 ou 1 est un élément non nul de norme minimale.

- si $1 \in I$: on a donc $a, b, a', b' \in \mathbb{Z}$ tels que

$$1 = (a + b\omega_d)2 + (a' + b'\omega_d)\omega_d.$$

De plus, on a $\omega_d^2 = \omega_d - \frac{1+d}{4}$, et donc on obtient :

$$1 = 2a - b'\frac{1+d}{4} + \omega_d(2b + b' + a').$$

En identifiant la partie imaginaire puis la partie réelle, on obtient

$$1 = 2a - b'\frac{1+d}{4},$$

ce qui est impossible car le terme de droite est pair (par hypothèse, $\frac{d+1}{4}$ est pair).

- Ainsi, $2 \in I$ est non nul de norme minimale. D'après le lemme, si I est principal, $I = (2)$. C'est impossible car $\omega_d \in I$ mais $\omega_d \notin (2) = \{a + b\omega_d; a, b \in 2\mathbb{Z}\}$.

I est donc un idéal non principal de $\mathcal{O}_d$.

□

III Racines de l'unité

III.1 Groupe des racines de l'unité

Définition 47 (Racine de l'unité, racine primitive de l'unité)**.** $z \in \mathbb{C}$ est une racine de l'unité s'il existe $n \in \mathbb{N}^*$ tel que $z^n = 1$. On note $\mathbb{U}_n = \{z \in \mathbb{C} | z^n = 1\}$ l'ensemble des racines n^e de l'unité. $\mathbb{U}_n$ est alors un groupe multiplicatif. On note également $\mathbb{P}_n$ l'ensemble des racines primitives n^e de l'unité, *i.e.* l'ensemble des générateurs de $\mathbb{U}_n$.

Remarque 48. Les racines de l'unité sont donc des entiers algébriques, puisqu'elles sont annulées par $X^n - 1$ pour un certain entier $n > 0$.

Proposition 49. (i) $\mathbb{U}_n$ est un sous-groupe cyclique de $\mathbb{C}^*$, de cardinal n.

(ii) $\mathbb{U}_n = \{\exp\left(\frac{2ik\pi}{n}\right); 0 \leq k \leq n-1\}$

(iii) Si ω est une racine primitive n^e de l'unité, $\mathbb{U}_n = \{\omega^k; 0 \leq k \leq n-1\}$ et $\mathbb{P}_n = \{\omega^k | k \wedge n = 1\}$.

Remarque 50. $\mathbb{U}_n$ est l'ensemble des sommets d'un polygone régulier à n côtés.

III.2 Polynômes cyclotomiques

Définition 51 (Polynôme cyclotomique)**.** Pour $n \in \mathbb{N}^*$, on pose

$$\Phi_n = \prod_{\zeta \in \mathbb{P}_n} (X - \zeta) \in \mathbb{C}[X].$$

Proposition 52.

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

Démonstration. Cette relation s'obtient en partitionnant $\mathbb{U}_n$ selon l'ordre de ses éléments. En faisant cela, on obtient

$$\mathbb{U}_n = \bigsqcup_{d|n} \mathbb{P}_d$$

et la formule découle du fait que

$$\prod_{\omega \in \mathbb{U}_n} (X - \omega) = X^n - 1$$

et de la définition de Φ_d. □

Cette formule permet de montrer par récurrence la proposition suivante (en utilisant également entre autres le lemme de Gauss).

Proposition 53. $\Phi_n(X) \in \mathbb{Z}[X]$

Théorème 54. Pour tout $n \geq 1$, $\Phi_n(X)$ est irréductible sur $\mathbb{Q}$.

En particulier, $\Phi_n(X)$ est alors le polynôme minimal de tout $\zeta \in \mathbb{P}_n$.

III.3 Extension cyclotomique

Définition 55 (Extension cyclotomique)**.** Si $n \in \mathbb{N}^*$, une extension cyclotomique (ou corps cyclotomique) d'indice n est une extension de $\mathbb{Q}$ de la forme $\mathbb{Q}(\omega)$ où ω est une racine primitive n^e de l'unité.

Remarque 56. L'extension ne dépend pas de la racine primitive n^e choisie, puisque si ω et ω' sont des racines primitives n^e, ω est une puissance de ω' et réciproquement d'après la proposition 49. On a également $\mathbb{Q}(\omega) = \mathbb{Q}(\mathbb{U}_n)$.

Proposition 57. Une extension cyclotomique est de degré $\varphi(n)$.

Proposition 58. Soit $m, n \in \mathbb{N}^*$ tels que $m \wedge n = 1$. Alors

$$\mathbb{Q}(\mathbb{U}_m, \mathbb{U}_n) = \mathbb{Q}(\mathbb{U}_{mn}) \text{ et } \mathbb{Q}(\mathbb{U}_m) \cap \mathbb{Q}(\mathbb{U}_n) = \mathbb{Q}.$$

Démonstration. On va montrer la première égalité, qui est celle qui sert dans la preuve du théorème 59. Soit α (resp. β) une racine primitive m^e (resp. n^e) de l'unité. On a alors $\mathbb{Q}(\mathbb{U}_m, \mathbb{U}_n) = \mathbb{Q}(\alpha, \beta)$. Posons $\omega = \alpha\beta$. Comme α est d'ordre m et β est d'ordre n dans le groupe abélien $(\mathbb{C}^*, \cdot)$, avec $m \wedge n = 1$, on sait que $\omega = \alpha\beta$ est d'ordre mn. Ainsi ω est une racine primitive mn^e de l'unité et $\mathbb{Q}(\mathbb{U}_{mn}) = \mathbb{Q}(\omega)$. On a donc une première inclusion $\mathbb{Q}(\mathbb{U}_{mn}) = \mathbb{Q}(\alpha\beta) \subset \mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\mathbb{U}_m, \mathbb{U}_n)$.

Ecrivons maintenant une relation de Bézout entre m et n : on a $u, v \in \mathbb{Z}$ tels que $mu + nv = 1$. On a alors $\alpha = \alpha^{mu+nv} = (\alpha^n)^v$ (car $\alpha^m = 1$). Mais on a également $\omega^n = \alpha^n\beta^n = \alpha^n$ (car $\beta^n = 1$). Ainsi, $\alpha = \omega^{nv} \in \mathbb{Q}(\omega)$. Par le même raisonnement, on obtient $\beta = \omega^{mu} \in \mathbb{Q}(\omega)$. Cela donne donc l'autre inclusion : comme $\alpha, \beta \in \mathbb{Q}(\omega)$, $\mathbb{Q}(\alpha, \beta) \subset \mathbb{Q}(\omega)$ ou encore $\mathbb{Q}(\mathbb{U}_m, \mathbb{U}_n) \subset \mathbb{Q}(\mathbb{U}_{mn})$. □

Théorème 59 (Kronecker-Weber, version faible)**.** Toute extension quadratique de $\mathbb{Q}$ est contenue dans une extension cyclotomique.

Démonstration. Etape 1 : Extensions quadratiques de $\mathbb{Q}$.

Au vu de la description des extensions quadratiques de $\mathbb{Q}$ faite en proposition 38, on doit montrer que si $d \in \mathbb{Z} \setminus \{0,1\}$ est un entier sans facteurs carrés, alors il existe $m \in \mathbb{N}^*$ tel que $\mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(\mathbb{U}_m)$.

Etape 2 : Cas $d = 2$.

Soit $\omega \in \mathbb{P}_8$ une racine primitive 8^e de l'unité. On a $\omega^4 = -1$ (car $\left(\omega^4\right)^2 = 1$ et $\omega^4 \neq 1$) donc $\omega^2 = -\omega^{-2}$, puis $(\omega + \omega^{-1})^2 = \omega^2 + \omega^{-2} + 2 = 2$. Ainsi $\sqrt{2} = \pm(\omega + \omega^{-1}) \in \mathbb{Q}(\omega)$, d'où $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\omega) = \mathbb{Q}(\mathbb{U}_8)$.

Notons pour la suite que comme $\omega^4 = -1$, on a $\omega^2 = \pm i$ et donc $i \in \mathbb{Q}(\omega)$, donc $\mathbb{Q}(i, \sqrt{2}) \subset \mathbb{Q}(\mathbb{U}_8)$.

Dans ce premier cas, on a "miraculeusement" trouvé une expression de 2 en fonction de racines de l'unité. Il faudrait faire cela pour tous les nombres premiers mais cela semble compliqué de partir à la pêche à la relation. L'étape suivante permet de trouver une relation qui va marcher pour tous les nombres premiers impairs.

Etape 3 : Calcul d'une somme de Gauss.

Rappel 60 (Symbole de Legendre)**.** Soit p un nombre premier impair. Si $a \in \mathbb{F}_p^*$, on définit le symbole de Legendre

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ est un carré dans } \mathbb{F}_p^* \\ -1 & \text{sinon.} \end{cases}$$

On rappelle que $\forall x \in \mathbb{F}_p^*, \left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$, dont on déduit que

$$\left(\frac{\cdot}{p}\right) : \left| \begin{array}{ccc} \mathbb{F}_p^* & \longrightarrow & \{\pm 1\} \\ x & \longmapsto & \left(\frac{x}{p}\right) \end{array} \right.$$

est un morphisme de groupes. De plus, avec le morphisme de groupes $\mathbb{F}_p^* \to \mathbb{F}_p^*, x \mapsto x^2$ et le premier théorème d'isomophisme, on sait qu'il y a $\frac{p-1}{2}$ carré dans $\mathbb{F}_p^*$. En particulier, le morphisme $\left(\frac{\cdot}{p}\right)$ est non constant.

Soit p premier impair et $\omega \in \mathbb{C}$ une racine primitive p^e de l'unité. On pose

$$s = \sum_{x \in \mathbb{F}_p^*} \left(\frac{x}{p}\right) \omega^x \in \mathbb{C}$$

où, si $y \in \mathbb{F}_p^*$, $\omega^y := \omega^k$ pour n'importe quel $k \in y$ (c'est bien défini car $\omega^p = 1$, et c'est compatible avec les sommes et produits). On va calculer s^2 :

$$\begin{aligned} s^2 &= \left(\sum_{x \in \mathbb{F}_p^*} \left(\frac{x}{p}\right) \omega^x\right) \left(\sum_{y \in \mathbb{F}_p^*} \left(\frac{y}{p}\right) \omega^y\right) \\ &= \sum_{x \in \mathbb{F}_p^*} \sum_{y \in \mathbb{F}_p^*} \left(\frac{x}{p}\right) \left(\frac{y}{p}\right) \omega^{x+y} \\ &= \sum_{x \in \mathbb{F}_p^*} \sum_{t \in \mathbb{F}_p^*} \left(\frac{x}{p}\right) \left(\frac{tx}{p}\right) \omega^{(1+t)x} \end{aligned}$$

en réindexant la deuxième somme avec la bijection de $\mathbb{F}_p^* : y \mapsto x^{-1}y = t$. Comme $\left(\frac{\cdot}{p}\right)$ est un morphisme de groupes et qu'on a $\left(\frac{x}{p}\right)^2 = (\pm 1)^2 = 1$ pour tout $x \in \mathbb{F}_p^*$, on obtient :

$$s^2 = \sum_{x \in \mathbb{F}_p^*} \sum_{t \in \mathbb{F}_p^*} \left(\frac{t}{p}\right) \omega^{(1+t)x} = \sum_{t \in \mathbb{F}_p^*} \left(\frac{t}{p}\right) \sum_{x \in \mathbb{F}_p^*} \omega^{(1+t)x}.$$

Fixons $t \in \mathbb{F}_p^*$. On s'intéresse à la somme géométrique $\sum_{x\in\mathbb{F}_p^*} \omega^{(1+t)x} = \sum_{k=1}^{p-1} \left(\omega^{1+t}\right)^k$. Elle vaut $p-1$ si $\omega^{1+t} = 1$, *i.e.* si $t = \overline{p-1} = \overline{-1}$ dans $\mathbb{F}_p$ (car ω est primitive), et $\frac{\omega^{1+t} - \left(\omega^{1+t}\right)^p}{1-\omega^{1+t}} = -1$ sinon (car $\left(\omega^{1+t}\right)^p = (\omega^p)^{1+t} = 1$). Ainsi,

$$s^2 = \left(\frac{-1}{p}\right)(p-1) - \sum_{t\in\mathbb{F}_p^*, t\neq -1} \left(\frac{t}{p}\right) = \left(\frac{-1}{p}\right) p - \sum_{t\in\mathbb{F}_p^*} \left(\frac{t}{p}\right).$$

Montrons enfin que la somme de droite est nulle.

Comme le morphisme $\left(\frac{\cdot}{p}\right)$ est non constant, on peut prendre $t_0 \in \mathbb{F}_p^*$ tel que $\left(\frac{t_0}{p}\right) = -1$. L'application $t \mapsto t_0 t$ étant une bijection sur $\mathbb{F}_p^*$, on a :

$$\sum_{t\in\mathbb{F}_p^*} \left(\frac{t}{p}\right) = \sum_{t\in\mathbb{F}_p^*} \left(\frac{t_0 t}{p}\right) = \left(\frac{t_0}{p}\right) \sum_{t\in\mathbb{F}_p^*} \left(\frac{t}{p}\right) = -\sum_{t\in\mathbb{F}_p^*} \left(\frac{t}{p}\right).$$

Comme on regarde cette somme dans $\mathbb{C}$ de caractéristique nulle, cela entraîne qu'elle est nulle. Ainsi,

$$s^2 = \left(\frac{-1}{p}\right) p. \tag{3}$$

Etape 4 : Cas $d = p$ avec p premier impair.

On va pouvoir utiliser la relation obtenue pour faire la même chose que dans l'étape 2. Si ω est une racine primitive p^e de l'unité, la somme de Gauss $s = \sum_{x\in\mathbb{F}_p^*} \left(\frac{x}{p}\right) \omega^x$ est un élément de $\mathbb{Q}(\omega)$. De plus, d'après la relation (3), $s^2 = \pm p$, donc $\sqrt{p} \in \{s, -s, is, -is\}$. Dans tous les cas, $\sqrt{p} \in \mathbb{Q}(i, s) \subset \mathbb{Q}(i, \omega)$, ou encore

$$\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(i, \mathbb{U}_p).$$

On n'a pas exactement le résultat, mais on peut s'arrêter là : on est prêt.e pour le cas général.

Etape 5 : Cas général

Pour démontrer le cas général, on va utiliser la décomposition en facteurs premiers, les deux premiers cas traités et la proposition 58 pour tout recoller.

Le cas $d = -1$ est évident car $\mathbb{Q}(i)$ est une extension cyclotomique (i est une racine primitive 4^e de l'unité). Soit alors $d \in \mathbb{Z} \setminus \{-1, 0, 1\}$ sans facteurs carrés. On peut écrire

$$d = \pm 2^\alpha p_1 \dots p_r$$

avec $\alpha + r > 0$ (car $d \neq \pm 1$), $p_1, \dots, p_r$ des nombres premiers impairs distincts et $\alpha \in \{0, 1\}$ (car d est sans facteurs carrés). Alors

$$\sqrt{d} = 2^{\frac{\alpha}{2}} \sqrt{p_1} \dots \sqrt{p_r} \text{ ou } \sqrt{d} = i 2^{\frac{\alpha}{2}} \sqrt{p_1} \dots \sqrt{p_r}.$$

Dans tous les cas, on a $\sqrt{d} \in \mathbb{Q}(i, \sqrt{2}, \sqrt{p_1}, \dots, \sqrt{p_r})$ et donc

$$\mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(i, \sqrt{2}, \sqrt{p_1}, \dots, \sqrt{p_r}).$$

Avec les étapes 2 et 4, on a $\mathbb{Q}(i, \sqrt{2}) \subset \mathbb{Q}(\mathbb{U}_8)$ et $\mathbb{Q}(\sqrt{p_j}) \subset \mathbb{Q}(i, \mathbb{U}_{p_j}) \subset \mathbb{Q}(\mathbb{U}_8, \mathbb{U}_{p_j})$. Ainsi,

$$\mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(\mathbb{U}_8, \mathbb{U}_{p_1}, \dots, \mathbb{U}_{p_r}).$$

Or $8, p_1, \dots, p_r$ sont deux à deux premiers entre eux. Donc en itérant le résultat de la proposition 58, on obtient

$$\mathbb{Q}(\mathbb{U}_8, \mathbb{U}_{p_1}, \dots, \mathbb{U}_{p_r}) = \mathbb{Q}(\mathbb{U}_{8p_1 \dots p_r})$$

.

Ainsi, en posant $m = 8p_1 \dots p_r$, on a

$$\mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(\mathbb{U}_m).$$

□

Remarque 61. Ce théorème est un cas particulier du théorème de Kronecker-Weber, qui stipule que toute extension finie abélienne de $\mathbb{Q}$ est contenue dans un corps cyclotomique. Ce théorème permet notamment de classifier les extensions finies abéliennes de $\mathbb{Q}$.

Références

[1] Josette Calais. *Extensions de corps. Théorie de Galois. Niveau M1-M2.* Paris : Ellipses, 2006.

[2] Daniel Duverney. *Théorie des nombres : cours et exercices corrigés.* Paris : Dunod, 1998.

[3] Rémi Goblot. *Algèbre commutative. Cours et exercices résolus.* Paris : Masson, 1996.

[4] Xavier Gourdon. *Les maths en tête. Algèbre et probabilités.* Paris : Ellipses, 3rd edition, 2021.

[5] Ivan Gozard. *Théorie de Galois. Niveau L3 – M1.* Paris : Ellipses, 2nd edition, 2009.

[6] Daniel Perrin. *Cours d'algèbre.* Paris : Ellipses, 1996.