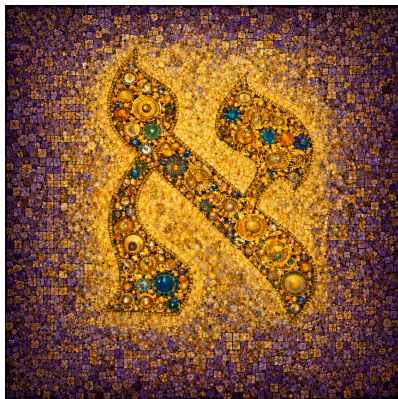




Articulated Course

in

Mathematics

IV

Correspondences

FROM CLASS FIELD THEORY TO THE LANGLANDS PROGRAM

William de France

CLEMENTINIUM EDITIONS

Clem

CORRESPONDENCES

*The problems of mathematics are not isolated from one another. There is
a vast web of connections.*

ROBERT LANGLANDS

Articulated Course in Mathematics

IV

Correspondences

FROM CLASS FIELD THEORY TO THE LANGLANDS PROGRAM

William de France

CLEMENTINIUM EDITIONS

Copyright © 2026 William de France

CLEMENTINIUM EDITIONS

Collection ARTICULATED COURSE IN MATHEMATICS

All rights reserved.

PREFACE

The same equation can be read through its solutions, through its symmetries, or through the functions recording their traces. The Langlands program asks how to pass between such descriptions without losing the operations that give them meaning. This volume follows that question from number fields to the geometric correspondence and a path through its 2024 proof.

Together with Mathematical Physics, Correspondences opens the research level of the Articulated Course in Mathematics. It assumes the background of Graduate Mathematics, particularly Galois theory, functional analysis, and differential geometry. More specialized algebraic and geometric tools are introduced when a question makes them necessary. The book addresses readers who want to understand how the domains connect, then return to the sources for the complete constructions and proofs.

The journey comprises thirty-seven chapters and two hundred thirty-eight articles, distributed across eight parts. The first establishes the local and global languages of arithmetic and reciprocity. The second constructs modular forms, L-functions, dual groups, and automorphic representations. The third develops arithmetic geometry through modularity, periods, and special values. The fourth examines methods and realizations of the arithmetic program; the fifth explores Shimura varieties, motives, and p-adic geometry.

The last three parts change the objects of the correspondence. Differential modules, stacks of bundles, and derived categories prepare the geometric statement. The abelian case supplies a guiding calculation; Hecke and Satake then lead to the general theorem. The proof chapters distinguish construction of the functor, local and global compatibilities, and the control that makes the functor an equivalence. The final chapter opens toward physics through charges, lines, and branes.

Distinguishing these routes is part of the book's purpose. The unramified de Rham geometric theorem does not resolve the whole arithmetic program. Its physical interpretation does not by itself prove a duality of gauge theories. Hypotheses, normalizations, and the nature of the categories are therefore

retained in the statements. Difficult results are identified as being used without proof when an article explains their role rather than reproducing their demonstration.

The article remains the unit of reading: a question, a construction, a worked example, and its interpretation. Numbered references let the reader recover earlier material without repeating its exposition. Further reading leads to the sources; the research questions closing the chapters extend a calculation, test a distinction, or situate a conjecture. They are not all open problems: their role is to give the reader an operation to pursue.

Familiar objects return with new functions. In $\mathbb{Q}(\sqrt{2})$, integers, units, and places bring algebra and arithmetic together. An elliptic curve carries rational points, Tate modules, and an L-function. The group GL_2 lets us compare a representation, an automorphic form, and a modification of a bundle. These returns make the continuity of the collection tangible.

A dictionary becomes useful only when it preserves what sentences allow us to do. The limit of this image matters: matching names does not construct a correspondence. By following operations, their compatibilities, and their proofs, the reader can measure what the different languages have learned to convey to one another.

TO THE READER

Across five volumes, this course articulates the grammar through which reality composes itself: more than thirteen hundred mathematical articles, from the first integer to the Langlands correspondence and from the brachistochrone to the amplituhedron. The undertaking is vast. The author does not claim that it is without flaws; he affirms that it is sincere.

Each article develops a single idea, from its motivation to its interpretation. Definitions are framed; major theorems are also framed, in red, in Volumes 2 and 3 of the collection. Proofs are present where they illuminate, sketched where full rigor would obscure the purpose, and stated as omitted when their difficulty exceeds the article's scope. The reader will be able to distinguish the three cases.

Ten mathematical objects recur throughout the collection: the circle S^1 , the integers $\mathbb{Z}$, the extension $\mathbb{Q}(\sqrt{2})$, the elliptic curve $y^2 = x^3 - x$, the group GL_2 , the function $\zeta(s)$, the space L^2 , the ring $K[X]$, the symmetric group $\mathfrak{S}_3$, and the torus T^2 . From trigonometric calculation to the Langlands dual group, from the harmonic oscillator to Montonen–Olive duality, each returns at every level with new depth. When one appears, the text points it out.

The figures, more than eight hundred across the collection, have been drawn with the care required by a pocket format: each line has a reason to be there, each label is clear of every curve, and the palette is limited to four colors. They do not replace proof; they precede it. Readers who look at the figure before reading the theorem will often understand the statement before reading a word of it.

Each chapter extends into Further reading, chosen to lead to sources and deepen the constructions, then Research questions. These invite the reader to extend an example, clarify a hypothesis, or compare two operations. When a conjecture appears, its status is distinguished from proved results; not all these questions are open problems in current research.

Readers may follow the linear path or use connections between volumes. Volumes I–III form a continuous progression from secondary-level to graduate mathematics. Volume IV rises toward the Langlands program; Volume V, toward mathematical physics. Both assume Volume III but may be read independently of one another.

In this English edition, reading recommendations use verified English editions where appropriate. Original sources and historical attributions are preserved; references retained in another language are identified. Section references concern the editions actually cited.

Every error reported is an error corrected.

wdf@clementinium.com

NOTE ON THE LEVELS

The five volumes follow a progression from the first mathematical objects to questions of research:

- Elements (I): *secondary-school mathematics, from arithmetic to the first proofs.*
- Foundations (II): *the foundations of university mathematics.*
- Graduate Mathematics (III): *deeper study and preparation for research.*
- Correspondences (IV): *the research level, from class field theory to the Langlands program.*
- Mathematical Physics (V): *the research level, from symmetries to strings.*

These levels guide the reader without imposing an academic timetable. Parts and chapters mark the stages of the journey; the pace depends on the reader's background and the questions they wish to explore.

Volumes I, II, and III successively build the prerequisites for the next volume. Readers may enter at the level for which they have the necessary background. Volumes IV and V share the foundation of Graduate Mathematics and may be read independently of each other. The bridges at the beginning of each volume explain the change in perspective.

NOTATIONS

$\mathbb{N}$	<i>natural numbers</i>
$\mathbb{Z}$	<i>integers</i>
$\mathbb{Q}$	<i>rational numbers</i>
$\mathbb{R}$	<i>real numbers</i>
$\mathbb{C}$	<i>complex numbers</i>
$\in$	<i>belongs to</i>
$\subset$	<i>is a subset of (equality allowed)</i>
$\cup, \cap, \emptyset$	<i>union, intersection, empty set</i>
$\mathcal{P}(E)$	<i>power set of E</i>
$\forall, \exists$	<i>for all, there exists</i>
$\Rightarrow, \Leftrightarrow$	<i>implies, is equivalent to</i>
$ x $	<i>absolute value of x</i>
$\sqrt{x}$	<i>square root of x</i>
$\leq, \geq$	<i>less than or equal to, greater than or equal to</i>
π	<i>circumference divided by diameter</i>
∞	<i>infinity</i>
$\sin, \cos, \tan$	<i>trigonometric functions</i>
$f'(x)$	<i>derivative of f at x</i>
$\int_a^b f(x) dx$	<i>integral of f from a to b</i>
$\sum, \prod$	<i>sum, product</i>
$n!, \binom{n}{k}$	<i>factorial, binomial coefficient</i>
i	<i>imaginary unit, $i^2 = -1$</i>
$\bar{z}, z , \arg(z)$	<i>conjugate, modulus, argument</i>
$\operatorname{Re}(z), \operatorname{Im}(z)$	<i>real part, imaginary part</i>
$\rightarrow$	<i>tends to</i>
$x \mapsto f(x)$	<i>map sending x to $f(x)$</i>
$\vec{u}$	<i>vector u</i>
$f \circ g$	<i>composition of f and g</i>
$\ x\ $	<i>norm of x</i>
$\langle x, y \rangle$	<i>inner product of x and y</i>
$\dim V$	<i>dimension of a vector space V</i>
$\ker f, \operatorname{Im} f$	<i>kernel, image of a linear map</i>
$\det A$	<i>determinant of a matrix A</i>
$\operatorname{GL}_n, \operatorname{SL}_n, \operatorname{O}_n$	<i>general linear, special linear, orthogonal groups</i>
$a \equiv b \pmod{n}$	<i>congruence modulo n</i>

$\cong, \simeq$	<i>isomorphic to, equivalent to</i>
$\oplus, \otimes$	<i>direct sum, tensor product</i>
$\lim$	<i>limit</i>
$\sup, \inf$	<i>supremum, infimum</i>
$O(\cdot), o(\cdot), \sim$	<i>Landau notation, asymptotic equivalence</i>
$\frac{d}{dx}, \frac{\partial}{\partial x}$	<i>ordinary differentiation, partial differentiation</i>
C^k	<i>functions with continuous derivatives through order k</i>
C^∞	<i>smooth functions</i>
$\mathcal{L}(E, F)$	<i>continuous linear maps from E to F</i>
E^*, E^{**}	<i>continuous dual, bidual of E</i>
$\sigma(T), \rho(T)$	<i>spectrum, resolvent set of an operator T</i>
$W^{k,p}(\Omega), H^s(\Omega)$	<i>Sobolev spaces</i>
$\mathcal{D}'(\Omega)$	<i>distributions on Ω</i>
$\mathcal{S}(\mathbb{R}^n), \mathcal{S}'(\mathbb{R}^n)$	<i>Schwartz space, tempered distributions</i>
$\text{Spec } A$	<i>spectrum of a ring A</i>
$\text{Hom}, \text{Ext}, \text{Tor}$	<i>homological algebra functors</i>
$\wedge$	<i>exterior product</i>
H^n, π_1	<i>degree-n cohomology, fundamental group</i>
$\text{Gal}(L/K), [L : K]$	<i>Galois group, extension degree</i>
$\mathcal{O}_K, \text{Cl}(K), h_K$	<i>ring of integers, class group, class number of K</i>
$v_{\mathfrak{p}}$	<i>$\mathfrak{p}$-adic valuation</i>
$\mathbb{Q}_p, \mathbb{Z}_p$	<i>p-adic numbers, p-adic integers</i>
$\mathbb{A}_K, \mathbb{I}_K, C_K$	<i>adeles, ideles, idele classes of K</i>
$\text{Gal}(\bar{K}/K)$	<i>absolute Galois group of K</i>
$\text{Frob}_{\mathfrak{p}}$	<i>Frobenius element at $\mathfrak{p}$</i>
$\rho : G_K \rightarrow \text{GL}(V)$	<i>Galois representation</i>
$\zeta(s)$	<i>Riemann zeta function</i>
$L(s, \pi), L(s, \chi)$	<i>automorphic and Dirichlet L-functions</i>
$\hat{G}, {}^L G$	<i>Langlands dual, L-group of G</i>
Bun_G	<i>stack of G-bundles</i>
$H_{\text{ét}}^i$	<i>degree-i étale cohomology</i>
$D\text{-mod}$	<i>category of D-modules</i>
$\text{Loc}_{\hat{G}}$	<i>$\hat{G}$-valued local systems</i>
$\text{QCoh}(Y)$	<i>quasi-coherent sheaves on Y</i>
$\text{IndCoh}_{\text{Nilp}}(Y)$	<i>ind-coherent sheaves with nilpotent singular support</i>
$\text{DMod}^{1/2}$	<i>half-twisted D-modules</i>
Gr_G	<i>affine Grassmannian of G</i>
$\tilde{G}$	<i>another notation for the Langlands dual</i>

Contents

Preface	v
To the Reader	vii
Note on the Levels	ix
Notations	x
From Graduate Mathematics to Correspondences	i
 I Reciprocity and the Language of Arithmetic	 2
1 Number Fields and Rings of Integers	3
2 Local Fields and p -adic Numbers	20
3 Adeles and Ideles	35
4 Reciprocity and Class Field Theory	47
5 Galois Representations: Examples and Questions	66

II	Forms, Symmetries, and Automorphic Representations	77
6	The Upper Half-Plane, Modular Groups, and Modular Curves	78
7	Modular Forms and Hecke Operators	95
8	L-Functions and First Dictionaries	III
9	Reductive Groups and the Dual Group	127
10	Automorphic Forms and Representations	143
III	Arithmetic Geometry and the First Major Theorems	159
11	Algebraic Varieties and Curves	160
12	Schemes, Sheaves, and Families	175
13	Elliptic Curves and Arithmetic	192
14	Abelian Varieties, Duality, and Tate Modules	209
15	Étale Cohomology and the Weil Theorems	225
16	Modularity, Deformations, and Fermat	240
17	Periods, Special Values, and the Arithmetic of Forms	257

IV	Arithmetic Correspondences: Methods and Realizations	271
18	Harmonic Analysis and Local Correspondences	272
19	Trace Formulas and Endoscopy	291
20	Functoriality: Results and Program	307
21	Function Fields, Shtukas, and Langlands Theorems	322
V	Further Arithmetic Developments	336
22	Shimura Varieties	337
23	Motives, Correspondences, and Motivic L-Functions	351
24	p-adic Geometry and Contemporary Local Correspondences	365
VI	Tools for Geometric Langlands	382
25	Differential Modules and Riemann–Hilbert	383
26	Bundles on Curves and the Stack Bun_G	408
27	Local Systems, Higgs Bundles, and Hitchin	420
28	Derived Categories, Ind-Coherent Sheaves, and Singular Support	435

VII	Geometric Langlands and the 2024 Proof	449
29	From Classical to Geometric: the Abelian Case	450
30	Geometric Hecke, the Affine Grassmannian, and Satake	479
31	The Geometric Langlands Theorem: Statement and Scope	496
32	Constructing the Functor and Whittaker Normalization	511
33	Kac–Moody Localization and Fundamental Local Equivalence	526
34	Eisenstein, Constant Terms, and Induction on Levi Groups	544
35	Ambidexterity and the Equivalence Problem	564
36	Multiplicity One and Completion of the Proof	583
VIII	Toward Physics	603
37	Correspondences and Dualities: Toward Physics	604
	At the End of This Volume	616
	Bibliography	617
	Index	621

FROM GRADUATE MATHEMATICS TO CORRESPONDENCES

Until now, each branch of mathematics had its own language. Analysis spoke of limits and measures; algebra, of groups and ideals; geometry, of manifolds and sheaves. What follows is the story of a discovery: these languages are dialects of a common grammar.

The Langlands program, toward which the parts of Correspondences converge, is one of contemporary mathematics' most ambitious undertakings. It posits deep correspondences between number theory, harmonic analysis, and algebraic geometry, three domains that might seem independent but are connected by hidden symmetries whose reach we are only beginning to grasp.

The route begins with arithmetic foundations: number fields, p -adic numbers, adeles, and reciprocity. It then constructs modular and automorphic forms, followed by arithmetic geometry through the Weil and modularity theorems. The methods of the Langlands program, $shtukas$, Shimura varieties, motives, and p -adic geometry precede the tools of the geometric language. Differential modules, stacks, and categories then make a path through the 2024 proof possible. The final stage prepares the physical reading without introducing it into the theorem's proof.

Lie groups, used throughout this volume, are developed in Chapter 78 of Graduate Mathematics; the reader may return there before approaching reductive groups.

The grammar through which reality composes itself is unfinished. What we know of it, what we glimpse, and what remains to be discovered are the subject of this volume.

Part I

Reciprocity and the Language of Arithmetic

Number fields provide the global setting; their completions isolate each place. Adeles and ideles gather these data before reciprocity identifies the quotients governing abelian extensions. Galois representations then broaden the question: how can we retain an action when the group is no longer captured by its characters?

CHAPTER I

NUMBER FIELDS AND RINGS OF INTEGERS

Adjoining a number to the rationals changes the operations available, but also what it means to be an integer. A fraction may satisfy a monic equation; a number may lose unique factorization; an ideal may retain that uniqueness without having a generator. These differences call for an arithmetic that recognizes its objects before counting them. Embeddings make them visible from several perspectives, and lattices allow us to measure their differences. Passing to number fields does not replace ordinary integers with more complicated numbers: it reveals the precise conditions that made their arithmetic work.

Articles in this chapter:

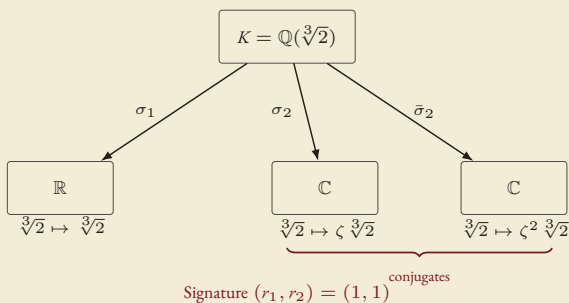
- 001.** *Number Fields* — The roots of the minimal polynomial give the embeddings and signature.
- 002.** *Rings of Integers* — A basis of the field need not generate all its integers.
- 003.** *Norm, Trace, Discriminant* — Matrix calculations distinguish invariants of an element from those of a basis.
- 004.** *Dedekind Ideals* — Two factorizations of an element recover the same ideal factorization.
- 005.** *Class Group* — A finite bound makes the failure of principality computable.
- 006.** *Dirichlet Units* — Logarithms reveal a lattice, with a normalization to respect.

I. NUMBER FIELDS. *WHAT* happens when we adjoin $\sqrt{-5}$ to the rationals? We obtain a field $\mathbb{Q}(\sqrt{-5})$ whose ring of integers $\mathbb{Z}[\sqrt{-5}]$ gives the integer 6 two essentially different factorizations: $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Factorization therefore requires

objects beyond those that sufficed in $\mathbb{Z}$. Before returning to this calculation with ideals, we need to understand the different ways of representing the field itself.

DEFINITION 1.1: A *number field* is a finite extension K of $\mathbb{Q}$. Its *degree* is the integer $n = [K : \mathbb{Q}]$. The field $\mathbb{Q}$ itself is a number field of degree 1. The quadratic fields $\mathbb{Q}(\sqrt{d})$ (with $d \in \mathbb{Z}$ squarefree, $d \neq 0, 1$) have degree 2, and the cyclotomic fields $\mathbb{Q}(\zeta_m)$ have degree $\varphi(m)$.

Every number field admits exactly n embeddings into $\mathbb{C}$, some real and others complex. Their distribution determines the arithmetic nature of the field.



The three embeddings of $\mathbb{Q}(\sqrt[3]{2})$: one real and a pair of complex conjugates, giving signature $(1, 1)$.

DEFINITION 1.2: Let K be a number field of degree n . An *embedding* of K is a field homomorphism $\sigma : K \hookrightarrow \mathbb{C}$. There are exactly n of them. Of these, r_1 are *real* (their images lie in $\mathbb{R}$), and the remaining $n - r_1$ form r_2 pairs of complex conjugates. The pair (r_1, r_2) , with $r_1 + 2r_2 = n$, is the *signature* of K .

PROPOSITION 1.3: By the primitive element theorem, every number field can be written $K = \mathbb{Q}(\alpha)$ for an algebraic α , a root of an irreducible polynomial $f \in \mathbb{Q}[x]$ of degree n . A basis of K over $\mathbb{Q}$ is then $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$.

Separability in characteristic zero and the primitive element theorem are recalled from the article “Separability” in *Graduate Mathematics*. Here they reduce the count of embeddings to a count of roots.

FROM ROOTS TO EMBEDDINGS: If $K = \mathbb{Q}(\alpha)$ and f is the minimal polynomial of α , an embedding must send α to a root of f . Conversely, each root β defines a homomorphism $\mathbb{Q}[X]/(f) \rightarrow \mathbb{C}$ by evaluation at β . This field homomorphism is injective. Since f is separable of degree n , its n roots give exactly n embeddings.

EXAMPLE: The field $\mathbb{Q}(\sqrt{2})$ has signature $(2, 0)$: its two embeddings send $\sqrt{2}$ to $\pm\sqrt{2}$, both real. The field $\mathbb{Q}(i)$ has signature $(0, 1)$: its two embeddings send i to $\pm i$, forming a conjugate pair. The field $\mathbb{Q}(\sqrt[3]{2})$ has signature $(1, 1)$: one real cube root and two complex conjugate roots.

REMARK 1.4: The signature (r_1, r_2) governs the rank of the unit group (Dirichlet’s theorem: rank $r_1 + r_2 - 1$), the sign of the discriminant $((-1)^{r_2})$, and the form of the canonical embedding of K into $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. It condenses into two integers the archimedean constraints on the entire arithmetic of K .

Embeddings thus give several compatible readings of the same number: algebraic relations are preserved even as its images change.

This multiplicity does not turn the field into several independent fields; it lets us observe it in all its archimedean directions. It does not yet tell us which elements will play the role of integers. To begin arithmetic, we must choose within the field the ring that contains them all.

2. RINGS OF INTEGERS. ORDINARY integers form a well-defined subring of $\mathbb{Q}$. But when we pass to a number field K , which elements play the role of integers? The answer is not immediate: in $\mathbb{Q}(\sqrt{5})$, the golden ratio $\varphi = \frac{1+\sqrt{5}}{2}$, which scarcely looks like an integer, satisfies $\varphi^2 - \varphi - 1 = 0$ and deserves the name algebraic integer.

DEFINITION 2.1: An *algebraic integer* is a complex number α that is a root of a monic polynomial with coefficients in $\mathbb{Z}$: $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$, with $a_i \in \mathbb{Z}$. All algebraic integers together form a subring $\overline{\mathbb{Z}}$ of $\mathbb{C}$.

The module characterization clarifies this notion: α is an algebraic integer if and only if $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$ -module. Integrality can be read from the finite generation of this module.

DEFINITION 2.2: Let K be a number field. The *ring of integers* of K is $\mathcal{O}_K = K \cap \overline{\mathbb{Z}}$, the set of algebraic integers belonging to K .

PROPOSITION 2.3: If K is a number field of degree n , then $\mathcal{O}_K$ is a free $\mathbb{Z}$ -module of rank n . In other words, there is an *integral basis* $\{\omega_1, \dots, \omega_n\}$ such that $\mathcal{O}_K = \mathbb{Z}\omega_1 \oplus \cdots \oplus \mathbb{Z}\omega_n$.

We use this theorem from the article “Algebraic Integers and Dedekind Domains” in *Graduate Mathematics*. It says more than that the field has a basis: the coordinates of its integers in this particular basis are themselves ordinary integers. A basis over $\mathbb{Q}$ need not have this property.

THE BASIS COMPLETED BY THE GOLDEN RATIO: In $K = \mathbb{Q}(\sqrt{5})$, the quadratic formula for the ring of integers, stated without proof below, gives

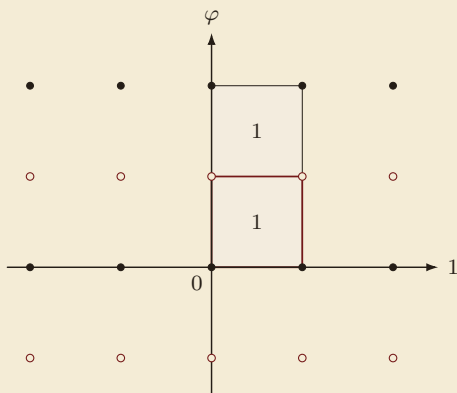
$$\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\varphi, \quad \varphi = \frac{1 + \sqrt{5}}{2}, \quad \varphi^2 = \varphi + 1.$$

The element φ does not belong to $\mathbb{Z}[\sqrt{5}]$: its coordinates in the basis $(1, \sqrt{5})$ are $1/2$ and $1/2$. Conversely, $\sqrt{5} = 2\varphi - 1$, so

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

The index is 2: the two cosets are represented by 0 and φ . Adjoining a generator of the field had not produced the ring of all its integers.

In the coordinates of the integral basis $(1, \varphi)$, the index becomes visible: the subring occupies every other row of the lattice. A fundamental cell of this sublattice contains two cells of the full lattice.



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

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

Coordinates in the basis $(1, \varphi)$, not a Minkowski embedding. Solid dots represent $\mathbb{Z}[\sqrt{5}]$; hollow dots complete $\mathcal{O}_K$. Each of the two cells has area one in these coordinates.

EXAMPLE: For $K = \mathbb{Q}(\sqrt{d})$, with d squarefree and $d \neq 0, 1$, the formula stated without proof is $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ if $d \equiv 2$ or $3 \pmod{4}$, and $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ if $d \equiv 1 \pmod{4}$. The ring of Gaussian integers $\mathbb{Z}[i]$ (the case $d = -1$) is the most familiar example. For cyclotomic fields, $\mathcal{O}_{\mathbb{Q}(\zeta_p)} = \mathbb{Z}[\zeta_p]$ when p is prime.

REMARK 2.4: Determining $\mathcal{O}_K$ is a nontrivial algorithmic problem, even for cubic fields. The inclusion $\mathbb{Z}[\alpha] \subset \mathcal{O}_K$ can be strict: the ring of integers is larger than a naive choice of generator suggests, and its finer arithmetic structure lies in that excess.

An integral basis governs the expression of every integer in the field, like a grammar specifying which coefficients are allowed. It is not canonical: several bases give the same ring. The next calculation

must therefore distinguish what depends on this expression from what survives a change of basis.

3. NORM, TRACE, DISCRIMINANT. *CHANGING* a basis can multiply a discriminant without changing the field. In $\mathbb{Q}(\sqrt{5})$, the bases $(1, \sqrt{5})$ and $(1, \varphi)$ describe the same vector space, but only one generates all the integers over $\mathbb{Z}$. To measure this difference, we first return to two invariants of an endomorphism: its trace and its determinant.

DEFINITION 3.1: For $\alpha \in K$, multiplication $m_\alpha : x \mapsto \alpha x$ is an endomorphism of the $\mathbb{Q}$ -vector space K . Its trace is the *trace* of α , and its determinant is the *norm*:

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

The equalities involving embeddings follow from the separable decomposition $K \otimes_{\mathbb{Q}} \mathbb{C} \simeq \mathbb{C}^n$, which we use here as a known result.

Trace is additive and norm is multiplicative. Both send algebraic integers to $\mathbb{Z}$, because multiplication by an integer has an integer matrix in an integral basis. The algebraic norm is not a vector-space norm: it can be negative and does not by itself measure all the absolute values of the conjugates.

A MULTIPLICATION WORKED OUT: Keep $\varphi^2 = \varphi + 1$. For $\alpha = a + b\varphi$, with $a, b \in \mathbb{Q}$, the images of 1 and φ give

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

Thus $\mathrm{Tr}(\alpha) = 2a + b$ and $N(\alpha) = a^2 + ab - b^2$. In particular, $\mathrm{Tr}(\varphi) = 1$, $N(\varphi) = -1$, and $\mathrm{Tr}(\varphi^2) = 3$.

For a basis $B = (\omega_1, \dots, \omega_n)$ of K over $\mathbb{Q}$, its *discriminant* is

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

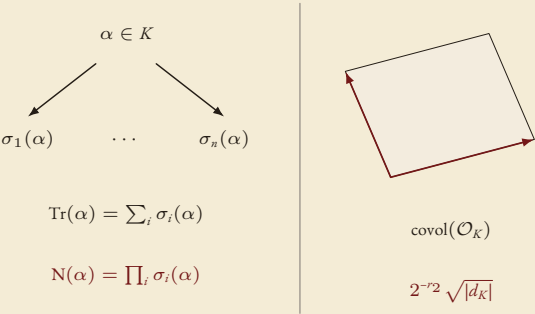
The second equality follows from the matrix identity $T = S^{\dagger}S$. Separability guarantees that the trace form is nondegenerate, so this determinant is nonzero.

TWO BASES, TWO DISCRIMINANTS: The trace matrices are, respectively,

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

Their determinants are 5 and 20. If $B' = BP$, then $T_{B'} = P^{\dagger}T_BP$, hence $\text{disc}(B') = (\det P)^2 \text{disc}(B)$. Here $\sqrt{5} = 2\varphi - 1$ gives $\det P = 2$: the index calculated in the preceding article appears squared.

Two integral bases of the same ring are related by an integer matrix invertible over $\mathbb{Z}$, with determinant ± 1 . Their common discriminant is the *field discriminant*, denoted d_K . Thus $d_{\mathbb{Q}(\sqrt{5})} = 5$, not 20.



Trace adds conjugates and norm multiplies them. For an integral basis, the real covolume of the unscaled Minkowski embedding is $2^{-r_2} \sqrt{|d_K|}$.

The discriminant describes the fabric of the integers through their embeddings. This geometric reading requires a fixed measure: the complex determinant of all embeddings is not directly the real volume in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. The factor in the caption mediates between

the two conventions. The sign of d_K is $(-1)^{r_2}$; its absolute value enters the arithmetic bounds we shall meet.

The basis has changed, but the field has stayed the same. The discriminant has distinguished two rings within it; ideal factorization will now reveal how their primes behave.

4. DEDEKIND IDEALS. IN $\mathbb{Z}[\sqrt{-5}]$, the equality $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ is more than a reordering of factors. Put $s = \sqrt{-5}$. The norm $N(a + bs) = a^2 + 5b^2$ takes neither the value 2 nor the value 3 on integers. Since the norms of 2, 3, and $1 \pm s$ are 4, 9, and 6, a decomposition of any of them into two nonunits would force one of these impossible values. All four factors are irreducible. The only units are ± 1 , and the two factorizations are not associate.

The discussion of Dedekind domains in *Graduate Mathematics* promised a recovery of uniqueness at the level of ideals. We keep its convention: a *Dedekind domain* is an integral domain that is Noetherian, integrally closed in its fraction field, and of dimension 1. It is therefore not a field, and its nonzero prime ideals are maximal.

The ring $\mathcal{O}_K$ satisfies these conditions. It is Noetherian because it is finite over $\mathbb{Z}$; it is integrally closed by transitivity of integrality. Dimension 1 is a known result: every quotient by a nonzero prime ideal is a finite field.

FACTORIZATION AND INVERTIBILITY: Every nonzero proper ideal is, uniquely up to order, a product of powers of distinct nonzero prime ideals. A nonzero fractional ideal is a submodule I of K such that $dI \subset \mathcal{O}_K$ for some $d \in \mathcal{O}_K \setminus \{0\}$. We take as given that every nonzero ideal is invertible, with

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

This is the substantial step in factorization. Uniqueness then follows directly: a prime ideal containing a product contains one

factor; maximality identifies the prime factors, and their inverses allow cancellation. Existence also uses the Noetherian property and is not proved again here.

The empty product gives the unit ideal. Nonzero fractional ideals thus form the free abelian group on the nonzero prime ideals. For calculations, we use the norm of a nonzero integral ideal, $N(\mathfrak{a}) = [\mathcal{O}_K : \mathfrak{a}]$. Its multiplicativity and the equality $N((\alpha)) = |N_{K/\mathbb{Q}}(\alpha)|$ are stated without proof.

THE SAME PRODUCT BEHIND BOTH EXPRESSIONS: In $\mathbb{Z}[s]$, put

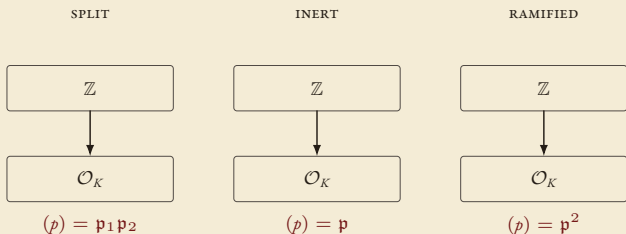
$$\mathfrak{p}_2 = (2, 1 + s), \quad \mathfrak{p}_3 = (3, 1 + s), \quad \bar{\mathfrak{p}}_3 = (3, 1 - s).$$

The quotients are $\mathbb{F}_2$, $\mathbb{F}_3$, and $\mathbb{F}_3$, by substituting 1, -1, and 1 for s , respectively. These ideals are therefore prime, of norms 2, 3, and 3. The generators of $\mathfrak{p}_2^2$ are 4, $2(1+s)$, and $(1+s)^2 = -4+2s$: all are divisible by 2. The inclusion $\mathfrak{p}_2^2 \subset (2)$ is an equality because both norms are 4. Similarly, the generators give the following inclusions, and the norms give equalities:

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

Thus $(6) = \mathfrak{p}_2^2 \mathfrak{p}_3 \bar{\mathfrak{p}}_3$ is the unique ideal factorization of both original products.

A rational prime p is *ramified* when an exponent in the factorization of $p\mathcal{O}_K$ exceeds 1. The equivalent criterion $p \mid d_K$ is stated without proof. Here $d_K = -20$: only 2 and 5 ramify, and the square $\mathfrak{p}_2^2$ already shows this for 2.



In a quadratic field, a prime splits, remains inert, or ramifies. The last case is identified by a repeated ideal factor.

Ideals give a common expression for the two decompositions of 6. This expression does not make every ideal principal: it preserves precisely the factors that no single element represents. The class group will measure this difference.

5. CLASS GROUP. If ideals factor uniquely, why do elements not do so? One condition is missing: every ideal factor would have to be generated by an element. In $\mathbb{Z}[\sqrt{-5}]$, the ideal $\mathfrak{p}_2 = (2, 1 + \sqrt{-5})$ has norm 2, but no element has that norm. The quotient identifying ideals that differ by a principal factor retains exactly this obstruction.

DEFINITION 5.1: The *class group* of K is the quotient

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

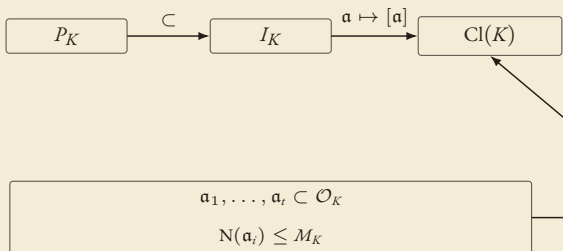
where I_K is the group of nonzero fractional ideals and P_K its subgroup of principal ideals (α) , $\alpha \in K^\times$. It is trivial if and only if $\mathcal{O}_K$ is a principal ideal domain, a condition equivalent here to unique factorization.

Two ideals thus have the same class when one is obtained by multiplying the other by a nonzero element of the field. The question is how many classes remain after this identification.

MINKOWSKI'S BOUND, STATED WITHOUT PROOF: Every class contains a nonzero *integral* ideal $\mathfrak{a}$ whose norm, the index $[\mathcal{O}_K : \mathfrak{a}]$, satisfies

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

The adjective integral means $\mathfrak{a} \subset \mathcal{O}_K$. It makes the bound effective: there are only finitely many subgroups of bounded index in the free group $\mathcal{O}_K \simeq \mathbb{Z}^n$. For a given index m , each contains $m\mathbb{Z}^n$ and comes from a subgroup of the finite group $(\mathbb{Z}/m\mathbb{Z})^n$. The class group is therefore finite; its order h_K is the *class number*.



Every class has a representative in this finite set.

The quotient by principal ideals retains the classes; Minkowski allows them to be represented by finitely many integral ideals of bounded norm.

COMPUTING TWO CLASSES: For $K = \mathbb{Q}(\sqrt{-5})$, the signature is $(0, 1)$ and $d_K = -20$, so

$$M_K = \frac{2}{\pi} \sqrt{20} \simeq 2.85 < 3.$$

Every class has a representative of norm 1 or 2. The only ideal of norm 1 is $\mathcal{O}_K$. An ideal of norm 2 has quotient $\mathbb{F}_2$; the image of $\sqrt{-5}$ must be a root of $X^2 + 5 = (X + 1)^2$ modulo 2. There is only one choice: this ideal is $\mathfrak{p}_2$.

If $\mathfrak{p}_2 = (a + b\sqrt{-5})$, then $a^2 + 5b^2 = 2$, which is impossible for integers a, b . Its class is therefore nontrivial. The equality $\mathfrak{p}_2^2 = (2)$ shows that its square is trivial. Thus

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

The quotient classifies ideals as one classifies expressions up to an allowed change. This identification does not remove the ideals themselves: it forgets only their principal factor. The bound has let us run through all the classes, not merely exhibit two of them. For $\mathbb{Q}(i)$, the same bound is $4/\pi < 2$, so only the unit ideal is needed and $h_K = 1$. The contrast with $\mathbb{Q}(\sqrt{-5})$ has now been calculated. The invariant also has an analytic expression, which we cite as a preview:

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

Here w_K counts the roots of unity, and R_K is the regulator introduced next. This formula, stated without proof, brings classes and units together. The former distinguish ideals without a generator; the latter describe how many generators a single principal ideal can have.

6. DIRICHLET UNITS. THE equation $x^2 - 2y^2 = 1$ has infinitely many integer solutions, yet the unit $1 + \sqrt{2}$ has norm -1 . Its square, $3 + 2\sqrt{2}$, has norm $+1$. This change of sign distinguishes the group of all units from the subgroup solving Pell's equation. To understand their infinitude, we must look at absolute values in the different embeddings.

DEFINITION 6.1: The *units* of $\mathcal{O}_K$ are its invertible elements:

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

The equivalence can be checked on multiplication by α : its integer matrix is invertible over $\mathbb{Z}$ exactly when its determinant is ± 1 . The assumption $\alpha \in \mathcal{O}_K$ is necessary; the norm of an element of the field alone does not make it an integer.

DIRICHLET'S THEOREM, STATED WITHOUT PROOF: For a field of signature (r_1, r_2) ,

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

where μ_K is the finite cyclic group of roots of unity in K .

The free part can therefore be infinite, but it has finitely many generators. Logarithms explain the stated rank. Choose the real embeddings σ_i and one embedding τ_j from each complex conjugate pair. Put

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

The absolute norm is the product of the real absolute values and the squares of the complex absolute values. For a unit it is 1; taking logarithms gives

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

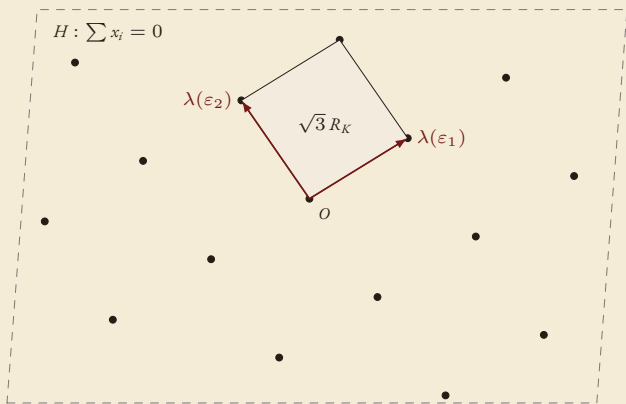
The image lies in the hyperplane H of coordinate sum zero. The kernel is μ_K , by Kronecker's theorem, stated without proof. That the image is discrete *and has full rank* in H is the geometry-of-numbers step that we also take as given. Containment in a hyperplane would not, by itself, prove the rank.

DEFINITION 6.2: Put $m = r_1 + r_2$ and $r = m - 1$. For fundamental units $\varepsilon_1, \dots, \varepsilon_r$, the *regulator* is

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

after deleting one of the m rows. Since the row sum is zero, all resulting determinants have the same absolute value. A change of lattice basis multiplies this determinant by ± 1 . In rank zero, we set $R_K = 1$.

With the usual inner product on $\mathbb{R}^m$, the covolume in H is $\sqrt{m} R_K$. Indeed, the parametrization by the first $m - 1$ coordinates has Gram matrix $I + \mathbf{1}\mathbf{1}^t$, of determinant m . The regulator is therefore a normalized volume, not this Euclidean volume itself.



A schematic rank-2 drawing: the vectors generate the lattice in $H \subset \mathbb{R}^3$. The Euclidean area of the cell is $\sqrt{3} R_K$.

THE TWO SIGNS IN PELL'S EQUATION: We use the known fact that $\varepsilon = 1 + \sqrt{2}$ is a fundamental unit for $\mathbb{Q}(\sqrt{2})$. Its units are $\pm \varepsilon^k$, $k \in \mathbb{Z}$,

with norm $(-1)^k$. Those of norm $+1$ are exactly $\pm(3 + 2\sqrt{2})^\ell$, $\ell \in \mathbb{Z}$. If $L = \log(1 + \sqrt{2})$, then

$$\lambda(\varepsilon) = (L, -L), \quad R_K = L \simeq 0.88.$$

The vector has length $\sqrt{2}L$, as required by the normalization. For $\mathbb{Q}(i)$, in contrast, the signature $(0, 1)$ gives rank zero: the only units are $1, i, -1, -i$, and $R_K = 1$.

The logarithmic map translates multiplication into addition, but its translation loses the roots of unity. Keeping them separately recovers the whole group. In the analytic class number formula, the product $h_K R_K$ accompanies this torsion: classes and units describe two aspects of the same arithmetic. Archimedean embeddings have made them visible; valuations associated with primes will offer the next perspective.

FURTHER READING

- **Dedekind, R.**, Über die Theorie der ganzen algebraischen Zahlen, *supplement to Dirichlet's Vorlesungen über Zahlentheorie. Historical source for ideal theory (German)*.
- **Samuel, P.** (2008), Algebraic Theory of Numbers, *Dover, translated by Allan J. Silberger. English translation of Théorie algébrique des nombres; a concise treatment of the arithmetic foundations*.
- **Neukirch, J.** (1999), Algebraic Number Theory, *Springer, Grundlehren 322. Ideals, places, and reciprocity*.
- **Cassels, J.W.S. and Fröhlich, A.** (eds., 1967), Algebraic Number Theory, *Academic Press. Reference accounts extending to class field theory*.
- **Milne, J.S.** (2020), Algebraic Number Theory, *version 3.08, Chapters 2–5: integers, ideals, classes, and units; Theorem 4.3 for Minkowski's bound*.

RESEARCH QUESTIONS

- (1) Beyond Brumer–Stark. *The link between ideal classes, L -values, and units now has an integral theorem: Dasgupta–Kakde–Silliman–Wang prove Brumer–Stark over $\mathbb{Z}$ in their work first posted in 2023. Research therefore concerns extensions of this setting and the explicit constructions they would allow, rather than another proof of the same statement.*
- (2) Stark and higher rank. *How can leading coefficients of L -functions be expressed through units? Higher-rank formulations involve logarithmic determinants and exterior powers of unit groups. Rubin’s 1996 paper specifies an integral version in the abelian setting. Its hypotheses and proved cases must be distinguished: the Brumer–Stark theorem is not an undifferentiated resolution of all Stark conjectures.*
- (3) Hilbert’s twelfth problem. *Construct abelian extensions through special values of functions: cyclotomic fields over $\mathbb{Q}$ and complex multiplication over imaginary quadratic fields are the classical models. For totally real fields, Dasgupta–Kakde, Brumer–Stark Units and Explicit Class Field Theory, introduction, §1.4, give a p -adic construction. They explicitly distinguish it from the complex-analytic setting envisaged by Hilbert. The nature of the allowed functions is therefore part of the problem and must accompany any claim of a solution.*