Théorie des nombres II, mars-avril 2021

polycopié de cours

Pierre Charollois

18 février 2021

Table des matières

1 Entiers algébriques, résultant et applications arithmétiques **4**
- 1.1 Polynômes symétriques . . . 4
- 1.2 Formules de Newton . . . 6
- 1.3 Résultant . . . 7
- 1.4 Réciprocité quadratique . . . 9
- 1.5 Discriminant d'un polynôme . . . 12
- 1.6 Entiers algébriques . . . 12

2 L'anneau des entiers d'un corps de nombres **15**
- 2.1 Les corps de nombres et leurs plongements . . . 15
- 2.2 Discriminant associé à une $\mathbb{Q}$-base . . . 17
- 2.3 Trace, norme . . . 17
- 2.4 Structure additive de $\mathcal{O}_K$ . . . 19
- 2.5 Interlude : structure des groupes abéliens de type fini . . . 21
- 2.6 Anneaux d'entiers quadratiques . . . 22
- 2.7 Cas monogène . . . 22
- 2.8 Une stratégie pour construire des $\mathbb{Z}$-bases de $\mathcal{O}_K$ . . . 23
- 2.9 Entiers des corps cyclotomiques . . . 24
- 2.10 $\mathcal{O}_K$ est un anneau de Dedekind . . . 25
- 2.11 Idéaux fractionnaires de K . . . 26
- 2.12 Idéaux premiers de $\mathcal{O}_K$ . . . 27
  - 2.12.1 Norme des idéaux . . . 27
  - 2.12.2 Construire des idéaux premiers . . . 29

3 Un théorème de Dedekind à propos de la ramification **31**

4 La géométrie des nombres en renfort de l'algèbre **32**
- 4.1 Réseaux de $\mathbb{R}^n$ . . . 32
- 4.2 Lemme du corps convexe de Minkowski . . . 33
- 4.3 Quelques premières applications arithmétiques . . . 34
- 4.4 $\mathcal{O}_K$ comme réseau de $\mathbb{R}^r \times \mathbb{C}^s$ . . . 35
- 4.5 Finitude du nombres de classes, théorème de Minkowski . . . 36

5 L'analyse en renfort de l'algèbre **39**
- 5.1 Caractères d'un groupe abélien fini . . . 39
  - 5.1.1 Lemme de prolongement des caractères . . . 40
  - 5.1.2 Formules d'orthogonalité des caractères . . . 40

5.2 Fonctions $L(s,\chi)$ de Dirichlet 41
5.2.1 Produits Eulériens 43
5.2.2 Un pas vers la gauche 43
5.3 Fonction zêta de Dedekind 44
5.3.1 Caractère associé à une extension quadratique 45
5.3.2 Factorisations dans le cas quadratique 46
5.3.3 Autres factorisations 47
5.4 Le théorème de progression arithmétique de Dirichlet 48
5.4.1 Produit de tous les caractères modulo m 50
5.4.2 Le lemme de Landau 51
5.4.3 où $L(1,\chi) \neq 0$ 52
5.5 Autres preuves de $L(1,\chi) \neq 0$ 53
5.5.1 Le cas d'un caractère complexe. 53
5.5.2 Cas d'un caractère réel 54
5.5.3 La formule de Dirichlet pour les corps quadratiques imaginaires . . . 54
5.5.4 Carrés de l'intervalle $[1, \frac{p-1}{2}]$. 55

1 Entiers algébriques, résultant et applications arithmétiques

1.1 Polynômes symétriques

Definition 1. Soit A un anneau intègre. Un polynôme $f(X_1, \dots X_n) \in A[X_1, \dots, X_n]$ est symétrique si, pour toute permutation $\sigma \in S_n$,

$$f(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = f(X_1, \dots, X_n).$$

Exemple

$e_1 = X_1 + \cdots + X_n, e_2 = \sum_{i<j} X_i X_j, \dots, e_n = X_1 \cdots X_n$ sont des polynômes symétriques, aussi appelés les polynômes, ou fonctions, *symétriques élémentaires*. La fonction symétrique élémentaire e_j est homogène de degré j. Toutes les fonctions symétriques élémentaires sont obtenues via les relations coefficients-racines en développant l'expression

$$\prod_{i=1}^{n}(T - X_i) = T^n - e_1 T^{n-1} + e_2 T^{n-2} + \ldots + (-1)^n e_n. \tag{1.1.1}$$

Théorème 2. *Soit $f \in A[X_1, \dots, X_n]$ un polynôme symétrique. Alors il existe un unique polynôme $P \in A[Y_1, \dots, Y_n]$ tel que*

$$f = P(e_1, \dots, e_n).$$

En d'autres termes, f s'écrit de manière unique comme un polynôme en les fonctions symétriques élémentaires.

Démonstration. L'unicité de P ne nous sera pas utile dans la suite ; on ne démontre que l'existence, en soulignant son aspect effectif. Un outil crucial en est *l'ordre lexicographique* sur les monômes, où l'on décide que $X_1^{i_1} \cdots X_n^{i_n} \ll X_1^{j_1} \cdots X_n^{j_n}$ si la première fois que l'on a $i_k \neq j_k$, k variant de 1 à n, alors $i_k < j_k$.

Cet ordre vérifie les propriétés suivantes

i) (transitivité)

si $X_1^{i_1} \cdots X_n^{i_n} \ll X_1^{j_1} \cdots X_n^{j_n}$ et $X_1^{j_1} \cdots X_n^{j_n} \ll X_1^{\ell_1} \cdots X_n^{\ell_n}$, alors $X_1^{i_1} \cdots X_n^{i_n} \ll X_1^{\ell_1} \cdots X_n^{\ell_n}$.

ii) (totalité) : deux mônomes $M = X_1^{i_1} \cdots X_n^{i_n}$ et $\tilde{M} = X_1^{j_1} \cdots X_n^{j_n}$ sont ou égaux, ou bien $M \ll \tilde{M}$, ou bien $\tilde{M} \ll M$, ces trois cas s'excluant mutuellement.

iii) (multiplicativité) Si M, N, L sont trois monômes avec $M \ll N$, alors $LM \ll LN$.

iv) (comparaison aux constantes) on a $1 \ll X_i$ pour tout i.

Cet ordre permet de comparer les degrés des monômes, et de trier les monômes de même degré par ordre décroissant.

Pour $P = \sum a_{i_1,\dots,i_n} X_1^{i_1} \cdots X_n^{i_n} \in R$ on notera $\text{Lm}\,(P) = a_{i_1,\dots,i_n} X_1^{i_1} \cdots X_n^{i_n}$ le monôme dominant de P, i.e. celui qui domine les autres pour l'ordre lexicographique. Par exemple $\text{Lm}\,(3X_1^2 + 5X_1X_2 + X_3^4) = 3X_1^2$.

Lemme 3. *a)* $\textit{Lm}\,(PQ) = \textit{Lm}\,(P)\textit{Lm}\,(Q)$.

b) En particulier, si $0 \leq k_n \leq k_{n-1} \leq \cdots \leq k_1$ *sont des entiers, on a pour les fonctions symétriques élémentaires*

$$\textit{Lm}\,(e_1^{k_1-k_2} e_2^{k_2-k_3} \cdots e_n^{k_n}) = X_1^{k_1} \cdots X_n^{k_n}.$$

Démonstration. (du lemme) On écrit $P = \text{Lm}\,(P) + r_P$ avec $r_P \ll \text{Lm}\,(P)$ et $Q = \text{Lm}\,(Q) + r_Q$ avec $r_Q \ll \text{Lm}\,(Q)$. Dans le produit

$$PQ = \text{Lm}\,(P)\text{Lm}\,(Q) + r_P\text{Lm}\,(Q) + r_Q\text{Lm}\,(P) + r_P r_Q,$$

les trois derniers termes sont dominés par le premier en vertu des axiomes i-ii-iii), d'où l'assertion a). L'assertion b) découle immédiatement du a), en observant que $\text{Lm}\,(e_j) = X_1X_2\cdots X_j$. □

Revenons à la preuve du Th. 2. Soit $M = \text{Lm}\,(f) = aX_1^{m_1} \cdots X_n^{m_n}$ le monôme dominant du polynôme symétrique f. Comme f est symétrique, le monôme $(12).M = aX_2^{m_1}X_1^{m_2} \cdots X_n^{m_n}$ apparaît aussi dans f. Ceci implique que $m_2 \leq m_1$. Le même argument avec les transpositions $(kk+1)$ montre que

$$0 \leq m_n \leq \ldots \leq m_2 \leq m_1.$$

Par suite, le Lemme 3.b) assure que

$$f - ae_1^{m_1-m_2} e_2^{m_2-m_3} \ldots e_n^{m_n},$$

encore symétrique, possède un monôme dominant qui est $\ll M$. On construit ainsi une suite strictement décroissante, pour l'ordre total $\ll$, de monômes dominants. Cette suite est finie, et l'algorithme termine. □

Exemple 4.

$$X^3 + Y^3 = e_1^3 - 3e_2e_1$$

exprime $X^3 + Y^3$ en terme des fonctions symétriques élémentaires $e_1 = X + Y, e_2 = XY$.

Corollaire 5. *Soient* $\theta_1, \ldots, \theta_n$ *des nombres complexes racines d'un polynômes unitaire à coefficients entiers. Si* $P(X_1, \ldots, X_n)$ *est un polynôme symétrique, alors* $P(\theta_1, \ldots, \theta_n) \in \mathbb{Z}$.

Démonstration. En effet, $P = Q(e_1, \ldots, e_n)$ pour Q à coefficients entiers, et la substitution $X_i = \theta_i$ conduit à évaluer Q en les fonctions symétriques élémentaires en les θ_j, qui sont des entiers par hypothèse. □

1.2 Formules de Newton

Definition 6. La collection de polynômes symétriques remarquables

$$N_k = X_1^k + \ldots + X_n^k$$

de $K[X_1, \ldots, X_n]$ s'appelle la famille des *sommes de Newton* N_k.

Ils s'expriment, d'après le Th. 2, comme des polynômes $N_k = Q_k(e_1, \ldots, e_n)$ en les fonctions symétriques élémentaires $e_1, \ldots, e_n$. Il y a des formules explicites universelles qui donnent les polynômes Q_k. Celles-ci permettent donc d'établir de manière directe le Th. 2 dans le cas particulier important des sommes de Newton.

Pour retrouver ces formules, on calcule la série génératrice des sommes de Newton

$$\mathcal{N}(T) := \sum_{k\geq 1} N_k T^k \tag{1.2.1}$$

$$= \sum_{j=1}^{n} \sum_{k\geq 1} X_j^k T^k \tag{1.2.2}$$

$$= \sum_{j=1}^{n} \frac{TX_j}{1-TX_j}. \tag{1.2.3}$$

Il apparaît que c'est une *fraction rationnelle*, qui s'exprime même en terme du polynôme réciproque

$$h(T) = \prod_{j=1}^{n}(1-TX_j) = 1 - e_1 T + e_2 T^2 + \ldots + (-1)^n e_n T^n. \tag{1.2.4}$$

En effet, la dérivée logarithmique de h est la fraction rationnelle

$$\frac{h'(T)}{h(T)} = -\sum_{j=1}^{n} \frac{X_j}{1-TX_j} \tag{1.2.5}$$

$$= -T^{-1}\mathcal{N}(T), \tag{1.2.6}$$

de sorte que la somme de Newton N_k se calcule, au signe près, comme le coefficient de T^{k+1} dans le développement de Laurent de h'/h en $T = 0$. De la formule $-Th'(T) = h(T)\sum_{k\geq 1} N_k T^k$ on conclut en collectant le coefficient de T^k des deux côtés à un système linéaire *triangulaire* :

Corollaire 7.

$$N_k - e_1 N_{k-1} + e_2 N_{k-2} + \ldots + (-1)^{k-1} e_{k-1} N_1 = (-1)^{k+1} k e_k,$$

où le second membre vaut zéro lorsque $k > n$.

En particulier, on retrouve l'identité $X^3 + Y^3 = e_1^3 - 3e_2 e_1$ en choisissant $n = 2, k = 3$.

Exemple 8. (applications, cf TD)

a) (Kronecker). Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire. On suppose que ses racines complexes $P = \prod_{j=1}^{n}(X - \theta_j)$ sont toutes dans le disque unité, $|\theta_j| \leq 1$. Alors chaque θ_j est une racine de l'unité.

b) Soit $P = \prod_{j=1}^{n}(X - x_j)$ un polynôme à coefficients entiers. Alors pour tout $k \geq 1$, $P_k = \prod_{j=1}^{n}(X - x_j^k)$ est aussi à coefficients entiers.

1.3 Résultant

Le résultant est une quantité calculable qui détermine si deux polynômes sont premiers entre eux.

Lemme 9. *Soit K un corps, $P(X) = a_nX^n + \ldots + a_0$ et $Q(X) = b_mX^m + \ldots + b_0$ deux polynômes non nuls de $K[X]$ de degrés respectifs n et m. On définit une application linéaire*

$$\begin{array}{rccccc} f: & K_{m-1}[X] & \times & K_{n-1}[X] & \to & K_{n+m-1}[X] \\ & (U & , & V) & \longmapsto & PU + QV. \end{array}$$

Alors cette application est bijective si et seulement si P et Q sont premiers entre eux (i.e. sans facteurs commun dans $K[X]$).

Démonstration. Si P et Q ont un facteur commun non trivial D, alors D divise tous les éléments de $\mathrm{Im}(f)$. En particulier, le polynôme 1 ne peut pas être atteint, et f n'est pas surjective.

Réciproquement, supposons P et Q sont premiers entre eux. Un élément du noyau de f vérifie $UP = -VQ$. Mais alors P doit diviser V par le lemme de Gauss, ce qui ne peut pas être si $V \neq 0$ pour des raisons de degré. Donc f est injective, et la comparaison des dimensions montre que f est bijective. □

La matrice de f relativement aux bases $\{(X^{m-1}, 0), \ldots (1, 0), (0, X^{n-1}), \ldots, (0, 1)\}$ et $\{X^{n+m-1}, \ldots, X, 1\}$ conduit à poser :

Definition 10. Le résultant de P et Q est le déterminant de de taille $(m + n)$ de la **matrice de Sylvester** de f (ou plutôt de f^t) relativement à ces bases, i.e.

$$\mathrm{Res}(P, Q) := \det \begin{pmatrix} a_n & a_{n-1} & a_{n-2} & \ldots & a_0 & 0 & \ldots & 0 \\ 0 & a_n & a_{n-1} & \ldots & a_1 & a_0 & 0 & \ldots \\ 0 & \ddots & \ddots & \ldots & \ldots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & a_n & \ldots & \ldots & a_1 & a_0 \\ b_m & b_{m-1} & \ldots & b_1 & b_0 & 0 & \ldots & 0 \\ 0 & b_m & b_{m-1} & \ldots & b_1 & b_0 & 0 & \ldots \\ 0 & \ddots & \ddots & \ldots & \ldots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & b_m & \ldots & \ldots & b_1 & b_0 \end{pmatrix} \tag{1.3.1}$$

Proposition 11. *1. Res(P, Q) est un élement de K. Mieux : si P et Q sont à coefficients dans un anneau intègre A, (K = Frac (A)), alors Res$(P, Q) \in A$. Les cas les plus notables sont les anneaux $A = \mathbb{Z}$ et $A = K[Y]$.*

2. *a) Res*$(P,Q) \neq 0$ *ssi* $(P,Q) = 1$ *dans* $K[X]$.
   b) Res$(P,Q) = 0$ *ssi* P *et* Q *ont une racine commune dans une extension de degré fini de* K.
3. $$\textit{Res}(P,Q) = (-1)^{nm}\textit{Res}(Q,P). \tag{1.3.2}$$
4. *Soit* $E = K[X]/P$, *et* $m_Q : E \to E$ *la multiplication par* Q *comme endomorphisme du* K*-ev de dimension finie* E. *Alors*
$$\textit{Res}(P,Q) = a_n^m \ \det(m_Q).$$

Corollaires : *i) Si* $P = a_n(X-\alpha_1)\dots(X-\alpha_n)$ *est scindé,*
$$\textit{Res}(P,Q) = a_n^m \prod_{j=1}^{n} Q(\alpha_j). \tag{1.3.3}$$

ii) Si P *et* Q *sont scindés dans* K, *de racines respectives* $(\alpha_j)_1^n$ *et* $(\beta_k)_1^m$, *alors*
$$\textit{Res}(P,Q) = a_n^m b_m^n \prod_{j=1}^{n}\prod_{k=1}^{m}(\alpha_j - \beta_k).$$

Démonstration. 1) est une conséquence de la formule pour le déterminant
$$\det((a_{ij})) = \sum_{\sigma\in S_n} \epsilon(\sigma) a_{\sigma(1)1}\dots a_{\sigma(n)n}.$$

2) résulte directement du lemme ci-dessus.

3) Pour prouver la formule de réciprocité du résultant, il suffit de prendre la 1ère ligne du déterminant et de la descendre des m premières lignes. On fait cela n fois, cela change le signe par un $(-1)^{nm}$.

4) On écrit pour $0 \leq i < n$: $X^iQ = SP + R_i$ la division de X^iQ par P, ce qui définit une suite R_i avec $\deg(R_i) < \deg(P) = n$. La matrice B de m_Q est exactement la matrice des polynômes colonnes R_i dans la base $(1,\dots X^{n-1})$. Par ailleurs, la (transposée) de la matrice de Sylvester est composée de $n+m$ colonnes, qui sont, exprimés dans la base anticanonique de $K_{n+m-1}[X]$, les vecteurs
$$(X^{m-1}P,\dots,XP,P,X^{n-1}Q,\dots,XQ,Q).$$

Par multilinéarité du déterminant, et puisque l'on peut soustraire aux n dernières colonnes une combinaison linéaire des m premières, on obtient exprimés dans cette même base le déterminant des vecteurs
$$(X^{m-1}P,\dots,XP,P,R_{n-1},\dots,R_1,R_0).$$

Mais cette matrice est triangulaire inférieure par blocs,
$$\text{Res}(P,Q) = \det\begin{pmatrix} A & 0 \\ C & B \end{pmatrix} \tag{1.3.4}$$

avec $B = Mat_{\text{can}}(m_Q)$ de taille $n \times n$ (*Noter que, si B dépend du choix de la base,* $\det(B) = \det(m_Q)$ *ne dépend pas de la base choisie pour E)* et A triangulaire inférieure comportant seulement des a_n sur la diagonale. La formule 4) s'ensuit.

Afin d'établir le premier corollaire, on utilise les matrices $m_{Q_1 Q_2} = m_{Q_1} m_{Q_2}$ pour montrer la multiplicativité du résultant par rapport à Q, puis par rapport à P grâce à la réciprocité. On se ramène ainsi au cas où $P = X - a$, auquel cas $\dim(E) = 1$ et $R_0 = Q(a)$. La matrice en (1.3.4) est triangulaire inférieure, avec n 1 consécutifs sur la diagonale et $Q(a)$ en bas à droite, et le 1er corollaire s'ensuit. Pour le second corollaire, il suffit d'insérer la forme scindée du polynôme Q. □

1.4 Réciprocité quadratique

On rappelle que, si $p > 2$ est un nombre premier, le symbole d'Euler de la classe x modulo p, clairement multiplicatif en x, est donné par

$$\left(\frac{x}{p}\right) := x^{\frac{p-1}{2}} \mod p. \tag{1.4.1}$$

Comme il y a au plus 2 racines à l'équation $y^2 = 1$, on en déduit que l'image de l'application $y \in \mathbb{F}_p^* \mapsto y^2 \in \mathbb{F}_p^*$ coïncide avec les $x \neq 0$ tels que $\left(\frac{x}{p}\right) = 1$. Par suite, $x^{\frac{p-1}{2}} = 0, 1, -1$ selon que x est divisible par p, ou bien un carré non nul mod p, ou bien x non carré. Le symbole d'Euler définit précédemment caractérise les carrés modulo p, on l'appelle aussi symbole de Legendre de x modulo p.

Noter que l'on a les formules

$$\left(\frac{1}{p}\right) = 1, \quad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \quad \text{et} \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}. \tag{1.4.2}$$

Les deux premières sont faciles. La formule complémentaire se trouve dans [Ser],3.2.

"deux applications typiques : "
1) Résoudre une équation quadratique $\mod p$:

$$X^2 + 3X + 3 \mod 17 \text{ a-t-elle une solution ? deux ? zéro ?}$$

2) Est-ce que l'idéal principal engendré $p = (13)$ reste premier dans l'anneau $\mathbb{Z}[i]$? dans $\mathbb{Z}[\sqrt{127}]$?

Pour calculer efficacement le symbole de Legendre (et pour bien d'autres raisons profondes), il est bon de connaître la loi réciprocité quadratique. Elle permet d'établir un lien entre le fait que p est un carré mod q et q est un carré mod p. Aucune démonstration n'est considérée comme facile.

Théorème 12. *Si p et q sont des nombres premiers impairs distincts, alors*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})}. \tag{1.4.3}$$

Démonstration. Au vu de la loi de réciprocité du résultant, où P et Q jouent des rôles symétriques, on dispose (et c'est notable) d'une *stratégie* claire pour établir la loi de réciprocité quadratique de Gauss : il suffit de trouver une collection de polynômes $\Psi_p \in \mathbb{Z}[X]$, de degré $\frac{p-1}{2}$, tels que $\mathrm{Res}(\Psi_p, \Psi_q) = \left(\frac{q}{p}\right)$.

Le polynôme Ψ_p n'est pas exactement le polynôme cyclotomique $\Phi_p := X^{p-1} + \ldots + 1$, mais presque : on écrit

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{\frac{p-1}{2}} L_p(X). \tag{1.4.4}$$

La fraction rationnelle $L_p(X)$ est invariante quand on change X en $1/X$. En posant récursivement $P_{d+1}(Y) = YP_d(Y) - P_{d-1}(Y), P_0 = 1, P_1 = Y$, on définit une suite de polynômes unitaires $P_d \in \mathbb{Z}[X]$ de degré d qui satisfont $X^d + X^{-d} = P_d(X + 1/X)$. (il suffit de remarquer que

$$X^{d+1} + X^{-(d+1)} = (X + 1/X)(X^d + X^{-d}) - (X^{d-1} + X^{-(d-1)})$$

et procéder par récurrence sur d). On pose finalement

$$\Psi_p := \sum_{j=0}^{\frac{p-1}{2}} P_j,$$

de sorte que

$$L_p(X) = \Psi_p(X + 1/X).$$

Le polynôme Ψ_p possède le bon degré $\frac{p-1}{2}$, il est unitaire. Il reste à voir que

$$\mathrm{Res}(\Psi_p, \Psi_q) = \left(\frac{q}{p}\right). \tag{1.4.5}$$

Commençons par montrer que le membre de gauche de (1.4.5), un entier d'après la Prop. 11.1, est dans $\{\pm 1\}$. Procédant par l'absurde, sinon il existe un nombre premier ℓ tel que

$$\mathrm{Res}(\Psi_p, \Psi_q) = 0 \mod \ell.$$

Mais, d'après la preuve de la Prop. 11.1, cette dernière quantité n'est autre que $\mathrm{Res}(\overline{\Psi_p}^{\ell}, \overline{\Psi_q}^{\ell})$. Cela signifie que $\overline{\Psi_p}^{\ell}$ et $\overline{\Psi_q}^{\ell}$ ont un facteur commun non trivial dans $\mathbb{F}_\ell[X]$, ou encore une racine commune α dans une extension finie $\mathbb{F}_{\ell^k}$ de $\mathbb{F}_\ell$. On souhaite en déduire une racine commune de la réduction mod ℓ des polynômes cyclotomiques Φ_p, Φ_q correspondants.

Pour cela, il suffit de prendre une extension (quadratique au maximum) de $\mathbb{F}_\ell$ contenant une solution de $z + \frac{1}{z} = \alpha$. Alors $z \neq 0$ et

$$0 = \Psi_p(\alpha) = \Psi_p(z + 1/z) = z^{-\frac{p-1}{2}} \Phi_p(z).$$

En traitant de même Φ_q, z est racine commune de ces deux polynômes.

Cas 1 : $z \neq 1$: Alors $0 = \frac{z^p-1}{z-1} = \frac{z^q-1}{z-1}$, donc $z^p = z^q = 1$. Une relation de Bezout donne $z = 1$, contradiction.

Cas 2 : $z = 1$. Alors $0 = \Phi_p(z) = 1 + \ldots + 1 = p$, donc $p = \ell = q$, contradiction.

Ainsi

$$\mathrm{Res}(\Psi_p, \Psi_q) = \pm 1.$$

Calculons finalement cette quantité **mod** p (ce qui ne perd pas d'information sur ce nombre), tout en faisant apparaitre une formule simple pour $\Psi_p \mod p$. : (1.4.4) devient modulo p

$$\begin{aligned}
\Phi_p(X) \mod p &= (X-1)^{p-1} && (1.4.6)\\
&= X^{\frac{p-1}{2}} X^{\frac{p-1}{2}} \left((1-1/X)^2\right)^{\frac{p-1}{2}} && (1.4.7)\\
&= X^{\frac{p-1}{2}} \left(X - 2 + 1/X\right)^{\frac{p-1}{2}} && (1.4.8)
\end{aligned}$$

où la dernière ligne s'obtient en développement le carré à l'intérieur des parenthèses. Il s'ensuit par identification que

$$\Psi_p(Y) = (Y-2)^{\frac{p-1}{2}} \mod p,$$

ce qui explicite ses racines sur $\mathbb{F}_p$. Le corollaire de la Prop.11 donne alors

$$\mathrm{Res}(\Psi_p, \Psi_q) = \prod_{j=1}^{\frac{p-1}{2}} \Psi_q(2) = \Psi_q(2)^{\frac{p-1}{2}} \mod p.$$

On conclut en notant que cette dernière expression est le symbole de Legendre $(\frac{q}{p})$ puisque

$$\begin{aligned}
\Psi_q(2)^{\frac{p-1}{2}} \mod p = \Psi_q(1+1)^{\frac{p-1}{2}} \mod p &= \Phi_q(1)^{\frac{p-1}{2}} \mod p\\
= (1 + \ldots + 1)^{\frac{p-1}{2}} \mod p&\\
= q^{\frac{p-1}{2}} \mod p.&
\end{aligned}$$

□

Cerise sur le gâteau, nous retrouvons une formule impressionnante obtenue par Eisenstein [1] à la base de sa démontration la loi de réciprocité quadratique.

Corollaire 13. *(Formule d'Eisenstein)([Ser], Appendice à la partie 3.)*

$$\left(\frac{q}{p}\right) = \prod_{r=1}^{\frac{q-1}{2}} \prod_{k=1}^{\frac{p-1}{2}} \left[4\sin^2\left(\frac{2\pi r}{q}\right) - 4\sin^2\left(\frac{2\pi k}{p}\right)\right].$$

1. "Application de l'algèbre transcendante à l'Arithmétique", 1845, Journal de Crelle vol. **29** p. 177. En français ! http://www.digizeitschriften.de/dms/toc/?PID=PPN243919689. Cette publication anticipe d'ailleurs le résultant, mis au point par Sylvester quelques années après

Démonstration. On a compris que $\alpha \in \mathbb{C}$ est racine de $\Psi_p \iff \alpha = z + z^{-1} = 2\cos(\frac{2\pi k}{p})$ avec $z = e^{2i\pi k/p}$. Or $\alpha = 2(\cos^2 \frac{\pi k}{p} - \sin^2 \frac{\pi k}{p}) = 2 - 4\sin^2(\frac{\pi k}{p})$. Puisque Ψ_p et Ψ_q sont unitaires, la formule souhaitée s'obtient donc comme l'expression

$$\left(\frac{q}{p}\right) = \text{Res}(\Psi_p, \Psi_q) = \prod_{k,r}(\text{racine de } \Psi_p - \quad \text{racine de } \Psi_q).$$

□

1.5 Discriminant d'un polynôme

Definition 14. Soit $P = a_n X^n + \ldots + a_0 \in \mathbb{C}[X]$ de degré n, de racines $\alpha_i, 1 \leq i \leq n$. Le discriminant de P est

$$\text{Disc}(P) = a_n^{2n-2} \prod_{i<j}(\alpha_i - \alpha_j)^2 \tag{1.5.1}$$

$$= (-1)^{\frac{n(n-1)}{2}} a_n^{-1} \text{Res}(P, P'), \tag{1.5.2}$$

C'est un élément du corps K d'après le Th. 2 ou la Prop. 11. Il est non-nul si et seulement si P est à racines simples. La deuxième identité est une conséquence de la formule $\frac{1}{a_n}P' = \sum_i \prod_{j\neq i}(X - \alpha_j)$ évaluée en α_i.

Exemple 15. Lorsque $P = aX^2 + bX + c$ est de degré 2, son discriminant est $b^2 - 4ac$. Dans le cas cubique, $\text{Disc}(X^3 + pX + q) = -27q^2 - 4p^3$.

Exemple 16. (cf TD) Soit p un nombre premier impair, et $\zeta_p = e^{2i\pi/p}$. Alors le polynôme minimal $\Phi_p = X^{p-1} + \ldots + X + 1$ de ζ_p sur $\mathbb{Q}$ a pour discriminant

$$\text{Disc}(\Phi_p) = (-1)^{\frac{p-1}{2}} p^{p-2}. \tag{1.5.3}$$

Remarque 17. Si P est à coefficients entiers, alors son discriminant est entier d'après le Th. 2, ou la Prop. 11.

1.6 Entiers algébriques

Definition 18. (rappel du cours de TN1) Un nombre complexe $\alpha \in \mathbb{C}$ est un *nombre algébrique* s'il annule un polynôme unitaire à coefficients rationnels ; c'est un *entier algébrique* s'il annule un polynôme unitaire à coefficients entiers. On note $\overline{\mathbb{Z}} \subset \mathbb{C}$ l'ensemble des entiers algébriques.

Par exemple, 5, $\sqrt{2}$, $\sqrt{\sqrt{3}+5}$ et le nombre d'or sont tous des entiers algébriques. Par contre, le nombre $5/3$ n'en est pas un.

Lemme 19. *(critère pour être entier) Un nombre algébrique $x \in \mathbb{C}$ est un entier algébrique si et seulement si son polynôme minimal $\pi_{x,\mathbb{Q}}$ est dans $\mathbb{Z}[X]$. En particulier, $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$.*

Démonstration. Une des implications est claire ; pour l'autre, si $P(x) = 0$ avec P unitaire à coefficients entiers, alors $\pi_{x,\mathbb{Q}}$ divise P dans $\mathbb{Q}[X]$. Le lemme des contenus de Gauss (TdN1) permet de conclure que $\pi_{x,\mathbb{Q}}$ est unitaire à coefficients entiers. Autre preuve : l'équation $\pi_{x,\mathbb{Q}}(x) = 0$ montre que le coefficient constant a_0 de $\pi_{x,\mathbb{Q}}$ est dans $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$. On soustrait a_0 et en divisant par x, il s'ensuit de manière similaire que a_1 est dans $\mathbb{Z}$. etc... □

Proposition 20. *$\overline{\mathbb{Z}}$ est un sous-anneau de $\mathbb{C}$.*

Démonstration. Soit $\alpha, \beta \in \overline{\mathbb{Z}}$ annulés respectivement par $P = \prod(X - \alpha_i)$ et $Q = \prod(X - \beta_j)$ unitaires à coefficients entiers. On montre que $R = \prod_{i,j}(X - \alpha_i\beta_j)$ et $S = \prod_{i,j}(X - \alpha_i - \beta_j)$ sont à coefficients entiers grâce au Th. 2, **ou** grâce à la Prop. 11 : $S = Res_Y(Q(Y), P(X - Y)), R = Res_Y(Q(Y), Y^n P(X/Y))$. Noter que la preuve est effective dans les deux cas. □

Proposition 21. *(entier sur entier est entier) Soit $x \in \mathbb{C}$ un nombre complexe qui annule un polynôme unitaire $P \in \overline{\mathbb{Z}}[X]$ dont les coefficients sont des entiers algébriques. Alors x est lui-même un entier algébrique.*

Démonstration. Chaque coefficient $a_j, 0 \leq j \leq d-1$, de P est un entier algébrique qui possède un nombre fini $m_j \geq 1$ de conjugués complexes $\alpha_{i,j}, 1 \leq i \leq m_j$ (le premier de cette liste étant $\alpha_{1,j} = a_j$ lui-même. Les $\alpha_{i,j}$ sont aussi des entiers algébriques. Quitte à rajouter des termes $\alpha_{i,j}$ nuls, on peut d'ailleurs supposer que $m_j = m$ est une constante indépendante de j. L'*observation clef* est que, pour chaque $0 \leq j \leq d$, les fonctions symétriques élémentaires $\sigma_{i,j}, 1 \leq i \leq m$ en les $\alpha_{i,j}, 1 \leq i \leq m$ sont des *entiers de* $\mathbb{Z}$ par hypothèse sur a_j qui annule le polynôme $\prod_{i=1}^{m}(X - \alpha_{ij}) \in \mathbb{Z}[X]$.

Soit $Q(X)$ le produit de tous les polynômes obtenus en substituant à chaque a_j un de ses conjugués. C'est un polynôme unitaire, et il s'annule en x car P est dans cette liste de polynômes. Il nous reste à voir que Q est à coefficients dans $\mathbb{Z}$. Or Q est obtenu par spécialisation en $A_{ij} = \alpha_{i,j}$ du polynôme à coefficients entiers

$$\tilde{Q} = PP_2P_3 \dots P_{m^d} \tag{1.6.1}$$

$$= \prod_{i_0,\dots,i_{d-1}=1}^{m} (X^d + \sum_{j=0}^{d-1} A_{i_j,j}X^j) \in \mathbb{Z}[\{A_{ij}\}_{1\leq i\leq m, 0\leq j\leq d-1}, X]. \tag{1.6.2}$$

Les coefficients de $\tilde{Q}$ sont des fonctions symétriques en les $(A_{i,j})_i$, puisque pour $i_k \neq i'_k$, on écrit en regroupant

$$\tilde{Q} = Q_{i_k}Q_{i'_k} \prod_{i\neq i_k, i'_k} Q_i,$$

qui est invariant sous la transposition (i_k, i'_k). Le théorème fondamental sur les fonctions symétriques appliqué pour chaque j montre que $\tilde{Q}$ est un polynôme en les fonctions symétriques $\Sigma_{ij}(A_{ij}), 1 \leq i \leq m$, de sorte que $\tilde{Q}$ est dans $\mathbb{Z}[\Sigma_{ij}, X]$. Par spécialisation en $A_{ij} = \alpha_{ij}$, chaque $\Sigma_{ij}(A_{ij})$ devient un entier σ_{ij}, de sorte que la spécialisation Q de $\tilde{Q}$ est dans $\mathbb{Z}[X]$. □

Exemple 22. Soit x une racine complexe de $X^2 - \sqrt{5}X - \sqrt{3}$. Montrer que x est un entier algébrique en trouvant un polynôme annulateur de x à coefficients entiers. (En considérant $(X^2 + AX + B)(X^2 + A'X + B)(X^2 + AX + B')(X^2 + A'X + B')$, on trouvera $Q = X^8 - 10X^6 + 19X^4 - 30X^2 + 9$.)

2 L'anneau des entiers d'un corps de nombres

A la suite des travaux de Dedekind, le dernier élève de Gauss, la définition des anneaux d'entiers $\mathcal{O}_K$ d'un corps de nombre K s'est dégagée ; Jouant pour K le rôle que $\mathbb{Z}$ joue pour $\mathbb{Q}$, elle englobe le cas de l'anneau des entiers de Gauss $\mathbb{Z}[i]$, de l'anneau des entiers d'Eisenstein $\mathbb{Z}[j]$, et plus généralement celui des entiers cyclotomiques $\mathbb{Z}[e^{2i\pi/n}]$ étudiés par Kummer.

Nous commençons par développer les outils nécessaires à leur étude, à savoir les notion de trace et de norme. Le résultat principal de cette partie est la structure de $\mathcal{O}_K$ comme groupe additif, tandis que sa structure arithmétique sera étudiée plus tard.

2.1 Les corps de nombres et leurs plongements

Tout sous-corps L de $\mathbb{C}$ contenant un sous-corps K admet en outre une structure de K-espace vectoriel.

Definition 23. Un corps de nombres K est un sous-corps de $\mathbb{C}$ qui est de dimension finie comme $\mathbb{Q}$-espace vectoriel. On note $[K : \mathbb{Q}]$ cette dimension, c'est le *degré* de K sur $\mathbb{Q}$. L'anneau des entiers de K est $\mathcal{O}_K = \overline{\mathbb{Z}} \cap K$.

Les éléments d'un corps de nombres K sont des nombres algébriques, et les éléments de $\mathcal{O}_K$ forment un sous-anneau de K d'après la Prop. 20.

Si $x_1, \dots x_n \in \overline{\mathbb{Q}}$ on note $K(x_1, \dots, x_n)$ le corps de nombres défini récursivement par $K(x_1, \dots, x_n) = K(x_1, \dots, x_{n-1})(x_n)$.

Proposition 24. *(multiplicativité des degrés) Lorsque $K \subset L \subset M$ sont deux extensions successives de corps de nombres, on a*

$$[M : K] = [M : L][L : K].$$

Démonstration. On vérifie qu'à partir d'une base $e_1, \dots e_n$ du K-espace vectoriel L et d'une base $f_1, \dots f_m$ du L-espace vectoriel M, les $(e_i f_j)$ forment une base de M sur K. □

Proposition 25. *(Th. de l'élément primitif) Tout corps de nombres K est de la forme $K = \mathbb{Q}(\theta)$ pour un $\theta \in K$. On peut même choisir $\theta \in \mathcal{O}_K$.*

Démonstration. On renvoie au Th. 3.7.3 du polycopié de TN1 et à sa démonstration élémentaire : elle fournit un $\theta \in K$ élément primitif. Il est annulé par un polynôme unitaire $P(X)$ à coefficients rationnels. Notons N le plus petit commun multiple des dénominateurs des coefficients de P, de sorte que NP est à coefficients entiers. L'égalité $N^n P(\theta) = 0$ implique que $N\theta$ est un entier algébrique. □

Definition 26. Si $k \subset K$ est une extension de corps de nombres, on note $\Sigma(K/k)$ l'ensemble des morphismes de K dans $\mathbb{C}$ qui sont l'identité sur le sous-corps k, i.e. qui sont k-linéaires. Lorsque $k = \mathbb{Q}$, on le note simplement $\Sigma(K)$.

On rappelle que si $x \in \mathbb{C}$ est un nombre algébrique, les conjugués de x sur $\mathbb{Q}$ sont les racines complexes du polynôme minimal $\pi_{x,\mathbb{Q}}$. Comme ce polynôme est irréductible sur $\mathbb{Q}$, il est à racines simples dans $\mathbb{C}[X]$. Plus généralement, si k est un corps de nombres, les *conjugués de* $x \in \overline{\mathbb{Q}}$ *sur* k sont les racines (distinctes) du polynôme minimal $\pi_{x,k} \in k[t]$ de x sur k.

Lemme 27. *Soit $K = \mathbb{Q}(\theta)$ un corps de nombres de degré n sur $\mathbb{Q}$. Alors il y a exactement n plongements distincts $\sigma_i : K \to \mathbb{C}$. Plus précisément, l'application $\sigma \mapsto \sigma(\theta)$ est une bijection entre $\Sigma(K)$ et les n racines distinctes $\theta_i, i = 1, \ldots, n$ du polynôme minimal $\pi_{\theta,\mathbb{Q}}$ de θ sur $\mathbb{Q}$ (les θ_i sont les conjugués de θ sur $\mathbb{Q}$).*

Démonstration. Si θ est un plongement, alors sur chaque élément $\alpha = r(\theta) \in K, r \in \mathbb{Q}[X]$, on a $\sigma(\alpha) = r(\sigma(\theta))$. En particulier, $\sigma(\theta)$ est un des θ_i. Réciproquement, comme $\pi_{\theta,\mathbb{Q}} \in \mathbb{Q}[X]$ est irréductible, c'est le polynôme minimal sur $\mathbb{Q}$ de chacune de ses racines θ_i. Le morphisme naturel d'anneaux $P \mapsto P(\theta_i) \in \mathbb{C}$ donne, par composition, un isomorphisme de corps $\sigma_i : \mathbb{Q}(\theta) \to \mathbb{Q}(\theta_i)$ tel que $\sigma_i(\theta) = \theta_i$. □

Si K est un corps de nombres, la conjugaison complexe $y \mapsto \overline{y} \in \mathbb{C}$ induit une involution de $\Sigma(K)$ car si $\sigma : K \to \mathbb{C}$ est un plongement de K, alors

$$\overline{\sigma} : x \mapsto \overline{\sigma(x)}$$

est aussi un plongement de K dans $\mathbb{C}$.

Definition 28. Lorsque $\overline{\sigma} = \sigma$, on dit que σ est un *plongement réel* de K, dans le cas $\overline{\sigma} \neq \sigma$, on dit que $(\sigma, \overline{\sigma})$ est une paire de *plongements complexes*. La *signature* (r, s) du corps K est le nombre r de ses plongements réels, et celui s de la moitié du nombre de ses plongements complexes.

Les plongements réels de $K = \mathbb{Q}(\theta)$ sont en bijection naturelle avec les conjugués θ_i de θ sur $\mathbb{Q}$ qui sont des nombres réels (Lemme 27). Comme les conjugués complexes viennent par paires, on en déduit aussitôt la relation

$$[K : \mathbb{Q}] = r + 2s.$$

Exemple 29. Le corps quadratique réel $\mathbb{Q}(\sqrt{2})$ a signature $(2, 0)$; Le corps $\mathbb{Q}(i)$ a signature $(0, 1)$. Le corps cyclotomique $\mathbb{Q}(e^{\frac{2i\pi}{n}})$ a signature $(0, \frac{\varphi(n)}{2})$. Quelle est la signature de son sous-corps $\mathbb{Q}(\cos(\frac{2\pi}{n}))$? Donnez des exemples de corps de nombres de signature $(3, 0)$, puis $(2, 1)$. Si K est un corps de nombres de degré 4, quelle peut-être sa signature (r, s) ? Donnez des exemples dans chaque cas.

2.2 Discriminant associé à une $\mathbb{Q}$-base

Definition 30. Soit K un corps de nombres de degré n, et $\sigma_1, \dots, \sigma_n : K \to \mathbb{C}$ la liste de ses plongements. Lorsque $\omega_1, \dots, \omega_n$ forment une $\mathbb{Q}$-base de K, on leur associe le discriminant

$$\Delta_{K/\mathbb{Q}}(\omega_1, \dots, \omega_n) = \det(\sigma_i(\omega_j))^2. \tag{2.2.1}$$

Proposition 31. *1. $\Delta_{K/\mathbb{Q}}(\omega_1, \dots, \omega_n)$ est un élément non-nul de $\mathbb{Q}$. Si les ω_j sont dans $\mathcal{O}_K$, alors $\Delta_{K/\mathbb{Q}}(\omega_1, \dots, \omega_n)$ est dans $\mathbb{Z}$.*

2. Soit $v_1, \dots v_n$ une autre $\mathbb{Q}$-base de K, avec $v_j = \sum_{i=1}^n a_{ij} w_i$, où $a_{ij} \in \mathbb{Q}$. Alors

$$\Delta_{K/\mathbb{Q}}(v_1, \dots, v_n) = \det(A)^2 \Delta_{K/\mathbb{Q}}(\omega_1, \dots, \omega_n), \tag{2.2.2}$$

où $A = (a_{ij}) \in GL_n(\mathbb{Q})$.

3. Soit $\theta \in K$ un élément primitif de $K/\mathbb{Q}$, de polynôme minimal $\pi_{\theta,\mathbb{Q}} = \prod_{i=1}^n (X - \theta_j)$, alors

$$\Delta_{K/\mathbb{Q}}(1, \theta, \dots, \theta^{n-1}) = \prod_{1 \le i < j \le n} (\theta_i - \theta_j)^2 \tag{2.2.3}$$

$$= \mathrm{Disc}(\pi_{\theta,\mathbb{Q}}). \tag{2.2.4}$$

Démonstration. On commence par démontrer 2. Notons V la matrice des colonnes $\sigma_i(v_j)$, et W celle des $\sigma_i(w_j)$. L'hypothèse s'écrit $V = WA$, et on conclut avec le déterminant. Pour démontrer ensuite 3), on observe que $\sigma_i(\theta^k) = \theta_i^k$, de sorte que $\Delta_{K/\mathbb{Q}}(1, \theta, \dots, \theta^{n-1})$ est, par définition, un déterminant de Vandermonde en $\theta_1, \dots, \theta_n$. C'est un résultat classique (**TD**) qu'il est donné par (2.2.3). Il est non-nul, puisque les θ_i sont distincts car $\pi_{\theta,\mathbb{Q}}$ est irréductible. L'égalité (2.2.4) est une autre forme de (1.5.2), et elle établit que $\Delta_{K/\mathbb{Q}}(1, \theta, \dots, \theta^{n-1})$ est un nombre rationnel non-nul. L'assertion 1 est alors une conséquence de 2 et 3, puisque $w_j = \sum_{i=1}^n a_{ij} \theta^{j-1}$: on en déduit que $\Delta_{K/\mathbb{Q}}(\omega_1, \dots, \omega_n)$ est un nombre rationnel. Supposons enfin que les ω_j soient des entiers algébriques ; il en va de même des $\sigma_i(\omega_j)$, et donc de $\Delta_{K/\mathbb{Q}}(\omega_1, \dots, \omega_n)$. Cette dernière quantité est dans $\overline{\mathbb{Z}} \cap \mathbb{Q}$, donc c'est un nombre entier. □

2.3 Trace, norme

Plus généralement, fixons $K = \mathbb{Q}(\theta)$ un corps de nombres de degré n, et $\sigma_1, \dots, \sigma_n$ ses plongements. Pour un éléments $\alpha \in K$, les *K-conjugués de α* sont les nombres complexes $\sigma_i(\alpha)$. Pour $\alpha = \theta$, ce sont aussi les conjugués de θ sur $\mathbb{Q}$. Mais en général (par ex. pour $\alpha = 1$), les K-conjugués de α ne sont pas nécessairement distincts.

On définit le polynôme d'un élément arbitraire $\alpha \in K$ sur K par

$$f_\alpha(t) = \prod_{\sigma \in \Sigma(K)} (t - \sigma_i(\alpha)) \in \mathbb{C}[t].$$

Proposition 32. *a) f_α est dans $\mathbb{Q}[t]$, et f_α est une puissance pure de $\pi_{\alpha,\mathbb{Q}}$.*

b) les K-conjugués de α sont les racines de $\pi_{\alpha,\mathbb{Q}}$, répétées n/m fois, avec $m = \deg \pi_{\alpha,\mathbb{Q}}$.

c) Un élément $\alpha \in K$ est dans $\mathbb{Q}$ si et seulement si tous ses K-conjugués sont égaux.

d) $\mathbb{Q}(\alpha) = \mathbb{Q}(\theta)$ si et seulement si tous les K-conjugués de α sont distincts.

Démonstration. a) $\alpha = r(\theta)$ pour un $r \in \mathbb{Q}[t]$, de sorte que $\sigma_i(\alpha) = r(\sigma_i(\theta)) = r(\theta_i)$. Le polynôme f_α est la spécialisation en $Y_i = \theta_i$ du polynôme $\prod_i (t - r(Y_i)) \in \mathbb{Q}[t]$, qui est symétrique en les θ_i. D'après le Th. fondamental des fonctions symétriques, $f_\alpha(t)$ est donc dans $\mathbb{Q}[t]$ car les fonctions symétriques élémentaires en les θ_i sont des nombres rationnels.

Comme $\pi_{\alpha,\mathbb{Q}}$ est irréductible, $f_\alpha = \pi^s_{\alpha,\mathbb{Q}} h$ dans $\mathbb{Q}[X]$, avec h unitaire et premier à $\pi_{\alpha,\mathbb{Q}}$. Montrons que $h = 1$. En effet, sinon un des $\alpha_i = \sigma_i(\alpha) = r(\theta_i)$ est racine de h. Mais alors $h(r(\theta_i)) = 0$, et $\pi_{\theta,\mathbb{Q}}$ divise donc $h(r(X))$. En particulier, $h(r(\theta)) = 0$, donc $\pi_{\alpha,\mathbb{Q}}$ divise h, contradiction.

b) Noter que $m = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ divise $n = [K : \mathbb{Q}]$. Et b) suit immédiatement de a).

Pour c), un sens est clair. Réciproquement, si tous les $\sigma_i(\alpha)$ sont égaux, alors comme les racines de $\pi_{\alpha,\mathbb{Q}}$ sont simples et que $f_\alpha = \pi^s_{\alpha,\mathbb{Q}}$, il s'ensuit que $\pi_{\alpha,\mathbb{Q}}$ est de degré 1 et α est rationnel.

Pour d), $\mathbb{Q}(\alpha) = \mathbb{Q}(\theta)$ ssi $\deg \pi_{\alpha,\mathbb{Q}} = n$, ce qui arrive ssi les $\sigma_i(\alpha)$ sont distincts. □

Lemme 33. *(prolongement des plongements) i) Soient $K \subset L$ des corps de nombres. L'application de restriction $\Sigma(L) \to \Sigma(K), \sigma \mapsto \sigma_{|_K}$ est surjective, chaque élément de $\Sigma(K)$ ayant exactement $[L : K]$ antécédents.*

ii) (conjugués et plongements). Fixons un $x \in \overline{\mathbb{Q}}$. L'application $\Sigma(K(x)/K) \to \mathbb{C}, \sigma \mapsto \sigma(x)$ est une injection, d'image l'ensemble des conjugués de x sur K.

Démonstration. Grâce à la Prop. 25, on peut supposer que $L = K(x)$. Fixons $\tau \in \Sigma(K)$, et notons $\pi^\tau_{x,K}$ le polynôme (irréductible) obtenu en appliquant τ aux coefficients de $\pi_{x,K}$. L'application $\sigma \in T \mapsto \sigma(x)$, où $T = \{\sigma \in \Sigma(K(x)), \sigma|_K = \tau\}$, est injective (car $\sigma(x)$ et τ déterminent σ sur $K(x)$ tout entier). Son image est l'ensemble des racines complexes y de $\pi^\tau_{x,K}$: en effet, l'application naturelle $K^\tau[X] \to K^\tau(y), X \mapsto y$ a pour noyau $(\pi^\tau_{x,K})$, et induit un plongement $\sigma : K(x) \to K^\tau(y) \subset \mathbb{C}$ convenable. Il y a donc $|T| = [K(x) : K]$ tels plongements σ qui prolongent τ. Ceci démontre le i). Le ii) est le cas où $\tau = Id$. □

Definition 34. Soit L/K une extension finie de corps, et $\alpha \in L$. On appelle *norme* de α, et l'on note $\mathrm{N}_{L/K}(\alpha)$, le déterminant de l'application K-linéaire

$$m_\alpha : L \to L,\ \beta \mapsto \alpha\beta.$$

i.e. $\mathrm{N}_{L/K}(\alpha) = \det\, m_\alpha \in K$. De même, la *trace* de α est $\mathrm{Tr}_{L/K}(\alpha) = \mathrm{tr}\, m_\alpha \in K$. On note $\chi_{\alpha,L/K}(t)$ le polynôme caractéristique (unitaire) de m_α.

En fixant une K-base $\mathcal{B}$ de L, on peut calculer explicitement la matrice de m_α dans la base $\mathcal{B}$ et en déduire la norme et la trace de α.

Exemple 35. $\mathrm{N}_{\mathbb{Q}(i)/\mathbb{Q}}(x + iy) = x^2 + y^2,\ \mathrm{Tr}_{\mathbb{Q}(i)/\mathbb{Q}}(x + iy) = 2x.$

Proposition 36. *Soit $\alpha \in L$. Alors $\chi_{\alpha,L/K} = \pi^{[L:K(x)]}_{\alpha,K}$*

Démonstration. On choisit une base $e_1, \dots e_r$ de L sur $K(\alpha)$, de sorte que $e_1, \dots e_r, \alpha e_1, \dots \alpha e_r, \dots, \alpha^{n-1} e_r$ est une $K-$base de L. La matrice de m_α dans cette base est une matrice par blocs, chaque bloc étant la matrice compagnon de $\pi_{\alpha,K}$.(cf TN1 Prop. 3.8.2). □

On en déduit :

Corollaire 37. *Soit $x \in K$. Alors $x \in \mathcal{O}_K$ si et seulement si $\chi_{x,K/\mathbb{Q}}$ est dans $\mathbb{Z}[X]$. En particulier, sa trace et sa norme sont des entiers.*

Proposition 38. *Soit L/K une extension de corps de nombres, et $x \in L$. Alors*

i) $Tr_{L/K}(x) = \sum_{\sigma \in \Sigma(L/K)} \sigma(x)$.

ii) $N_{L/K}(x) = \prod_{\sigma \in \Sigma(L/K)} \sigma(x)$.

iii) $\chi_{x,L/K}(t) = \prod_{\sigma \in \Sigma(L/K)}(t - \sigma(x))$ *dans* $\mathbb{C}[X]$.

Démonstration. Prouvons iii), qui implique les autres assertions. On sait que $\pi_{x,K}(t) = \prod(t - \sigma(x))$, où le produit porte sur les $\sigma \in \Sigma(K(x)/K)$. D'après la proposition 33, chacun de ces plongements se prolonge de $[L : K(x)]$ façons en un plongement de L/K. La Prop. 36 permet de conclure. □

Proposition 39. *(1ères propriétés de la norme) Soit L/K une extension finie de corps. Alors $N_{L/K} : L \to K$ satisfait*

i) $N_{L/K}(\alpha\beta) = N_{L/K}(\alpha)N_{L/K}(\beta)$ *pour* $\alpha, \beta \in L$.

ii) $N_{L/K}(a) = a^{[L:K]}$ *si* $a \in K$.

iii) Si $K \subset M \subset L$, *alors* $N_{L/K} = N_{M/K} \circ N_{L/M}$.

Démonstration. La première assertion résulte de ce que $m_{\alpha\beta} = m_\alpha \circ m_\beta$. La deuxième assertion résulte de ce que m_a est une homothétie de rapport a. Pour démontrer la dernière assertion, on utilise la Prop. 38. □

Proposition 40. *(1ères propriétés de la trace) Soit L/K une extension finie de corps. Alors $Tr_{L/K} : L \to K$ satisfait*

i) $Tr_{L/K}(\alpha + \beta) = Tr_{L/K}(\alpha) + Tr_{L/K}(\beta)$ *pour* $\alpha, \beta \in L$.

ii) $Tr_{L/K}(a) = [L : K]a$ *si* $a \in K$.

iii) Si $K \subset M \subset L$, *alors* $Tr_{L/K} = Tr_{M/K} \circ Tr_{L/M}$.

Démonstration. similaire à la précédente. □

2.4 Structure additive de $\mathcal{O}_K$.

Théorème 41. *(Dedekind) Soit K un corps de nombre de degré $n = [K : \mathbb{Q}]$, et I un idéal non-nul de l'anneau des entiers $\mathcal{O}_K$. Alors I admet une $\mathbb{Z}$-base à n éléments. En particulier, il existe $\omega_1, \ldots, \omega_n$ tels que*

$$\mathcal{O}_K = \mathbb{Z}\omega_1 + \ldots + \mathbb{Z}\omega_n.$$

Autrement dit, I et $\mathcal{O}_K$ sont isomorphes à $\mathbb{Z}^n$ comme groupes abéliens.

Démonstration. La démonstration originale (due à Dedekind) est très efficace. Commençons par traiter le cas de $\mathcal{O}_K$ lui-même. Quitte à les multiplier par des nombres entiers, on peut trouver une $\mathbb{Q}$-base de K formée d'éléments de $\mathcal{O}_K$. D'après la Prop. 31, toutes les bases de ce type ont un discriminant qui est un entier non-nul. Parmi celles-ci, choisissons $v_1, \ldots, v_n$ telle que $|\Delta(v_1, \ldots, v_n)| > 0$ est minimal, et démontrons que c'est une $\mathbb{Z}$-base de $\mathcal{O}_K$. *Sinon,*

il y a $\omega \in \mathcal{O}_K, \omega = \sum a_j v_i$ avec un des a_j, disons a_1, est un rationnel non-entier. Notons m la partie entière de $a_1 = m + r, 0 < r < 1$. Alors la famille $\omega - mv_1, v_2, \ldots, v_n$ est encore une $\mathbb{Q}$-base de K formée d'éléments de $\mathcal{O}_K$, et la matrice de passage associée est

$$\begin{pmatrix} a_1 - m & 0 & 0 \ldots & 0 & \\ a_2 & 1 & 0 & \ldots & \\ a_3 & 0 & 1 \ldots & 0 & \\ \ldots & \ldots & \ldots & \ldots & \\ a_n & 0 & 0 & \ldots & 1 \end{pmatrix}. \tag{2.4.1}$$

D'après la Prop. 31, son discriminant est donc un entier, égal à $r^2\Delta(v_1, \ldots, v_n)$. Ceci qui contredit la condition de minimalité de $v_1, \ldots, v_n$.

• Dans le cas d'un idéal $I \neq 0$ de $\mathcal{O}_K$, on procède de façon similaire : I possède un élément $x \neq 0$ et donc une $\mathbb{Q}$-base de K : $\{x\omega_1, \ldots, x\omega_n\}$ formée d'éléments de $I \subset \mathcal{O}_K$. L'argument fonctionne encore.

□

Un problème pratique important : déterminer une $\mathbb{Z}$-base explicite de l'anneau des entiers de $\mathcal{O}_K$. Un des outils essentiels sera la notion de discriminant absolu de K.

Definition 42. Soit K un corps de nombres de degré n. Le *discriminant (absolu)* de K est $\Delta_{K/\mathbb{Q}} = \Delta_{K/\mathbb{Q}}(\omega_1, \ldots, \omega_n)$, où $\{\omega_1, \ldots, \omega_n\}$ forme une $\mathbb{Z}$-base de $\mathcal{O}_K$. Plus généralement, lorsque A est un sous-groupe abélien de K qui possède une $\mathbb{Z}$-base à n éléments $v_1, \ldots, v_n$, son discriminant est $\Delta_{K/\mathbb{Q}}(v_1, \ldots, v_n)$.

La définition précédente ne dépend que de A, et pas de l'ordre des plongements ni du choix de la base en vertu de la Prop. 31.

Quelques propriétés supplémentaires du discriminant de $K/\mathbb{Q}$:

Proposition 43. *Soit $K/\mathbb{Q}$ un corps de nombre de degré n et de signature (r, s). Son discriminant $\Delta_K = \Delta_{K/\mathbb{Q}}(\omega_1, \ldots, \omega_n) \in \mathbb{Z}$ satisfait*

a)

$$\operatorname{sign}(\Delta_K) = (-1)^s. \tag{2.4.2}$$

b) (Stickelberger)

$$\Delta_K \equiv 0, 1 \mod 4. \tag{2.4.3}$$

Démonstration. a) notons $M = (\sigma_i(\omega_j))$. La matrice conjuguée $\overline{M}$ s'obtient en échangeant s lignes deux à deux, de sorte que $\det(\overline{M}) = (-1)^s \det M$. Il s'ensuit que $0 < |\det M|^2 = (-1)^s (\det M)^2$, ce qui conclut.

b) On développe $\det(\sigma_i(\omega_j))$ comme

$$\det(\sigma_i(\omega_j))_{i,j} = \sum_{g \in S_n} \epsilon(g) \prod_{i=1}^{n} \sigma_i(\omega_{g(i)}) = P - I,$$

où P (resp I) désigne la somme sur les permutations paires, $\epsilon(g) = 1$ (resp. impaires, $\epsilon(g) = -1$) de S_n. Comme $\Delta_{K/\mathbb{Q}} = (P - I)^2 = (P + I)^2 - 4PI$, il suffit de montrer que $P + I$

et PI sont dans $\mathbb{Z}$ pour obtenir la congruence souhaitée. Soit L le corps de nombres engendré sur $\mathbb{Q}$ par les entiers algébriques $\sigma_i(\omega_j)$. C'est une extension de K. D'après La Prop. 32.c, il nous suffit de montrer que $P+I$ et PI sont invariants sous les plongements $\tau \in \Sigma(L)$. Par composition, tout $\tau \in \Sigma(L)$ engendre une permutation $g_\tau \in S_n$ des n plongements $\sigma_1, \dots, \sigma_n \in \Sigma(K)$ induite par $\sigma \mapsto \tau\circ\sigma : K \to \mathbb{C}$. Si g_τ est paire, on a $\tau(P) = P, \tau(I) = I$, tandis que si g_τ est impaire, on a $\tau(P) = I, \tau(I) = P$. Dans les deux cas, on a $\tau(P+I) = P+I$ et $\tau(PI) = PI$. □

2.5 Interlude : structure des groupes abéliens de type fini

Pour plus de détails de cette section classique autour du "théorème de la base adaptée", on renvoie par exemple au Th. 6.4.3 du cours TN1, ou au polycopié de L3 de PV. Koseleff (dans le moodle), pour une présentation privilégiant l'approche matricielle esquissée ci-dessous.

Proposition 44. *(version allégée du Th. de structure des groupes abéliens de type fini). Soit $L \subset \mathbb{Z}^n$ un sous-groupe engendré par n vecteurs $a_1, \dots, a_n \in \mathbb{Z}^n$. Soit $A \in M_n(\mathbb{Z})$ la matrice formée des vecteurs colonnes $a_1, \dots, a_n$. Alors L est un sous-groupe d'indice fini de $\mathbb{Z}^n$ si et seulement si $\det A \neq 0$, et dans ce cas $|\det A|$ est l'indice $[\mathbb{Z}^n : L] = |\ \mathbb{Z}^n/L\ |$.*

Démonstration. Mettons A sous forme diagonale grâce à des opérations élémentaires sur les lignes et les colonnes. Quitte à faire des échanges de lignes ou de colonnes, on peut supposer que $|a_{1,1}| \neq 0$. Ce sera la taille cette quantité qui va mesurer si l'algorithme que nous décrivons stoppe.

Grâce à des opérations élémentaires de type $L_i \leftarrow L_i - qL_j$ sur les lignes et sur les colonnes, on peut supposer que $a_{1,1}$ divise tous les éléments de sa colonne, i.e. est le pgcd des éléments de sa colonne, ET de sa ligne. (s'il ne divise pas $a_{1,j}$, on peut remplacer $a_{1,1}$ par $\mathrm{pgcd}(a_{1,1}, a_{1,j})$ ce qui a pour effet de diminuer strictement $|a_{1,1}| > 0$). L'itération de cette procédure sur la ligne L_1 et la colonne C_1 doit donc stopper : on peut donc supposer que $a_{1,1}$ divise tous les éléments de sa propre ligne et de sa propre colonne, et mettre des zéros à la place des $a_{1,j}, a_{i,1}, i, j \geq 2$).

Puis on se demande si $a_{1,1}$ divise $a_{i,j}, i, j \geq 2$. Si non, on ajoute la colonne correspondante à C_1, et on reprend l'étape no.1. Ce procédé s'arrête, puisque de nouveau $0 < |a_{1,1}|$ ne peut diminuer strictement qu'un nombre fini de fois. A l'arrêt, le nouveau $a_{1,1}$ est le pgcd des éléments de la nouvelle matrice, et il a des 0 en-dessous et à sa droite. On travaille finalement avec la sous-matrice de taille $(n-1)\times(n-1)$ en itérant, ce qui amène à une matrice diagonale $D = \mathrm{Diag}(d_1, \dots, d_n) \in M_n(\mathbb{Z})$ (on peut même supposer que $d_1 \mid d_2 \cdots \mid d_n$).

Ainsi, on peut trouver des matrices $E_1, E_2 \in GL_n(\mathbb{Z})$, produits de matrices élémentaires, et une matrice diagonale $D = \mathrm{Diag}(d_1, \dots, d_n) \in M_n(\mathbb{Z})$ telles que $A = E_1 D E_2$. Alors le groupe quotient s'identifie à

$$\mathbb{Z}^n/L = \mathbb{Z}^n/E_1 D E_2 \mathbb{Z}^n = E_1\mathbb{Z}^n/E_1 D\mathbb{Z}^n \simeq \mathbb{Z}^n/D\mathbb{Z}^n \simeq \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_n\mathbb{Z}.$$

Ce groupe est fini si et seulement si $d_1 \cdots d_n \neq 0$, et dans ce cas son ordre est $|d_1 \dots d_n| = |\det A|$. □

Remarque 45. On peut démontrer que tout sous-groupe L de $\mathbb{Z}^n$ possède automatiquement $s \leq n$ générateurs, ce qui rend une hypothèse de la proposition superflue. (Th. de classification des groupes abéliens libres de type fini, cf Stewart-Tall chap 1.5 ou le polycopié de L3 déjà cité.).

En combinant (Eq. (2.2.2) et Prop. 44), on obtient le critère suivant, qui peut suffire à déterminer quelques anneaux d'entiers bien choisis :

Lemme 46. *Soit A un sous-groupe abélien de $\mathcal{O}_K$ de $\mathbb{Z}$-bases respectives $A =< v_1, \ldots, v_n >$ et $\mathcal{O}_K =< \omega_1, \ldots, \omega_n >$. Alors l'indice de A dans $\mathcal{O}_K$ est donné par*

$$\Delta_{K/\mathbb{Q}}(v_1, \ldots, v_n) = [\mathcal{O}_K : A]^2 \Delta_{K/\mathbb{Q}}(\omega_1, \ldots, \omega_n). \tag{2.5.1}$$

Exemple 47. L'anneau des entiers de $\mathbb{Q}(\sqrt{5})$ est $\mathbb{Z}[\omega_0]$, où $\omega = \frac{1+\sqrt{5}}{2}$ est le nombre d'or. En effet, le sous-anneau $\mathbb{Z}[\omega_0] \subset \mathcal{O}_K$ possède une $\mathbb{Z}$-base $\{1, \omega_0\}$ de discriminant 5. La formule (2.5.1) montre alors que l'entier $[\mathcal{O}_K : \mathbb{Z}[\omega_0]]^2$ divise 5, donc il vaut 1.

2.6 Anneaux d'entiers quadratiques

Soit $d \in \mathbb{Z}, d \neq 0, 1$ un entier sans facteurs carrés. En guise d'exemple d'anneau d'entiers déterminé explicitement, nous rappelons le cas des entiers de $\mathbb{Q}(\sqrt{d})$, déjà étudié en TN1.

Proposition 48. *L'anneau des entiers de $\mathbb{Q}(\sqrt{d})$ est*

$$\mathbb{Z} + \sqrt{d}\,\mathbb{Z} \text{ si } d = 2, 3 \bmod 4, \ \mathbb{Z} + \left(\frac{1+\sqrt{d}}{2}\right)\mathbb{Z} \text{ si } d = 1 \bmod 4.$$

Dans le premier cas, son discriminant est $\Delta_{K/\mathbb{Q}} = 4d$, dans le second cas $\Delta_{K/\mathbb{Q}} = d$.

Démonstration. Une inclusion est évidente. Pour l'inclusion réciproque, soit $x \in \mathcal{O}_K, x = a + b\sqrt{d}, a, b \in \mathbb{Q}, x' = a - b\sqrt{d} \in \mathcal{O}_K$. Alors xx' et $x + x'$ sont dans $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$, de sorte que $2a$ et $z = a^2 - db^2$ sont dans $\mathbb{Z}$. Par suite, $4z = (2a)^2 - d(2b)^2$ est dans $4\mathbb{Z}$, donc $d(2b)^2$ est un entier. Comme d est sans facteur carré, $2b$ est entier. Cas no1 : $2b$ est un entier pair. Alors $a = x - b\sqrt{d}$ est aussi un entier, et on a gagné.

Cas no2 : $2b$ est un entier impair. La congruence $(2a)^2 = d(2b)^2 \mod 4$ implique que $d = 1 \mod 4$ et $2a$ est un entier impair. Par suite, $x' = x - \frac{1+\sqrt{d}}{2}$ est dans $\mathbb{Z} + \mathbb{Z}\sqrt{d} \subset \mathbb{Z} + \frac{1+\sqrt{d}}{2}\mathbb{Z}$, ce qui conclut.

Le calcul du discriminant s'effectue en considérant la $\mathbb{Z}$-base ainsi obtenue. □

2.7 Cas monogène

On regroupe ici quelques lemmes utiles.

Lemme 49. *Soit $\alpha \in \overline{\mathbb{Z}}$ et $K = \mathbb{Q}(\alpha)$. Alors l'homomorphisme naturel d'anneau $ev_\alpha : \mathbb{Z}[X] \to \mathbb{C}, P \mapsto P(\alpha)$ induit un isomorphisme d'anneau $\mathbb{Z}[X]/(\pi_{\alpha,\mathbb{Q}}) \simeq \mathbb{Z}[\alpha]$. En particulier, $1, \alpha, \ldots, \alpha^{n-1}$ est une $\mathbb{Z}$-base de l'anneau $\mathbb{Z}[\alpha] \subset \mathcal{O}_K$.*

Démonstration. L'image du morphisme d'évaluation est, par définition, l'anneau $\mathbb{Z}[\alpha]$. Le noyau contient l'idéal principal $(\pi_{\alpha,\mathbb{Q}})$. Si $P(\alpha) = 0, P \in \mathbb{Z}[X]$, alors $\pi_{\alpha,\mathbb{Q}}$ divise P dans $\mathbb{Q}[X]$. Le même argument que celui du Lemme 19 utilisant le lemme de Gauss et $\pi_{\alpha,\mathbb{Q}}$ unitaire, montre que $\pi_{\alpha,\mathbb{Q}}$ divise P dans $\mathbb{Z}[X]$. □

Definition 50. La *norme* d'un idéal non-nul I de $\mathcal{O}_K$ est l'indice de I dans $\mathcal{O}_K$:

$$\mathrm{N}(I) =\mid \mathcal{O}_K/I \mid .$$

Cet indice est fini d'après le Th. 41 et la Prop. 44, car I et $\mathcal{O}_K$ possèdent tous les deux une $\mathbb{Z}$-base à n-éléments formés d'éléments de $\mathcal{O}_K$.

Dans le cas où l'idéal I est principal, $I = \alpha\mathcal{O}_K = (\alpha)$, sa norme (comme idéal) est liée à la norme de α (comme élément de K) : $\mathrm{N}((\alpha)) = |\mathrm{N}_{K/\mathbb{Q}}(\alpha) \mid$:

Proposition 51. *Pour $\alpha \in \mathcal{O}_K$ un élément non-nul, on a*

$$\mid \mathcal{O}_K/\alpha\mathcal{O}_K \mid= |\mathrm{N}_{K/\mathbb{Q}}(\alpha) \mid . \tag{2.7.1}$$

Démonstration. On fixe une $\mathbb{Z}$-base $\omega_1, \ldots, \omega_n$ de $\mathcal{O}_K$. Alors $\alpha\omega_1, \ldots, \alpha\omega_n$ est une $\mathbb{Z}$-base de $\alpha\mathcal{O}_K$. écrivons

$$\alpha\omega_j = \sum_{i=1}^{n} p_{ij}\omega_i,$$

de sorte que la matrice de la multiplication par α dans la base $\mathcal{B} = \{\omega_1, \ldots, \omega_n\}$ est donnée par $\mathrm{mat}_{\mathcal{B}}(m_\alpha) = P = p_{ij} \in M_n(\mathbb{Z})$. Son déterminant est, par définition, $\mathrm{N}_{K/\mathbb{Q}}(\alpha)$. En appliquant un plongement arbitraire $\sigma_k : K \to \mathbb{C}$, on voit aussi que $\sigma_k(\alpha\omega_j) = \sum_i a_{ij}\sigma_k(\omega_i)$, de sorte que

$$\sigma_k(\alpha\omega_j) = \sigma_k(\alpha\omega_j)P.$$

En passant aux déterminants, on trouve

$$\mathrm{Disc}(\alpha\mathcal{O}_K) = (\det P)^2 \,\mathrm{Disc}(\mathcal{O}_K),$$

et le Lemme 46 permet de conclure. □

2.8 Une stratégie pour construire des $\mathbb{Z}$-bases de $\mathcal{O}_K$.

L'exemple 47 montre comment on peut tirer profit d'un discriminant sans facteur carré. Nous expliquons maintenant comment on peut procéder lorsque p^2 divise le discriminant de notre candidat $A = \mathbb{Z}v_1 + \ldots + \mathbb{Z}v_n$.

Proposition 52. *Soit $A \subset \mathcal{O}_K$ un sous-groupe additif de $\mathcal{O}_K$ de rang n et de $\mathbb{Z}$-base $v_1, \ldots, v_n$. On suppose que $A \neq \mathcal{O}_K$. Alors il existe un premier p tel que p^2 divise $\Delta_{K/\mathbb{Q}}(v_1, \ldots, v_n)$, et dans $\mathcal{O}_K - A$ un élément de la forme*

$$\frac{1}{p}(\lambda_1 v_1 + \ldots + \lambda_n v_n) \tag{2.8.1}$$

avec $0 \leq \lambda_i \leq p-1, \lambda_j \in \mathbb{Z}$.

Démonstration. On a déjà vu que $\mathcal{O}_K/A$ est un groupe abélien fini (Lemme 49 et Prop. 44). Soit $p \geq 2$ un nombre premier divise son cardinal. D'après la preuve de la Prop. 44), ce quotient contient un sous-groupe cyclique d'ordre divisible par p, donc un élément d'ordre p : il y a donc un élément $u \in \mathcal{O}_K$ d'ordre p dans ce quotient, ie $g = pu$ est dans A. Par suite, u possède un représentant $\mod A$ de la forme voulue. Le fait que p^2 divise Δ_K découle de la formule (2.5.1). □

De ceci on déduit une stratégie pour trouver une $\mathbb{Z}$-base de $\mathcal{O}_K$:
1) on commence par chercher un anneau candidat de la forme A avec une $\mathbb{Z}$-base $(v_1, \dots, v_n)$.
2) on calcule $\Delta_{K/\mathbb{Q}}(v_1, \dots, v_n)$.
3) Pour chaque premier p qui divise $\Delta_{K/\mathbb{Q}}(v_1, \dots, v_n)$, chercher des éléments de la forme (2.8.1) qui soient des entiers.
4) lorsque c'est le cas, agrandir A en rajoutant ces éléments, et recommencer, jusqu'à ce qu'on ne trouve plus d'entiers algébriques.

Exemple 53. (TD) Ex. 1 : L'anneau des entiers de $\mathbb{Q}(\sqrt[3]{5})$ est $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{5}]$.
Ex. 2 : le polynôme minimal de $\theta = \sqrt[3]{175})$ est $X^3 - 5^2 7$, de discriminant $-3^3 5^4 7^2$. On peut montrer que $\mathbb{Z}[\theta]$ est d'indice 5 dans $\mathcal{O}_K = \mathbb{Z}[\theta, \frac{\theta^2}{5}]$, qui est de discriminant $\Delta_K = -3^2 5^2 7^2$.

2.9 Entiers des corps cyclotomiques

On rappelle (**TD**) que, si $n \geq 1$ est un entier et $\zeta = e^{\frac{2i\pi}{n}}$, le n-ième polynôme cyclotomique

$$\Phi_n(X) = \prod_{1 \leq k \leq n, (k,n)=1} (X - \zeta^k)$$

est à coefficients entiers, et il est irréductible dans $\mathbb{Q}[X]$. (Lorsque $n = p^a$ est une puissance d'un nombre premier, une démonstration élémentaire de l'irréductibilité de Φ_{p^a} repose sur le fait que $\Phi_{p^a}(X+1)$ satisfait le critère d'Eisenstein en p).

Théorème 54. *Soit $\zeta = e^{\frac{2i\pi}{n}}$ et $K = \mathbb{Q}(\zeta)$ le corps cyclotomique associé. Alors $\mathcal{O}_K = \mathbb{Z}[\zeta]$.*

Le cas n général est un peu délicat, nous donnons une démonstration dans le cas $n = p$ premier, démonstration qui résulte immédiatement de la proposition suivante, combinée au discriminant calculé en (1.5.3).

Proposition 55. *Soit x un entier algébrique et $K = \mathbb{Q}(x)$. On suppose que son polynôme minimal $\pi_{x,\mathbb{Q}} \in \mathbb{Z}[X]$ satisfait les hypothèses du critère d'Eisenstein en un nombre premier p. Alors $\mathbb{Z}[x]$ est d'indice premier à p dans $\mathcal{O}_K$.*

Démonstration. Par l'absurde : on a déjà vu que $\mathcal{O}_K/\mathbb{Z}[x]$ est un groupe abélien fini (Lemme 49 et Prop. 44). Supposons que le nombre premier p divise son cardinal. D'après la preuve de la Prop. 44, ce quotient contient un sous-groupe cyclique d'ordre divisible par p, donc un élément d'ordre p : il y a donc un élément $z \in \mathcal{O}_K$ d'ordre p dans ce quotient, de sorte que

$$pz = \sum_{j=0}^{n-1} b_j x^j \tag{2.9.1}$$

est dans $p\mathcal{O}_K$, avec $b_j \in \mathbb{Z}$. On va obtenir une contradiction en montrant que p divise chaque b_j dans $\mathbb{Z}$. Par hypothèse sur $\pi_{x,\mathbb{Q}}$, les $x^i, \underline{i \geq n}$, sont dans $p\mathcal{O}_K$, de sorte que, par multiplication par x^{n-1} on trouve

$$b_0 x^{n-1} = pa, a \in \mathcal{O}_K.$$

En prenant la norme et en notant que $N_{K/\mathbb{Q}}(x) = a_0$ est divisible par p mais pas par p^2 par hypothèse, il s'ensuit que p divise b_0. En reprenant l'équation (2.9.1) et la multipliant par $x^{n-2}, x^{n-3}, \ldots, x, 1$, on démontre successivement que les entiers $b_1, \ldots, b_{n-1}$ sont divisibles par p. Contradiction, puisque z n'est pas dans $\mathbb{Z}[x]$. □

Exemple 56. L'anneau des entiers de $K = \mathbb{Q}(x), x = \sqrt[p]{p}$ est $\mathbb{Z}[x]$, en observant que $\mathrm{disc}(x^p - p) = (-1)^{\frac{p(p-1)}{2}} p^{p(p-1)}$, et le polynôme $x^p - p$ vérifie le critère d'Eisenstein en p. D'autres exemples en **TD**.

2.10 $\mathcal{O}_K$ est un anneau de Dedekind

Soit A un anneau intègre. On rappelle qu'un idéal $\mathfrak{p} \neq A$ est *premier* si $\alpha\beta \in \mathfrak{p}$ implique α ou $\beta \in \mathfrak{p}$, autrement dit si $A/\mathfrak{p}$ est un anneau intègre. Un idéal $\mathfrak{m}$ est *maximal* si $A/\mathfrak{m}$ est un corps.

L'anneau A est *noethérien* si tout idéal I de A est de type fini, i.e. s'il existe un nombre fini d'éléments $x_1, \ldots, x_k \in I$ avec $I = x_1 A + \ldots + x_k A$.

Théorème 57. *Soit K un corps de nombres. L'anneau des entiers de K vérifie les propriétés suivantes, qui en font un anneau de Dedekind :*

1. *$\mathcal{O}_K$ est un anneau intègre, son corps des fractions est K.*
2. *$\mathcal{O}_K$ est un anneau noethérien.*
3. *$\mathcal{O}_K$ est intégralement clos : si $\alpha \in K$ vérifie une équation algébrique à coefficients dans $\mathcal{O}_K$, alors α appartient à $\mathcal{O}_K$.*
4. *Tout idéal premier non-nul $\mathfrak{p}$ est maximal.*

Démonstration. 1. est clair. 2. découle du Th. de Dedekind, car une $\mathbb{Z}$-base engendre déjà un idéal I comme groupe abélien ($\mathbb{Z}$-module), donc comme $\mathcal{O}_K$-module. Le point 3. provient de la Prop. 21. Pour établir le point 4., on se donne un idéal premier $\mathfrak{p}$ non-nul. Le quotient $\mathcal{O}_K/\mathfrak{p}$ est un groupe fini (de cardinal $\mathrm{N}(\mathfrak{p})$), et c'est un anneau intègre car $\mathfrak{p}$ est premier. Si z est une classe non-nulle de ce quotient, la multiplication par z est donc injective, et l'anneau étant fini, elle est aussi surjective : ce quotient est donc un corps, et $\mathfrak{p}$ est un idéal maximal. □

Lorsque I et J sont des idéaux d'un anneau intègre A, on note IJ l'idéal de A *engendré* par les éléments de la forme $xy, x \in I, y \in J$. On a évidemment $(a)(b) = (ab)$, et plus généralement IJ est de type fini engendré par les produits $a_i b_j$ si $I = Aa_1 + \ldots + Aa_n$ et $J = Ab_1 + \ldots + Ab_m$. Le produit des idéaux est associatif et commutatif.

Lemme 58. *Soit K un corps de nombres, et I, J deux idéaux propres de $\mathcal{O}_K$. Alors IJ est contenu dans un idéal maximal $\mathfrak{q}$, et si un idéal premier $\mathfrak{p}$ contient IJ, alors $\mathfrak{p}$ contient I ou $\mathfrak{p}$ contient J.*

Démonstration. Le produit IJ n'est pas trivial, donc le quotient $\mathcal{O}_K/IJ$ non plus, et il suffit de prendre l'image réciproque d'un idéal maximal par le morphisme naturel $\mathcal{O}_K \to \mathcal{O}_K/IJ$ pour trouver $\mathfrak{q}$. Pour la 2nde partie, si I n'est pas contenu dans $\mathfrak{q}$, on prend $\beta \in \mathfrak{q} - I$. Tout $y \in J$ vérifie $\beta y \in \mathfrak{q}$, et comme $\mathfrak{q}$ est premier ceci implique que $y \in \mathfrak{q}$. □

L'anneau $\mathcal{O}_K$ n'est pas un anneau factoriel en général. Cependant (d'après le cours TN1, Th. 2.4.1 et 2.4.5), comme $\mathcal{O}_K$ est un anneau de Dedekind :

Théorème 59. *Tout idéal non-nul I de $\mathcal{O}_K$ se factorise, de manière unique à l'ordre près, sous la forme*

$$I = \mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_r^{k_r} \tag{2.10.1}$$

en un produit d'idéaux premiers distincts $\mathfrak{p}_j$ de $\mathcal{O}_K$.

On dit que l'entier k_j est la *valuation en* $\mathfrak{p}_j$ de l'idéal I, et on le note aussi $k_j = v_{\mathfrak{p}_j}(I)$. L'unicité de la décomposition montre que $v_{\mathfrak{p}}(IJ) = v_{\mathfrak{p}}(I) + + v_{\mathfrak{p}}(J)$.

2.11 Idéaux fractionnaires de K.

(courte section de rappel de TN1).

Definition 60. (TN1, 1.3, 1.4) Soit K un corps de nombres de degré n. Un idéal fractionnaire $\mathfrak{a}$ de K est un un sous-groupe additif de K pour lequel il existe $r \in \mathcal{O}_K$ tel que $r\mathfrak{a}$ est un idéal ordinaire de $\mathcal{O}_K$. Un idéal fractionnaire $\mathfrak{a}$ est dit inversible s'il existe idéal fractionnaire $\mathfrak{a}'$ tel que $\mathfrak{a}\mathfrak{a}' = \mathcal{O}_K$.

Par exemple, les idéaux ordinaires sont des idéaux fractionnaires. Un idéal principal non-nul $\alpha\mathcal{O}_K$ est inversible, d'inverse (fractionnaire) $\alpha^{-1}\mathcal{O}_K$.

Puisque l'idéal ordinaire $r\mathfrak{a}$ possède une $\mathbb{Z}$-base à n éléments, il en va de même pour l'idéal fractionnaire $\mathfrak{a}$.

Les idéaux fractionnaires de K sont munis des lois $+, \times$ naturelles qui prolongent les opérations sur les idéaux ordinaires.

Definition 61. Soient $\mathfrak{a}, \mathfrak{b}$ deux idéaux fractionnaires de K. On dit que $\mathfrak{b}$ divise $\mathfrak{a}$, et l'on note $\mathfrak{b} \mid \mathfrak{a}$, s'il existe un idéal *ordinaire* $\mathfrak{c}$ tel que $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$.

D'après le cours TN1 (Th. 2.4.5), l'anneau $\mathcal{O}_K$ étant de Dedekind, **tout idéal fractionnaire non-nul $\mathfrak{a}$ est inversible**. En particulier, les idéaux fractionnaires de K possèdent les propriétés suivantes (TN1 1.4) :

Lemme 62. *Soit $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ des idéaux fractionnaires d'un corps de nombres K avec $\mathfrak{c}$ non-nul.*
i) (effacement) si $\mathfrak{a}\mathfrak{c} = \mathfrak{b}\mathfrak{c}$ alors $\mathfrak{a} = \mathfrak{b}$.
ii) $\mathfrak{c} \mid \mathfrak{b}$ si et seulement si $\mathfrak{b} \subset \mathfrak{c}$.

Démonstration. Il suffit de multiplier par $\mathfrak{c}^{-1}$. Voir aussi TN1, 2.1.3, 2.1.4. □

Corollaire 63. *De manière analogue à la situation "factorielle", pour deux idéaux fractionnaires $\mathfrak{a}, \mathfrak{b}$, $\mathfrak{a}$ divise $\mathfrak{b}$ si et seulement si, pour tout idéal premier $\mathfrak{p}$, $v_{\mathfrak{p}}(\mathfrak{a}) \leq v_{\mathfrak{p}}(\mathfrak{b})$.*

Definition 64. Soit K un corps de nombres. Le groupe des classes de K, ou groupe de Picard de $\mathcal{O}_K$, noté $\mathrm{Cl}(\mathcal{O}_K)$, est le groupe abélien (multiplicatif) quotient

$$\mathrm{Cl}(\mathcal{O}_K) = \{\text{idéaux fractionnaires de } K\}/\{\text{idéaux fractionnaires principaux}\}.$$

Lorsque $\mathcal{O}_K$ est un anneau principal, son groupe des classes/groupe de Picard est trivial : $\mathrm{Cl}(\mathcal{O}_K) = \{1\}$. Comme conséquence des résultats de géométrie des nombres obtenus par Minkowski, nous verrons en Cor. 86 que le groupe $\mathrm{Cl}(\mathcal{O}_K)$ est un groupe abélien fini. Ce groupe, dont la taille varie assez mystérieusement avec K, permet de mesurer le défaut de $\mathcal{O}_K$ à être un anneau principal (cf TN1 1.4).

2.12 Idéaux premiers de $\mathcal{O}_K$

Lemme 65. *Soit K un corps de nombres de degré n. i) Soit $\mathfrak{p}$ un idéal premier non-nul de $\mathcal{O}_K$. Alors $\mathfrak{p} \cap \mathbb{Z}$ est un idéal premier de $\mathbb{Z}$, donc de la forme $p\mathbb{Z}$ pour un nombre premier p. De plus, $\mathcal{O}_K/\mathfrak{p}$ est un corps fini à p^f éléments, pour un entier $f \leq n$.*

ii) Réciproquement, pour tout nombre premier p, l'ensemble des idéaux de $\mathcal{O}_K$ contenant p est fini et non vide.

Démonstration. i) L'anneau intègre $\mathcal{O}_K/\mathfrak{p}$ est un anneau fini, donc un corps fini. Son cardinal est donc de la forme p^f, pour un nombre premier p qui est sa caractéristique. En particulier, p est dans $\mathfrak{p}$. (autre preuve plus directe : si I est un idéal non-nul, alors $I \cap \mathbb{Z}$ est non-nul : il suffit de prendre le polynôme minimal de $x \neq 0$ dans I : son coefficient constant, non-nul, est dans $I \cap \mathbb{Z}$.) L'idéal $\mathfrak{p} \cap \mathbb{Z}$ étant premier, on en déduit qu'il est de la forme $p\mathbb{Z}$. La surjection $\mathcal{O}_K/p\mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p}$ assure que $f \leq n$.

ii) Les idéaux de $\mathcal{O}_K$ contenant $p\mathcal{O}_K$ sont en bijection avec les idéaux du quotient $\mathcal{O}_K/p\mathcal{O}_K$. En fixant une $\mathbb{Z}$-base de $\mathcal{O}_K$, il est aisé de voir que ce quotient est d'ordre p^n. Il suffit alors de prendre un idéal de cardinal maximal dans ce quotient pour en déduire un idéal maximal de $\mathcal{O}_K$ contenant $p\mathcal{O}_K$. □

2.12.1 Norme des idéaux

Proposition 66. *Soit K un corps de nombres, et I, J deux idéaux de $\mathcal{O}_K$. Alors*

$$\mathrm{N}(IJ) = \mathrm{N}(I)\mathrm{N}(J).$$

Démonstration. L'énoncé est vrai si I, J sont premiers entre eux (i.e. sont sans facteur premier commun, car ces idéaux sont alors étrangers : $I + J = \mathcal{O}_K$) d'après le théorème chinois (cf. TN1, Annexe B). Au vu de la factorisation unique (2.10.1), il suffit donc de démontrer que $\mathrm{N}(\mathfrak{p}^m) = \mathrm{N}(\mathfrak{p})^m$ lorsque $\mathfrak{p}$ est un idéal premier, sachant que $\mathrm{N}(\mathfrak{p}) = p^f$. Les idéaux $\mathfrak{p}^{m+1}$ et $\mathfrak{p}^m$ étant distincts par factorisation unique, on a une chaîne d'inclusion strictes

$$\cdots \subset \mathfrak{p}^{m+1} \subset \mathfrak{p}^m \subset \mathfrak{p}^{m-1} \subset \cdots \subset \mathfrak{p} \subset \mathcal{O}_K.$$

On fixe $\alpha \in \mathfrak{p}^m - \mathfrak{p}^{m+1}$. La multiplication par α induit un morphisme de groupe abélien $\mu_\alpha : \mathcal{O}_K \to \mathfrak{p}^m/\mathfrak{p}^{m+1}$, surjectif de noyau $\mathfrak{p}$. En effet,

i) les inclusions $\mathfrak{p}^{m+1} \subset \alpha\mathcal{O}_K + \mathfrak{p}^{m+1} \subset \mathfrak{p}^m$ montrent que seul l'idéal $\mathfrak{p}$ peut diviser l'idéal $\alpha\mathcal{O}_K + \mathfrak{p}^{m+1}$, qui est donc de la forme $\mathfrak{p}^a$, avec $m \leq a < m+1$. D'où la surjectivité.

ii) Ensuite, si $\alpha\beta \in \mathfrak{p}^m$, alors $v_{\mathfrak{p}}(\alpha\beta) \geq m$, et l'hypothèse sur α montre que β appartient à $\mathfrak{p}$.

On en déduit un isomorphisme de groupes abéliens (et même de $k = \mathcal{O}/\mathfrak{p}$-espaces vectoriels) $\mathcal{O}_K/\mathfrak{p} \cong \mathfrak{p}^m/\mathfrak{p}^{m+1}$, et on conclut par dévissage. □

Proposition 67. *-(définition) Soit $p \in \mathbb{Z}$ un nombre premier, et K un corps de nombres de degré n. On a la factorisation*

$$p\mathcal{O}_K = \prod_{j=1}^{g} \mathfrak{p}_j^{e_j}, \tag{2.12.1}$$

où les $\mathfrak{p}_j$ sont les idéaux premiers de $\mathcal{O}_K$ contenant p. On a la relation

$$n = \sum_{j=1}^{g} e_j f_j, \tag{2.12.2}$$

où $p^{f_j} = \mathrm{N}\mathfrak{p}_j$. L'entier $e_j \geq 1$ est l'indice de ramification de p en $\mathfrak{p}_j$, et l'entier f_j est le degré résiduel de p en $\mathfrak{p}_j$.

On dit que $p \in \mathbb{Z}$ est ramifié dans K si au moins un des indices de ramification e_j est > 1. Lorsque $p\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ (tous les $e_j = 1$ et $g = n$), on dit que p est *totalement décomposé* dans K. Lorsque $p\mathcal{O}_K = \mathfrak{p}$ (ie. $g = 1$ et $e_j = 1$), on dit que p est inerte dans K.

Exemple 68. cas des corps quadratiques (cf TN1) : $K = \mathbb{Q}(\sqrt{d})$ avec $d = 3$ modulo 4 un nombre premier fixé, et $p > 2$ pour simplifier : comme $[K : \mathbb{Q}] = 2$ et grâce aux isomorphismes

$$\mathbb{Z}[\sqrt{d}]/(p) \cong \mathbb{Z}[X]/(X^2 - d, p) \cong \mathbb{F}_p[X]/(X^2 - d),$$

la discussion peut se formuler en termes du symbole d'Euler et de Legendre (1.4.1) :

1. p est inerte dans $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ ($p\mathcal{O}_K = \mathfrak{p}, \mathrm{N}\mathfrak{p} = p^2$) si et seulement si $\left(\frac{d}{p}\right) = -1$ (ce qui arrive pour une proportion de 50% des nombres premiers d'après la loi de réciprocité + th. de progression arithmétique de Dirichlet, car cela revient à fixer la moitié des classes de $(\mathbb{Z}/4d\mathbb{Z})^\times$ et demander que la classe de p mod $4d$ appartienne à ces classes).
2. p est totalement décomposé ($p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$, $\mathrm{N}\mathfrak{p}_j = p$) si et seulement si
$$\left(\frac{d}{p}\right) = 1$$
(ce qui arrive pour 50% des nombres premiers).
3. p est ramifié ($p\mathcal{O}_K = \mathfrak{p}^2$, $\mathrm{N}\mathfrak{p} = p$) si et seulement si p divise d.

Concrètement, dans $K = \mathbb{Q}(\sqrt{3})$, les nombres premiers $p = 5, 7, 17, 19, 29, 31, 41, 43, ...$ sont inertes, les nombres premiers $p = 11, 13, 23, 37, 47, ...$ sont totalement décomposés, et le nombre premier 3 est ramifié. (ci-dessous la table pour $d = 3, 4d = 12$ et $p \leq 50$) :

	premiers décomposés		premiers inertes	
p	$13,\ 37$	$11,\ 23,\ 47$	$5, 17,\ 29,\ 41$	$7, 19, 31,\ 43$
classe mod 12	1 mod 12	11 mod 12	5 mod 12	7 mod 12

Décomposition des premiers $p \leq 50$ dans $\mathbb{Q}(\sqrt{3}), 4d = 12$.

Démonstration. (de la Prop. 67). D'après le Lemme 65, les seuls idéaux premiers $\mathfrak{p}_j$ qui peuvent apparaître dans la factorisation de $p\mathcal{O}_K$ sont ceux qui contiennent p, et ils apparaissent tous. La formule (2.12.2) résulte alors de la multiplicativité de la norme des idéaux établie dans la Prop. 66, qui implique que $p^n = \prod_{j=1}^{g} p^{e_j f_j}$. □

2.12.2 Construire des idéaux premiers

Sous des hypothèses favorables sur $\mathcal{O}_K$, la stratégie qui suit permet d'en construire des idéaux premiers de manière algorithmique.

Lemme 69. *On suppose que $\mathcal{O}_K = \mathbb{Z}[\theta]$, et l'on note $\pi = \pi_{\theta,\mathbb{Q}} \in \mathbb{Z}[X]$ son polynôme minimal. Soit p un nombre premier, et P_j un des facteurs irréductibles de $\overline{\pi} = \pi_{\theta,\mathbb{Q}}$ modulo p. Soit $\tilde{P}_j$ un relevé arbitraire de P_j à $\mathbb{Z}[X]$, et posons $\mathfrak{p}_j = (p, \tilde{P}_j(\theta)) \subset \mathcal{O}_K$. Alors*

i) $\mathfrak{p}_j$ est un idéal premier de $\mathcal{O}_K$ qui ne dépend que de P_j et pas du choix du relevé $\tilde{P}_j$.

ii) $\mathrm{N}\mathfrak{p}_j = p^{\deg P_j}$.

iii) si P_i est un facteur irréductible de $\overline{\pi}$ différent de P_j, alors $\mathfrak{p}_j \neq \mathfrak{p}_i$.

Proposition 70. *Soit K un corps de nombres. On suppose que $\mathcal{O}_K = \mathbb{Z}[\theta]$, et l'on note $\pi = \pi_{\theta,\mathbb{Q}} \in \mathbb{Z}[X]$ son polynôme minimal. Soit p un nombre premier, et*

$$\overline{\pi} = P_1^{e_1} \cdots P_r^{e_r} \in \mathbb{F}_p[X]$$

la factorisation de $\pi_{\theta,\mathbb{Q}}$ modulo p en produit de facteurs irréductibles distincts dans $\mathbb{F}_p[X]$. Alors la factorisation de $p\mathcal{O}_K$ en idéaux premiers de $\mathcal{O}_K$ s'écrit

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r},$$

où $\mathfrak{p}_j = (p, \tilde{P}_j(\theta)) \subset \mathcal{O}_K$.

Démonstration. D'après le lemme précédent, $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ est un produit de puissances de diviseurs premiers distincts. C'est un idéal contenu dans $p\mathcal{O}_K$, car il est engendré par des produits d'éléments visiblement chacun dans $p\mathcal{O}_K$, à l'exception possible d'un élément qui est de la forme $\tilde{P}_1(\theta)^{e_1} \cdots \tilde{P}_r(\theta)^{e_r}$, mais celui-ci appartient aussi à $\pi(\theta) + p\mathcal{O}_K = p\mathcal{O}_K$.
L'inclusion réciproque s'obtient grâce la norme en observant que $\sum e_i f_j = \deg \tilde{\pi} = n$. □

Rem : le résultat reste vrai même si $\mathcal{O}_K \neq \mathbb{Z}[\theta]$, tant que $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$.

Exemple 71. L'anneau des entiers de $\mathbb{Q}(\sqrt[3]{5})$ est $\mathbb{Z}[\sqrt[3]{5}]$. La factorisation de $f(X) = X^3 - 5$ modulo 2 donne

$$f \equiv X^3 - 1 = (X-1)(X^2 + X + 1) \in \mathbb{F}_2[X].$$

On en déduit que

$$(2) = (2, \sqrt[3]{5} - 1)(2, (\sqrt[3]{5})^2 + \sqrt[3]{5} + 1)$$

et que ces deux idéaux sont premiers, de norme respective 2 et 4. La factorisation de $f(X) = X^3 - 5$ modulo 3 donne

$$f \equiv X^3 - 2^3 = (X-2)^3 \in \mathbb{F}_3[X].$$

On en déduit que

$$(3) = (2, \sqrt[3]{5} - 2)^3$$

est ramifié, ce que confirme le calcul du discriminant $\text{disc}(X^3 - 5) = -3^3 5^2$.

3 Un théorème de Dedekind à propos de la ramification

un polycopié de J.P. Dos Santos, disponible sur Moodle.
Le résultat principal est le suivant :

Théorème 72. *Soit K un corps de nombres, et $p \in \mathbb{Z}$ un nombre premier. Alors*

$$p \text{ se ramifie dans } \mathcal{O}_K \iff p \text{ divise } \Delta_K.$$

4 La géométrie des nombres en renfort de l'algèbre

4.1 Réseaux de $\mathbb{R}^n$.

On rappelle qu'une partie D de $\mathbb{R}^n$ est *discrète* si pour tout $r > 0$, $D \cap B(0, r)$ est fini.

Definition 73. Soit V un $\mathbb{R}$-espace vectoriel de dimension finie, muni d'une norme. Un réseau de V est un sous-groupe discret qui engendre V comme espace vectoriel.

Autrement dit, c'est une partie discrète $L \subset V$ telle que si $a, b \in L$ alors $a - b$ est dans L, et qui contient une base $v_1, \ldots, v_n$ du $\mathbb{R}$-espace vectoriel V.

Exemples : a) $L = \mathbb{Z}^n, V = \mathbb{R}^n$

b)

$$L_0 = \{(a, b) \in \mathbb{Z}^2, a = 2b \mod 3\}, V = \mathbb{R}^2. \tag{4.1.1}$$

c) Pour $v_1, \ldots, v_n$ une $\mathbb{R}$-base de $\mathbb{R}^n$, $L(v) = \mathbb{Z}v_1 + \ldots + \mathbb{Z}v_n$ est un réseau de $\mathbb{R}^n$.

Definition 74. Soit $L = L(v)$ un réseau de $\mathbb{R}^n$ et X une partie mesurable de $\mathbb{R}^n$. On dit que X est un *domaine fondamental* (pour l'action) de $L(v)$ si tout $w \in \mathbb{R}^n$ s'écrit de manière unique sous la forme $w = \lambda + x, \lambda \in L, x \in X$.

Lemme 75. *Soit $v = (v_1, \ldots, v_n)$ une $\mathbb{R}$-base de $\mathbb{R}^n$. Alors le pavé*

$$\Pi(v) = \{\sum_{i=1}^{n} a_i v_i, 0 \leq a_i < 1\}$$

est un domaine fondamental pour le réseau $L(v) = \mathbb{Z}v_1 + \ldots + \mathbb{Z}v_n$, de mesure $|\det(v_1, \ldots, v_n)|$.

Démonstration. $L(v)$ est discret et contient une base de $\mathbb{R}^n$, c'est donc un réseau. Tout $w \in \mathbb{R}^n$ s'écrit de manière unique

$$w = \sum w_i v_i = \sum_{i=1}^{n} [w_i] v_i + \sum_{i=1}^{n} \{w_i\} v_i, \tag{4.1.2}$$

donc $\Pi(v)$ est un domaine fondamental. Sa mesure est $|\det(v_1, \ldots, v_n)|$ en vertu de la formule pour la jacobienne dans la formule du changement de variable pour la mesure de Lebesgue sur $\mathbb{R}^n$. □

Si v et v' sont deux $\mathbb{Z}$-bases du réseau L de $\mathbb{R}^n$, il existe une matrice $P \in GL_n(\mathbb{Z})$ telle que $v = Pv'$. Il s'ensuit que la mesure de $\Pi(v)$ ne dépend que du réseau L et pas du choix de sa $\mathbb{Z}$-base.

Definition 76. (covolume d'un réseau) Soit $L(v)$ un réseau de $\mathbb{R}^n$. Son covolume $\mathrm{covol}(L) > 0$ est la mesure commune des domaines fondamentaux (ou de la maille) $\Pi(v)$ de $L(v)$.

Proposition 77. *Soit L un sous-groupe de V. Alors*
i) L est un réseau de V
$\iff$
ii) L admet une famille finie $\mathbb{Z}$-génératrice qui est une $\mathbb{R}$-base de V.
En particulier, tout réseau L de $\mathbb{R}^n$ possèdent une $\mathbb{Z}$-base formée de n-éléments : il est de la forme $L = L(e)$.

Démonstration. ii) implique i) facilement. Pour la réciproque, soit $v_1, \ldots, v_n$ $\mathbb{R}$-base de $\mathbb{R}^n$ contenue dans L. On montre d'abord que $L(v)$ est d'indice fini dans L en utilisant l'ensemble borné $\Pi(v)$ défini ci-dessous : tout élément ℓ de L s'écrit $\ell = \ell_0 + \lambda$ avec $\ell_0 \in L(v)$ et $\lambda \in \Pi(v)$ comme en (4.1.2). Comme $L(v) \subset L$, il vient $\lambda - \ell - \ell_0 \in L \cap \Pi(v)$. Comme $\Pi(v)$ est borné et que L est un réseau, l'ensemble $L \cap \Pi(v)$ est donc fini, et $L/L(v)$ l'est aussi car l'application $L/L(v) \to L \cap \Pi(e)$ est injective. Le Th. de Lagrange montre alors que $NL \subset L(v)$ pour $N = [L : L(v)]$.

Par suite $L(v) \subset L \subset \frac{1}{N} L(v)$ pour un entier N. Fixons maintenant une $\mathbb{R}$-base $v' = (v'_1, \ldots, v'_n)$ de $\mathbb{R}^n$ formée d'éléments de L, dont le covolume de $L(v')$ est minimal. On sait que $L(v') \subset L \subset \frac{1}{N} L(v')$, où $N = [L : L(v')]$. Tout élément ℓ de L s'écrit donc $\ell = \sum_i \frac{m_i}{N} v'_i$ avec des entiers m_i. Le même argument qu'en (2.4.1) montre que, si un des $\frac{m_{i_0}}{N}$ n'est pas un entier, en remplaçant v'_{i_0} par $\ell - \left[\frac{m_{i_0}}{N}\right] v_{i_0}$, on construit une nouvelle base v'' contenue dans L, de covolume $\mathrm{covol}(L(v'')) < \mathrm{covol}(L(v'))$. Contradiction, donc v' est une $\mathbb{Z}$-base de L. □

4.2 Lemme du corps convexe de Minkowski

Lemme 78. *(Blichfeldt) Soit L un réseau de $\mathbb{R}^n$, et $X, Y \subset \mathbb{R}^n$ deux parties mesurables. On suppose que X est un domaine fondamental de L et que $\forall x, y \in Y$,*

$$x - y \in L \implies x = y.$$

Alors $\mu(Y) \leq \mu(X)$.

Démonstration. Par hypothèse

$$\mathbb{R}^n = \sqcup_{\lambda \in L} (X + \lambda).$$

Comme évidemment

$$(Y \cap (X + \lambda)) - \lambda = X \cap (Y - \lambda),$$

en intersectant avec Y et par invariance par translation de la mesure de Lebesgue il vient

$$\mu(Y) = \sum_{\lambda \in L} \mu(X \cap (Y - \lambda)).$$

Par hypothèse sur Y, les $Y - \lambda$ sont des parties disjointes de $\mathbb{R}^n$, donc la somme de droite est $\leq \mu(X)$. □

Une partie $\mathcal{C}$ de $\mathbb{R}^n$ est symétrique si $x \in \mathcal{C}$ implique $-x \in \mathcal{C}$. Le résultat suivant est fondamental.

Théorème 79. *(Lemme du corps convexe de Minkowski) Soit $C \subset \mathbb{R}^n$ une partie mesurable symétrique convexe, et soit L un réseau de $\mathbb{R}^n$. Si covol $(L) < \mu(C)/2^n$, ou si C est compact et covol $(L) \leq \mu(C)/2^n$, alors il existe un élément non nul dans $L \cap C$.*

Démonstration. Soit e une $\mathbb{Z}$-base de L. Le sous-groupe $L' = 2L$ de L, de $\mathbb{Z}$-base $2e$, est un réseau de $\mathbb{R}^n$ de covolume $\text{covol}(L') = 2^n \text{covol}(L)$.

Supposons d'abord $\text{covol}(L') < \mu(C)$. Le Lemme de Blichfeldt appliqué à $X = \Pi(2e)$ et $Y = C$ assure qu'il existe $x, y \in C$ distincts tels que $x - y \in 2L$. Mais C est convexe symétrique, donc la moyenne $\frac{x-y}{2}$, non-nulle, est dans $C \cap L$, ce qui conclut dans ce cas.

Traitons maintenant le cas $\text{covol}(L') \leq \mu(C)$ avec C compact. Pour tout $\epsilon > 0$, l'épaississement

$$C_\epsilon = \{z \in \mathbb{R}^n, \exists x \in C, \, |z - x| < \epsilon\}$$

de C est un ensemble borné symétrique convexe qui contient C, de mesure $> \mu(C)$. Le cas précédent fournit un élément z_ϵ non-nul de $L - \{0\} \cap C_\epsilon$. Comme L est discret, cet ensemble non-vide est fini, et il décroit avec ϵ. Il est donc constant (par rapport à ϵ) pour ϵ assez petit. Comme $C = \cap_\epsilon C_\epsilon$ est fermé, $L - \{0\} \cap C_\epsilon$ est non-vide (potentiellement avec plusieurs éléments). □

Pour calculer certains covolumes de réseaux, le lemme suivant est utile.

Lemme 80. *Soit $L \subset \mathbb{R}^n$ un réseau, et $L' \subset L$ un sous-groupe. Alors L' est un réseau $\iff$ L' est d'indice fini dans L. Sous cette hypothèse, on a*

$$\textit{covol}\,(L') = |L/L'| \textit{covol}\,(L).$$

Démonstration. c'est une conséquence la proposition 44. □

Par exemple, le réseau $L_0 \subset \mathbb{R}^2$ en (4.1.1) est de covolume 3, car on peut montrer que $(2, 1)$ et $(3, 0)$ en sont une $\mathbb{Z}$-base, en vertu de l'identité $(a, b) = (\frac{a-2b}{3})(3, 0) + b(2, 1)$.

4.3 Quelques premières applications arithmétiques

Théorème 81. *(Fermat, Euler) Tout nombre premier $p \equiv 1 \mod 4$ est somme de deux carrés.*

Démonstration. Choisir $u \in \mathbb{Z}$ tel que $u^2 = -1 \mod p$ (pourquoi est-ce possible ?). Considérer le réseau

$$L = \{(a, b) \in \mathbb{Z}^2, a = ub \mod p\},$$

qui est d'indice p dans $\mathbb{Z}^2$ car l'application $(a, b) \mapsto a - ub$ modulo p induit un isomorphisme entre $\mathbb{Z}^2/L$ et $\mathbb{Z}/p\mathbb{Z}$. Appliquer le lemme du corps convexe de Minkowski avec C la boule ouverte $B(0, 2p)$ fournit une paire $(a, b) \neq (0, 0)$ telle que $0 < a^2 + b^2 < 2p$, et $a^2 + b^2 = 0$ modulo p, ce qui permet de conclure. (Comparer avec Samuel p. 96). □

Théorème 82. *(Lagrange) Tout entier $n \geq 0$ est somme de 4 carrés.*

Démonstration. Supposer que $n = p$ est premier suffit, par multiplicativité de la norme des quaternions $q = a + ib + jc + ijd$. Commencer par choisir $u, v \in \mathbb{Z}$ tel que $1 + u^2 + v^2 = 0 \mod p$ (pourquoi est-ce possible ?). Considérer

$$LL = \{(a, b, c, d) \in \mathbb{Z}^4, c = au + bv \mod p, d = av - du \mod p\}.$$

C'est le noyau du morphisme surjectif $(a, b, c, d) \mapsto (c-au-bv, d-av+du) \in \mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$. Ainsi LL est d'indice p^2 dans $\mathbb{Z}^4$, et appliquer le lemme du corps convexe de Minkowski avec C la boule ouverte $B(0, 2p)$ fournit (a, b, c, d) avec $0 < a^2+b^2+c^2+d^2 < 2p$, et nul modulo p, ce qui conclut. (on pourra comparer avec la preuve de Samuel p. 98-100). □

4.4 $\mathcal{O}_K$ comme réseau de $\mathbb{R}^r \times \mathbb{C}^s$

Soit K un corps de nombres de degré n de signature (r, s), et $\sigma_1, \ldots, \sigma_r, \sigma_{r+1} \ldots \sigma_{r+s}$ la collection de ses r plongements réels et s plongements complexes non-conjugués 2 à 2, comme dans la définition 28. Le plongement associé est $\iota : K \to \mathbb{R}^r \times \mathbb{C}^s, x \mapsto (\sigma_i(x))_{i=1}^{r+s}$, qui collectionne les plongements réels puis complexes (dans un ordre arbitraire, mais fixé une fois pour toutes). On munit $\mathbb{C}$ de la $\mathbb{R}$-base $(1, i)$, ce qui identifie $\mathbb{R}^r \times \mathbb{C}^s$ avec $\mathbb{R}^n$ et y fixe une mesure de Lebesgue.

Lemme 83. *Soient $\omega_1, \ldots, \omega_n$ une $\mathbb{Q}$-base de K. Alors $(\iota(\omega_1), \ldots, \iota(\omega_n)))$ forme une famille $\mathbb{R}$-libre qui engendre un réseau de $\mathbb{R}^r \times \mathbb{C}^s$ de covolume $2^{-s}\sqrt{\Delta_{K/\mathbb{Q}}(\omega_1, \ldots, \omega_n)}$.*

Démonstration. Supposons d'abord que $s = 0$. Soit P la matrice des $\iota(\omega_j)$ dans la $\mathbb{R}$-base canonique de $\mathbb{R}^n$. On conclut avec (2.2.1). Dans le cas $s > 0$, on fixe la $\mathbb{R}$-base f formée des $f_j = (0, \ldots, *, 0, \ldots 0)$ de $\mathbb{R}^r \times \mathbb{C}^s$, où $* = 1$ si $j \leq r$, et $* = 1$ puis $* = i$ pour $r < j \leq s+r$. La matrice $P \in M_{r+2s}(\mathbb{R})$ des vecteurs $\iota(\omega_j)$ exprimés dans la $\mathbb{R}$-base f a donc pour colonne numéro j le vecteur

$$(\sigma_1(\omega_j), \ldots \sigma_r(\omega_j), \text{Re } \sigma_{r+1}(\omega_j), \text{Im } \sigma_{r+1}(\omega_j), \ldots, \text{Re } \sigma_{r+s}(\omega_j), \text{Im } \sigma_{r+s}(\omega_j))^t .$$

Il suffit d'observer que

$$\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix} \begin{pmatrix} \text{Re } \sigma(\omega_1) & \cdots & \text{Re } \sigma(\omega_n) \\ \text{Im } \sigma(\omega_1) & \cdots & \text{Im } \sigma(\omega_n) \end{pmatrix} = \begin{pmatrix} \sigma(\omega_1) & \cdots & \sigma(\omega_n) \\ \overline{\sigma}(\omega_1) & \cdots & \overline{\sigma}(\omega_n) \end{pmatrix} \tag{4.4.1}$$

pour conclure comme le cas $s = 0$. □

Exemple : en guise d'illustration, traitons le cas $n = 2, r = 0, s = 1$. Le corps quadratique imaginaire K possède une $\mathbb{Q}$-base $\{\omega_1, \omega_2\}$, deux plongements complexes $\{\sigma, \overline{\sigma}\}$, et

$$\Delta_K = \det \begin{pmatrix} \sigma(\omega_1) & \sigma(\omega_2) \\ \overline{\sigma}(\omega_1) & \overline{\sigma}(\omega_2) \end{pmatrix}^2 .$$

Le covolume du réseau $L \subset \mathbb{C}$ engendré par $\sigma(\omega_1), \sigma(\omega_2)$ est quant à lui

$$\text{covol}(L) = | \det P | = | \det \begin{pmatrix} \text{Re } \sigma(\omega_1) & \text{Re } \sigma(\omega_2) \\ \text{Im } \sigma(\omega_1) & \text{Im } \sigma(\omega_2) \end{pmatrix} | .$$

La relation matricielle (4.4.1) permet de conclure que $\mathrm{covol}(L) = \frac{1}{2}\sqrt{|\Delta_K|}$.

Théorème 84. *$\iota(\mathcal{O}_K)$ est un réseau de $\mathbb{R}^r \times \mathbb{C}^s$.*

Démonstration. Comme $\mathcal{O}_K$ contient une $\mathbb{Q}$-base de K, son image par le plongement ι contient une $\mathbb{R}$-base de $V = \mathbb{R}^n \cong \mathbb{R}^r \times \mathbb{C}^s$ d'après le lemme précédent. La Prop. 77 permet de conclure. On peut aussi vérifier directement que $\iota(\mathcal{O}_K)$ est discret avec l'argument de dénombrement suivant : soit $r > 0$, et munissons V de sa norme sup. dans la base canonique. Si $x \in \mathcal{O}_K$ vérifie $|\iota(x)| < r$, alors $|\sigma(x)| < r$ pour tout plongement réel σ, et $|\mathrm{Re}\ \sigma(x)|, |\mathrm{Im}\ \sigma(x)| < 2\sqrt{r}$ pour tout plongement complexe. Mais x est annulé par

$$\chi_{x,K/\mathbb{Q}} = \prod_{\sigma \in \Sigma(K)} (X - \sigma(x)) \in \mathbb{Z}[X].$$

La borne précédente, combinée aux relations coefficients-racines (1.1.1), montre que les coefficients, entiers, de $\chi_{x,K/\mathbb{Q}}$ sont bornés par une quantité qui ne dépend que de r et de n. Il n'y a qu'un nombre fini de possibilités pour $\chi_{x,K/\mathbb{Q}}$, donc pour x. □

4.5 Finitude du nombres de classes, théorème de Minkowski

Une référence proche du cours est P. Pollack chap. 21, ou Samuel p. 66 et suivantes. Définissons $c(s,n) = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}$.

Théorème 85. *(Minkowski) Soit K un corps de nombres de degré n, de signature (r,s), de discriminant $\Delta_K = \Delta_{K/\mathbb{Q}}$. Soit I un idéal non-nul de $\mathcal{O}_K$. Alors il existe un élément non-nul $x \in I$ tel que*

$$|\mathrm{N}_{K/\mathbb{Q}}(x)| \leq c(s,n)\mathrm{N}(I).\sqrt{|\Delta_K|}. \tag{4.5.1}$$

Démonstration. L'ensemble

$$B_t = \{(y_1, \dots, y_r, z_{r+1}, \dots, z_{r+s}) \in \mathbb{R}^r \times \mathbb{C}^s, \sum |y_i| + 2\sum |z_j| \leq t\}$$

est convexe symétrique. Son volume est $2^t \left(\frac{\pi}{2}\right)^s \frac{t^n}{n!}$ (cf. Samuel, p. 76, ou Pollack chap. 21). Le covolume de $\iota(I)$ est donné par le Lemme 83, donc le lemme du corps convexe 79 entraîne dès que $t^n > (\frac{4}{n})^s n!\sqrt{\Delta_K}\mathrm{N}(I)$ l'existence d'un élément non-nul $x \in \mathcal{O}_K$ tel que $\iota(x) \in B_t$. D'après l'inégalité arithmético-géométrique, un tel élément vérifie

$$|\mathrm{N}_{K/\mathbb{Q}}(x)| = \prod_{i=1}^{r} |\sigma_i(x)| \prod_{j=r+1}^{r+s} |\sigma_j(x)|^2 \tag{4.5.2}$$

$$\leq \frac{1}{n}\left(\sum |\sigma_i(x)| + 2\sum |\sigma_j(x)|\right)^n \leq \frac{t^n}{n^n}. \tag{4.5.3}$$

D'où le résultat. □

Corollaire 86. *Toute classe d'idéaux fractionnaires de $Cl(\mathcal{O}_K)$ admet comme représentant un idéal ordinaire $J \subset \mathcal{O}_K$ de norme inférieure ou égale à la constante de Minkowski $M_K = c(s,n)\sqrt{|\Delta_K|}$. En particulier, le groupe des classes $Cl(\mathcal{O}_K)$ est fini.*

Démonstration. Soit C une classe d'idéaux de $\mathcal{O}_K$, et $\mathfrak{a}$ un représentant entier de la classe inverse C^{-1}. Le Théorème 85 de Minkowski fournit $x \in \mathfrak{a}$ non nul de norme $\leq M_K \mathrm{N}(\mathfrak{a})$. L'idéal fractionnaire $\mathfrak{b} = x\mathfrak{a}^{-1}$ est dans la classe C (il ne diffère de $\mathfrak{a}^{-1}$ que d'un idéal principal), c'est un idéal entier car $x\mathfrak{a}^{-1} \subset \mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}_K$, et comme $\mathfrak{a}\mathfrak{b} = x\mathcal{O}_K$ sa norme est $\mathrm{N}(\mathfrak{b}) = |\mathrm{N}(x)|/\mathrm{N}(\mathfrak{a}) \leq M_K$. □

Definition 87. Le nombre de classes d'un corps de nombres K est l'ordre de son groupe des classes

$$h_K = \mathrm{Cl}(\mathcal{O}_K).$$

Pour tout idéal I de $\mathcal{O}_K$, I^{h_k} est un idéal principal, et l'anneau $\mathcal{O}_K$ est principal si et seulement si $h_K = 1$.

Exemple 88. Soit $K = \mathbb{Q}(\sqrt{-5})$, d'anneau d'entiers $\mathbb{Z}[\sqrt{-5}]$. Son discriminant est $\Delta_K = -20$, et la constante de Minkowski vérifie $M_K < 3$. Chaque classe non-triviale possède éventuellement un représentant de norme 2. Or 2 est ramifié car $x^2 + 5 \mod 2 \equiv (x+1)^2$, donc $2\mathcal{O}_K = \mathfrak{p}^2$, et $\mathfrak{p}$ est de norme 2. Enfin, $\mathfrak{p}$ n'est pas principal car l'équation $x^2 + 5y^2 = 2$ n'a pas de solutions entières. Par conséquent $\mathrm{Cl}([\sqrt{-5}]) = \mathbb{Z}/2\mathbb{Z}$.

Exemple 89. Soit $K = \mathbb{Q}(\theta)$, avec $\theta \in \mathbb{R}$ la racine réelle de $f(x) = x^5 - x^3 + 1$, de signature $(1,2)$. Son discriminant divise $\mathrm{disc}(f) = 3017$, qui est sans facteurs carrés ; donc $\mathcal{O}_K = \mathbb{Z}[\theta]$ et $\Delta_K = 3017$ d'après le Lemme 46. Ainsi $M_K = \left(\frac{4}{\pi}\right)^2 \frac{5!}{5^5}\sqrt{3017} = 3.41....$, de sorte que toute classe non-triviale du groupe des classes possède donc un représentant entier de norme 2 ou 3. Le critère Prop. 70 donne la forme des idéaux premiers au-dessus de $p = 2$ et $p = 3$:

1. $p = 2$ est inerte dans K puisque $f \mod 2$ est irréductible dans $\mathbb{F}_2[X]$.
2. $f(x) \equiv (x^2 - x - 1)(x^3 + x^2 + x + 1) \in \mathbb{F}_3[x]$, donc les idéaux premiers au-dessus de 3 ont norme 3^2 et 3^3.

Il n'y a pas d'idéaux de $\mathcal{O}_K$ de norme 2 ou 3, donc $\mathrm{Cl}(\mathcal{O}_K)$ est trivial, $h_K = 1$.

Autres corollaires :

Corollaire 90. *(Hermite) Le corps $\mathbb{Q}$ est le seul corps de discriminant* 1.

Démonstration. Les idéaux entiers non-nuls sont de norme ≥ 1. D'après le Cor. 86.b), on en déduit l'inégalité

$$\left(\frac{\pi}{4}\right)^{2s} \frac{n^{2n}}{(n!)^2} = c(s,n)^{-2} \leq \Delta_K.$$

Puisque $s \leq n$, le membre de gauche est minoré par $B_n = \left(\frac{\pi}{4}\right)^{2n} \frac{n^{2n}}{(n!)^2}$. Comme $\frac{3\pi}{4} \leq \frac{B_{n+1}}{B_n}$ et $B_2 = \frac{\pi^2}{4}$, il est facile de voir que

$$1 < \frac{\pi^2}{4}\left(\frac{3\pi}{4}\right)^{n-2} \leq |\Delta_K| \tag{4.5.4}$$

lorsque $n \geq 2$, ce qui implique le résultat. □

Théorème 91. *(Hermite 1857) Soit $X > 0$. Il n'y a qu'un nombre fini de corps de nombres K tels que*

$$| \Delta_K | < X.$$

Démonstration. D'après (4.5.4), l'hypothèse borne également le degré de K, donc il suffit de montrer qu'il y a un nombre fini de corps de nombres K de degré n qui satisfont $|\Delta_K| \leq X$. On considère la région

$$\mathcal{R} = \{(x_1, \ldots, x_n) \in \mathbb{R}^n, \max_{i=1}^{n-1}(|x_i|) \leq \frac{1}{2}, |x_n| \leq T\}$$

avec $T = 2^n\sqrt{X}$. Alors $\mathcal{R}$ est convexe symétrique, de volume $2^{n+1}\sqrt{X}$, tandis que $2^n \text{covol}(\iota(\mathcal{O}_K)) \leq 2^n\sqrt{X}$. D'après le lemme convexe de Minkowski, il existe $\alpha \in \mathcal{O}_K$ non-nul tel que $\iota(\alpha) \in \mathcal{R}$. Pour ce α on a

$$|\sigma_i(\alpha)| \leq \sqrt{T^2 + \frac{1}{4}} < T + 1$$

pour tout plongement $\sigma : K \to \mathbb{C}$. D'après les relations coefficients racines (1.1.1), il n'y a donc qu'un nombre fini de polynôme minimal $\pi_{\alpha,\mathbb{Q}} \in \mathbb{Z}[X]$ possible pour α. On va en déduire la conclusion souhaitée à condition de montrer que α est primitif pour K, i.e. $K = \mathbb{Q}(\alpha)$. Soit $k = \mathbb{Q}(\alpha)$. Chaque plongement $\tau \in \Sigma(k)$ prend une valeur différente en α d'après le Lemme 33, et se prolonge de $[K : k]$ façons en un plongement de K. Il suffit donc de montrer que $\sigma_{r+s}(\alpha)$ diffère de tous les $\sigma_i(\alpha), i < r + s$, pour s'assurer que σ_{r+s} n'est pas issu d'un prolongement de $\Sigma(k)$ à $\Sigma(K)$, i.e. que α est primitif pour K. Nous exécutons cette stratégie dans le cas $s = 0$, et on renvoie à (Pollack Th. 21.11) pour le cas général. Comme $|\sigma_i(\alpha)| \leq \frac{1}{2}, i = 1...n-1$ il s'ensuit que

$$|\sigma_n(\alpha)| = |\mathrm{N}_{K/\mathbb{Q}}(\alpha)| \prod_{i=1}^{n-1} |\sigma_i(\alpha)|^{-1} \tag{4.5.5}$$

$$\geq |\mathrm{N}_{K/\mathbb{Q}}(\alpha)| 2^{n-1} \geq 1. \tag{4.5.6}$$

Donc $\sigma_n(\alpha) \neq \sigma_i(\alpha), i = 1, \ldots n-1$, et α engendre K sur $\mathbb{Q}$. □

5 L'analyse en renfort de l'algèbre

Dans cette partie, nous démontrons deux résultats de Dirichlet : le théorème de progression arithmétique de Dirichlet, et la formule des classes. En guise de préliminaire, nous introduisons notamment les caractères χ du groupe $(\mathbb{Z}/m\mathbb{Z})^\times$, et les séries de Dirichlet $L(s,\chi)$ qui leur sont attachées, en établissant leur prolongement analytique partiel.

5.1 Caractères d'un groupe abélien fini

Definition 92. Soit G un groupe *abélien* fini d'ordre n (noté multiplicativement). Un caractère de G est un morphisme $\chi : G \to (\mathbb{C}^*, \times)$. On note $\hat{G}$ le groupe multiplicatif abélien formé des caractères de G, pour la loi naturelle issue de celle de $\mathbb{C}^* : \chi.\chi'(g) := \chi(g)\chi'(g)$.

Remarque 93.

1. Comme $g^n = 1$ dans G, il est clair que $\chi(g^n) = \chi(g)^n = 1$, de sorte que $\chi \in \hat{G}$ est à valeur dans le groupe μ_n des racines n-èmes de l'unité.
2. Le caractère *trivial* sur G est la fonction constante $\mathbf{1}$.
3. Le groupe dual $\hat{G}$ d'un groupe fini est un groupe abélien fini : si $g_1, \ldots, g_n$ sont les éléments de G, alors $\chi \mapsto (\chi(g_1), \ldots, \chi(g_n))$ est une injection de $\hat{G}$ dans μ_n^n.
4. Un point clef sera d'établir au plus tôt que G et $\hat{G}$ sont tous les deux de même cardinal n. Commençons par le vérifier lorsque G est un groupe *cyclique* d'ordre n en déterminant complètement la structure de $\hat{G}$ dans ce cas : $G \simeq \mu_n =< e^{2i\pi/n} >$. Tout caractère χ de G est déterminé par sa valeur en $\zeta_n = e^{2i\pi/n}$. Mieux : on peut poser
$$\chi_0(\zeta_n^k) := e^{\frac{2ik\pi}{n}}.$$
L'application $k \mapsto e^{\frac{2ik\pi}{n}}$ est un morphisme surjectif de $(\mathbb{Z}, +)$ vers $(\mu_n, \times)$, elle induit donc par passage au quotient un morphisme surjectif (donc non-trivial) χ_0 de G dans μ_n. Tout caractère χ de G est une puissance de χ_0, puisque χ est déterminé par sa valeur en ζ_n, générateur de G. Ainsi, lorsque $G \simeq \mu_n$ est cyclique d'ordre n, $\hat{G} \simeq <\chi_0>$ est aussi cyclique d'ordre n. (noter que l'isomorphisme $G \simeq \hat{G}, \zeta_n \mapsto \chi_0$ n'est pas canonique, on a eu besoin de fixer un générateur $e^{2i\pi/n}$ pour μ_n pour réaliser cet isomorphisme).
5. Cette notion de "dualité ", et d'isomorphisme (non) canonique rappelle et éclaire (en tout cas pour moi) celle d'algèbre linéaire. D'ailleurs, le groupe bi-dual $\hat{\hat{G}}$ de G va bientôt faire une apparition cruciale, et c'est lui qui est en bijection naturelle avec G.
6. Autre exemple de caractère : le symbole de Legendre $\left(\frac{\cdot}{q}\right) : x \mapsto \left(\frac{x}{q}\right)$, dont les principales propriétés ont été énoncées en 1.4, est un caractère de $G = (\mathbb{Z}/q\mathbb{Z})^\times$. Plus généralement, un caractère *modulo* D est un caractère du groupe multiplicatif $(\mathbb{Z}/D\mathbb{Z})^\times$.

5.1.1 Lemme de prolongement des caractères

Lemme 94. *Soit G un groupe (multiplicatif) abélien fini, et H un sous-groupe de G. Tout caractère de H se prolonge en un caractère de G.*

Démonstration. (attention aux fausses preuves). Soit χ_H un caractère de H. On procède par récurrence sur l'indice $d = [G : H]$. Lorsque $d = 1$, il n'y a rien à faire. Lorsque $d > 1$, on fixe $x \in G$ hors de H. Pour étendre χ_H en un caractère χ du plus grand groupe $H' = H \cup < x > \subset G$, on doit définir $\chi_H(x)$ avec les contraintes suivantes :

- le prolongement doit être un morphisme, et être bien défini.

- La valeur de χ en x ne peut PAS être arbitraire : on sait que $x^d \in H$ (Lagrange). Plus précisément, il y a un plus petit entier $n = n_x > 1$, (qui divise d), tel que x^n est dans H. La valeur de notre caractère χ qui coïncide sur H avec χ_H est donc prescrite en x^n. Pour préserver la propriété de morphisme on DOIT donc poser $\chi(x) = \chi_H(x^n)^{\frac{1}{n}} =$ une racine n-ème arbitraire de $\chi_H(x^n)$. (il y a donc $n = [H' : H]$ choix possibles car $\mathbb{C}^*$ est algébriquement clos).

Le point clef est de vérifier que, ce choix étant fait, χ est bien définie : si $g \in H \cup < x >$, alors $g = h_1 x^a = h_2 x^b$ et il s'agit de vérifier que $\chi(h_1 x^a) = \chi(h_2 x^b)$, avec la définition précédente.

Or l'hypothèse montre que $x^{a-b} = h_2 h_1^{-1}$ est dans H. Ainsi, en effectuant la *division euclidienne* de $a - b$ par $n = n_x$, on voit que n divise $a - b$. On écrit donc $nq = (a - b)$, et

$$\begin{aligned}
\chi_H(h_2 h_1^{-1}) &= \chi_H(h_2)\chi_H(h_1)^{-1} && (5.1.1)\\
&= \chi_H(x^{a-b}) && (5.1.2)\\
&= \chi_H(x^{nq}) && (5.1.3)\\
&= \chi_H(x^n)^q && (5.1.4)\\
&= \chi_H(x^n)^{\frac{a-b}{n}}, && (5.1.5)
\end{aligned}$$

ce qui implique le résultat. □

5.1.2 Formules d'orthogonalité des caractères

Proposition 95. *Pour $\chi \in \hat{G}$,*

$$\sum_{g \in G} \chi(g) = 0 \text{ sauf si } \chi \text{ est le caractère trivial } \mathbf{1}.$$

Pour $g \in G$,

$$\sum_{\chi \in \hat{G}} \chi(g) = 0, \text{ sauf si } g \text{ est l'élément trivial (le neutre } e_G) \text{ de } G.$$

Démonstration. Notons $R_\chi = \sum_g \chi(g)$. Si χ n'est pas constant, il existe $g_0 \in G, \chi(g_0) \neq 1$. Alors $\chi(g_0)R_\chi = \sum_g \chi(g_0)\chi(g) = \sum_g \chi(g_0 g) = R_\chi$. Ceci implique que $R_\chi = 0$.

Notons $S_g = \sum_\chi \chi(g)$. Pour tout $\chi' \in \hat{G}$ on a

$$\chi'(g) S_g = \sum_\chi \chi\chi'(g) = \sum_{\chi'' \in \hat{G}} \chi''(g) = S_g.$$

Supposons que g n'est pas le neutre de G. Alors $H =< g >$ est un groupe cyclique non-trivial, et la Remarque d) ci-dessus montre que H possède au moins un caractère qui ne vaut pas 1 en g. Le lemme de prolongement 94 permet d'en déduire un caractère χ' de G qui ne vaut pas 1 en g, de sorte que $S_g = 0$. □

Corollaire 96. *(les points 2. et 3. ne sont pas utilisés dans la suite)*

1. *Si G est un groupe abélien d'ordre m, alors $\hat{G}$ est d'ordre m.*
2. *G et $\hat{\hat{G}}$ sont (canoniquement) isomorphes.*
3. *G et $\hat{G}$ sont isomorphes.*

Démonstration. 1. Il suffit d'évaluer la somme finie double

$$\mathcal{D} = \sum_{\chi \in \hat{G}} \sum_{g \in G} \chi(g)$$

au moyen des formules d'orthogonalité des caractères : la seule contribution non-nulle est celle du caractère $\mathbf{1}$, et cette contribution vaut $|G|$, donc $\mathcal{D} = |G|$. En intervertissant les sommes, toutes les contributions sont nulles sauf celle de $g = e_G$. Cette contribution est $|\hat{G}|$, donc $|\hat{G}| = \mathcal{D} = |G|$.

2. Le groupe $\hat{G}$ étant un groupe abélien fini, son groupe dual $\hat{\hat{G}}$ est un groupe abélien fini. L'application naturelle $G \to \hat{\hat{G}}$ qui envoie $g \in G$ sur l'évaluation $(\chi \in \hat{G} \mapsto \chi(g)) \in \hat{\hat{G}}$ est, comme toujours, injective : si $\chi(g) = 1$ pour tous les $\chi \in \hat{G}$, alors lemme de prolongement (plus exactement sa contraposée) implique que $g = e_G$. Comme G et $\hat{G}$ ont même cardinal d'après 1, ils sont isomorphes.

3. Si A et B sont des groupes cycliques, il est assez formel de voir que $\widehat{A \times B} \simeq \hat{A} \times \hat{B}$. Or on sait que $\hat{A} \simeq A$ dans le cas des groupes cycliques, cf. Rem 93.c. Ainsi $\widehat{A \times B} \simeq A \times B$. On conclut dans le cas général en utilisant la classification des groupes abéliens finis, qui décompose G en un produit de groupes cycliques. (notez que cette preuve à gros marteau ne se sert pas des formules d'orthogonalité). □

5.2 Fonctions $L(s, \chi)$ de Dirichlet

Une série de Dirichlet est une série à paramètre de la forme

$$L(s) = \sum_{n \geq 1} \frac{a_n}{n^s},$$

où les a_n sont des nombres complexes fixés, et où s est une variable complexe. On rappelle que $n^s = e^{s \log n}$, où log est le logarithme népérien. La fonction $s \mapsto n^s$ est une fonction entière qui ne s'annule pas.

Lemme 97. *Si (a_n) est une suite bornée, alors $L(s)$ converge normalement sur tout demi-plan de la forme Re$(s) > s_0$ avec $s_0 > 1$. En particulier, elle définit une fonction holomorphe sur le demi-plan ouvert Re$(s) > 1$.*

Démonstration. On observe que $|n^s| = n^{\mathrm{Re}(s)}$. Le lemme découle alors de la convergence bien connue de la série de Riemann à termes positifs $\sum_{n\geq 1} n^{-s_0}$ où $s_0 > 1$ est un nombre réel, qui est majorée par $1 + \int_1^\infty t^{-s_0} dt = 1 + \frac{1}{s_0 - 1}$. □

Definition 98. Soit $D \geq 1$ un entier, et χ un caractère du groupe mulitplicatif $G_D = (\mathbb{Z}/D\mathbb{Z})^\times$. On étend χ en un "caractère de Dirichlet", i.e.une fonction sur $\mathbb{Z}$ en posant $\chi(k) = 0$ si $(k, D) \neq 1$, et $\chi(k) := \chi(k \mod D)$ si $(k, D) = 1$.

La fonction L de Dirichlet associée au caractère χ est donnée par

$$L(s, \chi) = \sum_{n\geq 1} \frac{\chi(n)}{n^s}.$$

Comme $|\chi(n)| \leq 1$, cette fonction $L(s, \chi)$ est une fonction entière sur le demi-plan Re$(s) > 1$. Un des objectifs principaux dans la suite est d'étudier le prolongement analytique de cette fonction holomorphe à $\mathbb{C}$ tout entier, et de déterminer s'il y a un pôle éventuel en $s = 1$.

Proposition 99. *La fonction zêta de Riemann*

$$\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s},$$

qui correspond au caractère de Dirichlet trivial $\chi = \mathbf{1}$, se prolonge en une fonction méromorphe sur Re$(s) > 0$. Elle possède un unique pôle, en $s = 1$. Ce pôle est simple, et le résidu correspondant est 1.

Démonstration. On commence par montrer que

$$\zeta(s) - \frac{1}{s-1} = \sum_{n=1}^{\infty} \left[\frac{1}{n^s} - \int_n^{n+1} t^{-s} \mathrm{d}t \right]. \tag{5.2.1}$$

On pose $\phi_n(s) = \int_n^{n+1} (n^{-s} - t^{-s})\mathrm{dt}$. Le théorème des accroissement finis pour la fonction $t \mapsto (n^{-s} - t^{-s})$ sur l'intervalle $[n, n + 1]$ montre que $\mid \phi_n(s) \mid \leq \frac{|s|}{n^{\sigma+1}}$ avec $\sigma = \mathrm{Re}(s)$. La série $\sum \phi_n(s)$ converge donc normalement sur chaque demi-plan Re$(s) > \epsilon > 0$, donc elle donne naissance à une série qui est holomorphe sur Re$(s) > 0$. □

Remarque 100. On peut montrer que $\zeta(s)$ s'étend en une fonction méromorphe sur $\mathbb{C}$ tout entier, avec un seul pôle simple en $s = 1$; pour cela, on part de l'identité $\Gamma(s)\zeta(s) = \int_0^\infty \frac{t^s}{e^t - 1} \frac{dt}{t}$, valable pour Re$(s) > 1$. On procède ensuite par intégrations par parties (**TD**).

5.2.1 Produits Eulériens

$\mathcal{P}$ est l'ensemble des nombres premiers.

Lemme 101.

$$\zeta(s) = \prod_{p\in\mathcal{P}} (1-p^{-s})^{-1}, \tag{5.2.2}$$

$$L(s,\chi) = \prod_{p\in\mathcal{P}} (1-\chi(p)p^{-s})^{-1}. \tag{5.2.3}$$

Démonstration. On indexe les nombres premiers $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, \dots$ de $\mathcal{P}$. On considère d'abord pour $r > 0$ le produit fini (avec $\chi = \mathbf{1}$ pour le cas de $\zeta(s)$)

$$T_r(\chi) = \sum_{k_1,\dots k_r\geq 0} \frac{\chi(p_1^{k_1}\cdots p_r^{k_r})}{(p_1^{k_1}\dots p_r^{k_r})^s} = \sum_{n\in P_r} \frac{\chi(n)}{n^s}.$$

Comme $\mathbb{Z}$ est un anneau factoriel, l'ensemble P_r est exactement l'ensemble des entiers $n \geq 1$ dont les facteurs premiers sont exclusivement parmi $p_1, \dots p_r$. Cette série est absolument convergente pour $\mathrm{Re}(s) > 1$, la somme des valeurs absolues de son terme général est majorée par $\zeta(s)$ (uniforme en r). Sa limite quand $r \to \infty$ est $L(s,\chi)$. En outre, par multiplicativité de χ et sommation géométrique,

$$T_r(\chi) = \sum_{k_1\geq 0} \frac{\chi(p_1)^{k_1}}{p_1^{sk_1}} \cdots \sum_{k_r\geq 0} \frac{\chi(p_r)^{k_r}}{p_r^{sk_r}} \tag{5.2.4}$$

$$= \prod_{j=1}^{r} \left(1 - \frac{\chi(p_j)}{p_j^s}\right)^{-1}. \tag{5.2.5}$$

On conclut par passage à la limite en $r \to \infty$. □

5.2.2 Un pas vers la gauche

Dans cette sous-partie, on explique comment la fonction de Dirichlet $L(s,\chi)$ se prolonge en une fonction méromorphe sur le demi-plan un peu plus grand $\mathrm{Re}\, s > 0$ au moyen du lemme d'Abel.

Lemme 102. *On suppose qu'il existe $r > 0$ avec $S_N = \sum_{n\leq N} a_n = O(N^r)$. Alors la série de fonctions $\sum_{n\geq 1} \frac{a_n}{n^s}$ converge uniformément sur tout compact du demi-plan $\mathrm{Re}(s) > r$. En particulier, sa somme est holomorphe sur ce demi-plan.*

Démonstration. C'est la transformation d'Abel (i.e. l'analogue de l'intégration dans ce contexte discret), sachant que $|S_N| < CN^r$ pour une constante $C > 0$.

$$\sum_{n=N}^{M} \frac{a_n}{n^s} = \sum_{n=N}^{M} \frac{S_n - S_{n-1}}{n^s} \tag{5.2.6}$$

$$= \frac{S_M}{M^s} - \frac{S_{N-1}}{N^s} + \sum_{n=N}^{M-1} S_n \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right). \tag{5.2.7}$$

Comme $| \frac{1}{n^s} - \frac{1}{(n+1)^s} | = | s \int_n^{n+1} t^{-s-1} dt |$ est majoré par $\frac{|s|}{n^{\mathrm{Re}(s)+1}}$ (faire un dessin), il s'ensuit en majorant terme à terme que la tranche de Cauchy entre N et M satisfait

$$| \sum_{n=N}^{M-1} \frac{a_n}{n^s} | \leq \frac{CM^r}{M^{\mathrm{Re}(s)}} + \frac{CN^r}{N^{\mathrm{Re}(s)}} + \sum_{n=N}^{M-1} Cn^r |s| \left(\frac{1}{n^{\mathrm{Re}(s)+1}} \right). \tag{5.2.8}$$

Le critère de Riemann permet alors de conclure. □

Corollaire 103. *a) Si χ est un caractère non-trivial modulo D, la série $L(s,\chi)$ définit une fonction holomorphe sur le demi-plan $Re(s) > 0$.*

b) Lorsque $\chi = \mathbf{1}_D$ est le caractère trivial modulo D, la fonction $L(s,\chi)$ possède un pôle simple en $s = 1$.

Démonstration. a) Soit χ un caractère non-trivial modulo D. Les formules d'orthogonalité des caractères montrent les sommes partielles $N \mapsto S_N = \sum_{k=1}^{N} a_k$ sont D-périodiques, donc elles satisfont les hypothèses du Lemme 102 avec $r > 0$ arbitraire.

b) Dire que χ est le caractère trivial $\mathbf{1}_D$ modulo D, c'est dire que $\chi : \mathbb{Z} \to \mathbb{C}$ vaut 1 sur les entiers premiers à D, et qu'il vaut 0 ailleurs. Il résulte du Lemme 101 que

$$L(s, \mathbf{1}_D) = \sum_{n \geq 1, (n,D)=1} \frac{1}{n^s} \tag{5.2.9}$$

$$= \zeta(s) \prod_{p|D} \left(1 - \frac{1}{p^s} \right). \tag{5.2.10}$$

Le produit fini étant une fonction entière qui ne s'annule pas en $s = 1$, l'assertion sur les pôles de $L(s, \mathbf{1}_D)$ se déduit du résultat semblable pour $\zeta(s)$. □

5.3 Fonction zêta de Dedekind

Soit K un corps de nombres de degré n. On note $\mathcal{P}_K$ l'ensemble des idéaux premiers de $\mathcal{O}_K$.

Definition 104. (-Proposition)
La fonction zêta de Dedekind associée au corps K est définie par

$$\zeta_K(s) = \sum_{\mathfrak{a}\subset\mathcal{O}_K} \frac{1}{(\mathrm{N}\mathfrak{a})^s}, \tag{5.3.1}$$

la somme portant sur tous les idéaux $\mathfrak{a}$ de $\mathcal{O}_K$. Cette série est absolument convergente pour $\mathrm{Re}(s) > 1$, domaine où elle coïncide avec le produit Eulérien

$$\zeta_K(s) = \prod_{\mathfrak{p}\in\mathcal{P}_K} \left(1 - (\mathrm{N}\mathfrak{p})^{-s}\right)^{-1}, \tag{5.3.2}$$

le produit portant sur les idéaux premiers $\mathfrak{p}$ de $\mathcal{O}_K$.

Démonstration. (du fait que les deux formules (5.3.1) et (5.3.2) coïncident et convergent).

On commence développer le produit Eulérien : comme l'anneau $\mathcal{O}_K$ est un anneau de Dedekind, l'unicité de la factorisation de $\mathfrak{a}$ en produit d'idéaux premiers et l'argument du Lemme 101 montrent que, sous réserve de convergence absolue, (5.3.2) coïncide avec (5.3.1).

Pour étudier cette convergence, on regroupe les idéaux premiers $\mathfrak{p} \subset \mathcal{O}_K$ selon le nombre premier $p \in \mathbb{Z}$ qu'ils divisent (cf la partie 2.12), de sorte que

$$\zeta_K(s) = \prod_{p\in\mathcal{P}} \prod_{\mathfrak{p}|p} \left(1 - (\mathrm{N}\mathfrak{p})^{-s}\right)^{-1}. \tag{5.3.3}$$

On rappelle que tout nombre premier p possède $g \leq n$ idéaux premiers $\mathfrak{p}_j$ qui le divisent, et que pour chacun $p \leq \mathrm{N}\mathfrak{p}_j = p^{f_j} \leq p^n$. Ainsi pour $\sigma = \mathrm{Re}(s) > 1$, la somme de termes positifs $\sum_{k\geq 0} \mathrm{N}\mathfrak{p}_j^{-k\sigma}$ est dominée par $\sum_{k\geq 0} p^{-k\sigma} = (1-p^{-\sigma})^{-1}$. Pour $j = 1, \ldots, g$, la première série est ≥ 1, donc le cas le pire est $g = n$, d'où la majoration

$$\prod_{j=1}^{g} \left(\sum_{k\geq 0} \mathrm{N}\mathfrak{p}_j^{-k\sigma} \right) \leq \left(1 - p^{-\sigma}\right)^{-n}.$$

En comparant avec (5.3.3), on en déduit que $\zeta_K(s)$ converge absolument dès que $\zeta(s)^n$ converge absolument, donc au moins pour $\sigma = \mathrm{Re}(s) > 1$. □

5.3.1 Caractère associé à une extension quadratique

- La partie 1.4 décrit le symbole de Legendre, qui définit sur $\mathbb{Z}$ une application $a \mapsto \left(\frac{a}{p}\right)$ pour tout nombre premier p.
- Le *symbole de Jacobi* (cf TdN1 chap. 5.4) consiste à étendre cette définition, en forçant la multiplicativité en b, en un symbole $\left(\frac{a}{b}\right)$ défini pour tout b entier impair par $\left(\frac{a}{-1}\right) = \mathrm{sign}\ a$ et

$$\left(\frac{a}{p_1^{k_1}\cdots p_r^{k_r}}\right)_{\text{Jacobi}} = \prod_{j=1}^{r} \left(\frac{a}{p_j}\right)^{k_j}.$$

- Le *symbole de Kronecker* en est une extension supplémentaire, totalement multiplicative, obtenue en rajoutant la condition

$$\left(\frac{a}{2}\right) = \begin{cases} 0 & \text{si } 2 \mid a, \\ 1 & \text{si } a = \pm 1 \mod 8, \\ -1 & \text{si } a = \pm 3 \mod 8. \end{cases} \tag{5.3.4}$$

On obtient ainsi un symbole $\left(\frac{a}{b}\right)$ défini pour tous les entiers a et b. [1]

Soit $d \in \mathbb{Z}$ un entier sans facteur carré, et D le discriminant du corps quadratique $K = \mathbb{Q}(\sqrt{d})$ (de sorte que $D = d$ ou $D = 4d$, cf la partie 2.6).
On associe au corps K le symbole non-trivial $\chi_D(n) = \left(\frac{D}{n}\right)$.

Lemme 105. *-(définition) Lorsque D est le discriminant d'un corps quadratique, le symbole $\chi_D : \mathbb{Z} \to \{0, \pm 1\}$ est un caractère non-trivial modulo $|D|$.*

Démonstration. Il s'agit de vérifier que, si $D = d$ ou $D = 4d$ est un discriminant, la fonction $n \mapsto \left(\frac{D}{n}\right)$ est $|D|$-périodique. cf **TD**. □

On observe aussi (TD 6, exercice 1) que

$$\chi_D(p) = \begin{cases} 0 & \text{si } p \text{ ramifie dans } K, \\ 1 & \text{si } p \text{ se décompose dans } K, \\ -1 & \text{si } p \text{ est inerte dans } K, \end{cases} \tag{5.3.5}$$

et

$$\chi_D(-1) = \begin{cases} 1 & \text{si } K \text{ est quadratique réel ,} \\ -1 & \text{si } K \text{ est quadratique imaginaire} \end{cases} \tag{5.3.6}$$

Exemple 106. Modulo 8, on a $G(8) = (\mathbb{Z}/8\mathbb{Z})^\times$. Son dual est un groupe d'ordre 4, dont les éléments sont
i) le caractère trivial $\mathbf{1}_8$,
ii) le caractère χ_{-4},
iii) le caractère χ_8.
iv) le caractère χ_{-8},

Exercice : a) écrire la "table des caractères de $G(8)$: quelles sont les valeurs que prennent ces caractères sur les éléments de $G(8)$?
b) Quel corps est associé à chacun de ces caractères ?

5.3.2 Factorisations dans le cas quadratique

Nous relions les trois séries de Dirichlet introduites jusqu'ici.

Théorème 107. *Soit K un corps quadratique de discriminant D. Alors*

$$\zeta_K(s) = \zeta(s) L(s, \chi_D). \tag{5.3.7}$$

1. le symbole de Kronecker est une notion un peu délicate ; ce n'est pas toujours un caractère : par exemple χ_3 n'est pas périodique, donc pas un caractère. cf https://web.williams.edu/Mathematics/lg5/Kronecker.pdf. Pour éviter ces pathologies, nous considérons uniquement χ_D lorsque D est un discriminant, ce qui suffit à nos besoins.

Démonstration. Il suffit d'établir cette identité entre trois fonctions méromorphes lorsque $\mathrm{Re}(s) > 1$, domaine où l'on peut comparer les trois produits Eulériens. En regroupant les idéaux premiers $\mathfrak{p}$ de $\mathcal{O}_K$ selon le nombre premier $p \in \mathcal{P}$ qu'ils divisent dans $\mathcal{O}_K$, p ramifié, décomposé ou inerte, on trouve d'abord

$$\zeta_K(s) = \left(\prod_{p|D} \frac{1}{1-p^{-s}}\right)\left(\prod_{p \text{ décomposé}} \frac{1}{(1-p^{-s})^2}\right)\left(\prod_{p \text{ inerte}} \frac{1}{(1-p^{-2s})}\right).$$

D'après (5.3.5), c'est aussi

$$\zeta_K(s) = \left(\prod_{p|D} \frac{1}{1-p^{-s}}\right)\left(\prod_{\chi_D(p)=1} \frac{1}{(1-p^{-s})^2}\right)\left(\prod_{\chi_D(p)=-1} \frac{1}{(1-p^{-2s})}\right).$$

En observant que $1-p^{-2s} = (1-p^{-s})(1+p^{-s})$, il vient

$$\begin{aligned}\zeta_K(s) &= \left(\prod_{p|D} \frac{1}{1-p^{-s}}\right)\left(\prod_{\chi_D(p)=1} \frac{1}{(1-p^{-s})^2}\right)\left(\prod_{\chi_D(p)=-1} \frac{1}{(1-p^{-s})(1+\chi(p)p^{s})}\right)\\ &= \zeta(s)L(s,\chi_D).\end{aligned}$$

□

Exemple 108. 1.

$$\frac{1}{4}\sum_{(m,n)\neq(0,0)} \frac{1}{(m^2+n^2)^s} = \zeta_{\mathbb{Q}(i)}(s) = \zeta(s)\cdot L(s,\chi_{-4}), \tag{5.3.8}$$

qui reflète donc la factorisation des nombres premiers dans l'anneau principal $\mathbb{Z}[i]$.

2.

$$\zeta_{\mathbb{Q}(\sqrt{2})}(s) = \zeta(s)\cdot L(s,\chi_8). \tag{5.3.9}$$

3.

$$\zeta_{\mathbb{Q}(\sqrt{-2})}(s) = \zeta(s)\cdot L(s,\chi_{-8}). \tag{5.3.10}$$

5.3.3 Autres factorisations

Dans cette sous-partie, on donne d'autres exemples, associés à des corps cyclotomiques particuliers. Observer comme le produit porte sur *tous* les caractères modulo $|D|$, ce qui éclaire et motive l'étude de la fonction $\zeta_m(s)$ qui sera introduite plus tard en (5.4.21).

Proposition 109. *Soit $\zeta_8 = e^{\frac{2i\pi}{8}}$. La fonction L du corps cyclotomique $\mathbb{Q}(\zeta_8)$ possède la factorisation*

$$\zeta_{\mathbb{Q}(\zeta_8)}(s) = \zeta(s)L(s,\chi_{-4})L(s,\chi_8)L(s,\chi_{-8}). \tag{5.3.11}$$

Démonstration. cf **TD**. □

Exercice : la fonction zêta du corps cyclotomique $K = \mathbb{Q}(\zeta_5)$, $\zeta_5 = e^{\frac{2i\pi}{5}}$ se factorise de manière similaire à (5.3.11) en un produit de 4 fonctions L de Dirichlet. Trouvez lesquelles, et établissez la factorisation souhaitée.

5.4 Le théorème de progression arithmétique de Dirichlet

Soit $m \geq 2$ un entier, et $a \in \mathbb{Z}$ premier à m : $(a,m) = 1$. Dans cette partie, nous allons démontrer, à la suite de Dirichlet, qu'il y a une infinité de nombres premiers congrus à a modulo m. Commençons par expliquer pourquoi la preuve repose sur le fait que $L(1,\chi) \neq 0$ pour tout caractère χ non-trivial modulo m.

La fonction caractéristique $\mathbf{1}_{a[m]} : \mathbb{Z} \to \mathbb{R}$ des entiers congrus à a modulo m est une combinaison linéaire des caractères sur le groupe $G(m)$: pour un entier $\ell \in \mathbb{Z}$,

$$\sum_{\chi \in \widehat{G(m)}} \chi(\ell a^{-1}) = \begin{cases} \varphi(m) & \text{si } \ell = a \mod m, \\ 0 & \text{si } \ell \neq a \mod m, \end{cases} \tag{5.4.1}$$

en vertu de la formule d'orthogonalité des caractères (Prop. 95).

Commençons par *un énoncé trivial*, qui explique tout de même la stratégie à l'oeuvre : démontrons, de manière inutilement sophistiquée, qu'il y a une infinité *d'entiers* ℓ qui sont congrus à a modulo m. Pour cela, on multiplie l'égalité (5.4.1) par ℓ^{-s} et l'on somme sur tous les entiers $\ell \geq 1$. On obtient la série de Dirichlet absolument convergente suivante, sous-somme de $\zeta(s)$:

$$\varphi(m) \sum_{\ell \geq 1, \ell = a \bmod m} \frac{1}{\ell^s} = \sum_{\ell \geq 1} \sum_{\chi \in \widehat{G(m)}} \chi(\ell a^{-1}) \ell^{-s} \tag{5.4.2}$$

$$= \sum_{\chi \in \widehat{G(m)}} \chi(a)^{-1} L(s,\chi) \tag{5.4.3}$$

$$= L(s, \mathbf{1}_m) + \sum_{\chi \in \widehat{G(m)}, \chi \neq \mathbf{1}_m} \chi(a)^{-1} L(s,\chi), \tag{5.4.4}$$

la dernière égalité consistant à séparer le caractère $\mathbf{1}_m$ trivial modulo m des autres.

L'argument pour montrer que la série du membre de gauche comporte une infinité de termes consiste à dire qu'elle possède un pôle simple en $s = 1$: en effet, dans le membre de droite, le terme $L(s, \mathbf{1}_m)$ possède un pôle simple d'après tandis que les autres termes $L(s,\chi)$ sont holomorphes en $s = 1$ d'après 103.

Pour démontrer le Théorème de progression arithmétique, la stratégie est similaire, mais l'argument plus délicat car il s'agit de détecter les ℓ qui sont des *nombres premiers* p congrus à a modulo m. Il faut pour cela modifier les poids dont on affuble l'égalité (5.4.1), en introduisant la fonction de von Mangoldt

$$\Lambda(\ell) = \begin{cases} \log p \text{ si } \ell = p^k \text{ est la puissance d'un nombre premier } p, \\ 0 \text{ sinon.} \end{cases}$$

En prenant le logarithme terme à terme des produits Eulériens 101 on trouve

$$\log \zeta(s) = \sum_{n\geq 2} \frac{\Lambda(n)}{\log n} n^{-s}, \tag{5.4.5}$$

$$\log L(s,\chi) = \sum_{n\geq 2} \frac{\Lambda(n)\chi(n)}{\log n} n^{-s}. \tag{5.4.6}$$

Par dérivation on en déduit

$$\frac{\zeta'(s)}{\zeta(s)} = -\sum_{n\geq 2} \frac{\Lambda(n)}{n^s}, \tag{5.4.7}$$

$$\frac{L'(s,\chi)}{L(s,\chi)} = -\sum_{n\geq 2} \frac{\Lambda(n)\chi(n)}{n^s}. \tag{5.4.8}$$

On multiplie l'égalité (5.4.1) par $\Lambda(\ell)/\ell^s$, et l'on somme pour $\mathrm{Re}(s) > 1$ sur les entiers $\ell \geq 1$ pour trouver

$$\varphi(m) \sum_{\ell\geq 1, \ell = a \bmod m} \frac{\Lambda(\ell)}{\ell^s} = -\sum_{\chi \in \widehat{G(m)}} \chi(a)^{-1} \frac{L'(s,\chi)}{L(s,\chi)} \tag{5.4.9}$$

$$= -\frac{L'(s,\mathbf{1}_m)}{L(s,\mathbf{1}_m)} - \sum_{\chi \in \widehat{G(m)}, \chi \neq \mathbf{1}_m} \chi(a)^{-1} \frac{L'(s,\chi)}{L(s,\chi)} \tag{5.4.10}$$

En prenant la dérivée logarithmique du produit (5.2.10), le premier terme du membre de droite n'est autre que

$$\frac{L'(s,\mathbf{1}_m)}{L(s,\mathbf{1}_m)} = \frac{\zeta'(s)}{\zeta(s)} + \sum_{p|m} \frac{\log p}{p^s - 1}, \tag{5.4.11}$$

et la somme finie est une fonction élémentaire holomorphe en $s = 1$. Comme $\zeta(s) = \frac{1}{s-1} + O(1)$ au voisinage de $s = 1$ et que les $L(s,\chi)$ sont des fonctions holomorphes en $s = 1$, on en déduit, **à condition de prouver que** $L(1,\chi) \neq 0$, que

$$\varphi(m) \sum_{k\geq 1} \sum_{p\in\mathcal{P},\, p = a \bmod m} \frac{\log p}{p^{ks}} = \frac{1}{s-1} + O(1) \tag{5.4.12}$$

au voisinage de $s = 1$. Pour ce qui est du membre de gauche, le morceau $\psi(s) = \sum_{k\geq 2} \sum_{p\in\mathcal{P},\, p = a \bmod m} \frac{\log p}{p^{ks}}$ est majoré (en notant $\sigma = \mathrm{Re(s)} \geq 1$) par

$$|\psi(s)| \leq \sum_{p\in\mathcal{P}} \sum_{k\geq 2} \frac{\log p}{p^{k\sigma}} = \sum_{p\in\mathcal{P}} \frac{\log p}{p^{\sigma}(p^{\sigma}-1)} \tag{5.4.13}$$

$$\leq \sum_{n\geq 2} \frac{\log n}{n^{\sigma}(n^{\sigma}-1)} \tag{5.4.14}$$

$$\leq \sum_{n\geq 2} \frac{\log n}{n(n-1)}, \tag{5.4.15}$$

de sorte que $\psi(s)$ est bornée (critère de Riemann)au voisinage de $s=1$.

En regroupant les informations obtenues, l'égalité (5.4.12) peut s'écrire au voisinage de $s=1$ sous la forme

$$\sum_{p\in\mathcal{P},\, p=a \bmod m} \frac{\log p}{p^s} = \frac{\frac{1}{\varphi(m)}}{s-1} + O(1), \tag{5.4.16}$$

à condition de prouver que $L(1,\chi)\neq 0$. Cette dernière estimée (5.4.16) implique qu'il y a une infinité de nombres premiers congrus à a modulo m, ce qui est le Théorème de progression arithmétique de Dirichlet. [2] La fin de cette partie 5.4 est consacrée à donner une (première) démonstration du point crucial qui manque encore, à savoir que que $L(1,\chi)\neq 0$ lorsque χ est un caractère de Dirichlet non trivial modulo m. Ce résultat est obtenu dans le Théorème 112.

5.4.1 Produit de tous les caractères modulo m

Soit $m\geq 1$ un entier, et $G(m)=(\mathbb{Z}/m\mathbb{Z})^{\times}$ le groupe multiplicatif des élements inversibles modulo m. Son cardinal, et donc le cardinal de son dual $\widehat{G(m)}$, est $\varphi(m)$. Pour tout nombre premier p qui ne divise pas m, on note $f(p)$ l'ordre de p dans $G(m)$. Par définition, $f(p)$ est le plus petit entier >0 tel que $p^f=1$ modulo m. On pose ensuite $g(p)=\frac{\varphi(m)}{f(p)}$. C'est l'ordre du groupe quotient $G(m)/<\overline{p}>$.

Lemme 110. *Si $p\nmid m$, on a l'identité*

$$\prod_{\chi\in\widehat{G(m)}} (1-\chi(p)T) = \left(1-T^{f(p)}\right)^{g(p)}. \tag{5.4.17}$$

Démonstration. Le polynôme $1-T^f$ se scinde en

$$1-T^f = \prod_{w\in\mu_f} (1-wT).$$

2. On notera que l'asymptotique du membre de droite est indépendant de a, les nombres premiers sont équirépartis, en un sens à préciser, entre toutes les classes a possibles. En précisant le terme asymptotique $O(1)$, il est possible de préciser s'il y a un *biais* qui favorise certaines classes a. Voir l'article de Granville-Martin (2004) https://dms.umontreal.ca/~andrew/PDF/PrimeRace.pdf pour plus de détails, un panorama historique et de jolies figures. Par exemple pour $m=3$, les premiers de la forme $4n+3$ mènent la course devant ceux de la forme $4n+1$ (au sens de Rubinstein-Sarnak), c'est le *biais de Tchebychev*.

D'après la preuve du Lemme de prolongement des caractères avec $H =< \overline{p} >$, pour chaque racine de l'unité $w \in \mu_{f(p)}$, il y a $g(p)$ caractères χ sur $G(m)$ tels que $\chi(\overline{p}) = w$. Le Lemme s'ensuit. □

5.4.2 Le lemme de Landau

On va faire usage du critère suivant de convergence des séries de Dirichlet *à coefficients positifs.*

Proposition 111. *(Landau) Soit $F(s) = \sum_{n\geq 1} \frac{c_n}{n^s}$ une série de Dirichlet à coefficients réels positifs $c_n \geq 0$. On suppose que la série $F(s)$ converge pour $Re\, s > \rho$, et que, comme fonction de la variable s, elle se prolonge en une fonction holomorphe sur un voisinage ouvert de $s = \rho$. Alors il existe $\epsilon > 0$ tel que la série définissant $F(s)$ converge pour $Re(s) > \rho - \epsilon$.*

(Autrement dit, le domaine de convergence de la série de Dirichlet $F(s)$ est borné par une singularité de F localisée sur l'axe réel).

Démonstration. Par translation, on se ramène à $\rho = 0$, de sorte que $F(s)$ est développable en série entière sur une boule ouverte centrée en 0, ainsi que sur le domaine $\mathrm{Re}(s) > 0$, donc sur un disque $D = \{s \in \mathbb{C}, |s-1| \leq 1+\epsilon\}$ pour un $\epsilon > 0$ (faire un dessin). Elle est donc égale à sa série de Taylor sur ce disque centré en $s = 1$, autrement dit

$$F(s) = \sum_{p\geq 0} \frac{(s-1)^p}{p!} F^{(p)}(1) \tag{5.4.18}$$

sur D. La dérivée $F^{(p)}(1)$ se calcule en dérivant terme à terme la série de Dirichlet normalement convergente qui définit F :

$$F^{(p)}(1) = \sum_{n\geq 1} c_n (-1)^p \frac{(\log n)^p}{n}.$$

En reportant dans (5.4.18) et en évaluant en $s = -\epsilon \in D$, il vient

$$F(-\epsilon) = \sum_{p\geq 0} \sum_{n\geq 1} c_n \frac{(\epsilon+1)^p}{p!} (\log n)^p \frac{1}{n}. \tag{5.4.19}$$

Cette série double, *à termes positifs*, est donc convergente. On échange les ordres de sommation (Fubini), et en utilisant $\sum_{p\geq 0} \frac{(\epsilon+1)^p}{p!} (\log n)^p = e^{(\epsilon+1)\log n} = n^{\epsilon+1}$, il vient

$$F(-\epsilon) = \sum_{n\geq 1} c_n n^{1+\epsilon} n^{-1} = \sum_{n\geq 1} c_n n^{\epsilon}. \tag{5.4.20}$$

La série initiale converge donc en $s = -\epsilon$, donc aussi pour $\mathrm{Re}(s) > -\epsilon$. □

5.4.3 où $L(1,\chi) \neq 0$

On définit maintenant une nouvelle fonction méromorphe en posant

$$\zeta_m(s) = \prod_{\chi} L(s,\chi), \tag{5.4.21}$$

où le produit porte sur tous les caractères χ sur $G(m)$. Au vu des exemples de la partie 5.3.3, on devine que cette fonction n'est autre que la fonction zêta de Dedekind du corps cyclotomique $K = \mathbb{Q}\left(e^{\frac{2i\pi}{m}}\right)$:

$$\zeta_m(s) = \zeta_{\mathbb{Q}\left(e^{\frac{2i\pi}{m}}\right)}(s). \tag{5.4.22}$$

La démonstration de cette identité dépasse (de peu) les techniques introduites dans ce cours. On se contentera donc de la définition (5.4.21), un peu ad-hoc, de $\zeta_m(s)$. Les propriétés a,b,c) du Théorème suivant ne doivent cependant pas nous étonner si l'on se rappelle que c'est (secrètement) une fonction zêta de Dedekind.

Théorème 112. *a) La fonction ζ_m est une fonction méromorphe sur le demi-plan $Re(s) > 0$.*

b) Sur le domaine $Re(s) > 1$, c'est une série de Dirichlet à coefficients ≥ 0.

c) Elle possède un pôle simple en $s = 1$.

d) $L(1,\chi) \neq 0$ pour tout caractère $\chi \neq \mathbf{1}$.

Démonstration. D'après le Lemme 110, le produit Eulérien issu de 101 de chaque $L(s,\chi)$ permet d'écrire (pour $\mathrm{Re}(s) > 1$, en choisissant $T = p^{-s}$)

$$\zeta_m(s) = \prod_{\chi} \prod_{p\in\mathcal{P}} \left(1 - \chi(p)p^{-s}\right)^{-1} \tag{5.4.23}$$

$$= \prod_{p\in\mathcal{P}, p\nmid m} \left(1 - p^{-f(p)s}\right)^{-g(p)} \tag{5.4.24}$$

$$= \prod_{p\in\mathcal{P}, p\nmid m} \left(\sum_{k\geq 0} \frac{1}{p^{kf(p)s}}\right)^{g(p)}. \tag{5.4.25}$$

En développant ce dernier produit infini, on obtient clairement une série de Dirichlet $\sum_{n\geq 1} \frac{b_n}{n^s}$ avec des coefficients b_n entiers ≥ 0. Ceci établit b).

a) résulte de ce que $L(s,\chi)$ et $\zeta(s)\prod_{p|m}(1-p^{-s})$ sont des fonctions méromorphes sur ce domaine d'après la Prop. 99 et le Cor. 103.

Le seul pôle éventuel de $\zeta_m(s)$ provient de celui de $\zeta(s)\prod_{p|m}(1-p^{-s})$ en $s = 1$, donc d) implique c).

Il reste donc à établir d), en procédant par l'absurde. Si $L(1,\chi) = 0$ pour un caractère non-trivial, alors $\zeta_m(s)$ serait une fonction holomorphe en $s = 1$, car ce zéro viendrait compenser le pôle simple de $\zeta(s)$. Mais alors $\zeta_m(s)$ serait holomorphe sur au moins tout le demi-plan $\mathrm{Re}(s) > 0$. D'après le critère 111, la série de Dirichlet à coefficients positifs qui coïncide avec

$\zeta_m(s)$ pour $\mathrm{Re}(s) > 1$ devrait converger sur le domaine plus grand $\mathrm{Re}(s) > 0$. Or le facteur en p est

$$\left(1 - p^{-f(p)s}\right)^{-g(p)} = \left(\sum_{k\geq 0} \frac{1}{p^{kf(p)s}}\right)^{g(p)},$$

et comme $f(p)g(p) = \varphi(m)$, ce facteur domine la série

$$1 + \frac{1}{p^{\varphi(m)s}} + \frac{1}{p^{2\varphi(m)s}} + \ldots = \frac{1}{1 - p^{s\varphi(m)}}.$$

Il s'ensuit que $\zeta_m(s)$ domine, pour $s > 0$, la fonction

$$\prod_{p\in\mathcal{P}, p\nmid m} \left(\frac{1}{1 - p^{s\varphi(m)}}\right) = \zeta(s\varphi(m)) \prod_{p|m} \left(1 - p^{-s}\right).$$

Comme la série de Dirichlet associée à $\zeta(s\varphi(m)) \prod_{p|m} \left(1 - p^{-s\varphi(m)}\right)$ diverge en $s = \frac{1}{\varphi(m)}$, ceci amène la contradiction attendue. □

5.5 Autres preuves de $L(1, \chi) \neq 0$

Originellement, la preuve de Dirichlet du Théorème de progression arithmétique diffère légèrement de celle exposée jusqu'ici : il démontre que $L(1, \chi) \neq 0$ en séparant le cas où le caractère χ est à valeurs complexes, de celui où χ est à valeurs réelles (pour lequel il établit la *formule du nombre de classes*, qui montre que la *valeur* $L(1, \chi)$ elle-même renferme des informations arithmétiques profondes.

5.5.1 Le cas d'un caractère complexe.

Proposition 113. *Soit χ un caractère modulo m non trivial, tel que $\chi \neq \overline{\chi}$. Alors $L(1, \chi) \neq 0$.*

Démonstration. On choisit $a = 1$ dans l'identité (5.4.1), équipée des poids $\frac{\Lambda(\ell)}{\ell^s \log \ell}$. En combinant avec (5.4.6), il vient

$$\varphi(m) \sum_{\ell\geq 1, \ell = 1 \bmod m} \frac{\Lambda(\ell)}{\ell^s \log \ell} = \sum_{\chi\in\widehat{G(m)}} \log L(s, \chi) \tag{5.5.1}$$

Pour $s > 1$ réel, le membre de gauche est ≥ 0. En prenant l'exponentielle, il s'ensuit que

$$\left| \prod_{\chi\in\widehat{G(m)}} L(s, \chi) \right| \geq 1. \tag{5.5.2}$$

Par ailleurs, lorsque s est réel $\overline{L(s, \chi)} = L(s, \overline{\chi})$, de sorte que $L(1, \chi) = 0$ implique $L(1, \overline{\chi}) = 0$. Sous l'hypothèse $\chi \neq \overline{\chi}$, ces deux caractères distincts modulo m contribuent au produit (5.5.2). Dans ce produit, les deux termes $L(s, \chi)$ et $L(s, \overline{\chi})$ s'annuleraient en $s = 1$, tandis que le caractère trivial $\mathbf{1}_m$ contribue pour un pôle simple d'après 103.b). Ainsi le membre de gauche de l'inégalité (5.5.2) tend vers 0 quand s réel tend vers 1, contradiction. □

5.5.2 Cas d'un caractère réel

D'après la Prop. 113, il reste à démontrer que $L(1,\chi) \neq 0$ lorsque χ est un caractère non-trivial à valeurs réelles, i.e. $\chi^2 = \mathbf{1}_m$. Comme Dirichlet, nous traitons dans cette sous-partie le cas de certains caractères de Kronecker.

5.5.3 La formule de Dirichlet pour les corps quadratiques imaginaires

Théorème 114. *Soit K un corps quadratique imaginaire de discriminant $D < 0$, de nombre de classes $h(D)$, avec w_D racines de l'unités. Alors au voisinage de $s = 1$,*

$$\zeta_K(s) = \frac{2\pi h(D)}{w_D\sqrt{|D|}}\frac{1}{(s-1)} + O(1), \tag{5.5.3}$$

$$L(1,\chi_D) = \frac{2\pi h(D)}{w_D\sqrt{|D|}}. \tag{5.5.4}$$

En particulier, $L(1,\chi_D) > 0$.

Démonstration. Les deux formules sont équivalentes à cause de la factorisation (107). On démontre la première formule, en découpant la preuve en plusieurs lemmes. Pour chaque classe C du groupe des classes de $\mathcal{O}_K$ et chaque entier $n > 0$, on dénombre les idéaux entiers de la classe C de norme n :

$$a_{n,C} = \mid \{I \in C, \mathrm{N}(I) = n\} \mid,$$

de sorte que

$$\zeta_K(s) = \sum_{C\in \mathrm{Cl}(\mathcal{O}_K)} \sum_{n\geq 1} \frac{a_{n,C}}{n^s}. \tag{5.5.5}$$

Lemme 115. *Pour chaque classe C de $Cl(\mathcal{O}_K)$, on a*

$$\sum_{k=1}^{n} a_{k,C} = \frac{2\pi n}{w_D\sqrt{|D|}} + O(\sqrt{n}). \tag{5.5.6}$$

Ce lemme implique la formule (5.5.3), puisque si l'on pose

$$\sum_{n\geq 1} \frac{b_n}{n^s} = \zeta_K(s) - \frac{2\pi h(D)}{w_D\sqrt{|D|}}\zeta(s),$$

il assure que $\sum_{k\leq n} b_k = O(\sqrt{n})$. D'après le lemme 102, cette estimation entraîne que $\zeta_K(s) - \frac{2\pi h(D)}{w_D\sqrt{|D|}}\zeta(s)$ est holomorphe sur le demi-plan $\mathrm{Re}(s) > \frac{1}{2}$, d'où l'asymptotique (5.5.3).

Il reste donc à démontrer le Lemme 115. On se ramène au cas des idéaux principaux grâce au principe qui suit :

Lemme 116. *Soit C une classe d'idéaux d'un corps de nombres K, et J un idéal entier dans la classe C^{-1}. Alors l'application $I \mapsto IJ$ est une bijection des idéaux de la classe C de norme n vers les idéaux principaux de $\mathcal{O}_K$ contenus dans J et de norme $n\mathrm{N}(J)$.*

En effet, $[I][J] = 1$ donc IJ est un idéal principal, qui contenu dans J, et sa norme est $n\mathrm{N}(J)$. L'application est injective car J est inversible, et elle est surjective : lorsque $I' \subset J$ est principal de norme $n\mathrm{N}(J)$, l'idéal $I = J^{-1}I'$ est un antécédent convenable.

Muni de la bijection issue de 116, on peut fixer un idéal J dans la classe C^{-1}. Il suffit pour démontrer (5.5.6) de dénombrer les idéaux principaux (z) contenus dans J et de norme $\leq n\mathrm{N}(J)$. Il y a w_D choix possibles de générateur pour l'idéal (z). Quitte à diviser le résultat par w_D, il suffit donc de dénombrer les éléments $z \in J$ de norme $|z|^2 \leq n\mathrm{N}(J)$. L'image de l'idéal J par le plongement canonique $\iota : K \to \mathbb{C}$ est un réseau de covolume covol $\iota(J) = \frac{\mathrm{N}(J)\sqrt{|D|}}{2}$ (voir 83). On conclut grâce au lemme suivant (pour lequel un dessin aide), appliqué avec $L = \iota(J)$ et $r = \sqrt{n\mathrm{N}(J)}$.

Lemme 117. *Soit $L \subset \mathbb{C}$ un réseau, et $f(r)$ le nombre de points de L dans la boule fermé $\overline{B}(0,r)$. Alors*

$$f(r) = \frac{\pi r^2}{covol(L)} + O(r) \text{ quand } r \to \infty.$$

□

5.5.4 Carrés de l'intervalle $[1, \frac{p-1}{2}]$.

Pour chaque nombre premier impair q, il y a autant de carrés que de non-carrés modulo q. La question qui va nous intéresser ici est de savoir comment se comporte cette répartition si on se restreint aux représentants dans la première moitié de l'intervalle, i.e. dans $[1, \frac{q-1}{2}]$.

Pour cela, on note $C = C(q)$ le nombre d'éléments dans $[1, \frac{q-1}{2}]$ qui sont des carrés modulo q, et $N = N(q)$ le nombre de non-carrés, de sorte que $C + N = \frac{q-1}{2}$.

La table suivante compare, lorsque q est congru à 3 modulo 4, la valeur de $C - N$ à celle du nombre de classe $h(-q)$ du corps quadratique imaginaire $K = \mathbb{Q}(\sqrt{-q})$.

q	3	7	11	19	23	31	43	47	59	67	71	79	83	103	107	127	131	139	151	163
$C - N$	1	1	3	3	3	3	3	5	9	3	7	5	9	5	9	5	15	9	7	3
$h(-q)$	1	1	1	1	3	3	1	5	3	1	7	5	3	5	3	5	5	3	7	1

Valeur de $C - N$ et $h(-q)$ pour $q = 3$ modulo 4 , $q \leq 163$.

On observe deux faits notables :

a) $C(q) - N(q)$ semble être toujours > 0 : il y a toujours plus de carrés que de non-carrés dans l'intervalle $[1, \frac{q-1}{2}]$.

b) $C(q) - N(q)$ semble corrélé à $h(-q)$, ou à $3h(-q)$.

Les observations a) et b) font précisément l'objet du résultat remarquable suivant. Sa démonstration occupe le reste de cette partie.

Théorème 118. *(Dirichlet) Soit $q > 3$ un nombre premier congru à 3 modulo 4, et K le corps quadratique imaginaire $K = (\sqrt{-q})$, de discriminant $D = -q$ et de nombre de classes $h(-q)$. Alors le caractère de Dirichlet associé au corps quadratique K est le symbole de Legendre $\chi_{-q}(a) = \left(\frac{a}{q}\right)$, et l'on a*

$$L(1, \chi_{-q}) = \frac{\pi}{\left(2 - \left(\frac{2}{q}\right)\right)} \frac{\sum_{a=1}^{\frac{q-1}{2}} \left(\frac{a}{q}\right)}{\sqrt{q}}, \quad \textit{de sorte que} \tag{5.5.7}$$

$$h(-q) = \frac{C - N}{2 - (-1)^{\frac{q^2-1}{8}}} > 0. \tag{5.5.8}$$

Démonstration. Le symbole de Kronecker χ_{-q} coïncide avec le symbole de Legendre modulo q d'après la loi de réciprocité quadratique (cf **TD10, Ex. 3.2**). La valeur $\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}}$ provient de (1.4.2). Ainsi la formule (5.5.8) se déduit de la combinaison de (5.5.7) et de (5.5.4), en notant que $w_{-q} = 2$ puisque l'équation diophantienne $x^2 + qy^2 = 1$ n'a que deux solutions lorsque $q > 3$.

La suite de la preuve s'attache donc à établir la formule (5.5.7). Soit $\zeta = e^{\frac{2i\pi}{q}}$, et $\log : \mathbb{C}^* \to \mathbb{C}$ la branche principale du logarithme complexe, dont la partie imaginaire est dans $[-\pi, \pi[$. Comme les sommes partielles $\sum_{k=N}^{M} \zeta^k$ sont bornées, le Lemme 102 montre que la série $\sum_{n\geq 1} \frac{\zeta^n}{n}$ est convergente (pas absolument, mais uniformément sur le segment $[0, \zeta]$), et le lemme de la limite radiale d'Abel assure que, pour $1 \leq a < q$,

$$\sum_{n\geq 1} \frac{\zeta^{an}}{n} = \lim_{z \to \zeta^a, |z|<1} \sum_{n\geq 1} \frac{z^n}{n} \tag{5.5.9}$$

$$= \lim_{z \to \zeta^a, |z|<1} -\log(1 - z) \tag{5.5.10}$$

$$= -\log(1 - \zeta^a) \tag{5.5.11}$$

$$= -\log(2 \sin \frac{\pi a}{q}) - i\pi \left(\frac{a}{q} - \frac{1}{2}\right), \tag{5.5.12}$$

la dernière égalité étant obtenue en écrivant séparément partie réelle et imaginaire de $1 - \zeta^a$.

Introduisons un dernier outil fondamental nécessaire, la **somme de Gauss** associée à un caractère χ modulo q :

$$G(\chi) = \sum_{a=1}^{q-1} \chi(a)\zeta^a, \tag{5.5.13}$$

et énonçons deux résultats sur ce nombre complexe : un changement de variable élémentaire $a' = ak$ assure que

$$\chi(n) = \frac{1}{G(\chi)} \sum_{a=1}^{q-1} \chi(a)\zeta^{an}. \tag{5.5.14}$$

Il n'est pas si difficile de trouver le module de la somme de Gauss du caractère χ_{-q},

$$G^2(\chi_{-q}) = -q,$$

tandis qu'un résultat profond de Gauss (1805) (cela lui a demandé 4 ans de recherches en y pensant chaque semaine !) donne son "signe" : (cf **TD12** pour la preuve élégante due à Dirichlet) :

$$\boxed{G(\chi_{-q}) = i\sqrt{q}}. \tag{5.5.15}$$

Ainsi équipés, on peut calculer

$$\begin{aligned} L(1,\chi_{-q}) &= \lim_{N\to\infty} \sum_{n=1}^{Nq} \frac{\chi_{-q}(n)}{n} && (5.5.16)\\ &= \lim_{N\to\infty} \frac{1}{G(\chi_{-d})} \sum_{a=1}^{q-1} \left(\frac{a}{q}\right) \sum_{n=1}^{Nq} \frac{\zeta^{an}}{n} && (5.5.17)\\ &= \frac{1}{i\sqrt{q}} \sum_{a=1}^{q-1} \left(\frac{a}{q}\right) \left[-\log(2\sin\frac{\pi a}{q}) - i\pi\left(\frac{a}{q} - \frac{1}{2}\right)\right] && (5.5.18)\\ &= \frac{1}{i\sqrt{q}} \sum_{a=1}^{q-1} \left(\frac{a}{q}\right) \left[-\log(2\sin\frac{\pi a}{q}) - \frac{i\pi a}{q}\right], && (5.5.19) \end{aligned}$$

la dernière identité provenant de ce que $\sum_{a=1}^{q-1}\left(\frac{a}{q}\right) = 0$. Le changement de variable $a \mapsto q-a$ adjoint à la propriété $\left(\frac{-1}{q}\right) = -1$ (parce que $q \equiv 3[4]$) permet ensuite d'écrire

$$\begin{aligned} L(1,\chi_{-q}) &= -\frac{\pi}{q\sqrt{q}} A, && (5.5.20)\\ A &= \sum_{a=1}^{q-1} \left(\frac{a}{q}\right) a. && (5.5.21) \end{aligned}$$

En posant $A' = \sum_{a=1}^{\frac{q-1}{2}} \left(\frac{a}{q}\right) a$ et $B = \sum_{a=1}^{\frac{q-1}{2}} \left(\frac{a}{q}\right)$, on voit que

$$\begin{cases} A = A' + \sum_{a=1}^{\frac{q-1}{2}} \left(\frac{q-a}{q}\right)(q-a) = 2A' - qB, \\ A = \sum_{a=1}^{\frac{q-1}{2}} \left(\frac{2a}{q}\right) 2a + \sum_{a=1}^{\frac{q-1}{2}} \left(\frac{q-2a}{q}\right)(q-2a) = 4\left(\frac{2}{q}\right) A' - q\left(\frac{2}{q}\right) B. \end{cases}$$

On en tire A en fonction de B seul, et en reportant dans (5.5.20), on trouve finalement (5.5.7). □

Bibliographie

[Ber] D. Bertrand. *cours de Master de théorie des nombres*. polycopié Paris 6.

[Che] G. Chenevier. *Un cours de théorie des nombres à Polytechnique*. à paraître.

[Pol] A. Pollack. *A conversational introduction to algebraic number theory* AMS (2017)

[Ser] J.P. Serre. *Cours d'arithmétique*. PUF