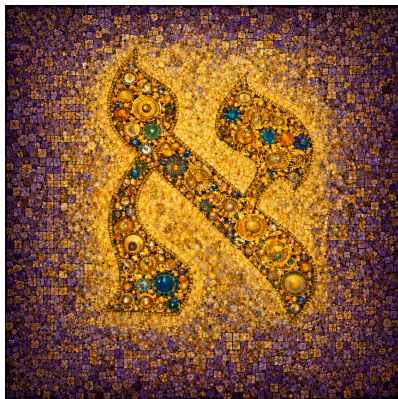




Cours articulé
de
mathématiques

IV

Correspondances

DU CORPS DE CLASSES AU PROGRAMME DE LANGLANDS

William de France

ÉDITIONS CLEMENTINIUM

Clem

CORRESPONDANCES

*Les problèmes de mathématiques ne sont pas isolés les uns des autres. Il y a
un vaste réseau de connexions.*

ROBERT LANGLANDS

Cours articulé de mathématiques

IV

Correspondances

DU CORPS DE CLASSES AU PROGRAMME DE LANGLANDS

William de France

ÉDITIONS CLEMENTINIUM

Copyright © 2026 William de France

ÉDITIONS CLEMENTINIUM

Collection COURS ARTICULÉ DE MATHÉMATIQUES

Tous droits réservés.

AVANT-PROPOS

Une même équation peut être lue par ses solutions, par ses symétries ou par les fonctions qui en enregistrent les traces. Le programme de Langlands demande comment passer entre de telles descriptions sans perdre les opérations qui leur donnent un sens. Ce volume suit cette question depuis les corps de nombres jusqu'à la correspondance géométrique et au parcours de sa preuve de 2024.

Les Correspondances ouvrent, avec la Physique mathématique, le cycle de recherche du Cours articulé de mathématiques. Elles supposent les acquis de la Maîtrise, notamment la théorie de Galois, l'analyse fonctionnelle et la géométrie différentielle. Les outils algébriques et géométriques plus spécialisés sont introduits lorsqu'une question les rend nécessaires. Le livre s'adresse au lecteur qui veut comprendre comment les domaines se relient, puis retrouver dans les sources les constructions et les preuves complètes.

Le parcours comprend trente-sept chapitres et deux cent trente-huit articles, distribués en huit parties. La première établit les langages local et global de l'arithmétique et la réciprocité. La deuxième construit les formes modulaires, les fonctions L , les groupes ad aux et les représentations automorphes. La troisième développe la géométrie arithmétique jusqu'à la modularité, aux périodes et aux valeurs spéciales. La quatrième examine les méthodes et les réalisations du programme arithmétique; la cinquième approfondit les variétés de Shimura, les motifs et la géométrie p -adique.

Les trois dernières parties changent les objets de la correspondance. Modules différentiels, champs de fibrés et catégories dérivées préparent l'énoncé géométrique. Le cas abélien fournit un calcul directeur; Hecke et Satake conduisent ensuite au théorème général. Les chapitres consacrés à la preuve distinguent la construction du foncteur, les compatibilités locales et globales, puis le contrôle qui rend ce foncteur équivalent. Le dernier chapitre ouvre vers la physique par les charges, les lignes et les branes.

La distinction entre ces parcours fait partie du propos. Le théorème géométrique de Rham non ramifié n'est pas la résolution de tout le programme

arithmétique. Son interprétation physique ne démontre pas à elle seule une dualité de théories de jauge. Les hypothèses, les normalisations et la nature des catégories sont donc conservées dans les énoncés. Les résultats difficiles sont identifiés comme admis lorsque l'article en explique le rôle plutôt qu'il n'en reproduit la démonstration.

L'article demeure l'unité de lecture : une question, une construction, un exemple calculé et son interprétation. Les renvois numérotés permettent de retrouver un acquis sans recommencer son exposition. Les lectures complémentaires orientent vers les sources ; les questions de recherche qui clôturent les chapitres prolongent un calcul, mettent à l'épreuve une distinction ou situent une conjecture. Elles ne sont pas toutes des problèmes ouverts : leur rôle est de donner au lecteur une opération à poursuivre.

Les objets familiers reviennent avec de nouvelles fonctions. Dans $\mathbb{Q}(\sqrt{2})$, les entiers, les unités et les places font travailler ensemble algèbre et arithmétique. Une courbe elliptique porte des points rationnels, des modules de Tate et une fonction L . Le groupe GL_2 permet de comparer une représentation, une forme automorphe et une modification de fibré. Ces retours rendent sensible la continuité de la collection.

Un dictionnaire ne devient utile que lorsqu'il conserve ce que les phrases permettent de faire. La limite de cette image est essentielle : rapprocher des noms ne construit pas une correspondance. C'est en suivant les opérations, leurs compatibilités et leurs preuves que le lecteur pourra mesurer ce que les différents langages ont appris à se transmettre.

AU LECTEUR

Ce cours articule en cinq volumes la grammaire par laquelle la réalité se compose elle-même : plus de mille trois cents articles de mathématiques, du premier nombre entier à la correspondance de Langlands et de la brachistochrone à l'amplituèdre. L'entreprise est vaste. L'auteur ne prétend pas qu'elle soit sans défauts ; il affirme qu'elle est sincère.

Chaque article développe une seule idée, de sa motivation à son interprétation. Les définitions sont encadrées ; les théorèmes majeurs le sont également, en rouge, dans les volumes 2 et 3 de la collection. Les preuves sont présentes là où elles éclairent, esquissées là où la rigueur complète aurait obscurci le propos, et admises lorsque leur difficulté excède le cadre de l'article. Le lecteur saura distinguer les trois cas.

Dix objets mathématiques traversent la collection comme des fils rouges : le cercle S^1 , les entiers $\mathbb{Z}$, l'extension $\mathbb{Q}(\sqrt{2})$, la courbe elliptique $y^2 = x^3 - x$, le groupe GL_2 , la fonction $\zeta(s)$, l'espace L^2 , l'anneau $K[X]$, le groupe symétrique $\mathfrak{S}_3$, et le tore T^2 . Du calcul trigonométrique au groupe dual de Langlands, de l'oscillateur harmonique à la dualité de Montonen-Olive, chacun de ces objets réapparaît à chaque cycle avec une profondeur nouvelle. Quand l'un se manifeste, le texte le signale.

Les figures, plus de huit cents au total, ont été dessinées avec le soin qu'exige un format de poche : chaque trait a une raison d'être, chaque label est dégagé de toute courbe, et la palette se limite à quatre couleurs. Elles ne remplacent pas la démonstration ; elles la précèdent. Le lecteur qui regarde la figure avant de lire le théorème comprendra souvent l'énoncé avant d'en avoir lu un mot.

Chaque chapitre se prolonge par des Lectures complémentaires, choisies pour rejoindre les sources et approfondir les constructions, puis par des Questions de recherche. Celles-ci invitent à prolonger un exemple, préciser une hypothèse ou comparer deux opérations. Lorsqu'une conjecture intervient, son statut est distingué des résultats démontrés ; toutes ces questions ne sont pas des problèmes ouverts au sens de la recherche actuelle.

Le lecteur peut suivre le chemin linéaire ou emprunter les passages transversaux entre volumes. Les volumes I à III forment une progression continue du lycée à la maîtrise. Le volume IV s'élève vers le programme de Langlands; le volume V, vers la physique mathématique. Tous deux supposent le volume III mais peuvent se lire indépendamment l'un de l'autre.

Toute erreur signalée est une erreur corrigée.

wdf@clementinium.com

NOTE SUR LES CYCLES

Les cinq volumes de la collection accompagnent une progression, des premiers objets mathématiques aux questions de recherche :

- *Éléments (I) : les mathématiques de l'enseignement secondaire, de l'arithmétique aux premières preuves.*
- *Licence (II) : les fondements des études universitaires de mathématiques.*
- *Maîtrise (III) : les approfondissements et la préparation à la recherche.*
- *Correspondances (IV) : le cycle de recherche, du corps de classes au programme de Langlands.*
- *Physique mathématique (V) : le cycle de recherche, des symétries aux cordes.*

Ces niveaux orientent la lecture sans imposer un calendrier universitaire. Les parties et les chapitres donnent les étapes du parcours ; le rythme dépend des acquis du lecteur et des questions qu'il souhaite approfondir.

Les volumes I, II et III construisent successivement les prérequis qui permettent d'aborder le suivant. Le lecteur peut entrer directement au niveau dont il possède les acquis. Les volumes IV et V partagent le socle de la Maîtrise et peuvent être lus indépendamment l'un de l'autre. Les passerelles en début de volume précisent le changement de perspective.

NOTATIONS

$\mathbb{N}$	<i>entiers naturels</i>
$\mathbb{Z}$	<i>entiers relatifs</i>
$\mathbb{Q}$	<i>nombres rationnels</i>
$\mathbb{R}$	<i>nombres réels</i>
$\mathbb{C}$	<i>nombres complexes</i>
$\in$	<i>appartient à</i>
$\subset$	<i>inclus dans</i>
$\cup, \cap, \emptyset$	<i>réunion, intersection, ensemble vide</i>
$\mathcal{P}(E)$	<i>ensemble des parties de E</i>
$\forall, \exists$	<i>pour tout, il existe</i>
$\Rightarrow, \Leftrightarrow$	<i>implique, équivaut à</i>
$ x $	<i>valeur absolue de x</i>
$\sqrt{x}$	<i>racine carrée de x</i>
$\leq, \geq$	<i>inférieur ou égal, supérieur ou égal</i>
π	<i>rapport de la circonférence au diamètre</i>
∞	<i>infini</i>
$\sin, \cos, \tan$	<i>fonctions trigonométriques</i>
$f'(x)$	<i>dérivée de f en x</i>
$\int_a^b f(x) dx$	<i>intégrale de f de a à b</i>
$\sum, \prod$	<i>somme, produit</i>
$n!, \binom{n}{k}$	<i>factorielle, coefficient binomial</i>
i	<i>unité imaginaire, $i^2 = -1$</i>
$\bar{z}, z , \arg(z)$	<i>conjugué, module, argument</i>
$\operatorname{Re}(z), \operatorname{Im}(z)$	<i>partie réelle, partie imaginaire</i>
$\rightarrow$	<i>tend vers</i>
$x \mapsto f(x)$	<i>application qui à x associe $f(x)$</i>
$\vec{u}$	<i>vecteur u</i>
$f \circ g$	<i>composée de f et g</i>
$\ x\ $	<i>norme de x</i>
$\langle x, y \rangle$	<i>produit scalaire de x et y</i>
$\dim V$	<i>dimension d'un espace vectoriel V</i>
$\ker f, \operatorname{Im} f$	<i>noyau, image d'une application linéaire</i>
$\det A$	<i>déterminant d'une matrice A</i>

GL_n, SL_n, O_n	groupes linéaire, spécial linéaire, orthogonal
$a \equiv b \pmod{n}$	congruence modulo n
$\cong, \simeq$	isomorphe à, équivalent à
$\oplus, \otimes$	somme directe, produit tensoriel
$\lim$	limite
$\sup, \inf$	borne supérieure, borne inférieure
$O(\cdot), o(\cdot), \sim$	notations de Landau, équivalence asymptotique
$\frac{d}{dx}, \frac{\partial}{\partial x}$	dérivation ordinaire, dérivation partielle
C^k	fonctions à dérivées continues jusqu'à l'ordre k
C^∞	fonctions indéfiniment dérivables
$\mathcal{L}(E, F)$	applications linéaires continues de E dans F
E^*, E^{**}	dual topologique, bidual de E
$\sigma(T), \rho(T)$	spectre, ensemble résolvant d'un opérateur T
$W^{k,p}(\Omega), H^s(\Omega)$	espaces de Sobolev
$\mathcal{D}'(\Omega)$	distributions sur Ω
$\mathcal{S}(\mathbb{R}^n), \mathcal{S}'(\mathbb{R}^n)$	espace de Schwartz, distributions tempérées
$\text{Spec } A$	spectre d'un anneau A
$\text{Hom}, \text{Ext}, \text{Tor}$	foncteurs d'algèbre homologique
$\wedge$	produit extérieur
H^n, π_1	cohomologie de degré n , groupe fondamental
$\text{Gal}(L/K), [L : K]$	groupe de Galois, degré d'une extension
$\mathcal{O}_K, \text{Cl}(K), h_K$	anneau des entiers, groupe des classes, nombre de classes de K
v_p	valuation p -adique
$\mathbb{Q}_p, \mathbb{Z}_p$	nombres p -adiques, entiers p -adiques
$\mathbb{A}_K, \mathbb{I}_K, C_K$	adèles, idéles, classes d'idèles de K
$\text{Gal}(\bar{K}/K)$	groupe de Galois absolu de K
Frob_p	élément de Frobenius en p
$\rho : G_K \rightarrow \text{GL}(V)$	représentation galoisienne
$\zeta(s)$	fonction zêta de Riemann
$L(s, \pi), L(s, \chi)$	fonctions L automorphes et de Dirichlet
$\hat{G}, {}^L G$	dual de Langlands, L -groupe de G
Bun_G	champ des G -fibrés
$H_{\text{ét}}^i$	cohomologie étale de degré i
$D\text{-mod}$	catégorie des D -modules
$\text{Loc}_{\hat{G}}$	systèmes locaux à valeurs dans $\hat{G}$
$\text{QCoh}(Y)$	quasi-cobérents sur Y
$\text{IndCoh}_{\text{Nilp}}(Y)$	ind-cobérents de support nilpotent
$D\text{Mod}^{1/2}$	D -modules avec demi-torsion
Gr_G	grassmannienne affine de G
$\check{G}$	autre notation du dual de Langlands

Table des matières

Avant-propos	v
Au lecteur	vii
Note sur les cycles	ix
Notations	x
De la Maîtrise aux Correspondances	i
I Réciprocité et langage arithmétique	2
1 Corps de nombres et anneaux d'entiers	3
2 Corps locaux et nombres p -adiques	20
3 Adèles et idèles	35
4 Réciprocité et théorie du corps de classes	47
5 Représentations galoisiennes : exemples et questions	66

II	Formes, symétries et représentations automorphes	77
6	Demi-plan, groupes modulaires et courbes modulaires	78
7	Formes modulaires et opérateurs de Hecke	96
8	Fonctions L et premiers dictionnaires	112
9	Groupes réductifs et groupe dual	129
10	Formes et représentations automorphes	146
III	Géométrie arithmétique et premiers grands théorèmes	162
11	Variétés et courbes algébriques	163
12	Schémas, faisceaux et familles	179
13	Courbes elliptiques et arithmétique	198
14	Variétés abéliennes, dualité et modules de Tate	215
15	Cohomologie étale et théorèmes de Weil	231
16	Modularité, déformations et Fermat	246
17	Périodes, valeurs spéciales et arithmétique des formes	263

IV	Correspondances arithmétiques : méthodes et réalisations	277
18	Analyse harmonique et correspondances locales	278
19	Formules des traces et endoscopie	296
20	Fonctorialité : résultats et programme	313
21	Corps de fonctions, chtoucas et théorèmes de Langlands	328
V	Approfondissements arithmétiques	343
22	Variétés de Shimura	344
23	Motifs, correspondances et fonctions L motiviques	358
24	Géométrie p-adique et correspondances locales contemporaines	372
VI	Les outils du Langlands géométrique	389
25	Modules différentiels et Riemann–Hilbert	390
26	Fibrés sur les courbes et champ Bun_G	416
27	Systèmes locaux, fibrés de Higgs et Hitchin	428
28	Catégories dérivées, ind-cohérents et support singulier	443

VII	Langlands géométrique et parcours de la preuve de 2024	458
29	Du classique au géométrique : le cas abélien	459
30	Hecke géométrique, grassmannienne affine et Satake	488
31	Le théorème de Langlands géométrique : énoncé et portée	506
32	Construction du foncteur et normalisation de Whittaker	523
33	Localisation de Kac–Moody et équivalence locale fondamentale	539
34	Eisenstein, termes constants et récurrence sur les Levi	558
35	Ambidextérité et réduction du problème d'équivalence	579
36	Multiplicité un et achèvement de la preuve	600
VIII	Passage vers la physique	620
37	Correspondances et dualités : passage vers la physique	621
	Au terme de ce volume	634
	Bibliographie	635
	Index des notions	639

DE LA MAÎTRISE AUX CORRESPONDANCES

Jusqu'ici, chaque branche des mathématiques avait son propre langage. L'analyse parlait de limites et de mesures; l'algèbre, de groupes et d'idéaux; la géométrie, de variétés et de faisceaux. Ce qui suit est l'histoire d'une découverte : ces langues sont des dialectes d'une même grammaire.

Le programme de Langlands, vers lequel convergent les parties des Correspondances, est l'une des entreprises les plus ambitieuses de la mathématique contemporaine. Il postule l'existence de correspondances profondes entre la théorie des nombres, l'analyse harmonique et la géométrie algébrique, trois domaines que l'on pourrait croire indépendants, mais qui sont reliés par des symétries cachées dont on commence à peine à mesurer la portée.

Le parcours commence par les fondations arithmétiques : corps de nombres, nombres p -adiques, adèles et réciprocity. Il construit ensuite les formes modulaires et automorphes, puis la géométrie arithmétique jusqu'aux théorèmes de Weil et de modularité. Les méthodes du programme de Langlands, les chtoucas, les variétés de Shimura, les motifs et la géométrie p -adique précèdent les outils du langage géométrique. Modules différentiels, champs et catégories rendent alors possible un parcours de la preuve de 2024. La dernière étape prépare la lecture physique sans l'introduire dans la démonstration du théorème.

Les groupes de Lie, dont ce volume fait un usage constant, sont exposés au chapitre 78 de la Maîtrise; le lecteur pourra s'y reporter avant d'aborder les groupes réductifs.

La grammaire par laquelle la réalité se compose n'est pas achevée. Ce que l'on en sait, ce que l'on en devine, et ce qu'il reste à découvrir, c'est l'objet de ce volume.

Première partie

Réciprocité et langage arithmétique

Les corps de nombres donnent le terrain global; leurs complétions permettent d'isoler chaque place. Les adèles et les idèles réunissent ces données avant que la réciprocité n'identifie les quotients qui gouvernent les extensions abéliennes. Les représentations galoisiennes élargissent ensuite la question : comment conserver une action lorsque le groupe ne se réduit plus à ses caractères ?

CHAPITRE I

CORPS DE NOMBRES ET ANNEAUX D'ENTRIERS

Adjoindre un nombre aux rationnels change les opérations possibles, mais aussi ce que signifie être entier. Une fraction peut satisfaire une équation unitaire; un nombre peut perdre sa factorisation unique; un idéal peut conserver cette unicité sans avoir de générateur. Ces différences demandent une arithmétique qui reconnaisse les objets avant de les compter. Les plongements les rendent visibles sous plusieurs aspects, et les réseaux permettent d'en mesurer les écarts. Le passage aux corps de nombres ne remplace pas les entiers ordinaires par des nombres plus compliqués : il révèle les conditions précises qui faisaient fonctionner leur arithmétique.

Articles de ce chapitre :

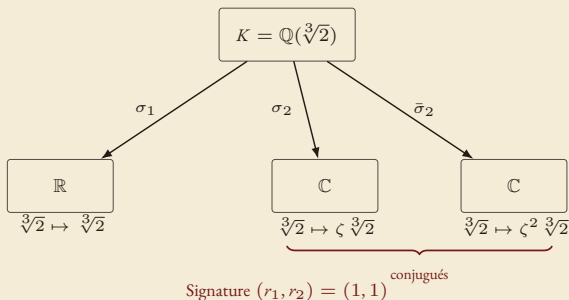
- 001.** *Corps de nombres — Les racines du polynôme minimal donnent les plongements et la signature.*
- 002.** *Anneaux d'entiers — Une base du corps n'engendre pas nécessairement tous ses entiers.*
- 003.** *Norme, trace, discriminant — Le calcul matriciel distingue les invariants d'un élément et ceux d'une base.*
- 004.** *Idéaux de Dedekind — Deux factorisations d'un élément retrouvent la même factorisation idéale.*
- 005.** *Groupe de classes — Une borne finie permet de calculer le défaut de principalité.*
- 006.** *Unités de Dirichlet — Le logarithme révèle un réseau, avec une normalisation à respecter.*

I. CORPS DE NOMBRES.

QU'ARRIVE-T-IL lorsqu'on adjoint $\sqrt{-5}$ aux rationnels? On obtient un corps $\mathbb{Q}(\sqrt{-5})$ dont l'anneau d'entiers $\mathbb{Z}[\sqrt{-5}]$ offre à l'entier 6 deux factorisations essentiellement distinctes : $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. La factorisation demande donc d'autres objets que ceux qui suffisaient dans $\mathbb{Z}$. Avant de reprendre ce calcul au niveau des idéaux, il faut comprendre les différentes façons de représenter le corps lui-même.

DÉFINITION 1.1 : Un *corps de nombres* est une extension finie K de $\mathbb{Q}$. Son *degré* est l'entier $n = [K : \mathbb{Q}]$. Le corps $\mathbb{Q}$ lui-même est un corps de nombres de degré 1. Les corps quadratiques $\mathbb{Q}(\sqrt{d})$ (avec $d \in \mathbb{Z}$ sans facteur carré, $d \neq 0, 1$) sont de degré 2, et les corps cyclotomiques $\mathbb{Q}(\zeta_m)$ sont de degré $\varphi(m)$.

Chaque corps de nombres admet exactement n plongements dans $\mathbb{C}$, certains réels et d'autres complexes. Leur répartition détermine la nature arithmétique du corps.



Les trois plongements de $\mathbb{Q}(\sqrt[3]{2})$: un réel et une paire de conjugués complexes, donnant la signature $(1, 1)$.

DÉFINITION 1.2 : Soit K un corps de nombres de degré n . Un *plongement* de K est un morphisme de corps $\sigma : K \hookrightarrow \mathbb{C}$. Il en existe exactement n . Parmi ceux-ci, r_1 sont *réels* (d'image contenue dans $\mathbb{R}$) et les $n - r_1$ restants se regroupent en r_2 paires de conjugués complexes. Le couple (r_1, r_2) , avec $r_1 + 2r_2 = n$, est la *signature* de K .

PROPOSITION 1.3 : Par le théorème de l'élément primitif, tout corps de nombres s'écrit $K = \mathbb{Q}(\alpha)$ pour un α algébrique, racine d'un polynôme irréductible $f \in \mathbb{Q}[x]$ de degré n . Une base de K sur $\mathbb{Q}$ est alors $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$.

La séparabilité en caractéristique zéro et le théorème de l'élément primitif sont repris de l'article « Séparabilité » de la *Maîtrise*. Ils ramènent ici le dénombrement des plongements à celui des racines.

DES RACINES AUX PLONGEMENTS : Si $K = \mathbb{Q}(\alpha)$ et si f est le polynôme minimal de α , un plongement doit envoyer α sur une racine de f . Réciproquement, chaque racine β définit un morphisme $\mathbb{Q}[X]/(f) \rightarrow \mathbb{C}$ par évaluation en β . Ce morphisme de corps est injectif. Comme f est séparable de degré n , ses n racines donnent exactement n plongements.

EXEMPLE : Le corps $\mathbb{Q}(\sqrt{2})$ a signature $(2, 0)$: ses deux plongements envoient $\sqrt{2}$ sur $\pm\sqrt{2}$, tous deux réels. Le corps $\mathbb{Q}(i)$ a signature $(0, 1)$: ses deux plongements envoient i sur $\pm i$, et forment une paire conjuguée. Le corps $\mathbb{Q}(\sqrt[3]{2})$ a signature $(1, 1)$: une racine cubique réelle et deux racines complexes conjuguées.

REMARQUE 1.4 : La signature (r_1, r_2) gouverne le rang du groupe des unités (théorème de Dirichlet : rang $r_1 + r_2 - 1$), le signe du discriminant $((-1)^{r_2})$ et la forme du plongement canonique de K dans $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Elle condense en deux entiers les contraintes archimédiennes qui pèsent sur toute l'arithmétique de K .

Les plongements donnent ainsi plusieurs lectures compatibles d'un même nombre : les relations algébriques sont conservées, même

lorsque ses images changent. Cette pluralité ne transforme pas le corps en plusieurs corps indépendants ; elle permet de l'observer dans toutes ses directions archimédiennes. Elle ne dit pas encore quels éléments joueront le rôle des entiers. Pour commencer l'arithmétique, il faut choisir à l'intérieur du corps l'anneau qui les contient tous.

2. ANNEAUX D'ENTIERES.

LES entiers ordinaires forment un sous-anneau bien déterminé de $\mathbb{Q}$. Mais lorsqu'on passe à un corps de nombres K , quels éléments jouent le rôle des entiers ? La réponse ne va pas de soi : dans $\mathbb{Q}(\sqrt{5})$, le nombre d'or $\varphi = \frac{1+\sqrt{5}}{2}$ (qui ne ressemble guère à un entier) vérifie $\varphi^2 - \varphi - 1 = 0$ et mérite le titre d'entier algébrique.

DÉFINITION 2.1 : Un *entier algébrique* est un nombre complexe α racine d'un polynôme unitaire à coefficients dans $\mathbb{Z}$: $\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_0 = 0$ avec $a_i \in \mathbb{Z}$. L'ensemble de tous les entiers algébriques forme un sous-anneau $\overline{\mathbb{Z}}$ de $\mathbb{C}$.

La caractérisation modulaire clarifie cette notion : α est entier algébrique si et seulement si $\mathbb{Z}[\alpha]$ est un $\mathbb{Z}$ -module de type fini. L'intégralité se lit dans la finitude du module engendré.

DÉFINITION 2.2 : Soit K un corps de nombres. L'*anneau des entiers* de K est $\mathcal{O}_K = K \cap \overline{\mathbb{Z}}$, l'ensemble des éléments de K qui sont entiers algébriques.

PROPOSITION 2.3 : Si K est un corps de nombres de degré n , alors $\mathcal{O}_K$ est un $\mathbb{Z}$ -module libre de rang n . Autrement dit, il existe une *base d'entiers* $\{\omega_1, \dots, \omega_n\}$ telle que $\mathcal{O}_K = \mathbb{Z}\omega_1 \oplus \dots \oplus \mathbb{Z}\omega_n$.

Nous reprenons ce théorème comme acquis de l'article « Entiers algébriques et anneaux de Dedekind » de la *Maîtrise*. Il affirme plus que l'existence d'une base du corps : les coefficients des entiers dans cette base particulière sont eux-mêmes des entiers ordinaires. Une base sur $\mathbb{Q}$ ne possède pas nécessairement cette propriété.

LA BASE QUE LE NOMBRE D'OR COMPLÈTE : Dans $K = \mathbb{Q}(\sqrt{5})$, la formule quadratique de l'anneau d'entiers, admise ci-dessous, donne

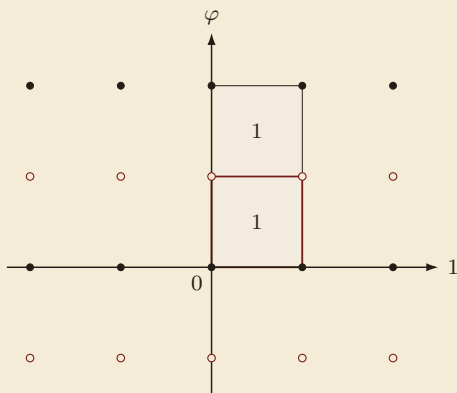
$$\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\varphi, \quad \varphi = \frac{1 + \sqrt{5}}{2}, \quad \varphi^2 = \varphi + 1.$$

L'élément φ n'appartient pas à $\mathbb{Z}[\sqrt{5}]$: ses coefficients dans la base $(1, \sqrt{5})$ sont $1/2$ et $1/2$. Inversement, $\sqrt{5} = 2\varphi - 1$, si bien que

$$\mathbb{Z}[\sqrt{5}] = \mathbb{Z} + 2\mathbb{Z}\varphi \subsetneq \mathcal{O}_K.$$

L'indice est 2 : les deux classes sont représentées par 0 et φ . Adjoindre un générateur du corps n'avait pas produit l'anneau de tous ses entiers.

Dans les coordonnées de la base entière $(1, \varphi)$, l'indice devient visible : le sous-anneau occupe une ligne sur deux du réseau. Une maille de ce sous-réseau contient deux mailles du réseau entier.



$$\mathbb{Z}[\sqrt{5}] = \mathbb{Z} + 2\mathbb{Z}\varphi$$

$$[\mathcal{O}_K : \mathbb{Z}[\sqrt{5}]] = 2$$

Coordonnées dans la base $(1, \varphi)$, et non plongement de Minkowski. Les points pleins représentent $\mathbb{Z}[\sqrt{5}]$; les points évidés complètent $\mathcal{O}_K$. Les deux cellules ont chacune aire un dans ces coordonnées.

EXEMPLE : Pour $K = \mathbb{Q}(\sqrt{d})$ avec d sans facteur carré, $d \neq 0, 1$, la formule admise est $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ si $d \equiv 2$ ou $3 \pmod{4}$, et $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ si $d \equiv 1 \pmod{4}$. L'anneau des entiers de Gauss $\mathbb{Z}[i]$ (cas $d = -1$) est le plus classique. Pour les corps cyclotomiques, $\mathcal{O}_{\mathbb{Q}(\zeta_p)} = \mathbb{Z}[\zeta_p]$ lorsque p est premier.

REMARQUE 2.4 : Déterminer $\mathcal{O}_K$ est un problème algorithmique non trivial, même pour les corps cubiques. L'inclusion $\mathbb{Z}[\alpha] \subset \mathcal{O}_K$ peut être stricte : l'anneau des entiers est plus grand que ce qu'un générateur naïf suggère, et c'est dans ce surplus que se cache la structure arithmétique fine.

Une base entière règle l'écriture de tous les entiers du corps, comme une grammaire qui fixe les coefficients autorisés. Elle n'est pas

canonique : plusieurs bases donnent le même anneau. Le prochain calcul devra donc distinguer ce qui dépend de cette écriture et ce qui demeure lorsque l'on en change.

3. NORME, TRACE, DISCRIMINANT.

CHANGER de base peut multiplier un discriminant sans changer le corps. Dans $\mathbb{Q}(\sqrt{5})$, les bases $(1, \sqrt{5})$ et $(1, \varphi)$ décrivent le même espace vectoriel, mais une seule engendre tous les entiers sur $\mathbb{Z}$. Pour mesurer cette différence, il faut d'abord retrouver deux invariants d'un endomorphisme : sa trace et son déterminant.

DÉFINITION 3.1 : Pour $\alpha \in K$, la multiplication $m_\alpha : x \mapsto \alpha x$ est un endomorphisme du $\mathbb{Q}$ -espace vectoriel K . Sa trace est la *trace* de α , son déterminant la *norme* :

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \sum_i \sigma_i(\alpha), \quad N_{K/\mathbb{Q}}(\alpha) = \prod_i \sigma_i(\alpha).$$

Les égalités avec les plongements résultent de la décomposition séparable $K \otimes_{\mathbb{Q}} \mathbb{C} \simeq \mathbb{C}^n$, utilisée ici comme acquis.

La trace est additive, la norme multiplicative. Elles envoient les entiers algébriques dans $\mathbb{Z}$, car la multiplication par un entier a une matrice entière dans une base entière. La norme algébrique n'est pas une norme d'espace vectoriel : elle peut être négative et ne mesure pas à elle seule toutes les valeurs absolues des conjugués.

UNE MULTIPLICATION CALCULÉE : Gardons $\varphi^2 = \varphi + 1$. Pour $\alpha = a + b\varphi$, avec $a, b \in \mathbb{Q}$, les images de 1 et de φ donnent

$$[m_\alpha]_{(1, \varphi)} = \begin{pmatrix} a & b \\ b & a + b \end{pmatrix}.$$

Ainsi $\mathrm{Tr}(\alpha) = 2a + b$ et $N(\alpha) = a^2 + ab - b^2$. En particulier, $\mathrm{Tr}(\varphi) = 1$, $N(\varphi) = -1$ et $\mathrm{Tr}(\varphi^2) = 3$.

Pour une base $B = (\omega_1, \dots, \omega_n)$ de K sur $\mathbb{Q}$, son *discriminant* est

$$\mathrm{disc}(B) = \det(\mathrm{Tr}(\omega_i \omega_j)) = \det(\sigma_i(\omega_j))^2.$$

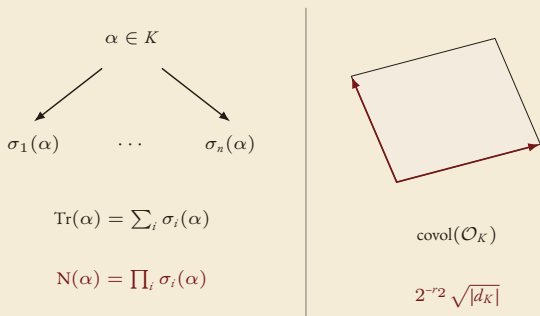
La seconde égalité vient de l'identité matricielle $T = S^t S$. La séparabilité garantit la non-dégénérescence de la forme trace, donc ce déterminant est non nul.

DEUX BASES, DEUX DISCRIMINANTS : Les matrices des traces sont respectivement

$$T_{(1,\varphi)} = \begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix}, \quad T_{(1,\sqrt{5})} = \begin{pmatrix} 2 & 0 \\ 0 & 10 \end{pmatrix}.$$

Leurs déterminants valent 5 et 20. Si $B' = BP$, alors $T_{B'} = P^t T_B P$, d'où $\text{disc}(B') = (\det P)^2 \text{disc}(B)$. Ici, $\sqrt{5} = 2\varphi - 1$ donne $\det P = 2$: l'indice calculé à l'article précédent apparaît au carré.

Deux bases entières du même anneau sont reliées par une matrice entière inversible sur $\mathbb{Z}$, de déterminant ± 1 . Leur discriminant commun est le *discriminant du corps*, noté d_K . Ainsi $d_{\mathbb{Q}(\sqrt{5})} = 5$, et non 20.



La trace additionne les conjugués et la norme les multiplie. Pour une base entière, le covolume réel du plongement de Minkowski non redimensionné vaut $2^{-r_2} \sqrt{|d_K|}$.

Le discriminant décrit la trame des entiers à travers leurs plongements. Cette lecture géométrique demande une mesure fixée : le déterminant complexe de tous les plongements n'est pas directement le volume réel dans $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Le facteur indiqué dans la légende

assure le passage entre les deux conventions. Le signe de d_K est $(-1)^{r_2}$; sa valeur absolue intervient dans les bornes arithmétiques que nous rencontrerons.

La base a changé, mais le corps est resté le même. Le discriminant a distingué deux anneaux dans ce corps ; la factorisation des idéaux va maintenant révéler comment leurs nombres premiers se comportent.

4. IDÉAUX DE DEDEKIND.

DANS $\mathbb{Z}[\sqrt{-5}]$, l'égalité $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ ne se réduit pas à un changement d'ordre des facteurs. Posons $s = \sqrt{-5}$. La norme $N(a + bs) = a^2 + 5b^2$ ne prend ni la valeur 2 ni la valeur 3 sur les entiers. Comme les normes de 2, 3 et $1 \pm s$ sont 4, 9 et 6, une décomposition de l'un d'eux en deux non-unités imposerait l'une de ces valeurs impossibles. Les quatre facteurs sont irréductibles. Les seules unités sont ± 1 , et les deux factorisations ne sont pas associées.

Le rappel de Dedekind dans la *Maîtrise* annonçait une unicité retrouvée au niveau des idéaux. Nous gardons sa convention : un anneau de Dedekind est intègre, noethérien, intégralement clos dans son corps des fractions et de dimension 1. Il n'est donc pas un corps, et ses idéaux premiers non nuls sont maximaux.

L'anneau $\mathcal{O}_K$ satisfait ces conditions. Sa noethérianité vient de sa finitude sur $\mathbb{Z}$; sa clôture intégrale, de la transitivité de l'intégralité. La dimension 1 est un acquis : tout quotient par un idéal premier non nul est un corps fini.

FACTORISATION ET INVERSIBILITÉ : Tout idéal propre non nul est, de manière unique à l'ordre près, un produit de puissances d'idéaux premiers non nuls distincts. Un idéal fractionnaire non nul est un sous-module I de K tel que $dI \subset \mathcal{O}_K$ pour un $d \in \mathcal{O}_K \setminus \{0\}$. Nous admettons que tout idéal non nul est inversible, avec

$$I^{-1} = \{x \in K : xI \subset \mathcal{O}_K\}.$$

C'est l'étape substantielle de la factorisation. L'unicité se lit alors directement : un premier contenant un produit contient un facteur ; la maximalité identifie les facteurs premiers, puis leur inverse permet de simplifier. L'existence utilise aussi la noethérianité et n'est pas redémontrée ici.

Le produit vide donne l'idéal unité. Les idéaux fractionnaires non nuls forment ainsi un groupe abélien libre sur les idéaux premiers non nuls. Pour calculer, on utilise la norme d'un idéal intégral non nul, $N(\mathfrak{a}) = [\mathcal{O}_K : \mathfrak{a}]$. Sa multiplicativité et l'égalité $N((\alpha)) = |N_{K/\mathbb{Q}}(\alpha)|$ sont admises.

LE MÊME PRODUIT DERRIÈRE LES DEUX ÉCRITURES : Dans $\mathbb{Z}[\varsigma]$, posons

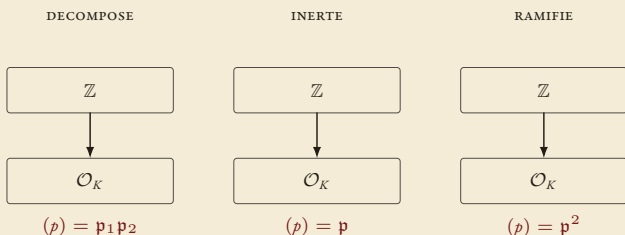
$$\mathfrak{p}_2 = (2, 1 + \varsigma), \quad \mathfrak{p}_3 = (3, 1 + \varsigma), \quad \bar{\mathfrak{p}}_3 = (3, 1 - \varsigma).$$

Les quotients sont $\mathbb{F}_2$, $\mathbb{F}_3$ et $\mathbb{F}_3$, par substitution de ς par 1, -1 et 1, respectivement. Ces idéaux sont donc premiers, de normes 2, 3 et 3. Les générateurs de $\mathfrak{p}_2^2$ sont 4, $2(1 + \varsigma)$ et $(1 + \varsigma)^2 = -4 + 2\varsigma$: tous sont divisibles par 2. L'inclusion $\mathfrak{p}_2^2 \subset (2)$ est une égalité puisque les deux normes valent 4. De même, les générateurs donnent les inclusions suivantes, et leurs normes donnent les égalités :

$$(3) = \mathfrak{p}_3 \bar{\mathfrak{p}}_3, \quad (1 + \varsigma) = \mathfrak{p}_2 \mathfrak{p}_3, \quad (1 - \varsigma) = \mathfrak{p}_2 \bar{\mathfrak{p}}_3.$$

Ainsi $(6) = \mathfrak{p}_2^2 \mathfrak{p}_3 \bar{\mathfrak{p}}_3$ est l'unique factorisation idéale des deux produits initiaux.

Un premier rationnel p est *ramifié* lorsqu'un exposant de la factorisation de $p\mathcal{O}_K$ est supérieur à 1. Le critère $p \mid d_K$, équivalent à cette ramification, est admis. Ici $d_K = -20$: seuls 2 et 5 ramifient, et le carré $\mathfrak{p}_2^2$ le montre déjà pour 2.



Dans un corps quadratique, un premier est décomposé, inerte ou ramifié. Le dernier cas se reconnaît à un facteur idéal répété.

Les idéaux donnent une écriture commune aux deux décompositions de 6. Cette écriture ne rend pas chaque idéal principal : elle conserve précisément les facteurs qu'aucun élément seul ne représente. Le groupe de classes va mesurer cette différence.

5. GROUPE DE CLASSES.

Si les idéaux se factorisent de manière unique, pourquoi les éléments ne le font-ils pas ? Il manque une condition : chaque facteur idéal devrait être engendré par un élément. Dans $\mathbb{Z}[\sqrt{-5}]$, l'idéal $\mathfrak{p}_2 = (2, 1 + \sqrt{-5})$ a norme 2, mais aucun élément n'a cette norme. Le quotient qui identifie les idéaux différant par un facteur principal conserve exactement cet obstacle.

DÉFINITION 5.1 : Le *groupe de classes* de K est le quotient

$$\text{Cl}(K) = I_K / P_K,$$

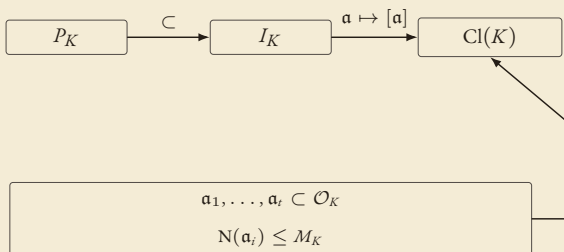
où I_K est le groupe des idéaux fractionnaires non nuls et P_K son sous-groupe des idéaux principaux (α) , $\alpha \in K^\times$. Il est trivial si et seulement si $\mathcal{O}_K$ est principal, condition équivalente ici à la factorialité.

Deux idéaux ont donc même classe lorsque l'un est obtenu en multipliant l'autre par un élément non nul du corps. Il reste à savoir combien de classes cette identification laisse subsister.

BORNE DE MINKOWSKI, ADMISE : Toute classe contient un idéal *intégral* non nul $\mathfrak{a}$ dont la norme, l'indice $[\mathcal{O}_K : \mathfrak{a}]$, satisfait

$$N(\mathfrak{a}) \leq M_K, \quad M_K = \frac{n!}{n^n} \left(\frac{4}{\pi} \right)^{r_2} \sqrt{|d_K|}.$$

L'adjectif intégral signifie $\mathfrak{a} \subset \mathcal{O}_K$. Il rend la borne effective : il n'y a qu'un nombre fini de sous-groupes d'indice borné dans le groupe libre $\mathcal{O}_K \simeq \mathbb{Z}^n$. Pour un indice m , chacun contient $m\mathbb{Z}^n$ et provient d'un sous-groupe du groupe fini $(\mathbb{Z}/m\mathbb{Z})^n$. Le groupe de classes est donc fini ; son ordre h_K est le *nombre de classes*.



Toutes les classes ont un représentant dans cet ensemble fini.

Le quotient par les idéaux principaux conserve les classes ; Minkowski permet de les représenter par un nombre fini d'idéaux intégraux de norme bornée.

CALCUL DE DEUX CLASSES : Pour $K = \mathbb{Q}(\sqrt{-5})$, la signature est $(0, 1)$ et $d_K = -20$, d'où

$$M_K = \frac{2}{\pi} \sqrt{20} \simeq 2,85 < 3.$$

Toute classe possède un représentant de norme 1 ou 2. Le seul idéal de norme 1 est $\mathcal{O}_K$. Un idéal de norme 2 a quotient $\mathbb{F}_2$; l'image de $\sqrt{-5}$ doit être une racine de $X^2 + 5 = (X + 1)^2$ modulo 2. Il n'y a qu'un choix : cet idéal est $\mathfrak{p}_2$.

Si $\mathfrak{p}_2 = (a + b\sqrt{-5})$, alors $a^2 + 5b^2 = 2$, impossible pour des entiers a, b . Sa classe n'est donc pas triviale. L'égalité $\mathfrak{p}_2^2 = (2)$ montre que son carré l'est. Ainsi

$$h_K = 2, \quad \text{Cl}(K) \simeq \mathbb{Z}/2\mathbb{Z}.$$

Le quotient classe les idéaux comme on classe des écritures modulo un changement autorisé. Cette identification ne supprime pas les idéaux eux-mêmes : elle oublie seulement leur facteur principal. La borne a permis ici de parcourir toutes les classes, pas seulement d'en exhiber deux.

Pour $\mathbb{Q}(i)$, la même borne vaut $4/\pi < 2$, donc seul l'idéal unité est nécessaire et $h_K = 1$. Le contraste avec $\mathbb{Q}(\sqrt{-5})$ est désormais calculé. L'invariant a aussi une expression analytique, que nous citons comme aperçu :

$$\text{Res}_{s=1} \zeta_K(s) = \frac{2^{r_1} (2\pi)^{r_2} h_K R_K}{w_K \sqrt{|d_K|}}.$$

Ici w_K compte les racines de l'unité, et R_K est le régulateur introduit ensuite. Cette formule, admise, fait intervenir ensemble les classes et les unités. Les premières distinguent les idéaux sans générateur ; les secondes décrivent combien de générateurs un même idéal principal peut posséder.

6. UNITÉS DE DIRICHLET.

L'ÉQUATION $x^2 - 2y^2 = 1$ possède une infinité de solutions entières, mais l'unité $1 + \sqrt{2}$ a norme -1 . Son carré, $3 + 2\sqrt{2}$, a norme $+1$. Ce changement de signe distingue le groupe de toutes les unités et le sous-groupe qui résout l'équation de Pell. Pour comprendre leur infinitude, il faut regarder les valeurs absolues dans les différents plongements.

DÉFINITION 6.1 : Les *unités* de $\mathcal{O}_K$ sont ses éléments inversibles :

$$\mathcal{O}_K^\times = \{\alpha \in \mathcal{O}_K : N_{K/\mathbb{Q}}(\alpha) = \pm 1\}.$$

L'équivalence se vérifie sur la multiplication par α : sa matrice entière est inversible sur $\mathbb{Z}$ exactement lorsque son déterminant vaut ± 1 . L'hypothèse $\alpha \in \mathcal{O}_K$ est nécessaire ; la seule valeur de la norme d'un élément du corps ne suffit pas à en faire un entier.

THÉORÈME 6.2 DE DIRICHLET, ADMIS : Pour un corps de signature (r_1, r_2) ,

$$\mathcal{O}_K^\times \simeq \mu_K \times \mathbb{Z}^{r_1+r_2-1},$$

où μ_K est le groupe fini cyclique des racines de l'unité de K .

La partie libre peut donc être infinie, mais elle possède un nombre fini de générateurs. Le logarithme explique le rang annoncé. Choisissons les plongements réels σ_i et un plongement τ_j par paire complexe conjuguée. Posons

$$\lambda(u) = ((\log |\sigma_i(u)|)_i, (2 \log |\tau_j(u)|)_j).$$

La norme absolue est le produit des valeurs réelles et des carrés des valeurs complexes. Pour une unité, elle vaut 1 ; en prenant le logarithme,

$$\sum_{k=1}^{r_1+r_2} \lambda_k(u) = 0.$$

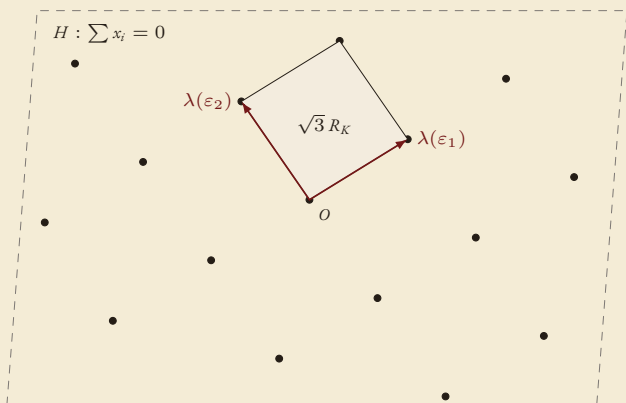
L'image est contenue dans l'hyperplan H de somme nulle. Le noyau est μ_K , par le théorème de Kronecker, admis. Que l'image soit discrète *et de rang plein* dans H est l'étape de géométrie des nombres que nous admettons également. L'inclusion dans un hyperplan, à elle seule, ne prouverait pas le rang.

DÉFINITION 6.3 : Posons $m = r_1 + r_2$ et $r = m - 1$. Pour des unités fondamentales $\varepsilon_1, \dots, \varepsilon_r$, le *régulateur* est

$$R_K = |\det(\lambda_i(\varepsilon_j))|,$$

après suppression d'une des m lignes. La somme des lignes étant nulle, les déterminants obtenus ont même valeur absolue. Un changement de base du réseau multiplie ce déterminant par ± 1 . En rang zéro, on pose $R_K = 1$.

Avec le produit scalaire usuel sur $\mathbb{R}^m$, le covolume dans H vaut $\sqrt{m} R_K$. En effet, la paramétrisation par les $m - 1$ premières coordonnées a une matrice de Gram $I + \mathbf{1}\mathbf{1}^t$, de déterminant m . Le régulateur est donc un volume normalisé, pas directement ce volume euclidien.



Dessin schématique de rang 2 : les vecteurs engendrent le réseau dans $H \subset \mathbb{R}^3$. L'aire euclidienne de la maille vaut $\sqrt{3} R_K$.

LES DEUX SIGNES DE PELL : On utilise comme acquis que $\varepsilon = 1 + \sqrt{2}$ est fondamentale pour $\mathbb{Q}(\sqrt{2})$. Ses unités sont $\pm \varepsilon^k$, $k \in \mathbb{Z}$, de

norme $(-1)^k$. Celles de norme $+1$ sont exactement $\pm(3 + 2\sqrt{2})^\ell$, $\ell \in \mathbb{Z}$. Si $L = \log(1 + \sqrt{2})$, alors

$$\lambda(\varepsilon) = (L, -L), \quad R_K = L \simeq 0,88.$$

Le vecteur a longueur $\sqrt{2}L$, conformément à la normalisation. Pour $\mathbb{Q}(i)$, la signature $(0, 1)$ donne au contraire rang zéro : les seules unités sont $1, i, -1, -i$ et $R_K = 1$.

L'application logarithmique traduit une multiplication en addition, mais sa traduction perd les racines de l'unité. Les conserver séparément restitue le groupe entier. Dans la formule analytique du nombre de classes, c'est le produit $h_K R_K$ qui accompagne cette torsion : classes et unités décrivent deux aspects d'une même arithmétique. Les plongements archimédiens les ont rendus visibles ; les valuations associées aux nombres premiers offriront le prochain point de vue.

LECTURES COMPLÉMENTAIRES

- **Dedekind, R.**, Über die Theorie der ganzen algebraischen Zahlen, *supplément aux Vorlesungen über Zahlentheorie de Dirichlet. Source historique pour la théorie des idéaux.*
- **Samuel, P.** (1967), Théorie algébrique des nombres, *Hermann. Présentation concise du socle arithmétique.*
- **Neukirch, J.** (1999), Algebraic Number Theory, *Springer, Grundlehren 322. Idéaux, places et réciprocité.*
- **Cassels, J.W.S. & Fröhlich, A.** (éds., 1967), Algebraic Number Theory, *Academic Press. Exposés de référence, jusqu'à la théorie du corps de classes.*
- **Milne, J.S.** (2020), Algebraic Number Theory, *version 3.08, chapitres 2–5 : entiers, idéaux, classes et unités ; théorème 4.3 pour la borne de Minkowski.*

QUESTIONS DE RECHERCHE

- (1) Au-delà de Brumer–Stark. *Le lien entre classes d'idéaux, valeurs de fonctions L et unités possède désormais un théorème intégral : Dasgupta–Kakde–Silliman–Wang donnent une preuve de Brumer–Stark sur $\mathbb{Z}$ dans leur travail déposé en 2023. Le problème de recherche porte donc sur les extensions de ce cadre et les constructions explicites qu'elles permettraient, non sur une preuve supplémentaire du même énoncé.*
- (2) Stark et le rang supérieur. *Comment exprimer les coefficients dominants des fonctions L au moyen d'unités ? Les formulations de rang supérieur font intervenir des déterminants logarithmiques et des puissances extérieures de groupes d'unités. Le texte de Rubin (1996) précise une version intégrale dans le cadre abélien. Il faut distinguer ses hypothèses et les cas démontrés : le théorème de Brumer–Stark ne doit pas être confondu avec une résolution indifférenciée de toutes les conjectures de Stark.*
- (3) 12^{e} problème de Hilbert. *Construire les extensions abéliennes par des valeurs spéciales de fonctions : les corps cyclotomiques sur $\mathbb{Q}$ et la multiplication complexe sur les corps quadratiques imaginaires sont les modèles classiques. Pour les corps totalement réels, Dasgupta–Kakde, Brumer–Stark Units and Explicit Class Field Theory, introduction, §1.4, proposent une construction p -adique. Ils distinguent explicitement ce résultat du cadre analytique complexe envisagé par Hilbert. La nature des fonctions autorisées fait donc partie du problème, et doit accompagner toute annonce de résolution.*