Math 225AB: Algebraic Number Theory

Simon Rubinstein–Salzedo

Winter and Spring 2006

0.1 Introduction

Professor: Adebisi Agboola.
Office Hours: Tuesday: 11:15-12:30, Thursday: 11:15-12:30 (225A), Wednesday 10:00-12:00 (225B).
Textbooks: *Algebraic Number Theory* by Fröhlich and Taylor, *Algebraic Number Theory* by Lang, *Number Fields* by Marcus, *Introduction to Cyclotomic Fields* by Washington.

Course Outline: We shall aim to cover the following topics. Additional topics will be covered if time permits.
Basic commutative algebra: Noetherian properties, integrality, ring of integers.
More commutative algebra: Dedekind domains, unique factorization of ideals, localization.
Norms, traces, and discriminants.
Decomposition of prime ideals in an extension field.
Class numbers and units. Finiteness of the class number: Minkowski bounds. Dirichlet's unit theorem. Explicit calculation of units.
Decomposition of prime ideals revisited: the decomposition group and the inertia group associated to a prime ideal. A nice proof of quadratic reciprocity.
Basic Theory of completions and local fields.
The Dedekind zeta function and the analytic class number formula.
Dirichlet characters; Dirichlet L-functions; primes in arithmetic progressions; the explicit class number formula for cyclotomic fields.
Artin L-functions: definitions and basic properties.
Miscellaneous topics, e.g. Stickelberger's theorem, p-adic L-functions, Stark's conjectures.

Additional books that may be of use are:
Galois Theory — Lang's *Algebra*
Number Theory — Hecke's *Theory of Algebraic Numbers*, Borevich and Shafarevich's *Number Theory*, and Serre's *A Course in Arithmetic*
Commutative Algebra — Atiyah and MacDonald's *Introduction to Commutative Algebra*, Zariski and Samuel's *Commutative Algebra*, and Eisenbud's *Commutative Algebra with a View Toward Algebraic Geometry*.

Chapter 1

Basic Commutative Algebra

Example. In $\mathbb{Z}[\sqrt{-6}]$, we do not have unique factorization of elements, e.g. $6 = -\sqrt{-6}\sqrt{-6} = 2 \cdot 3$. We shall later establish unique factorization into prime ideals. We will then have $6\mathbb{Z}[\sqrt{-6}] = (\sqrt{-6}, 2)^2(\sqrt{-6}, 3)^2$.

Definition 1.1 Let M be an R-module, where R is a commutative ring with a 1. We say that M is a noetherian R-module if every R-submodule is finitely generated over R.

Example.

1. M is finite.
2. R is a field and M is a finite-dimensional vector space.

Definition 1.2 We say that the ring R is noetherian iff R is a noetherian R-module, i.e. iff all ideals are finitely generated over R.

Example. A PID is a noetherian ring.

Proposition 1.3 (See 220ABC) The following are equivalent:

1. R is a noetherian ring.

2. Every ascending chain of R-ideals stabilizes.

3. Every nonempty set of R-ideals has a maximal element.

Proposition 1.4 Suppose that the following sequence of R-modules is exact:

$$0 \to M \to N \to P \to 0.$$

Then N is noetherian iff M and P are noetherian. (Since then the exact sequence is $0 \to M \to N \to M/N \to 0$.)

Proposition 1.5 If M is finitely generated as an R-module, and if R is a noetherian ring, then M is a noetherian R-module.

"Proof." $\bigoplus_1^n R \twoheadrightarrow M$ since M is finitely generated. Now apply Proposition 1.4.

Proposition 1.6 Suppose that S and R are rings with $S \supset R$. Suppose that R is a noetherian ring and S is finitely generated as an R-module. Then S is a noetherian ring.

Proof. $R[X_1, \ldots, X_n] \twoheadrightarrow S$, where $R[X_1, \ldots, X_n]$ is noetherian by the Hilbert Basis Theorem.

Recall that an R-module M is said to be free of rank n if there exists an R-module isomorphism $M \simeq \bigoplus_1^n R$. Then rank n is uniquely determined because R is commutative.

Proposition 1.7 Let M be a finitely generated R-module, and let R be a PID (or Euclidean domain). Then we have an isomorphism $M \simeq T(M) \oplus$ a free R-module of finite rank, where $T(M) \simeq \bigoplus_i R/a_iR$, with $a_i \mid a_{i+1}$.

Definition 1.8 (Abstract version) Let R and S be rings with $R \subset S$. We say that an element $x \in S$ is **integral over** R iff $R[x]$ is finitely generated as an R-module.

Definition 1.9 (Historical version) Let $x \in S \supset R$. We say that x is integral over R iff x satisfies some monic polynomial $m(T) \in R[T]$.

These definitions are equivalent.

1. Let $x \in S$ be a root of a monic polynomial $m(T) \in R[T]$. We wish to show that $R[x]$ is finitely generated over R. We claim that $\langle 1, x, \ldots, x^m \rangle_R = \langle 1, x, \ldots, x^{n-1} \rangle_R$ for any $m \geq n-1$, where $n = \deg(m(T))$. Suppose that $m(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0$. We know that $x^n = -a_{n-1}x^{n-1} - \cdots - a_0$, so $x^m = -a_{n-1}x^{m-1} - \cdots - a_0 x^{m-n}$. We have shown therefore that $\langle 1, x, \ldots, x^m \rangle_R = \langle 1, x, \ldots, x^{n-1} \rangle_R$. It follows by induction that $R[x] = \langle 1, x, \ldots, x^{n-1} \rangle_R$.
2. Suppose now that $R[x]$ is spanned by $f_1(x), \ldots, f_n(x)$, where $f_1, \ldots, f_n$ are polynomials over R. Set $N = \max_{1 \leq i \leq n}[\deg(f_i)]$. Then $x^{N+1} = \sum_{i=1}^n a_i f_i(x)$, where $a_i \in R$. Hence x is a root of the monic polynomial $T^{N+1} - \sum a_i f_i(T)$.

Examples. $i = \sqrt{-1}$ is integral over $\mathbb{Z}$ because it satisfies $T^2 + 1$. Also, $\sqrt[3]{5}$ is integral over $\mathbb{Z}$ since it satisfies $T^3 = 5$.

Definition 1.10 Let S and R be rings with $S \supseteq R$. We say that S is **integral over** R if every element of S is integral over R.

Proposition 1.11 Let $x \in S \supseteq R$. Then x is integral over R iff there is a subring Q of S so that $R[x] \subseteq Q \subseteq S$ and Q is finitely generated as an R-module.

Proof. For the forward direction, if x is integral, take $Q = R[x]$. For the reverse direction, suppose we are given Q as above, with $Q = \langle y_1, \ldots, y_n \rangle_R$ (as an R-module). Then

$$xy_i = \sum_j a_{ij} y_j, \qquad a_{ij} \in R. \tag{$\dagger$}$$

Let $A = xI_n - (a_{ij})$, $d = \det(A)$, and A^* the adjoint matrix of A. Then $AA^* = dI_n$. (†) implies that $yAA^* = 0$, where $y = \begin{pmatrix} y_1 & \cdots & y_n \end{pmatrix}$. Hence $y_i d = 0$ for each i. Now $1 \in Q$; write $1 = \sum_j b_j y_j$, where $b_j \in R$. Then $d = \sum_j b_j y_j = \sum_j b_j (d y_j) = 0$. Hence x satisfies the *monic* polynomial $d = \det(xI_n - (a_{ij})) = 0$.

Proposition 1.12 Suppose that $x_1, \ldots, x_n \in S \supseteq R$. Suppose that, for each i, x_i is integral over $R[x_1, \ldots, x_{i-1}]$. Then $R[x_1, \ldots, x_n]$ is finitely generated as an R-module.

Proof. The proof proceeds via induction on n. The case $n = 1$ is obvious from the definition of integrality. Now we perform the inductive step. Suppose that $B = R[x_1, \ldots, x_{i-1}]$ is finitely generated as an R-module. Now we are given that $B[x_i] = \sum_k B c_k$. By our inductive hypothesis, $B = \sum_j R d_j$. Hence $B[x_i] = \sum_{j,k} R d_j c_k$, and so the elements $\{c_k d_j\}$ span $B[x_1, \ldots, x_n]$ over R. The result now follows by induction.

Corollary 1.13 Let $x, y \in S \supseteq R$, with x and y integral over R. Then xy and $x \pm y$ are integral over R.

Proof. We are given that $R[x]$ is finitely generated over R, as is $R[y]$. Then $R[x, y]$ is finitely generated over $R[y]$, and so $R[x, y]$ is finitely generated over R. Consider the element $xy \in S$. We have $R[xy] \subset R[x, y]$, so in Proposition 1.11, take $Q = R[x, y]$. We deduce that xy is integral over R. Similarly for $x \pm y$.

Remark 1.14 If R is a noetherian ring, this can all be sped up. For concreteness, take $R = \mathbb{Z}$. Suppose α and β are integral over $\mathbb{Z}$. Then $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are finitely generated as $\mathbb{Z}$-modules, and so $\mathbb{Z}[\alpha, \beta]$ is a finitely generated $\mathbb{Z}$-module. Hence $\mathbb{Z}[\alpha, \beta]$ is a noetherian $\mathbb{Z}$-module. Now $\mathbb{Z}[\alpha\beta] \subset \mathbb{Z}[\alpha, \beta]$. Thus $\mathbb{Z}[\alpha, \beta]$ is finitely generated over $\mathbb{Z}$ (since $\mathbb{Z}[\alpha, \beta]$ is noetherian). Hence $\alpha\beta$ is integral over $\mathbb{Z}$.

Definition 1.15 Suppose that R and S are rings with $R \subseteq S$. We know that $\{x \in S : x \text{ is integral over } R\}$ is a ring. We call this ring the **integral closure** of R in S.

Definition 1.16 Suppose that R is an integral domain with field of fractions K. We say that R is **integrally closed** if it coincides with its integral closure in K.

Remark. Given R, any $r \in R$ is integral over R since it satisfies the monic polynomial $T - r$.

Examples 1.17

1. Let R be a PID with field of fractions K. Then R is integrally closed. (Exercise.)
2. If R is a field, then x is integral over R if and only if x is algebraic over R.

Definition 1.18 An (algebraic) number field is a finite extension of $\mathbb{Q}$.

Definition 1.19 Let K be a field. The **ring of algebraic integers** of K is the integral closure of $\mathbb{Z}$ in K. We denote this by $\mathfrak{o}_K$.

Examples.

1. The ring $\mathbb{Z}$ is the ring of integers of $\mathbb{Q}$.
2. The ring $\mathbb{Z}[i]$ is the ring of integers of $\mathbb{Q}(i)$ since i is integral over $\mathbb{Z}$.
3. If $\omega^3 = 1$, $\omega \neq 1$, then $\mathbb{Z}[\omega]$ is the ring of integers of $\mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$.

Examples.

	Algebraic	Integral	
$\sqrt[n]{m}$	Yes	Yes	
$1/7$	Yes	No	
π	No	No	
$1/\sqrt{2}$	Yes	No	
$\frac{1+i}{\sqrt{2}}$	Yes	Yes	(Exercise!)

Gauß's Lemma. Let $f(T) \in \mathbb{Z}[T]$. If f factors in $\mathbb{Q}[T]$, then it factors in $\mathbb{Z}[T]$.

Proof. Without loss of generality, we may assume that f is *primitive*, i.e. that the coefficients of f have no common prime factor. Let $f = gh$ be a nontrivial factorization in $\mathbb{Q}[T]$. Choose $a, b \in \mathbb{Q}$ such that $ag := g'$ is a primitive $\mathbb{Z}$-polynomial and similarly for $bh = h'$. Then we have $abf = g'h'$. Let $ab = c/d$, with $(c, d) = 1$. We claim that $ab = \pm 1$. For we have $cf = dg'h'$. If $ab \neq \pm 1$, then either

1. there is a prime p with $p \mid c$, and so we get $0 = \bar{d}\bar{g}'\bar{h}' \in \mathbb{F}_p[T]$, but $\bar{d}$, $\bar{g}'$, and $\bar{h}'$ are all nonzero, which is a contradiction, or

2. there is a prime p with $p \mid d$. Then $\bar{c}\bar{f} = 0 \in \mathbb{F}_p[T]$. But $\bar{f} \neq 0$ since f is primitive and $c \neq 0$ since $(c, d) = 1$, which is a contradiction.

Theorem 1.20 Let d be a squarefree integer with $d \neq 1$. Then the ring of integers of $\mathbb{Q}(\sqrt{d})$ is

$$\begin{cases} \mathbb{Z}[\sqrt{d}] & \text{if } d \not\equiv 1 \pmod 4, \\ \mathbb{Z}[(1+\sqrt{d})/2] & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

Proof. Suppose that $\alpha = a + b\sqrt{d}$, with $a, b \in \mathbb{Q}$ and $b \neq 0$. Let $\bar{\alpha} = a - b\sqrt{d}$. We shall determine whether α is integral over $\mathbb{Z}$. Now α is an integral over $\mathbb{Z}$ if and only if α satisfies a monic polynomial over $\mathbb{Z}$. (Note: α satisfies a minimal polynomial $m(T)$. Gauß's Lemma tells us that $f = mg$, and so $m(T)$ has coefficients in $\mathbb{Z}$.) Now $m(T) = (T - \alpha)(T - \bar{\alpha}) = T^2 - 2aT + \alpha^2 - db^2$, and this must be a polynomial over $\mathbb{Z}$. So we must have $a \in 1/2\mathbb{Z}$ and $a^2 - db^2 \in \mathbb{Z}$ (so $b \in 1/2\mathbb{Z}$).

Consider the case $d \equiv 2 \pmod 4$. Suppose that $a \in 1/2\mathbb{Z}$. Then $a^2 \equiv 1/4 \pmod{}Z$. Either $b \in \mathbb{Z}$, in which case $b^2 \equiv 0 \pmod{\mathbb{Z}}$, in which case $b^2 \equiv 0 \pmod{\mathbb{Z}}$, which is a contradiction since $a^2 - db^2 \in \mathbb{Z}$ or $b \in 1/2\mathbb{Z} \setminus \mathbb{Z}$, in which case $b^2 \equiv 1/4 \pmod{\mathbb{Z}}$, whence $db^2 \equiv 1/2 \pmod{\mathbb{Z}}$, since $d \equiv 2 \pmod 4$, which is a contradiction. Hence we must have $a \in \mathbb{Z}$, and so $b^2 d \in \mathbb{Z}$. If $b \equiv 1/2 \pmod{\mathbb{Z}}$, then $b^2 d \equiv 1/2 \pmod{\mathbb{Z}}$ since $d \equiv 2 \pmod 4$, which is a contradiction. So $a, b \in \mathbb{Z}$.

We leave the case of $d \equiv 3 \pmod 4$ as an exercise.

Finally, consider the case $d \equiv 1 \pmod 4$. Either $a, b \in \mathbb{Z}$ or $a, b \in 1/2\mathbb{Z} \setminus \mathbb{Z}$ (from the condition $a^2 - b^2 d \in \mathbb{Z}$). Examine the condition $a \equiv 1/2 \pmod{\mathbb{Z}}$ and $b \equiv 1/2 \pmod{\mathbb{Z}}$. Then $a^2 \equiv 1/4 \pmod{\mathbb{Z}}$ and $b^2 \equiv 1/4 \pmod{\mathbb{Z}}$. Therefore $b^2 d \equiv 1/4 \pmod{\mathbb{Z}}$ since $d \equiv 1 \pmod 4$. Hence $a^2 - db^2 \in \mathbb{Z}$, as required.

Terminology. If $d > 0$, then $\mathbb{Q}(\sqrt{d})$ is called a real quadratic field. If $d < 0$, then $\mathbb{Q}(\sqrt{d})$ is an imaginary quadratic field.

1.1 Interlude on Galois Theory

Let G be a group and K a field. A **character** of G is a homomorphism $\chi : G \to K^\times$. The **trivial character** is the homomorphism taking the constant value 1. Functions $f_i : G \to K$ for $1 \leq i \leq n$ are said to be **linearly independent** if whenever there is a relation $a_1 f_1 + \cdots + a_n f_n = 0$ with $a_i \in K$, then $a_i = 0$ for $1 \leq i \leq n$.

Theorem 1.21 (Artin's Theorem on linear independence of characters) Let G be a group and K a field. Suppose that $\chi_1, \ldots, \chi_n$ are distinct characters of G in K. Then these characters are linearly independent over K.

Proof. Suppose we have a relation

$$a_1 \chi_1 + \cdots + a_n \chi_n = 0 \tag{$\dagger$}$$

with $a_i \in K$ not all zero and n as small as possible. Then $n \geq 2$, and no $a_i = 0$. Since χ_1 and χ_2 are distinct, there is some $h \in G$ such that $\chi_1(h) \neq \chi_2(h)$. Then for each $g \in G$, we have $a_1 \chi_1(gh) + \cdots + a_n \chi_n(gh) = 0$, and so

$$a_1 \chi_1(h) \chi_1 + \cdots + a_n \chi_n(h) \chi_n = 0. \tag{$\ddagger$}$$

Dividing ($\ddagger$) by $\chi_1(h)$ and subtracting from ($\dagger$) gives

$$\left(a_2 \frac{\chi_2(h)}{\chi_1(h)} - a_2 \right) \chi_2 + \cdots = 0,$$

which is a contradiction since this is a relation of shorter length with a nonzero coefficient.

Corollary 1.22 Let L/K be a finite, normal extension of fields, and let $\sigma_1, \ldots, \sigma_n$ be distinct K-automorphisms of L. Then $\sigma_1, \ldots, \sigma_n$ are linearly independent over L.

Proof. View $\sigma_1, \ldots, \sigma_n$ are homomorphisms $L^\times \to L^\times$, and apply Artin's Theorem.

Proposition 1.23 Let L/K be a finite Galois extension of fields (not necessarily of characteristic 0) of degree n. Suppose that $x_1, \ldots, x_n$ is a basis of L over K. Let $\sigma_1, \ldots, \sigma_n$ be the distinct K-automorphisms of L. Then $\det(x_i^{\sigma_j}) \neq 0$.

Proof. Suppose that $\det(x_i^{\sigma_j}) = 0$. Then there exist $a_1, \ldots, a_n$, not all zero, so that $\sum_j a_j x_i^{\sigma_j} = 0$ for $1 \leq i \leq n$. Hence $\sum_j a_j \ell^{\sigma_j} = 0$ for every $\ell \in L$ (i.e. for any K-linear combination of the $\{a_i\}$). This contradicts Corollary 1.22.

Let L/K be a finite separable extension of fields. Let $n = [L : K]$, and let K^{sep} be a separable closure of K (so if $\text{char}(K) = 0$, then $K^{\text{sep}} = K^{\text{alg}}$). Let $\{\sigma_i\}$ be the distinct field embeddings $\sigma_i : L \hookrightarrow K^{\text{sep}}$ with $\sigma_i \mid K =$ identity. For $x \in L$, $\text{Tr}_{L/K}(x) = \sum_{i=1}^n x^{\sigma_i} \in K$ and $N_{L/K}(x) = \prod_{i=1}^n x^{\sigma_i} \in K$.

Alternatively, view multiplication by x on L as a K-linear automorphism of L. Call this endomorphism φ_x, so $\varphi_x(y) = xy$. Pick a basis $\{y_i\}_{i=1}^n$ of L/K, and let φ_x have matrix (a_{ij}) with respect to this basis.

Claim. $\text{Tr}(\varphi_x) = \text{Tr}_{L/K}(x)$, and $\det(\varphi_x) = N_{L/K}(x)$.

Proof. We have $xy_i = \sum_j a_{ij} y_j$. Apply an embedding σ_k to this equation:

$$x^{\sigma_k} y_i^{\sigma_k} = \sum_j a_{ij} y_j^{\sigma_k}.$$

So we have a matrix equality $(y_i^{\sigma_k}) \,\text{diag}(x^{\sigma_k}) = (a_{ij})(y_j^{\sigma_k})$. Now Proposition 1.23 tells

us that $\det(y_j^{\sigma_k}) \neq 0$. So the trace and determinant (and characteristic polynomials of $\mathrm{diag}(x^{\sigma_k} y_j^{\sigma_k})$ and (a_{ij})) coincide. This establishes the claim.

Exercise. Let L/K be a finite separable extension of degree n. Then $\mathrm{Tr}_{L/K} : L \times L \to K$ given by $(x, y) \mapsto \mathrm{Tr}_{L/K}(xy)$ is a nondegenerate symmetric bilinear form on the K-vector space L. Hence we have an isomorphism $L \xrightarrow{\sim} \mathrm{Hom}(L, K)$ given by $x \mapsto [y \mapsto \mathrm{Tr}_{L/K}(xy)]$. So if $\{x_i\}_{i=1}^n$ is a basis of L/K, then we can find a dual basis $\{y_i\}_{i=1}^n$ of L/K, i.e. a basis such that $\mathrm{Tr}_{L/K}(x_i y_j) = \delta_{ij}$.

Chapter 2

More Commutative Algebra

Definition 2.1 We say that an ideal $\mathfrak{m}$ of R is **maximal** if, given an ideal $\mathfrak{a}$ such that $\mathfrak{m} \subseteq \mathfrak{a} \subseteq R$, then either $\mathfrak{a} = R$ or $\mathfrak{a} = \mathfrak{m}$.

(Maximal ideals are prime.)

Definition 2.2 An integral domain R is said to be a **Dedekind domain** if

1. R is a noetherian ring.
2. R is integrally closed.
3. All nonzero prime ideals of R are maximal.

Example/Exercise. Every PID is necessarily a Dedekind domain.

We shall prove:

Theorem 2.3 Every nonzero ideal of a Dedekind domain R may be written uniquely as a product of prime (maximal) ideals.

Let R be an integral domain with field of fractions K.

Definition 2.4 We call any finitely generated R-module M in K a **fractional** R-ideal. If $M \subseteq R$, we say that M is an **integral** R-ideal.

Theorem 2.5 Let R be a Dedekind domain with field of fractions K. Let L/K be a finite separable extension. Then the integral closure S of R in L is a Dedekind domain.

(**Remark.** We won't prove this in full generality; we shall assume that $R = \mathbb{Z}$.)

Corollary 2.6 Any ring of integers is a Dedekind domain.

Corollary 2.7 Any ring of integers has unique factorization of ideals.

Proof of Theorem 2.5

1. We first show that S is integrally closed. Let $x \in L$ be integral over S. Then x is the root of some polynomial

$$T^n + s_1 T^{n-1} + \cdots + s_n = 0, \ s_i \in S. \qquad (*)$$

   We are required to prove that x is integral over R. Now $R[s_1, \ldots, s_n]$ is a finitely generated R-module (since all the s_i are integral over R). From $(*)$, it follows that $R[x, s_1, \ldots, s_n]$ is finitely generated over $R[s_1, \ldots, s_n]$. Hence $R[x, s_1, \ldots, s_n]$ is finitely generated over R, and so Proposition 1.11 implies that x is integral over R.

2. We now show that S is a noetherian ring. Let $x_1, \ldots, x_n$ be a K-basis of L. We claim that without loss of generality, we may take $x_i \in S$ for all i. For we know (after clearing denominators) that for example x_j is a root of a polynomial $a_0 T^n + \cdots + a_n = 0$, where $a_i \in R$ for each i. Multiply through by a_0^{n-1} to get $(a_0 T)^n + a_1 (a_0 T)^{n-1} + \cdots + a_n a_0^{n-1} = 0$. So $a_0 x_j$ is integral over R. Now let $\{y_i\}$ be a dual basis of L, so $\mathrm{Tr}(x_i y_j) = \delta_{ij}$. Suppose that $\alpha \in S$ with $\alpha = \sum a_r y_r$, say. Then $\alpha x_j = \sum a_r y_r x_j$. Applying $\mathrm{Tr}_{L/K}$ to both sides of this equation gives

$\mathrm{Tr}(\alpha x_j) = a_j \cdot 1$, and so $a_j \in R$ since $\alpha x_j \in S$. So $S \subseteq \sum Ry_i = \bigoplus Ry_i$. R is a Dedekind ring, so R is noetherian, so S is a noetherian R-module, so S is a finitely generated R-module, and Proposition 1.6 tells us that S is a noetherian ring.

Remark. Since $\{x_i\}$ is a basis of L, we have $\bigoplus_{i=1}^n Rx_i \subseteq S$, and so we in fact have $\bigoplus_{i=1}^n Rx_i \subseteq S \subseteq \bigoplus_{i=1}^n Ry_i$. Hence, if R is a PID, it follows from Proposition 1.10 that S is a free R-module of rank $n = [L : K]$.

3. Finally we show that all nonzero prime ideals of S are maximal. Take $R = \mathbb{Z}$, so $S = \mathfrak{o}_L$. Then S is free over $\mathbb{Z}$ of rank n, i.e. $S = \bigoplus_{i=1}^n \mathbb{Z}\omega_i$. Let $\mathfrak{p}$ be a nonzero prime ideal of S. We know that

$$\mathfrak{p} \cap \mathbb{Z} = \begin{cases} p\mathbb{Z} & \text{or} \\ 0. \end{cases}$$

Let $x \in \mathfrak{p} \setminus \{0\}$. Then $0 \neq N_{L/\mathbb{Q}}(x) \in \mathfrak{p} \cap \mathbb{Z}$, and so we must have $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. So we have $pS \subseteq \mathfrak{p} \subseteq S$, and so there is a surjection $S/pS \twoheadrightarrow S/\mathfrak{p}$. Now $S/pS \simeq \bigoplus_{i=1}^n \mathbb{F}_p\omega_i$, which is finite of cardinality p^n. Also $S/\mathfrak{p}$ is an integral domain since $\mathfrak{p}$ is prime. Thus $S/\mathfrak{p}$ is a finite integral domain, i.e. a field. Thus $\mathfrak{p}$ is a maximal ideal.

Lemma 2.8 Let R be a Dedekind domain. Then every nonzero R-ideal contains some product of nonzero primes.

Proof. Suppose that the assertion is false. Let $\mathscr{S}$ denote the set of nonzero R-ideals not containing a nonzero product of primes. By hypothesis, $\mathscr{S}$ is nonempty. By Proposition 1.3, $\mathscr{S}$ contains a maximal element, $\mathfrak{b}$, say. Now $\mathfrak{b}$ is definitely not a prime ideal, and so there exist elements $x, y \notin \mathfrak{b}$ with $xy \in \mathfrak{b}$. We have $(x, \mathfrak{b}) \supset \mathfrak{p}_1 \cdots \mathfrak{p}_n$ and $(y, \mathfrak{b}) \supset \mathfrak{q}_1 \cdots \mathfrak{q}_m$ ($\mathfrak{p}_i$ and $\mathfrak{q}_j$ are primes). Multiplying gives $\mathfrak{b} \supseteq (x, \mathfrak{b})(y, \mathfrak{b}) \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_n \mathfrak{q}_1 \cdots \mathfrak{q}_m$, which is a contradiction.

Theorem 2.9 Let R be a Dedekind domain and $\mathfrak{m}$ a maximal R-ideal. Then there exists a fractional ideal $\mathfrak{m}^{-1}$ in R so that $\mathfrak{m}\mathfrak{m}^{-1} = R$.

Proof. Set $\mathfrak{m}' = \{x \in R \mid x\mathfrak{m} \subseteq R\}$. We wish to show that $\mathfrak{m}\mathfrak{m}' = R$. Now $\mathfrak{m}'$ is clearly an R-module. It is also finitely generated, for pick $\mu \in \mathfrak{m} \setminus \{0\}$. Then $\mu\mathfrak{m}' \subseteq R$, and $\mu\mathfrak{m}' \simeq \mathfrak{m}'$ as an R-module. Since R is noetherian, it follows that $\mathfrak{m}'$ is finitely generated. Next, we observe that $R \subseteq \mathfrak{m}'$ implies that $\mathfrak{m} \subseteq \mathfrak{m}\mathfrak{m}'$. So we have $\mathfrak{m} \subseteq \mathfrak{m}\mathfrak{m}' \subseteq R$. Hence, since $\mathfrak{m}$ is maximal, we have either $\mathfrak{m} = \mathfrak{m}\mathfrak{m}'$ or $\mathfrak{m}\mathfrak{m}' = R$. We show that the former possibility does not hold. Suppose on the contrary that

$$\mathfrak{m} = \mathfrak{m}\mathfrak{m}' = \cdots = \mathfrak{m}(\mathfrak{m}')^n = \cdots .$$

Pick $x \in \mathfrak{m}' \setminus \{0\}$ and $y \in \mathfrak{m} \setminus \{0\}$. The above equalities imply that $R[x]y \subseteq R[x]\mathfrak{m} \subseteq \mathfrak{m}$. Since R is a noetherian ring, it follows that $R[x]y$ is finitely generated as an R-module. So $R[x]$ is finitely generated as an R-module, i.e. x is integral over R. Since R is integrally closed, it follows that $x \in R$, whence we deduce that $\mathfrak{m}' = R$. To complete the proof, we show that $\mathfrak{m}' = R$ is impossible. Choose $a \in \mathfrak{m} \setminus \{0\}$. Then Lemma 2.8 implies that

$$\mathfrak{m} \supseteq Ra \supseteq \mathfrak{p}_1 \cdots \mathfrak{p}_n$$

(where the $\mathfrak{p}_i$'s are nonzero primes). Choose n so that n is minimal for our given a. Now $\mathfrak{m}$ must contain one of the $\mathfrak{p}_i$'s, say $\mathfrak{p}_1$ without loss of generality. Since $\mathfrak{p}_1$ is maximal (as R is a Dedekind domain), we have $\mathfrak{m} = \mathfrak{p}_1$. Hence $Ra \supseteq \mathfrak{m}\mathfrak{b}$, where $\mathfrak{b} = \mathfrak{p}_2 \cdots \mathfrak{p}_n$. By minimality of n, $Ra \neq \mathfrak{b}$. Pick some $b \in \mathfrak{b}$, $b \notin Ra$, i.e. $b/a \notin R$. Then

$$\frac{b}{a}\mathfrak{m} \subseteq \frac{1}{a}\mathfrak{b}\mathfrak{m} \subseteq \frac{1}{a}Ra \subseteq R.$$

So $\frac{b}{a} \in \mathfrak{m}'$, and $\frac{b}{a} \notin R$, and this contradicts $\mathfrak{m}' = R$. This proves the result.

Proof of Theorem 2.3 We first show existence. Let Φ be the family of proper nonzero integral R-ideals which are *not* factorable as a product of primes. Suppose that $\Phi \neq \varnothing$. Then Proposition 1.3 implies that Φ has a maximal element, $\mathfrak{a}$, say. Then $\mathfrak{a} \subset R$ and $\mathfrak{a}$ is *not* a prime (or else we would have a trivial factorization). So we have $\mathfrak{a} \subseteq \mathfrak{m} \subseteq R$, where $\mathfrak{m}$ is a maximal ideal. So we have $\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{m}^{-1} \subseteq \mathfrak{m}\mathfrak{m}^{-1} = R$ (remember $R \subseteq \mathfrak{m}^{-1}$!). Either $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{m}^{-1}$, in which case, by maximality, $\mathfrak{a}\mathfrak{m}^{-1}$ has a prime factorization, and so $\mathfrak{a}$ has a prime factorization ($\mathfrak{m}$ is maximal and hence prime!), which is a contradiction, or

$$\mathfrak{a} = \mathfrak{a}\mathfrak{m}^{-1} = \cdots = \mathfrak{a}\mathfrak{m}^{-n} = \cdots . \qquad (*)$$

Pick $a \in \mathfrak{a} \setminus \{0\}$ and $m \in \mathfrak{m}^{-1} \setminus \{0\}$. Then $(*)$ implies that $aR[m] \subseteq \mathfrak{a}$. Since R is noetherian, we have that $R[m]$ is finitely generated over R, and so m is integral over R, and so $m \in R$, and so $\mathfrak{m}^{-1} = R$, which is a contradiction (c.f. the proof of

Theorem 2.9). It therefore follows that $\Phi = \varnothing$.

We now show uniqueness. Suppose $\mathfrak{p}_1 \cdots \mathfrak{p}_n = \mathfrak{q}_1 \cdots \mathfrak{q}_m$, where the $\mathfrak{p}_i$'s and $\mathfrak{q}_j$'s are primes. We shall show by induction on n that the $\mathfrak{q}_j$'s are some reordering of the $\mathfrak{p}_i$'s. Consider the case $n = 1$, i.e. $\mathfrak{p} = \mathfrak{q}_1 \cdots \mathfrak{q}_m$. By primality, $\mathfrak{p} = \mathfrak{q}_1$, say. Multiplying both sides by $\mathfrak{p}^{-1}$, we get $R = \mathfrak{q}_2 \cdots \mathfrak{q}_m$. So $m = 1$, and $\mathfrak{p} = \mathfrak{q}_1$. Now we do the general case. By primality, we have $\mathfrak{p}_1 \supseteq \mathfrak{q}_i$ (say $\mathfrak{q}_1$). Multiplying both sides by $\mathfrak{p}_1^{-1}$ yields $\mathfrak{p}_2 \cdots \mathfrak{p}_n = \mathfrak{q}_2 \cdots \mathfrak{q}_m$, so by induction we are done.

2.1 Valuations of Ideals

Let R be a Dedekind domain, and let $\mathfrak{a}$ be a fractional R-ideal. Then $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_\mathfrak{p}}$, where $n_\mathfrak{p} \in \mathbb{Z}$, with almost all of the $n_\mathfrak{p}$'s equal to zero. We write $v_\mathfrak{p}(\mathfrak{a}) = n_\mathfrak{p}$ (read as "the $\mathfrak{p}$-valuation of $\mathfrak{a}$"). Let K be the field of fractions of R, and let I_K be the set of fractional R-ideals. Then I_K is a group. We have a map $I_K \to \bigoplus_{\mathfrak{p}} \mathbb{Z}$ given by $\mathfrak{a} \mapsto \bigoplus_{\mathfrak{p}} v_\mathfrak{p}(\mathfrak{a})$.

Definition 2.10 We call a fractional ideal $\mathfrak{a} \in I_K$ **principal** if $\mathfrak{a} = aR$ for some $a \in K$. We denote the subgroup of principal ideals by P_K.

Definition 2.11 Let K be a number field. The **class group** of $\mathfrak{o}_K$ (or of K) ideals is defined to be the quotient group $I_K/P_K := C_K$, and $|C_K| = h_k$ (we shall show later that h_K is finite).

Remark. $\mathfrak{o}_K$ is a PID if and only if $h_K = 1$.

Definition 2.12 We call the group of invertible elements of $\mathfrak{o}_K$ the units of $\mathfrak{o}_K$ (or of K!), and we denote this group by $\mathfrak{o}_K^\times$.

We have a sequence

$$\begin{array}{ccccccccccccc} 1 & \to & \mathfrak{o}_K^\times & \hookrightarrow & K^\times & \to & P_K & \hookrightarrow & I_K & \to & C_K & \to & 0 \\ & & & & a & \mapsto & a\mathfrak{o}_K. & & & & & & \end{array}$$

Theorem 2.13 (Chinese Remainder Theorem — See 220B) Let R be a Dedekind domain, and let $\mathfrak{a} = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_k^{n_k}$. Then $R/\mathfrak{a} \simeq \prod_{i=1}^k R/\mathfrak{p}_i^{n_i}$.

Definition 2.14 Let K be an arbitrary field. A surjective map $v : K \to \mathbb{Z} \cup \{\infty\}$ is called a **valuation** of K iff for every $x, y \in K$:

1. $v(x) = \infty$ iff $x = 0$
2. $v(xy) = v(x) + v(y)$
3. $v(x + y) \geq \inf(v(x), v(y))$.

So (2) tells us that $v(1) = v(-1) = 0$.

Claim. $v(x) > v(y)$ implies that $v(x + y) = v(y)$. For we have $v(x + y) \geq \inf(v(x), v(y)) = v(y)$. Strict inequality would imply that $v(y) = v(y + x - x) \geq \inf(v(y + x), v(x)) > v(y)$, which is a contradiction, and so we must have $v(x + y) = v(y)$.

Key Example 2.15 Let R be a Dedekind domain with field of fractions K. For $x \in K^\times$, set $v_\mathfrak{p}(x) = v_\mathfrak{p}(xR)$; this defines a map $v_\mathfrak{p} : K^\times \to \mathbb{Z}$. Setting $v_\mathfrak{p}(0) = \infty$ defines a map $v_\mathfrak{p} : K \to \mathbb{Z} \cup \{\infty\}$. Since we can always find an x so that $x \in \mathfrak{p}$ but $x \notin \mathfrak{p}^2$, it follows that $v_\mathfrak{p}$ is surjective.

Exercise. Check that $v_\mathfrak{p}$ satisfies the conditions of Definition 2.14.

Definition 2.16 Given a valuation v of a field K, we set $\mathfrak{o}_v = \{x \in K : v(x) \geq 0\}$. Then $\mathfrak{o}_v$ is a ring, called the **valuation ring** of v in K. Next, set $\mathcal{P}_v = \{x \in K : v(x) > 0\}$. Then $\mathcal{P}_v$ is a proper $\mathfrak{o}_v$-ideal, the **valuation ideal** of v in K.

$\mathcal{P}_v$ is a prime ideal. Suppose $x, y \in \mathfrak{o}_v$ with $xy \in \mathcal{P}_v$. Then $v(xy) = v(x) + v(y) > 0$. Thus either $v(x) > 0$ or $v(y) > 0$, i.e. $x \in \mathcal{P}_v$ or $y \in \mathcal{P}_v$.

Proposition 2.17 $\mathfrak{o}_v$ is a PID with unique maximal ideal $\mathcal{P}_v$. Moreover, we have $\mathbb{Z} \xrightarrow{\sim} I_{\mathfrak{o}_v}$ via $m \mapsto \mathcal{P}_v^m$.

Proof. First observe that x is invertible in $\mathfrak{o}_v$ iff $v(x) \geq 0$ and $v(x^{-1}) \geq 0$, i.e. if $v(x) = 0$. Hence $\mathfrak{o}_v^\times = \mathfrak{o}_v \setminus \mathcal{P}_v$, and so $\mathcal{P}_v$ is the unique maximal ideal of $\mathfrak{o}_v$. Next, let $\mathfrak{a}$ be a nonzero $\mathfrak{o}_v$-ideal. Choose $b \in \mathfrak{a}$ with $v(b)$ minimal. We claim that $\mathfrak{a} = b\mathfrak{o}_v$, for plainly we have $b\mathfrak{o}_v \subseteq \mathfrak{a}$. If $c \in \mathfrak{a}$, then $v(b) \leq v(c)$, so $v(b^{-1}c) \geq 0$. Thus $b^{-1}c \in \mathfrak{o}_v$. Thus $c = bb^{-1}c \in b\mathfrak{o}_v$. Hence $\mathfrak{a} = b\mathfrak{o}_v$, as claimed. Finally, suppose that $\alpha\mathfrak{o}_v = \mathcal{P}_v$, and that $v(b) = n$ (where b is as above). Then $\alpha^n\mathfrak{o}_v = \mathcal{P}_v^n = b\mathfrak{o}_v = \{c \in K : v(c) \geq n\}$.

2.2 Localization

Suppose that R is an integral domain with field of fractions K. Let S denote a multiplicatively closed set (not containing zero) in R. Define $R_S \subseteq K$ as $R_S = \left\{ \frac{a}{b} \middle| a \in R, b \in S \right\}$.

Example. Let R be a Dedekind domain. Suppose that $\mathfrak{p}$ is a prime ideal in R. Then $S = R \setminus \mathfrak{p}$ is a multiplicatively closed set. In this case, we write $R_\mathfrak{p} = R_S$ from now on. The ring $R_\mathfrak{p}$ is called the **localization** of R at $\mathfrak{p}$.

Exercise. Show that $R_\mathfrak{p} = \mathfrak{o}_{v_\mathfrak{p}}$. Hence $R_\mathfrak{p}$ is a PID with only one maximal ideal, namely $\mathfrak{p}$.

Remark. If R is a ring of integers, then in general R is not a PID. However, by the above, each $R_\mathfrak{p}$ is a PID. This is very useful.

Lemma 2.18 Suppose that R is a Dedekind domain. Then $R/\mathfrak{p} \simeq R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$.

Proof. The natural inclusion $R \hookrightarrow R_\mathfrak{p}$ induces a map $i^* : R/\mathfrak{p} \to R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$. We now show injectivity. We have to show that $R \cap \mathfrak{p}R_\mathfrak{p} = \mathfrak{p}$. Suppose that $x \in R \cap \mathfrak{p}R_\mathfrak{p}$. Then we may write $x = \pi r/s$, where $\pi \in \mathfrak{p}$ and $s \notin \mathfrak{p}$. Hence we have $xs = \pi r$, and this implies that $\pi \in \mathfrak{p}$. Now we show surjectivity. Pick a/s ($s \notin \mathfrak{p}$) in $R_\mathfrak{p}$ representing a given class in $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$. Since $s \in R \setminus \mathfrak{p}$, there is some $b \in R$ so that $bs \equiv 1 \pmod{\mathfrak{p}}$. So we have $\frac{a}{s}(bs - 1) \in \mathfrak{p}R_\mathfrak{p}$. Hence $\frac{a}{s}$ and ab represent the same class in $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$. Thus $ab + \mathfrak{p} \mapsto \frac{a}{s} + \mathfrak{p}R_\mathfrak{p}$, and so surjectivity is shown.

2.3 Examples of "good behavior" with respect to localization

Proposition 2.19 Let R be an integral domain. Then

1. R is integrally closed iff $R_\mathfrak{p}$ is integrally closed for all primes $\mathfrak{p}$. (This is an example of the **Hasse principle**.)
2. If R is a noetherian ring, then $R_\mathfrak{p}$ is a noetherian ring for all primes $\mathfrak{p}$.

Let M be an R-module. Define $M_S := M \otimes_R R_S$. (If $S = R \setminus \mathfrak{p}$, then we write $M_\mathfrak{p}$ for M_S.)

Proposition 2.20 Let R be an integral domain. Then

1. $M = 0$ iff $M_\mathfrak{p} = 0$ for all primes $\mathfrak{p}$.
2. M is flat iff $M_\mathfrak{p}$ is flat for all primes $\mathfrak{p}$. (M is said to be **flat** if it preserves exact sequences under tensor products, i.e. if
$$0 \to A \to B \to C \to 0$$
is exact, then
$$0 \to A \otimes M \to B \otimes M \to C \otimes M \to 0$$
is also exact.)

3. M is torsionfree iff $M_{\mathfrak{p}}$ is torsionfree for all primes $\mathfrak{p}$.

4. $$0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$$

   is an exact sequence of R-modules iff

   $$0 \to M_{\mathfrak{p}} \xrightarrow{f_{\mathfrak{p}}} N_{\mathfrak{p}} \xrightarrow{g_{\mathfrak{p}}} P_{\mathfrak{p}} \to 0$$

   is exact for all primes $\mathfrak{p}$.

Chapter 3

Discriminants, Norms, and Traces

Let L/K be a finite, separable extension of fields. Let $n = [L : K]$ and K^{sep} be a separable closure of K. Let $\{\sigma_i\}_{i=1}^n$ be the distinct field embeddings $\sigma_i : L \hookrightarrow K^{\text{sep}}$ so that $\sigma_i \mid_K = id$. For $x \in L$, define $\text{Tr}_{L/K}(x) = \sum_{i=1}^n x^{\sigma_i} \in K$ and $N_{L/K}(x) = \prod_{i=1}^n x^{\sigma_i} \in K$.

Definition 3.1 Let K be a number field. Pick a $\mathbb{Z}$-basis $x_1, \ldots, x_n$ of $\mathfrak{o}_K$ (cf. the remark after the proof of Theorem 2.5). The **discriminant** of $\mathfrak{o}_K/\mathbb{Z}$ with respect to the trace form is $d(K/\mathbb{Q}) = \det(\text{Tr}_{K/\mathbb{Q}}(x_i x_j))$.

N.B. This is the discriminant of the quadratic module $(\mathfrak{o}_K, \text{Tr}_{K/\mathbb{Q}})$. $d(K/\mathbb{Q})$ is generally referred to as the discriminant of K!

Lemma 3.2 Let $\{\sigma_i\}$ denote the distinct $\mathbb{Q}$-embeddings of K into K^{sep}. We set $\Delta_{\mathbf{x}}(K/\mathbb{Q}) = \det(x_i^{\sigma_j})$. Then $\Delta_{\mathbf{x}}(K/\mathbb{Q})$ is independent of the particular basis $\{x_i\}$ *up to sign*, and $d(K/\mathbb{Q}) = \Delta_{\mathbf{x}}(K/\mathbb{Q})^2$.

Corollary 3.3 $d(K/\mathbb{Q})$ is independent of the choice of basis of $\mathfrak{o}_K/\mathbb{Z}$.

Proof of Lemma 3.2 Let $\{y_i\}$ be another $\mathbb{Z}$-basis of $\mathfrak{o}_K$. Then we have $y_i = \sum_j P_{ij} x_j$, where $(P_{ij}) \in \text{GL}_n(\mathbb{Z})$. Hence $y_i^{\sigma_k} = \sum_j P_{ij} x_j^{\sigma_k}$. Taking determinants yields $\Delta_{\mathbf{y}}(K/\mathbb{Q}) = \det(P_{ij})\Delta_{\mathbf{x}}(K/\mathbb{Q})$. Since (P_{ij}) is a change-of-basis matrix, we have $\det(P_{ij}) = \pm 1$. Hence $\Delta_{\mathbf{x}}(K/\mathbb{Q})$ depends upon $\{x_i\}$ only up to sign. Next, observe that $\sum_j x_i^{\sigma_j} x_k^{\sigma_j} = \text{Tr}_{K/\mathbb{Q}}(x_i x_k)$. Hence if we write $A = (x_i^{\sigma_j})$, then we have

$AA^t = (\mathrm{Tr}_{K/\mathbb{Q}}(x_i x_k))$. Taking determinants and using the fact that $\det(A) = \det(A^t)$ gives $\Delta_{\mathbf{x}}(K/\mathbb{Q})^2 = d(K/\mathbb{Q})$.

Corollary 3.4 $d(K/\mathbb{Q}) \neq 0$.

Proof. This follows from the fact that $\Delta_{\mathbf{x}}(K/\mathbb{Q}) = \det(x_i^{\sigma_j}) \neq 0$ (see Proposition 1.23).

Example 3.5 Suppose that $d \not\equiv 1 \pmod 4$ and that d is squarefree. Set $K = \mathbb{Q}(\sqrt{d})$. By Theorem 1.20, we have $\mathfrak{o}_K = \mathbb{Z} + \mathbb{Z}\sqrt{d}$, i.e. 1 and $\sqrt{d}$ are a $\mathbb{Z}$-basis of $\mathfrak{o}_K$. So $d(K/\mathbb{Q}) = \begin{vmatrix} 2 & 0 \\ 0 & 2d \end{vmatrix} = 4d$.

Exercise. Suppose that $d \equiv 1 \pmod 4$. Show that $d(K/\mathbb{Q}) = d$.

Notation. Suppose that K is a number field with $[K : \mathbb{Q}] = n$. Let $x_1, \ldots, x_n$ be any set of elements of K. (This will only be of interest when $\{x_i\}$ are a $\mathbb{Q}$-basis of K.) Then $D(x_1, \ldots, x_n) := \det(\mathrm{Tr}(x_i x_j))$ and $\Delta(x_1, \ldots, x_n) := \det(x_i^{\sigma_j})$. Then, as in the proof of Lemma 3.1, we have $D(x_1, \ldots, x_n) = \Delta(x_1, \ldots, x_n)^2$.

Interpretation. Set $\Lambda = \sum \mathbb{Z} x_i$. As before, $D(x_1, \ldots, x_n)$ only depends upon the lattice (module) Λ. So we can write $D_\Lambda = D(x_1, \ldots, x_n)$. In particular, $d(K/\mathbb{Q}) = D_{\mathfrak{o}_K}$. Suppose that $\Lambda \subseteq \mathfrak{o}_K$. We shall show later that $D_\Lambda = d(K/\mathbb{Q})[\mathfrak{o}_K : \Lambda]^2$.

[**Aside.** A useful tool in the evaluation of discriminants is the Vandermonde determinant: $\det_{1 \leq i,j \leq n}(x_j^i) = \pm \prod_{i<j}(x_i - x_j)$. To evaluate $\Delta(1, x, \ldots, x^{n-1})$, set $x_j = x^{\sigma_j}$.]

Uses of discriminants.

1. Suppose we have $p\mathfrak{o}_K = \prod_{i=1}^g \mathfrak{p}_i^{e_i}$. Then $e_i = 1$ for all i for almost all primes p. If some $e_i > 1$, then we say that p is **ramified**, and we call e_i the **ramification index**.

Dedekind's criterion. p ramifies iff $p \mid d(K/\mathbb{Q})$.

Example. Let $K = \mathbb{Q}(i)$ and $\mathfrak{o}_K = \mathbb{Z}[i]$. $2\mathbb{Z}[i] = (1-i)^2$, and so 2 ramifies in $\mathbb{Q}(i)/\mathbb{Q}$. $d(K/\mathbb{Q}) = 4$. There is also an analogue of ramification for Riemann surfaces...

2. **Calculating rings of integers.** Suppose that $[K : \mathbb{Q}] = n$. Usually we can find algebraic integers $x_1, \ldots, x_n$ that are $\mathbb{Q}$-linearly independent.

Question. Is $\{x_i\}$ a basis over $\mathbb{Z}$ for $\mathfrak{o}_K$?

Lemma 3.6 Set $\Lambda = \sum \mathbb{Z}x_i$ and $m = (\mathfrak{o}_K : \Lambda)$. Then $D(x_1, \ldots, x_n) = d(K/\mathbb{Q})m^2$.

Proof. Let $\{y_i\}$ be a $\mathbb{Z}$-basis of $\mathfrak{o}_K$. Then $x_i = \sum_{j=1}^n P_{ij}y_j$, and so $x_i^{\sigma_k} = \sum_j P_{ij}y_j^{\sigma_k}$. Taking discriminants yields $D(\mathbf{x}) = \Delta_{\mathbf{x}}^2 = d(K/\mathbb{Q})\det(P_{ij})^2$. By the theory of elementary divisors (see 220B), we can find matrices $A, B \in \mathrm{GL}_n(\mathbb{Z})$ such that

$$P = A \underbrace{\begin{pmatrix} d_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & d_n \end{pmatrix}}_{D} B.$$

Now $\mathbf{x} = P\mathbf{y}$, so $A^{-1}\mathbf{x} = DB\mathbf{y}$. Set $\mathbf{x}' = A^{-1}\mathbf{x}$ and $\mathbf{y}' = B\mathbf{y}$; then $\mathbf{x}' = D\mathbf{y}'$. Now Λ is spanned over $\mathbb{Z}$ by $\{x_i'\}$. Thus Λ is spanned over $\mathbb{Z}$ by $\{d_iy_i\}$. But $\mathfrak{o}_K$ is spanned by $\{y_i'\}$, and so we have $\mathfrak{o}_K/\Lambda \simeq \bigoplus \mathbb{Z}y_i / \bigoplus \mathbb{Z}d_iy_i$. Thus $(\mathfrak{o}_K : \Lambda) = \pm\prod_i d_i = \pm\det(P)$. Hence $D(\mathbf{x}) = \Delta\mathbf{x}^2 = d(K/\mathbb{Q})(\mathfrak{o}_K : \Lambda)^2$.

Now Lemma 3.6 gives us a method for computing rings of integers.

Proposition 3.7 Notation as in Lemma 3.6. Suppose that $\Lambda \neq \mathfrak{o}_K$. Then there exists an algebraic integer of the form $\frac{1}{p}(\lambda_1x_1 + \cdots + \lambda_nx_n)$, where $0 \leq \lambda_i \leq p-1$,

$\lambda_i \in \mathbb{Z}$, and p is a prime such that $p^2 \mid D_\Lambda$.

Proof. Since $\Lambda \neq \mathfrak{o}_K$, we have $(\mathfrak{o}_K : \Lambda) > 1$. Hence there is a prime p with $p \mid (\mathfrak{o}_K : \Lambda)$ and an element $u \in \mathfrak{o}_K \setminus \Lambda$ such that $u_1 = pu \in \Lambda$. By Lemma 3.6, $p^2 \mid D_\Lambda$. Also $u = \frac{1}{p}u_1 = \frac{1}{p}(\lambda_1 x_1 + \cdots + \lambda_n x_n)$ since $\{x_i\}$ forms a $\mathbb{Z}$-basis of Λ.

Corollary 3.8 If D_Λ is squarefree, then $\Lambda = \mathfrak{o}_K$.

Here is the basic idea:

1. Start with an initial guess Λ for $\mathfrak{o}_K$, $\Lambda = \sum_{i=1}^n \mathbb{Z}x_i$.
2. Compute D_Λ.
3. For each prime p so that $p^2 \mid D_\Lambda$, test all numbers of the form $\frac{1}{p}(\lambda_1 x_1 + \cdots + \lambda_n x_n)$, $0 \leq \lambda_i \leq p-1$, to determine whether they are algebraic integers.
4. If any new integers arise, enlarge Λ to Λ' by adding in the new integer. (Then $D_{\Lambda'} = \frac{1}{p^2}D_\Lambda$.)

Example. Find the ring of integers and discriminant of $\mathbb{Q}(\theta)/\mathbb{Q}$, where $\theta^3 - \theta - 1 = 0$. By Gauß's Lemma, $X^3 - X - 1$ is irreducible over $\mathbb{Q}$. Calculate $D(1, \theta, \theta^2) = \begin{vmatrix} 3 & 0 & 2 \\ 0 & 2 & 3 \\ 2 & 3 & 2 \end{vmatrix}$. To work out entries, we compute $\mathrm{Tr}(\theta) = 0$ (from the equation $X^3 - X - 1$), and $\mathrm{Tr}(\theta^3) = \mathrm{Tr}(\theta) + \mathrm{Tr}(1) = 3$. To compute $\mathrm{Tr}(\theta^2)$, we need to go back to first principles: find a matrix representing φ_{θ^2} (i.e. the "multiplication by θ^2" map on $\mathbb{Q}(\theta)$): we have a basis, namely $\{1, \theta, \theta^2\}$. $\theta^2 \cdot 1 = \theta^2$, $\theta^2 \cdot \theta = \theta^3 = 1 + \theta$, and $\theta^2 \cdot \theta^2 = \theta^4 = \theta^2 + \theta$. Thus $\varphi_{\theta^2} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$. Thus $\mathrm{Tr}(\theta^2) = 2$. Then $\mathrm{Tr}(\theta^4) = \mathrm{Tr}(\theta^2) + \mathrm{Tr}(\theta) = 2$. Hence $D(1, \theta, \theta^2) = 3 \cdot (-5) + 2 \cdot (-4) = -23$. Now -23 is squarefree, and so $\mathfrak{o}_K = \mathbb{Z}[\theta] = \mathbb{Z} + \mathbb{Z}\theta + \mathbb{Z}\theta^2$. Also, $d(K/\mathbb{Q}) = -23$.

Definition 3.9 Definition of the discriminant of a relative extension. If $\mathfrak{o}_L$ is a free $\mathfrak{o}_K$-module with basis $\{x_i\}$, then we set $\mathscr{D}(L/K) = (\det(\mathrm{Tr}_{L/K}(x_i x_j)))$ (where (—) is

the ideal in $\mathfrak{o}_K$).

Now in general, we only have a basis $\{x_i\}$ when $\mathfrak{o}_K$ is a PID. To define the relative discriminant $\mathscr{D}(L/K)$, it will suffice to define $v_\mathfrak{p}(\mathscr{D}(L/K))$ for each prime ideal $\mathfrak{p}$ of $\mathfrak{o}_K$. Recall that $\mathfrak{o}_{K,\mathfrak{p}}$ is a PID. Let $x_1, \ldots, x_n$ denote a basis for $\mathfrak{o}_{L,\mathfrak{p}} := \mathfrak{o}_L \otimes_{\mathfrak{o}_K} \mathfrak{o}_{K,\mathfrak{p}}$ over $\mathfrak{o}_{K,\mathfrak{p}}$. Set $v_\mathfrak{p}(\mathscr{D}(L/K)) = v_\mathfrak{p}(\det(\mathrm{Tr}(x_i x_j)))$. This is independent of the choice of basis (exactly as in Lemma 3.2). It remains to check that $v_\mathfrak{p}(\mathscr{D}) = 0$ for almost all $\mathfrak{p}$. Pick $y_1, \ldots, y_n$ a basis of L/K with all y_i's algebraic integers. Then $\mathfrak{o}_L \supseteq \sum \mathfrak{o}_K y_i \supseteq N\mathfrak{o}_L$, where $N = (\mathfrak{o}_L : \sum \mathfrak{o}_K y_i)$. If $\mathfrak{p} \nmid N$, then N is a unit in $\mathfrak{o}_{K,\mathfrak{p}}$, and so $\mathfrak{o}_{L,\mathfrak{p}} = \sum \mathfrak{o}_{K,\mathfrak{p}} y_i$. Suppose that $\mathfrak{p} \nmid N$ and $\mathfrak{p} \nmid \det(\mathrm{Tr}(y_i y_j))$. For such $\mathfrak{p}$, we conclude that by definition $v_\mathfrak{p}(\mathscr{D}(L/K)) = 0$. It follows therefore that $\mathscr{D}(L/K)$ is well-defined.

3.1 The absolute norm of an ideal

Definition 3.10 Let K be a number field, and let $\mathfrak{a}$ be an integral $\mathfrak{o}_K$-ideal. We define the **absolute norm** $N\mathfrak{a}$ of $\mathfrak{a}$ by $N\mathfrak{a} = |\mathfrak{o}_K/\mathfrak{a}| = (\mathfrak{o}_K : \mathfrak{a})$.

Proposition 3.11 Suppose that $\mathfrak{a}$ and $\mathfrak{b}$ are integral $\mathfrak{o}_K$-ideals. Then $N(\mathfrak{ab}) = (N\mathfrak{a})(N\mathfrak{b})$.

Proof. It suffices to prove this result when $\mathfrak{b} = \mathfrak{p}$, a prime. Observe that $\mathfrak{ap} \subset \mathfrak{a}$ and $\ker\left(\mathfrak{o}_K/\mathfrak{ap} \xrightarrow{\text{quotient}} \mathfrak{o}_K/\mathfrak{a}\right) = \mathfrak{a}/\mathfrak{ap}$. Now $\mathfrak{a}/\mathfrak{ap}$ is an $\mathfrak{o}_K/\mathfrak{p}$-module. We have that $\mathfrak{o}_K/\mathfrak{p} = \mathbb{F}$, a field, and so $\mathfrak{a}/\mathfrak{ap}$ is an $\mathbb{F}$-vector space. Thus $\mathfrak{a}/\mathfrak{ap}$ is trivial iff $\mathfrak{a} = \mathfrak{ap}$ iff $\mathfrak{o}_K = \mathfrak{p}$, which is a contradiction. We wish to show that $\mathfrak{a}/\mathfrak{ap}$ is a one-dimensional $\mathbb{F}$-vector space (since then it will follow that $|\mathfrak{a}/\mathfrak{ap}| = |\mathfrak{o}_K/\mathfrak{p}|$). Thus assume for a contradiction that $\dim_\mathbb{F}(\mathfrak{a}/\mathfrak{ap}) > 1$. Then there exists an M such that $0 \neq M \subsetneq \mathfrak{a}/\mathfrak{ap}$, where M is a one-dimensional $\mathbb{F}$-vector space. So, if $\pi : \mathfrak{a} \to \mathfrak{ap}$ is the canonical map, then we must have $\mathfrak{a} \supset N \supset \mathfrak{ap}$, so $\mathfrak{o}_K \supset \mathfrak{a}^{-1}N \supset \mathfrak{p}$, which is a contradiction since $\mathfrak{p}$ is maximal. Hence $\dim_\mathbb{F}(\mathfrak{a}/\mathfrak{ap}) = 1$, i.e. $|\mathfrak{a}/\mathfrak{ap}| = |\mathfrak{o}_K/\mathfrak{p}|$.

Remark. Note that the map N extends to all of I_K by multiplicativity.

Proposition 3.12 $|N_{K/\mathbb{Q}}(x)| = N(x\mathfrak{o}_K)$ for $x \in \mathfrak{o}_K$.

Proof. Since $\mathbb{Z}$ is a PID, we can find a $\mathbb{Z}$-basis $x_1, \ldots, x_n$ of $\mathfrak{o}_K$ such that $a_1x_1, \ldots, a_nx_n$ ($a_i \in \mathbb{Z}$) is a $\mathbb{Z}$-basis of $x\mathfrak{o}_K$. Then $\mathfrak{o}_K/x\mathfrak{o}_K \simeq \bigoplus_{i=1}^n \mathbb{Z}x_i / \bigoplus_{i=1}^n \mathbb{Z}a_ix_i$, and so $|\mathfrak{o}_K/x\mathfrak{o}_K| = \prod_{i=1}^n a_i$. Next, observe that $\{xx_i\}$ is also a $\mathbb{Z}$-basis of $x\mathfrak{o}_K$. Hence it follows that the maps $\varphi_x : x_i \mapsto xx_i$ and $\theta : x_i \mapsto ax_i$ satisfy $|\det \varphi_x| = |\det \theta| = \prod_{i=1}^n a_i = |\mathfrak{o}_K/x\mathfrak{o}_K|$. This proves the result.

Chapter 4

Decomposition of Ideals in Extension Fields

Suppose we have an extension of number fields L/K. We have $K \supset \mathfrak{o}_K \supset \mathfrak{p}$. We may write $\mathfrak{p}\mathfrak{o}_L = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}$.

Terminology.

1. e_i is called the **ramification index** of $\mathfrak{P}_i$ in L/K.
2. $\mathfrak{P}_i \cap \mathfrak{o}_K = \mathfrak{p}$. So $\mathfrak{o}_K/\mathfrak{p} = \mathbb{F}_q \hookrightarrow \mathfrak{o}_L/\mathfrak{P}_i = \mathbb{F}_{q^{f_i}}$. $f_i = \dim_{\mathbb{F}_q}(\mathfrak{o}_L/\mathfrak{P}_i)$. We call f_i the **residue class extension degree** of L/K.

Theorem 4.1 $\sum_{i=1}^{g} e_i f_i = [L : K]$.

Proof. We do the case $K = \mathbb{Q}$. Choose a $\mathbb{Z}$-basis $x_1, \ldots, x_n$ of $\mathfrak{o}_L$. Then $\mathfrak{o}_L/p\mathfrak{o}_L \simeq \sum_{i=1}^{n} \mathbb{F}_q x_i$, and so $(\mathfrak{o}_L : p\mathfrak{o}_L) = p^n$. Now consider the following series:

$$\mathfrak{o}_L \supset \mathfrak{P}_1 \supset \mathfrak{P}_1^2 \supset \cdots \supset \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g - 1} \supset \mathfrak{o}_L\mathfrak{p} = p\mathfrak{o}_L.$$

At each step, we have $\mathfrak{a} \supset \mathfrak{a}\mathfrak{P}_i$, $\mathfrak{a}/\mathfrak{a}\mathfrak{P}_i \simeq \mathfrak{o}_L/\mathfrak{P}_i$, and $|\mathfrak{o}_L/\mathfrak{P}_i| = p^{f_i}$. Continuing in this way, we obtain $(\mathfrak{o}_L : p\mathfrak{o}_L) = \prod_{i=1}^{g} p^{f_i e_i} = p^{\sum e_i f_i} = p^n$ (from the first part).

Remark. In general, the latter half of the argument goes through. However, we cannot in general find an $\mathfrak{o}_K$-basis of $\mathfrak{o}_L$. So we localize and use the isomorphism

$$\mathfrak{o}_L/\mathfrak{p}\mathfrak{o}_L \simeq \mathfrak{o}_{L,\mathfrak{p}}/\mathfrak{p}\mathfrak{o}_{L,\mathfrak{p}} \simeq \sum(\mathfrak{o}_{K,\mathfrak{p}}x_i/\mathfrak{p}\mathfrak{o}_{K,\mathfrak{p}})x_i$$

($\mathfrak{o}_{K,\mathfrak{p}}$ is a PID).

Lemma 4.2 Suppose we have an extension L/K with primes ideals $\mathfrak{P}$ and $\mathfrak{p}$ in L and K, respectively. Then $\mathfrak{P} \cap \mathfrak{o}_K = \mathfrak{p}$ if and only if $\mathfrak{P} \mid \mathfrak{p}\mathfrak{o}_L$.

Proof. Recall that $\mathfrak{P} \mid \mathfrak{p}\mathfrak{o}_L$ if and only if $\mathfrak{P} \supset \mathfrak{p}\mathfrak{o}_L$. Now if $\mathfrak{P} \mid \mathfrak{p}\mathfrak{o}_L$, then

$$\mathfrak{P} \cap \mathfrak{o}_K \supset \mathfrak{p}\mathfrak{o}_L \cap \mathfrak{o}_K \supset \mathfrak{p}.$$

Since $\mathfrak{p}$ is a maximal ideal of $\mathfrak{o}_K$, it follows that $\mathfrak{p} = \mathfrak{P} \cap \mathfrak{o}_K$. On the other hand, if $\mathfrak{P} \cap \mathfrak{o}_K = \mathfrak{p}$, then $(\mathfrak{P} \cap \mathfrak{o}_K)\mathfrak{o}_L = \mathfrak{p}\mathfrak{o}_L \subset \mathfrak{P}\mathfrak{o}_L$, and so $\mathfrak{P} \mid \mathfrak{p}$.

Theorem 4.3 Suppose that L/K is Galois. Then f_i and e_i are independent of the particular $\mathfrak{P}_i \mid \mathfrak{p}$.

Proof. First observe that if $\mathfrak{P} \supset \mathfrak{p}\mathfrak{o}_L$ and $\sigma \in \mathrm{Gal}(L/K)$, then $\mathfrak{P}^\sigma \supset \mathfrak{p}^\sigma\mathfrak{o}_L = \mathfrak{p}\mathfrak{o}_L$. Hence $\mathrm{Gal}(L/K)$ permutes the divisors of $\mathfrak{p}\mathfrak{o}_L$. We wish to show that this action is transitive. Choose

$$a \in \mathfrak{P}_1, \quad a \notin \mathfrak{P}_2 \cdots \mathfrak{P}_g. \tag{$*$}$$

(We can do this since the $\{\mathfrak{P}_i\}_{i=1}^g$ are distinct.) Consider $N_{L/K}(a) \in \mathfrak{P}_1 \cap \mathfrak{o}_K = \mathfrak{p}$, i.e. $\prod_{\sigma\in\mathrm{Gal}(L/K)} a^\sigma \in \mathfrak{P}_1 \cdots \mathfrak{P}_g$. Suppose we are given i with $1 \leq i \leq g$. We have $\prod_\sigma a^\sigma \in \mathfrak{P}_i$. Hence $a^\sigma \in \mathfrak{P}_i$ for some σ since $\mathfrak{P}_i$ is prime. We may apply our initial condition $(*)$ to obtain $a^\sigma \in \mathfrak{P}_1^\sigma$, $a^\sigma \notin \mathfrak{P}_2^\sigma \cdots \mathfrak{P}_g^\sigma$. So comparing, we may deduce that $\mathfrak{P}_i = \mathfrak{P}_1^\sigma$, whence it follows that the Galois action is indeed transitive.

Terminology.

1. If $g = n$, we say that $\mathfrak{p}$ is **completely split** in L/K.
2. If $e = n$, we say that $\mathfrak{p}$ is **totally ramified**.

3. If $f = n$, we say that $\mathfrak{p}$ is **totally inert** in L/K.

Definition 4.4 Let R be a commutative ring. The **Jacobson radical** J of R is the intersection of all the maximal ideals of R.

Proposition 4.5 $x \in J$ iff $1 - xy$ is a unit in R for all $y \in R$.

Proof. Suppose that $1 - xy$ is not a unit. Then it is contained in some maximal ideal $\mathfrak{m}$, say. Then $x \in J \subseteq \mathfrak{m}$, and therefore $1 \in \mathfrak{m}$, which is a contradiction. Now suppose that $x \notin \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. Then $(\mathfrak{m}, x) = R$, and so $1 = m + xy$ for some $m \in \mathfrak{m}$ and $y \in R$. Hence $1 - xy \in \mathfrak{m}$, and so $1 - xy$ is not a unit.

Proposition 4.6 (Nakayama's Lemma) Let M be a finitely generated R-module, and suppose that $\mathfrak{a}$ is an ideal of R contained in J. Suppose further that $\mathfrak{a}M = M$. Then $M = 0$.

Proof. Suppose that $M \neq 0$, and let $u_1, \ldots, u_n$ be a minimal set of generators of M. Since $u_n \in \mathfrak{a}M$, we have $u_n = a_1u_1 + \cdots + a_nu_n$, $a_i \in \mathfrak{a}$, and so $(1 - a_n)u_n = a_1u_1 + \cdots + a_{n-1}u_{n-1}$. Since $a_n \in J$, we have that $1 - a_n$ is a unit (Proposition 4.5), and so $u_n \in \langle u_1, \ldots, u_{n-1} \rangle$, which is a contradiction.

Corollary 4.7 Suppose that M is a finitely generated R-module. Let N be a submodule of M, and let $\mathfrak{a} \subseteq J$ be an ideal of R. Suppose that $M = \mathfrak{a}M + N$. Then $M = N$.

Proof. We have $\mathfrak{a}(M/N) = (\mathfrak{a}M + N)/N$. Now apply Proposition 4.6 to M/N.

Now suppose that R is a local ring with maximal ideal $\mathfrak{m}$ and residue field $k = R/\mathfrak{m}$. Let $\mathfrak{m}$ be a finitely generated R-module. Then $M/\mathfrak{m}M$ is a finite dimensional k-vector space.

Proposition 4.8 Suppose that $\{x_i\}_{i=1}^n \subseteq M$ are such that $\{\bar{x}_i\}_{i=1}^n \subseteq M/\mathfrak{m}M$ are a basis for that k-vector space. Then $\langle x_1, \ldots, x_n \rangle = M$.

Proof. Set $N = \langle x_1, \ldots, x_n \rangle$. Then the composite map $N \hookrightarrow M \to M/\mathfrak{m}M$ maps N onto $M/\mathfrak{m}M$. Hence $M = N + \mathfrak{m}M$, and so $M = N$.

Theorem 4.9 Let L/K be a finite extension of number fields. Then $\mathfrak{p}$ **ramifies** in L/K if and only if $\mathfrak{p} \mid \mathscr{D}(L/K)$.

Proof. Suppose that $\mathfrak{p}\mathfrak{o}_L = \prod_{i=1}^g \mathfrak{P}_i^{e_i}$.

1. Note that $\mathfrak{p}$ ramifies in L/K iff the finite ring $R_{L,\mathfrak{p}} := \mathfrak{o}_L/\mathfrak{p}\mathfrak{o}_L \simeq \prod_{i=1}^g \mathfrak{o}_L\mathfrak{P}_i^{e_i}$ has no nonzero nilpotent elements.

2. Recall that $v_\mathfrak{p}(\mathscr{D}(L/K)) := v_\mathfrak{p}(\mathscr{D}(\mathfrak{o}_{L,\mathfrak{p}}/\mathfrak{o}_{K,\mathfrak{p}}))$. Hence it suffices to prove that $R_{L,\mathfrak{p}}$ has nonzero nilpotents iff $\mathscr{D}(\mathfrak{o}_{L,\mathfrak{p}}/\mathfrak{o}_{K,\mathfrak{p}}) \equiv 0 \pmod{\mathfrak{p}}$.

3. Suppose that $\mathfrak{p}$ is ramified, and let $\bar{x}$ denote a nonzero nilpotent element of $R_{L,\mathfrak{p}}$. Now $R_{L,\mathfrak{p}}$ is an $\mathfrak{o}_{K,\mathfrak{p}}/\mathfrak{p}\mathfrak{o}_{K,\mathfrak{p}} := k$-vector space. Complete $\bar{x}_1 = \bar{x}, \ldots, \bar{x}_n$ to a k-basis of $R_{L,\mathfrak{p}}$. Let $x_1, \ldots, x_n \in \mathfrak{o}_{L,\mathfrak{p}}$ be such that $x_i \equiv \bar{x}_i \pmod{\mathfrak{p}}$. Then $x_1, \ldots, x_n$ is an $\mathfrak{o}_{K,\mathfrak{p}}$-basis of $\mathfrak{o}_{L,\mathfrak{p}}$ (Proposition 4.8). Now

   $$\mathscr{D}(\mathfrak{o}_{L,\mathfrak{p}}/\mathfrak{o}_{K,\mathfrak{p}}) = \det(\mathrm{Tr}_{L/K}(x_i x_j)) \pmod{\mathfrak{p}} = \det(\mathrm{Tr}_{R_{L,\mathfrak{p}}/k}(\bar{x}_i\bar{x}_j)) \pmod{\mathfrak{p}}.$$

   The elements $\bar{x}_i\bar{x}_j$ are all nilpotents. Hence they all have trace zero (via Jordan canonical form), and so it follows that $\mathscr{D}(\mathfrak{o}_{L,\mathfrak{p}}/\mathfrak{o}_{K,\mathfrak{p}}) \equiv 0 \pmod{\mathfrak{p}}$.

4. Suppose that $\mathfrak{p}$ is nonramified in L/K, with $\mathfrak{p}\mathfrak{o}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_g$. Then $R_{L,\mathfrak{p}} = \prod_{i=1}^g \mathfrak{o}_L/\mathfrak{P}_i = \prod_{i=1}^g F_i$, where the F_i's are finite fields. Let $\{\bar{x}_{i,j}\}_{i,j} \in R_{L,\mathfrak{p}}$ denote a k-basis of F_i. Then $\{\bar{x}_{i,j}\}_{i,j}$ are a k-basis of $R_{L,\mathfrak{p}}$. Pick $x_{i,j} \in \mathfrak{o}_L$ such that $x_{i,j} \equiv \bar{x}_{i,j} \pmod{\mathfrak{o}_{L,\mathfrak{p}}}$. By Nakayama's Lemma, we have that $\{x_{i,j}\}_{i,j}$ are a basis of $\mathfrak{o}_{L,\mathfrak{p}}$ over $\mathfrak{o}_{K,\mathfrak{p}}$. Then

   $$\overline{\mathscr{D}(\mathfrak{o}_{L,\mathfrak{p}}/\mathfrak{o}_{K,\mathfrak{p}})} = \overline{\det(\mathrm{Tr}(x_{ij}x_{\ell k}))_{(i,j),(\ell,k)}} \pmod{\mathfrak{p}} = \det(\mathrm{Tr}(\bar{x}_{ij}\bar{x}_{\ell k}))_{(i,j),(\ell,k)} \pmod{\mathfrak{p}}$$

   (where we are ordering lexicographically). We claim that if $i \neq \ell$, then $\mathrm{Tr}(\bar{x}_{ij}\bar{x}_{\ell k}) = 0$, for $\mathrm{Tr}(x_{ij}x_{\ell k})$ is the trace of $x_{ij}x_{\ell k}$ as an $\mathfrak{o}_K$-endomorphism of $\mathfrak{o}_L$. Thus $\mathrm{Tr}(\bar{x}_{ij}\bar{x}_{\ell k})$ is the trace of $\bar{x}_{ij}\bar{x}_{\ell k}$ as a k-endomorphism of $\mathfrak{o}_L/\mathfrak{p} = R_{L,\mathfrak{p}}$. We may

regard $\bar{x}_{ij}$ as $(0, 0, \ldots, 0, \bar{x}_{ij}, 0, \ldots, 0)$ (where the nonzero term is in the i^{th} position) since $R_{L,\mathfrak{p}} \simeq \prod_{h=1}^{g} F_h$. Hence $\mathrm{Tr}(\bar{x}_{ij}\bar{x}_{\ell k}) = 0$ when $i \neq \ell$. Therefore, as a matrix, $\det(\mathrm{Tr}(\bar{x}_{ij}\bar{x}_{\ell k}))$ is the determinant of a block diagonal matrix with g blocks, so the determinant of the i^{th} block is the discriminant of F_i over k. However, $d(F_i/k) = \det(x_{ij}^{\sigma})_{j,\sigma}^2$ ($\sigma \in \mathrm{Gal}(F_i/k)$), and this is nonzero (cf Proposition 1.23). Hence $\det(\mathrm{Tr}(\bar{x}_{ij}\bar{x}_{\ell k}))_{(i,j),(\ell,k)} \neq 0$.

Theorem 4.10 (Kronecker) Let $L = K(\theta)$, with θ an algebraic integer. Let θ have minimal polynomial $f(T)$ over K. Suppose that $\mathfrak{p} \subset \mathfrak{o}_K$ is a prime ideal such that $\mathfrak{p} \nmid [\mathfrak{o}_L : \mathfrak{o}_K[\theta]]$. Let $k = \mathfrak{o}_K/\mathfrak{p}$, and suppose that $\bar{f}(T) = \prod_j \bar{g}_j(T)^{e_j} \pmod{\mathfrak{p}}$, with $\bar{g}_j$ distinct, irreducible, monic polynomials over $k[T]$. Then $\mathfrak{p}\mathfrak{o}_L = \prod_j \mathfrak{P}_j^{e_j}$, where the $\mathfrak{P}_j$ are distinct prime ideals with $\mathfrak{P}_j = (\mathfrak{p}, g_j(\theta))\mathfrak{o}_L$.

Proof. Let $N = [\mathfrak{o}_L : \mathfrak{o}_K[\theta]]$. We are given that $\mathfrak{p} \nmid N$. We have that $N\mathfrak{o}_L \subseteq \mathfrak{o}_K(\theta) \subseteq \mathfrak{o}_L$. Tensoring with $\mathfrak{o}_{K,\mathfrak{p}}$ and using the fact that N is a $\mathfrak{p}$-unit gives $\mathfrak{o}_{L,\mathfrak{p}} \subseteq \mathfrak{o}_{K,\mathfrak{p}}[\theta] \subseteq \mathfrak{o}_{L,\mathfrak{p}}$, and so $\mathfrak{o}_{K,\mathfrak{p}}[\theta] = \mathfrak{o}_{L,\mathfrak{p}}$.

We show that the $\mathfrak{P}_j$'s are prime ideals of $\mathfrak{o}_L$. We have

$$\frac{\mathfrak{o}_L}{\mathfrak{P}_j} = \frac{\mathfrak{o}_L}{(\mathfrak{p}, g_j(\theta))} = \frac{\mathfrak{o}_{L,\mathfrak{p}}}{(\mathfrak{p}, g_j(\theta))} = \frac{\mathfrak{o}_{K,\mathfrak{p}}[\theta]}{(\mathfrak{p}, g_j(\theta))} \xleftarrow{\sim} \frac{\mathfrak{o}_{K,\mathfrak{p}}[T]}{(\mathfrak{p}, g_j(T), f(T))}.$$

Now

$$\frac{\mathfrak{o}_{K,\mathfrak{p}}[T]}{(\mathfrak{p}, g_j(T), f(T))} \simeq \frac{k[T]}{(\bar{g}_j(T), \bar{f}(T))} \simeq \frac{k[T]}{(\bar{g}_j(T))},$$

and this last quotient is a field.

We now show that $\mathfrak{p}\mathfrak{o}_L = \prod_j \mathfrak{P}_j^{e_j}$. First observe that

$$\prod_j \mathfrak{P}_j^{e_j} = \prod_j (\mathfrak{p}, g_j(\theta))^{e_j} = \prod_j (\bar{g}_j(\theta))^{e_j} \pmod{\mathfrak{p}} = \prod_j (\bar{f}(\theta)) = (0).$$

Hence

$$\prod_j \mathfrak{P}_j^{e_j} \subseteq \mathfrak{p}\mathfrak{o}_L. \qquad (*)$$

Now recall that the proof of Theorem 4.1 implies that

$$(\mathfrak{o}_L : \mathfrak{p}\mathfrak{o}_L) = |k|^{[L:K]} = |k|^{\deg(f)}. \qquad (**)$$

Calculate $\left(\mathfrak{o}_L : \prod_j \mathfrak{P}_j^{e_j}\right) = \prod_j (\mathfrak{o}_L : \mathfrak{P}_j)^{e_j}$. In the above step, we showed that $(\mathfrak{o}_L : \mathfrak{P}_j) = |k|^{\deg(\bar{g}_j)}$. Hence (cf proof of Theorem 4.1), we have that

$$\prod_j (\mathfrak{o}_L : \mathfrak{P}_j)^{e_j} = |k|^{\sum_j e_j \deg(\bar{g}_j)} = |k|^{\deg(\bar{f})}. \qquad (***)$$

It therefore follows that $(*)$ is an equality.

We leave it as an exercise to show that distinct $\bar{g}_j$'s give distinct primes.

Remark 4.11 With the same setup as in Theorem 4.10, we have

$$\Delta_{\mathfrak{p}}(L/K) = \Delta(f) = \prod_{i<j} (\theta_i - \theta_j)$$

and $\mathscr{D}_{\mathfrak{p}}(L/K) = (\Delta_{\mathfrak{p}}^2) \subset \mathfrak{o}_{K,\mathfrak{p}}$. Hence $\mathfrak{p} \mid \mathscr{D}(L/K)$ iff $\bar{f}$ has a repeated root $\pmod{\mathfrak{p}}$ iff $e_j > 1$ iff $\mathfrak{p}$ ramifies (cf Theorem 4.9).

Example. Calculate the ring of integers and discriminant of $K = \mathbb{Q}(\sqrt[3]{2})$. Set $\theta = \sqrt[3]{2}$. Calculate $D(1, \theta, \theta^2) = \begin{vmatrix} 3 & 0 & 0 \\ 0 & 0 & 6 \\ 0 & 6 & 0 \end{vmatrix} = -108 = -2^2 \cdot 3^3$. There are two possibilities:

1. Can $\alpha = \frac{1}{2}(\lambda_1 + \lambda_2\theta + \lambda_3\theta^2)$ be an integer, $0 \le \lambda_i \le 1$? We have $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \frac{3\lambda_1}{2} \in \mathbb{Z}$, and so $\lambda_1 \in 2\mathbb{Z}$. So $\lambda_1 = 0$, and therefore $\alpha' = \frac{1}{2}(\lambda_2\theta + \lambda_3\theta^2)$ is also an algebraic integer. $N_{K/\mathbb{Q}}(a\theta + b\theta^2) = 2(a^4 + 4b^3)$. Thus $N(\alpha') = \frac{\lambda_2^4}{8} + \lambda_3^3$. Thus the only possibility is $\lambda_2 = 0$, $\lambda_3 = 1$, i.e. $\alpha' = \frac{1}{2}\theta^2 = \frac{1}{\theta}$, and this is not an algebraic integer.

2. Can $\alpha = \frac{1}{3}(\lambda_1 + \lambda_2\theta + \lambda_3\theta^2)$ be an integer, $0 \le \lambda_i \le 2$? $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \lambda_1 \in \mathbb{Z}$. Now just check the possibilities. Suppose $\lambda_1 = 0$. Then $\alpha' = \frac{1}{3}(\lambda_2\theta + \lambda_3\theta^2)$ is an algebraic integer. Then $N(\alpha') = \frac{2\lambda_2^4 + 24\lambda_3^3}{81}$. Now $2\lambda_2^4 + 24\lambda_3^3 \equiv 0 \pmod{81}$, and so $2\lambda_2^4 \equiv 0 \pmod 3$, so $\lambda_2 \equiv 0 \pmod 3$. If $\lambda_2 \equiv 0 \pmod 3$, then $\frac{1}{3}\lambda_3\theta^2$ is

an algebraic integer. But $N\left(\frac{1}{3}\lambda_3\theta^2\right) = \frac{4\lambda_3^3}{27}$, and this lies in $\mathbb{Z}$ only if $\lambda_3 = 0$. Similarly, by considering $\alpha\theta$ and $\alpha\theta^2$, we may assume $\lambda_2 \neq 0$ and $\lambda_3 \neq 0$. Now just compute lots of norms.

Suppose that p is a prime and a is an integer with $(a, p) = 1$. The **Legendre symbol** $\left(\frac{a}{p}\right)$ is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } x^2 - a \equiv 0 \pmod{p} \text{ has a solution,} \\ -1 & \text{otherwise,} \end{cases}$$

i.e.

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue} \pmod{p}, \\ -1 & \text{if } a \text{ is a quadratic nonresidue} \pmod{p}. \end{cases}$$

The Legendre symbol induces a map $\mathbb{F}_p^\times \to \{\pm 1\}$ given by $a \mapsto \left(\frac{a}{p}\right)$. This is a homomorphism. (To see this, use the fact that $\mathbb{F}_p^\times = \langle z \rangle$, say, is cyclic.) Hence we have $z^{(p-1)/2} = -1$, so we obtain

Euler's Criterion. $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$.

So for example $(-1)^{(p-1)/2} = \left(\frac{-1}{p}\right)$.

Law of Quadratic Reciprocity. Let p and q be distinct odd primes. Then

1. $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.
2. $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.
3. $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)/2 \cdot (q-1)/2}$.

Example 4.12 Quadratic fields. Let $L = \mathbb{Q}(\sqrt{d})$ and $K = \mathbb{Q}$. Then p ramifies in L/K if and only if $p \mid d(L/K)$. Thus if $d \equiv 1 \pmod{4}$, p ramifies iff $p \mid d$. If $d \not\equiv 1$

(mod 4), p ramifies iff $p \mid 2d$. Set

$$\theta = \begin{cases} \sqrt{d} & \text{if } d \not\equiv 1 \pmod 4, \\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

Then, in each case $\mathfrak{o}_L = \mathbb{Z}[\theta]$.

1. Let $d \not\equiv 1 \pmod 4$ and $\theta = \sqrt{d}$. Then $f(T) = T^2 - d$. p splits in $L/\mathbb{Q}$ iff $\bar{f}(T)$ factors $\pmod p$ iff $T^2 \equiv d \pmod p$ has roots iff $\left(\frac{d}{p}\right) = 1$.

2. Suppose that $d \equiv 1 \pmod 4$ and that $p \nmid d$ and $\theta = \frac{1+\sqrt{d}}{2}$. Note that θ has minimal polynomial $(x-\theta)(x-\bar{\theta}) = x^2 - x + \frac{1-d}{4}$. Suppose $p \neq 2$. Then consider $\left(x - \frac{1}{2}\right)^2 - \frac{d}{4} \equiv 0 \pmod p$. Thus p splits iff $\left(\frac{d}{p}\right) = 1$. Now suppose that $p = 2$, and consider $x^2 + x \pm \frac{1-d}{4} \pmod 2$. This polynomial splits if $d \equiv 1 \pmod 8$, in which case 2 splits, and is irreducible, and hence 2 is inert, if $d \equiv 5 \pmod 8$.

Chapter 5

Class Numbers and Units

1. We show that $I_K/P_K = C_K$ is finite — not a very effective process, calculating $|C_K| = h_K$. We then give a second proof — due to Minkowski — which gives a very effective method of calculation.

2. $\mathfrak{o}_K^\times$ is a finitely generated $\mathbb{Z}$-module. Its torsion elements are those $u \in \mathfrak{o}_K^\times$ such that $u^n = 1$, i.e. roots of unity. The classification theorem for finitely generated abelian groups says that $\mathfrak{o}_K^\times = \mu_K \times \mathbb{Z}^r$, where μ_K is a finite group.

Theorem. (Dirichlet) Let K be a number field, and let μ_K be the group of roots of unity in K. Then $D_K^\times \xrightarrow{\sim} \mu_K \times \mathbb{Z}^{s+t-1}$, where s is the number of real embeddings $K \hookrightarrow \mathbb{R}$, and $2t$ is the number of complex embeddings $K \hookrightarrow \mathbb{C}$. (Note that if $K/\mathbb{Q}$ is Galois, then all embeddings are either real or complex.)

Example. Suppose $d > 1$, d squarefree, and let $K = \mathbb{Q}(\sqrt{d})$. Then $\mathfrak{o}_K^\times \cong \{\pm 1\} \times \mathbb{Z}$. Call a generator of $\mathfrak{o}_K^\times/\{\pm 1\} \simeq \mathbb{Z}$ a **fundamental unit** of $\mathfrak{o}_K^\times$.

[**Exercise.** Such ε "generate" solutions to Pell's equation $x^2 - dy^2 = \pm 1$.]

Theorem 5.1 $C_K = I_K/P_K$ is finite.

To prove the theorem, we prove the following assertion: Let $x_1, \ldots, x_n$ be a $\mathbb{Z}$-basis of $\mathfrak{o}_K$, and let $c \in C_K$. Then we can find an integral ideal $\mathfrak{c}$ with class c such that

$N(\mathfrak{c}) \leq \prod_\sigma \left(\sum_i |x_i^\sigma|\right)$, where the σ's run through all embeddings of K into $\mathbb{C}$.

Proof of assertion. Let $\mathscr{S} = \left\{\sum_{i=1}^n a_i x_i,\ a_i \in \mathbb{Z} \mid 0 \leq a_i \leq (N\mathfrak{a})^{1/n} + 1\right\}$, where $n = [K : \mathbb{Q}]$ and $\mathfrak{a}$ is an integral ideal in the class of c^{-1}. Note that $|\mathscr{S}| > N\mathfrak{a}$. So by the pigeonhole principle, there exist $\alpha, \beta \in \mathscr{S}$ such that $\alpha \equiv \beta \pmod{\mathfrak{a}}$, i.e. $(\alpha - \beta) = \mathfrak{c}\mathfrak{a}$ with $\mathfrak{c}$ an integral $\mathfrak{o}_K$-ideal. Since $(\alpha - \beta)$ is principal and $\mathfrak{a}$ is of class c^{-1}, it follows that $\mathfrak{c}$ has class c. Hence

$$|N_{K/\mathbb{Q}}(\alpha - \beta)| = \left|\prod_\sigma (\alpha^\sigma - \beta^\sigma)\right| \leq ((N\mathfrak{a})^{1/n} + 1)^n \prod_\sigma \left(\sum_i |x_i^\sigma|\right).$$

So

$$N\mathfrak{c}N\mathfrak{a} \leq ((N\mathfrak{a})^{1/n} + 1)^n \prod_\sigma \left(\sum_i |x_i^\sigma|\right).$$

Thus

$$N_\mathfrak{c} \leq \left(1 + \frac{1}{(N\mathfrak{a})^{1/n}}\right)^n \prod_\sigma \left(\sum_i |x_i^\sigma|\right).$$

We may make $\frac{1}{(N\mathfrak{a})^{1/n}}$ as small as we desire by replacing $\mathfrak{a}$ by $a\mathfrak{a}$. Hence it follows that $N_\mathfrak{c} \leq \prod_\sigma \left(\sum_i |x_i^\sigma|\right)$. Now observe that there are only a finite number of *integral* $\mathfrak{o}_K$-ideals with norm at most a given number m, for there are only finitely many primes $p \leq m$. So we have to show that there are only a finite number of ideals with norm a given prime power p^n. But note that such prime ideals must occur in the factorization of $p\mathfrak{o}_K$ since $p^n\mathfrak{o}_K \subseteq p\mathfrak{o}_K$, and these are finite in number.

Example 1. $K = \mathbb{Q}(i)$, $\mathfrak{o}_K = \mathbb{Z}[i]$. Thus $N\mathfrak{c} \leq (1 + |i|)(1 + |i|) = 4$. If $N\mathfrak{c} = 2$, then $2\mathfrak{o}_K = (1 - i)^2$, and $(1 - i) = \mathfrak{p}_2$ is principal. If $N\mathfrak{c} = 3$, then $3\mathfrak{o}_K = \mathfrak{p}_3$ is *inert* (since via considering $x^2 \equiv -1 \pmod 3$ and $\left(\frac{-1}{3}\right) = -1$, and so 3 is inert). Hence $\mathbb{Z}[i]$ is a PID.

Example 2. $K = \mathbb{Q}(\sqrt{551})$. Thus $\mathfrak{o}_K = \mathbb{Z}[\sqrt{551}]$, and $551 = 19 \cdot 29$. Then $\{1, \sqrt{551}\} = \{x_1, x_2\}$, say. Thus $N_\mathfrak{c} \leq (1 + \sqrt{551})^2 < 597$. Help! (However, Minkowski's bound gives $N\mathfrak{c} \leq 46$.)

Minkowski's Bound. Same setup as in Theorem 5.1. Then

$$N\mathfrak{c} \leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}|d(K/\mathbb{Q})|^{1/2}.$$

Example 3. Find the class group of $\mathbb{Z}[\sqrt{10}]$. By Minkowski's bound, we can find $\mathfrak{c}$ in each class such that $N\mathfrak{c} \leq \frac{2}{2^2}|4 \cdot 10|^{1/2} < 4$. Consider $\mathfrak{p}_2$. Now $2 \mid 40$, so $2\mathfrak{o}_K = \mathfrak{p}_2^2$. By Kronecker's Theorem, $\mathfrak{p}_2 = (2, \sqrt{10})$. Is this principal? Suppose that $\mathfrak{p}_2 = (\alpha)$, where $\alpha = x + y\sqrt{10}$. Then $2\mathfrak{o}_K = \mathfrak{p}_2\bar{\mathfrak{p}}_2 = (\alpha\bar{\alpha})$. So $\pm 2 = \alpha\bar{\alpha} = x^2 - 10y^2$, which is a contradiction, since reducing this equation $\pmod 5$ yields $\left(\frac{\pm 2}{5}\right) = 1$, which is false. Hence $\mathfrak{p}_2$ is not principal, and so its class has order 2. Now consider $\mathfrak{p}_3$. Consider $x^2 - 10 \pmod 3$. This splits, and so we get $3\mathfrak{o}_K = \mathfrak{p}_3\bar{\mathfrak{p}}_3$. Kronecker's Theorem tells us that $\mathfrak{p}_3 = (3, \sqrt{10} - 1)$ and $\bar{\mathfrak{p}}_3 = (3, \sqrt{10} + 1)$. Suppose that $\mathfrak{p}_3 = (\alpha)$, where $\alpha = x + y\sqrt{10}$. Then we get $\pm 3 = \alpha\bar{\alpha} = x^2 - 10y^2$, which is a contradiction as before.

5.1 Consequences of the Finiteness of the Class Number

1. Consider solutions to Diophantine equations of the form $x^3 = y^2 + d$ (where usually $d > 0$). We seek *integral* solutions. We shall suppose that $\mathbb{Q}(\sqrt{-d})$ has class number prime to 3. Let us take as an example the case $d = 200$. We work in $K = \mathbb{Q}(\sqrt{-2})$. We check that $\mathfrak{o}_K = \mathbb{Z}[\sqrt{-2}]$ is a PID (use the Minkowski bound). Look at the factorization of ideals $(x^3) = (y+\sqrt{-d})(y-\sqrt{-d})$. Observe that $\gcd((y+10\sqrt{-2}), (y-10\sqrt{-2})) \mid 20\sqrt{-2}$ (i.e. the gcd divides the difference of the two generators). We check on the behavior of 2 and 5 in K. Then $(2) = \mathfrak{p}_2^2$ (by inspection, since $2 \mid 8 = d(K/\mathbb{Q})$). $x^2 - 2 \pmod 5$ is irreducible, and so 5 is inert, i.e. $\mathfrak{p}_5 = (5)$. Hence $\gcd((y + 10\sqrt{-2}), (y - 10\sqrt{-2})) = \mathfrak{p}_2^a\mathfrak{p}_5^b$. Write $(y + 10\sqrt{-2}) = \mathfrak{a}\mathfrak{p}_2^a\mathfrak{p}_5^b$ with $(\mathfrak{a}, 10) = 1$. Applying complex conjugation to both sides gives $(y - 10\sqrt{-2}) = \bar{\mathfrak{a}}\mathfrak{p}_2^a\mathfrak{p}_5^b$, with $(\bar{\mathfrak{a}}, 10) = 1$. Hence $(y + 10\sqrt{-2})(y - 10\sqrt{-2}) = \mathfrak{a}\bar{\mathfrak{a}}\mathfrak{p}_2^{2a}\mathfrak{p}_5^{2b}$, and so $3 \mid a$ and $\mid b$. Now by definition, $(\mathfrak{a}, \bar{\mathfrak{a}}) = 1$, and so $\mathfrak{a}$ and $\bar{\mathfrak{a}}$ are both cubes. So $(y + 10\sqrt{-2}) = \mathfrak{b}^3$, say. Since $\mathfrak{o}_K$ is a PID, we have $\mathfrak{b} = (\alpha+\beta\sqrt{-2})$. [Note that to show that $\mathfrak{b}$ is principal, it would suffice to show that K has class number prime to 3.] Now $\mathfrak{o}_K^\times = \{\pm 1\}$ by Dirichlet's Theorem. So $y + 10\sqrt{-2}$ is a unit times $(\alpha + \beta\sqrt{-2})^3$, which is $\pm 1 \cdot (\alpha + \beta\sqrt{-2})^3$. Thus

without loss of generality

$$y + 10\sqrt{-2} = (\alpha + \beta\sqrt{-2})^3 = (\alpha^3 - 6\beta^2\alpha) + \sqrt{-2}(3\alpha^2\beta - 2\beta^3). \qquad (*)$$

Equating real and imaginary parts yields

$$10 = \beta(3\alpha^2 - 2\beta^2). \qquad (**)$$

Hence the possibilities for β are $\beta = \pm 1, \pm 2, \pm 5, \pm 10$. Suppose $\beta = \pm 1$. Then $10 = \pm(3\alpha^2 - 2)$. If we take $\beta = +1$, then $3\alpha^2 = 12$, and so $\alpha = \pm 2$. From $(*)$, $y = \alpha^3 - 6\beta^2\alpha = \pm 2(4 - 6) = \pm 4$, and so $x^3 = 16 + 200 = 6^3$ (from the defining equation). If we take $\beta = -1$, then we have $10 = -3\alpha^2 + 2$, which is a contradiction. This is called the method of descent. Other possibilities for β are left as an exercise.

2. Consider integers represented by the quadratic form $X^2 - 2Y^2$. We take $K = \mathbb{Q}(\sqrt{2})$. First observe that $n = x^2 - 2y^2$ iff $N_{K/\mathbb{Q}}(x + y\sqrt{2}) = n$. Note that $N_{K/\mathbb{Q}}(1-\sqrt{-2}) = -1$, and so henceforth we do not worry about signs. We claim that n is represented by $X^2 - 2Y^2$ iff $n = 2^a \prod_i p_i^{b_i} \prod_i q_i^{2c_i}$, with $\left(\frac{2}{p_i}\right) = 1$ and $\left(\frac{2}{q_i}\right) = -1$. To see necessity, suppose that $q^{2m+1} \| n = x^2 - 2y^2$, with $\left(\frac{2}{q}\right) = -1$, where q is an odd prime. Reduce modulo q. This yields $(x')^2 \equiv 2(y')^2 \pmod{q}$, with x' and y' nonzero modulo q. This is a contradiction, since otherwise $\left(\frac{2}{q}\right) = 1$. To see sufficiency, we first check that $\mathbb{Z}[\sqrt{2}]$ is a PID. The value set of solutions is closed under multiplication (by multiplication of norms). Obviously -1, 2, and q^2 are all represented. Thus we are required to prove the above p_i are represented. If $\left(\frac{2}{p_i}\right) = 1$, then $x^2 - 2 \pmod{p_i}$ splits, and so $p_i \mathfrak{o}_K = \mathfrak{p}_i \bar{\mathfrak{p}}_i$, with $\mathfrak{p}_i \neq \bar{\mathfrak{p}}_i$. Now $\mathbb{Z}[\sqrt{2}]$ is a PID, and so $\mathfrak{p}_i = (\alpha_i)$. $(p_i) = (\alpha_i \bar{\alpha}_i)$. Thus $p_i = \alpha_i \bar{\alpha}_i$. Let $\alpha = x_i + y_i\sqrt{2}$, and then we have $\pm p_i = x_i^2 - 2y_i^2$.

5.2 The Geometry of Numbers

Definition 5.2 Let $H \subseteq \mathbb{R}^n$ be a subgroup. We say that H is **discrete** if $H \cap K$ is finite for all compact K of $\mathbb{R}^n$.

Example 5.3 Suppose $v_1, \ldots, v_n$ is a basis in $\mathbb{R}^n$. Then $\sum_{i=1}^n \mathbb{Z}v_i \subseteq \mathbb{R}^n$ is discrete. $\mathbb{Z} + \mathbb{Z}\sqrt{2} \subseteq \mathbb{R}$ is not discrete.

Theorem 5.4 Let H be a discrete subgroup of $\mathbb{R}^n$. Then H is generated over $\mathbb{Z}$ by r vectors $e_1, \ldots, e_r$ *which are linearly independent over* $\mathbb{R}$.

Proof. Choose $e_1, \ldots, e_r \in H$ with $e_1, \ldots, e_r$ $\mathbb{R}$-linearly independent and with r maximal. Set $\mathcal{P}_{\mathbf{e}} = \{\sum_{i=1}^r \alpha_i e_i | \, \alpha_i \in [0,1]\}$. $\mathcal{P}_{\mathbf{e}}$ is called the **fundamental parallelogram** of H with respect to the basis $e_1, \ldots, e_r$. Note that $\mathcal{P}_{\mathbf{e}}$ is compact since it is homeomorphic to $[0,1]^r$. Let $x \in H$. We can write $x = \sum_{i=1}^r \lambda_i e_i$, with $\lambda_i \in \mathbb{R}$, since r is maximal, for otherwise we could adjoin x to the $\mathbf{e}$-basis. For $j \in \mathbb{Z}$, define $x_j := jx = \sum_{i=1}^r \lfloor \lambda_i j \rfloor e_i$ (where $\lfloor \cdot \rfloor$ means "integer part"). Thus $x_j = \sum_i (\lambda_i j - \lfloor \lambda_i j \rfloor) e_i$. So we have $x_j \in \mathcal{P}_{\mathbf{e}}$. In fact, $x_j \in \mathcal{P}_{\mathbf{e}} \cap H$. Recall that, since H is discrete, $|\mathcal{P}_{\mathbf{e}} \cap H| < \infty$. Consider $j = 1$. We have $x = x_1 + \sum \lfloor \lambda_i \rfloor e_i$, so x is in the $\mathbb{Z}$-span of a finite set, i.e. H is finitely generated over $\mathbb{Z}$. By finiteness of $\mathcal{P}_{\mathbf{e}} \cap H$, we can find $j \neq k$ so that $x_j = x_k$. Expanding gives

$$\sum \lambda_i (j-k) e_i = \sum (\lfloor j\lambda_i \rfloor - \lfloor k\lambda_i \rfloor) e_i,$$

and so $\lambda_i(j-k) = \lfloor j\lambda_i \rfloor - \lfloor k\lambda_i \rfloor$, and so $\lambda_i \in \mathbb{Q}$. Now let x vary in $\mathcal{P}_{\mathbf{e}} \cap H$, $x = \sum \lambda_i e_i$. Let d be the least common multiple of the λ_i's. For any $x \in H$, we have $x = x_1 + \sum \lfloor \lambda_i \rfloor e_i \in \frac{1}{d} \sum \mathbb{Z} e_i$. Thus $H \subseteq \frac{1}{d} \sum \mathbb{Z} e_i$. So $\sum \mathbb{Z} e_i \subseteq H \subseteq \frac{1}{d} \sum \mathbb{Z} e_i$. Hence H is $\mathbb{Z}$-free of rank r on some combination of the $\left\{\frac{1}{d} e_i\right\}$, so this basis is $\mathbb{R}$-linearly independent, as required.

Definition 5.5 With the above notation, call H a **lattice** in $\mathbb{R}^n$ if $r = n$.

Definition 5.6 Let $\mathbf{e} = \{e_1, \ldots, e_r\}$ and $\mathbf{f} = \{f_1, \ldots, f_r\}$ be $\mathbb{Z}$-bases of H. We define $\mathrm{Vol}(H) := \mathrm{Vol}(\mathcal{P}_{\mathbf{e}})$. Note that a change of basis $\mathbf{e} \to \mathbf{f}$ corresponds to a matrix in $\mathrm{GL}_r(\mathbb{Z})$, and so $\mathrm{Vol}(\mathcal{P}_{\mathbf{e}}) = \mathrm{Vol}(\mathcal{P}_{\mathbf{f}})$ since the change of basis matrix has determinant of absolute value 1.

Theorem 5.7 (Minkowski) Let H be an $\mathbb{R}^n$-lattice, and let $\mathscr{S} \subseteq \mathbb{R}^n$ be a measurable subset such that $\mathrm{Vol}(\mathscr{S}) > \mathrm{Vol}(H)$. Then there exist $x, y \in \mathscr{S}$ such that $x - y \in H \setminus \{0\}$ (i.e. x and y are distinct).

Proof. Let $e_1, \ldots, e_n$ be a $\mathbb{Z}$-basis of H. Write $\mathbb{R}^n = \bigcup_{h \in H} \mathcal{P}_{\mathbf{e}} + h$. Then $\mathscr{S} = \bigcup_{h \in H} [(h + \mathcal{P}_{\mathbf{e}}) \cap \mathscr{S}]$. (Note that if $h_1 \neq h_2 \in H$, then $(\mathcal{P}_{\mathbf{e}} + h_1) \cap (\mathcal{P}_{\mathbf{e}} + h_2)$ has measure zero.) Thus

$$\mathrm{Vol}(\mathscr{S}) = \sum_{h \in H} \mathrm{Vol}((h + \mathcal{P}_{\mathbf{e}}) \cap \mathscr{S}) = \sum_{h \in H} \mathrm{Vol}(\mathcal{P}_{\mathbf{e}} \cap (\mathscr{S} - h)). \qquad (*)$$

(Note that volumes are translation invariant.) Now suppose for a contradiction that the sets $\mathcal{P}_{\mathbf{e}} \cap (\mathscr{S} - h)$ are all disjoint. Then we would have

$$\mathrm{Vol}(\mathcal{P}_{\mathbf{e}}) \geq \sum_{h} \mathrm{Vol}(\mathcal{P}_{\mathbf{e}} \cap (\mathscr{S} - h)) = \mathrm{Vol}(\mathscr{S}),$$

and so we would have $\mathrm{Vol}(H) \geq \mathrm{Vol}(\mathscr{S})$, which would contradict the hypothesis. So we conclude that the sets $\mathcal{P}_{\mathbf{e}} \cap (\mathscr{S} - h)$ are *not* disjoint. So we can find $h \neq h'$ with $\mathcal{P}_{\mathbf{e}} \cap (\mathscr{S} - h) \cap (\mathscr{S} - h') \neq \varnothing$. Hence there exist $x, y \in \mathscr{S}$ such that $x - h = y - h'$. Since we then have $x - y = h - h' \in H$ and $h \neq h'$, it follows that $x - y \neq 0$.

Definition 5.8 We say that $\mathscr{S} \subseteq \mathbb{R}^n$ is **symmetric** if $x \in \mathscr{S}$ implies $-x \in \mathscr{S}$.

Definition 5.9 We say that $\mathscr{S} \subseteq \mathbb{R}^n$ is **convex** if for all $x, y \in \mathscr{S}$ and $\alpha \in [0, 1]$, we have that $\alpha x + (1 - \alpha) y \in \mathscr{S}$.

Corollary 5.10 (Blichfeldt) Let $\mathscr{S} \subseteq \mathbb{R}^n$ be a symmetric, convex, measurable subset, and suppose that $\mathrm{Vol}(\mathscr{S}) > 2^n \mathrm{Vol}(H)$ (where H is as above). Then $\mathscr{S}$ contains a nonzero point of H.

Proof. Set $\mathscr{S}' = \frac{1}{2}\mathscr{S}$. Then $\mathrm{Vol}(\mathscr{S}') = \frac{1}{2^n} \mathrm{Vol}(\mathscr{S}) > \mathrm{Vol}(H)$. Hence by Theorem 5.7, there exist $y, z \in \mathscr{S}'$ such that $x := y - z \in H \setminus \{0\}$. So $x = \frac{1}{2}(2y) + \frac{1}{2}(-2z) \in H$. Now $2y \in \mathscr{S}$, by definition, and $-2z \in \mathscr{S}$ by symmetry. Thus $x \in \mathscr{S}$ since $\mathscr{S}$ is convex. So $x \in (\mathscr{S} \cap H) \setminus \{0\}$, as required.

Embellishment. With our previous notation, suppose further that $\mathscr{S}$ is compact, but that $\mathrm{Vol}(\mathscr{S}) \geq 2^n \mathrm{Vol}(H)$. Then we can still find a nonzero element of $\mathscr{S} \cap H$.

Proof. Since $\mathscr{S}$ is compact, it is closed and therefore complete. Consider $\mathscr{S}_k := \left(1+\frac{1}{k}\right)\mathscr{S}$ for each positive integer k. Then $\mathrm{Vol}(\mathscr{S}_k) = \left(1+\frac{1}{k}\right)^n \mathrm{Vol}(\mathscr{S}) > 2^n \mathrm{Vol}(H)$. Hence, as before, we can find $x_k \in (\mathscr{S}_k \cap H) \setminus \{0\}$. Therefore $x_k \in (2\mathscr{S}) \cap H$, and this last set is finite since H is discrete. Hence there exists x_m such that $x_m \in \bigcap_k \mathscr{S}_k$. Since $\mathscr{S}$ is closed, it follows that $x_m \in \mathscr{S}$. ($\mathscr{S} = \bigcap_k \mathscr{S}_k$.)

Now we introduce notation that will apply for the rest of the chapter. Let $K/\mathbb{Q}$ be a given number field, and let $\{\sigma_i\}_{i=1}^n$ be distinct embeddings of $K \hookrightarrow \mathbb{C}$, where $n = [K : \mathbb{Q}]$. Let s be the number of real embeddings (so $\sigma_i(K) \subseteq \mathbb{R}$), and let $2t$ be the number of complex embeddings (so $\sigma_i(K) \not\subseteq \mathbb{R}$). Henceforth, we suppose that $\sigma_1, \ldots, \sigma_s$ are real and that $\bar{\sigma}_{s+j} = \sigma_{s+t+j}$. We have the fundamental embedding $\boldsymbol{\sigma} : K \hookrightarrow \mathbb{R}^s \times \mathbb{C}^t$ given by $x \mapsto \prod_{i=1}^{s+t} \sigma_i(x)$.

Note. $\boldsymbol{\sigma}$ is a homomorphism of $\mathbb{Q}$-algebras. (Often we shall identify $\mathbb{R}^s \times \mathbb{C}^t$ with $\mathbb{R}^n$ as *vector spaces* (not as rings!).)

Proposition 5.11 Let $M \subseteq K$ denote a $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$ with $\{x_1, \ldots, x_n\}$ a basis. Then $\boldsymbol{\sigma}(M)$ is an $\mathbb{R}^n$-lattice with $\mathrm{Vol}(\boldsymbol{\sigma}(M)) = 2^{-t} |\det(x_i^{\sigma_j})|$.

Proof. Let $x \in M$, and let $\boldsymbol{\sigma} : K \hookrightarrow \mathbb{R}^s \times \mathbb{C}^t$ be our fundamental embedding. Then

$$\boldsymbol{\sigma}(x) = \prod_{i=1}^{s} x^{\sigma_i} \times \prod_{i=s+1}^{s+t} (\Re(x^{\sigma_i}) \times \Im(x^{\sigma_i})) = \prod_{i=1}^{s} x^{\sigma_i} \times \prod_{i=s+1}^{s+t} \left(\frac{x^{\sigma_i} + \bar{x}^{\sigma_i}}{2} \times \frac{x^{\sigma_i} - \bar{x}^{\sigma_i}}{2\sqrt{-1}} \right).$$

Note that $\mathrm{Vol}(\boldsymbol{\sigma}(M)) = \mathrm{Vol}(\ldots, \boldsymbol{\sigma}(x_i), \ldots)$ (i.e. the volume of the object generated by $\{\boldsymbol{\sigma}(x_i)\}$) is equal to

$$\left| \det \begin{bmatrix} x_j^{\sigma_i} & \frac{x_j^{\sigma_i} + x_j^{\bar{\sigma}_i}}{2} & \frac{x_j^{\sigma_i} - x_j^{\bar{\sigma}_i}}{2\sqrt{-1}} \\ i \le s & s+1 \le i \le s+t & s+t+1 \le i \le 2t+s \\ A & B & C \end{bmatrix} \right|.$$

Multiplying block C by $\sqrt{-1}$ and adding to block B yields

$$\mathrm{Vol}(\boldsymbol{\sigma}(M)) = \left| \det \begin{bmatrix} x_j^{\sigma_i} & x_j^{\sigma_i} & \frac{x_j^{\sigma_i} - x_j^{\bar{\sigma}_i}}{2\sqrt{-1}} \\ A' & B' & C' \end{bmatrix} \right|.$$

Now $\left(B' \times \frac{1}{2\sqrt{-1}}\right) + C'$ yields

$$\mathrm{Vol}(\boldsymbol{\sigma}(M)) = \left|\det\begin{bmatrix} x_j^{\sigma_i} & x_j^{\sigma_i} & x_j^{\bar{\sigma}_i}\end{bmatrix}\right| 2^{-t} = 2^{-t}|\det(x_j^{\sigma_i})| \neq 0$$

(by Proposition 1.23). Hence the $\{\boldsymbol{\sigma}(x_i)\}_{i=1}^n$ are $\mathbb{R}$-linearly independent, and so $\boldsymbol{\sigma}(M)$ is a lattice.

Note that if $M = \mathfrak{o}_K$, then $\boldsymbol{\sigma}(M)$ is an RR^n-lattice, and $\mathrm{Vol}(\boldsymbol{\sigma}(M)) = 2^{-t}|d_{K/\mathbb{Q}}|^{1/2} \neq 0$.

Proposition 5.12 Let $\mathfrak{a}$ be an $\mathfrak{o}_K$-ideal. Then $\boldsymbol{\sigma}(\mathfrak{a})$ is an $\mathbb{R}^n$ lattice, and $\mathrm{Vol}(\boldsymbol{\sigma}(\mathfrak{a})) = 2^{-t}|d_{K/\mathbb{Q}}|^{1/2}N\mathfrak{a}$.

Proof. We know that $\mathfrak{a}$ is a free $\mathbb{Z}$-module of rank n. So we may apply Proposition 5.11 to deduce that $\boldsymbol{\sigma}(\mathfrak{a})$ is an $\mathbb{R}^n$-lattice. We evaluate $\mathrm{Vol}(\boldsymbol{\sigma}(\mathfrak{a}))$. Note that $(\mathfrak{o}_K : \mathfrak{a}) = N\mathfrak{a}$ implies that $(\boldsymbol{\sigma}(\mathfrak{o}_K) : \boldsymbol{\sigma}(\mathfrak{a})) = N\mathfrak{a}$ since $\boldsymbol{\sigma}$ is injective. Thus $\mathrm{Vol}(\boldsymbol{\sigma}(\mathfrak{o}_K)) = \mathrm{Vol}(\boldsymbol{\sigma}(\mathfrak{a}))N\mathfrak{a}^{-1}$. So

$$2^{-t}|d_{K/\mathbb{Q}}|^{1/2} = \mathrm{Vol}(\boldsymbol{\sigma}(\mathfrak{o}_K)) = \mathrm{Vol}(\boldsymbol{\sigma}(\mathfrak{a}))N\mathfrak{a}^{-1},$$

and so $\mathrm{Vol}(\boldsymbol{\sigma}(\mathfrak{a})) = 2^{-t}|d_{K/\mathbb{Q}}|^{1/2}N\mathfrak{a}$.

We now wish to apply Blichfeldt's corollary, et cetera, to this situation.

Proposition 5.13 Let $\mathfrak{a}$ be an integral $\mathfrak{o}_K$-ideal. Then there exists $x \in \mathfrak{a}$, $x \neq 0$, such that

$$|Nx| \leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}|d_{K/\mathbb{Q}}|^{1/2}N\mathfrak{a}$$

(where $N \equiv N_{K/\mathbb{Q}}$).

Proof. View $\boldsymbol{\sigma}$ as having values in $\mathbb{R}^s \times \mathbb{C}^t$. Let u be real and positive. Define $B_u \subseteq \mathbb{R}^s \times \mathbb{C}^t$ by

$$B_u = \left\{ (y_1, \ldots, y_s, z_1, \ldots, z_t) \in \mathbb{R}^s \times \mathbb{C}^t \middle| \sum |y_i| + 2\sum |z_j| \leq u \right\}.$$

B_u is compact since it is closed and bounded (e.g. by the u-hypercube). It is trivial that B_u is symmetric. To show that B_u is convex, suppose that $\sum |y_i| + 2\sum |z_j| \leq u$ (corresponding to a point P) and $\sum |y_i'| + 2\sum |z_j'| \leq u$ (corresponding to a point Q). It remains to prove that if $\alpha \in [0,1]$, then $\alpha P + (1-\alpha)Q \in B_u$. The triangle inequality implies that

$$LHS \leq \alpha \sum |y_i| + 2\alpha \sum |z_j| + (1-\alpha) \sum |y_i'| + 2(1-\alpha) \sum |z_j'| \leq \alpha u + (1-\alpha)u = u.$$

Hence B_u is convex.

For the present, assume that

$$\mathrm{Vol}(B_u) = 2^s \left(\frac{\pi}{2}\right)^t \frac{u^n}{n!}. \qquad (*)$$

We want to apply Blichfeldt (i.e. Corollary 5.10) to the lattice $\boldsymbol{\sigma}(\mathfrak{a})$ and B_u, with u well-chosen. We cunningly choose u such that $\mathrm{Vol}(B_u) = 2^n \mathrm{Vol}(\boldsymbol{\sigma}(\mathfrak{a})) = 2^{n-t}|d_{K/\mathbb{Q}}|^{1/2} N\mathfrak{a}$ (from Proposition 5.12). Then from Corollary 5.10, we can find $\boldsymbol{\sigma}(x) \in \boldsymbol{\sigma}(\mathfrak{a}) \setminus \{0\}$ with $\boldsymbol{\sigma}(x) \in B_u$. Now

$$|N(x)| = \prod_{i=1}^{n} |x^{\sigma_i}| = \prod_{i=1}^{s} |x^{\sigma_i}| \prod_{j=s+1}^{t} |x^{\sigma_j}|^2.$$

Recall that the geometric mean is less than or equal to the arithmetic mean for nonnegative numbers. Thus

$$|N(x)| \leq \left(\sum_{j=1}^{n} \frac{|x_j^{\sigma_j}|}{n} \right)^n \leq \frac{u^n}{n}$$

since $\boldsymbol{\sigma}(x) \in B_u$. So now we solve for our cunningly chosen value of u, i.e. $\mathrm{Vol}(B_u) = 2^n \mathrm{Vol}(\boldsymbol{\sigma}(\mathfrak{a}))$, so $2^s \left(\frac{\pi^t}{2^t}\right) \frac{u^n}{n!} = 2^{n-t}|d_{K/\mathbb{Q}}|^{1/2} N\mathfrak{a}$, so $u^n = \frac{4^t}{\pi^t} n! |d_{K/\mathbb{Q}}|^{1/2} N\mathfrak{a}$. Hence, finally we obtain $|N(x)| \leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} |d_{K/\mathbb{Q}}|^{1/2} N\mathfrak{a}$.

We now have to compute $\mathrm{Vol}(B_u(s,t))$. Set $V(s,t,u) = \mathrm{Vol}(B_u(s,t))$. We use double induction on s and t. Now $V(1,0,u) = 2u$ (the segment $[-u,u]$) and $V(0,1,u) = \frac{\pi u^2}{4}$ (the disc of radius $u/2$). Assume by induction that $(*)$ above gives $V(s,t,u)$. We compute $V(s+1,t,u)$. The set $B_u(s+1,t)$ is defined by the relation

$$|y| + \sum_{i=1}^{s} |y_i| + 2\sum_{j=1}^{t} |z_j| \leq u,$$

with $y \in \mathbb{R}$. Integrating "in strips" and noting that for $y > u$, $B_u = \varnothing$, we obtain

$$V(s+1,t,u) = \int_{-u}^{u} V(s,t,u-|y|)\,dy = 2\int_0^u 2^s \left(\frac{\pi}{2}\right)^t \frac{(u-y)^n}{n!}\,dy = 2^{s+1}\left(\frac{\pi}{2}\right)^t \frac{u^{n+1}}{(n+1)!},$$

and this agrees with $(*)$. Now we compute $V(s,t+1,u)$. The set $B_u(s,t+1)$ is defined by $\sum_{i=1}^{s}|y_i| + 2\sum_{j=1}^{t}|z_j| + 2|z| \le u$, with $z \in \mathbb{C}$. Again, "integrating in strips" yields

$$V(s,t+1,u) = \int_{|z|\le \frac{u}{2}} V(s,t,u-2|z|)\,d\mu(z),$$

where $d\mu(z)$ denotes Lebesgue measure on $\mathbb{C}$. Putting $z = \rho e^{i\theta}$ ($\rho \in \mathbb{R}^+$, $0 \le \theta \le 2\pi$) yields

$$V(s,t+1,u) = \int_0^{\frac{u}{2}}\int_0^{2\pi} 2^s \left(\frac{\pi}{2}\right)^t \frac{(u-2\rho)^n}{n!}\rho\,d\rho\,d\theta = 2^s\left(\frac{\pi}{2}\right)^t \frac{2\pi}{n!}\int_0^{\frac{u}{2}}(u-2\rho)^n\rho\,d\rho.$$

Calculating $\int_0^{u/2}(u-2\rho)^n\rho\,d\rho$ by substituting $2\rho = x$ and integrating by parts shows that this integral has the value $\frac{u^{n+2}}{4(n+1)(n+2)}$. So $V(s,t+1,u) = 2^s\left(\frac{\pi}{2}\right)^{t+1}\frac{u^{n+2}}{(n+2)!}$, which again agrees with $(*)$, since $s + 2(t+1) = n+2$. This completes the proof of Proposition 5.13.

Theorem 5.14 Each ideal class of K contains an integral ideal $\mathfrak{c}$ such that $N\mathfrak{c} \le \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}|d_{K/\mathbb{Q}}|^{1/2}$.

(Note that this yields another proof of the finiteness of the class number.)

Proof. Let c be a class in the ideal class group of K. Choose an integral ideal $\mathfrak{a} \in c^{-1}$. Apply Proposition 5.13 to find an $x \in \mathfrak{a}\setminus\{0\}$ such that $|N(x)| \le \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}|d_{K/\mathbb{Q}}|^{1/2}N\mathfrak{a}$. Now since $x \in \mathfrak{a}$, $(x) = \mathfrak{a}\Sigma$, with Σ integral. Hence

$$|N\mathfrak{a}N\mathfrak{c}| \le \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}|d_{K/\mathbb{Q}}|^{1/2}N\mathfrak{a},$$

so

$$N\mathfrak{c} \le \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}|d_{K/\mathbb{Q}}|^{1/2}.$$

Note that Σ lies in the ideal class c since $(x) = \mathfrak{a}\Sigma$.

Theorem 5.15 (Hermite, Minkowski) If $K \neq \mathbb{Q}$, then $|d_{K/\mathbb{Q}}| > 1$.

Corollary 5.16 If $K \neq \mathbb{Q}$, then there exists a ramified prime in $K/\mathbb{Q}$.

Proof of Theorem 5.15 Apply Theorem 5.14 to the identity class: $1 \leq N\mathfrak{c} \leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n} |d_{K/\mathbb{Q}}|^{1/2}$, so

$$|d_{K/\mathbb{Q}}|^{1/2} \geq \left(\frac{\pi}{4}\right)^t \frac{n^n}{n!} \geq \left(\frac{\pi}{4}\right)^{n/2} \frac{n^n}{n!} = u_n^{1/2},$$

say. It suffices to prove that $u_n > 1$:

$$\frac{u_{n+1}}{u_n} = \left(\frac{\pi}{4}\right) \frac{(n+1)^{2(n+1)}}{n^{2n}} \frac{(n!)^2}{((n+1)!)^2} = \frac{\pi}{4} \left(1 + \frac{1}{n}\right)^{2n} \geq \frac{3\pi}{4} > 1.$$

Now $u_2 = \frac{\pi^2}{4} > 1$, and so the result follows.

We now aim for Dirichlet's unit theorem.

Theorem 5.17 There is an isomorphism of groups $\mathfrak{o}_K^\times \simeq \mu_K \times \mathbb{Z}^{s+t-1}$, where μ_K denotes the roots of unity in K and $s + t - 1$ is the **rank** of $\mathfrak{o}_K^\times$.

Philosophy. Introduce a logarithmic map $L : K^\times \to \mathbb{R}^{s+t}$, where $L(x) = (\ldots, \log |x^{\sigma_i}|, \ldots)$. We then apply our work on lattices, et cetera, to the image $L(\mathfrak{o}_K^\times)$.

Lemma. An element $x \in \mathfrak{o}_K$ is a unit iff $N_{K/\mathbb{Q}}(x) = \pm 1$.

Proof. For the forward direction, if $x, x^{-1} \in \mathfrak{o}_K$, then $N_{K/\mathbb{Q}}(x)^{\pm 1} \in \mathbb{Z}$, so $N_{K/\mathbb{Q}}(x) = \pm 1$. For the reverse direction, suppose that $N_{K/\mathbb{Q}}(x) = \pm 1$. Consider the characteristic equation of multiplication by x on K, i.e. the characteristic equation of φ_x. We obtain $T^n + a_1 T^{n-1} + \cdots \pm 1 = 0$. Hence $x(x^{n-1} + a_1 x^{n-2} + \cdots + a_{n-1}) = \mp 1$, and so

x is invertible.

Warning/Remark. $\frac{1+2i}{1-2i} \in \mathbb{Q}(i)$ has norm 1. However, it is *not* an algebraic integer and so is not a unit. So norm ± 1 by itself is not sufficient.

Observations prior to the proof of Theorem 5.17 We set $n = [K : \mathbb{Q}]$, fixed.

1. Describe $\ker(L \mid \mathfrak{o}_K^\times)$. Let $x \in \ker(L \mid \mathfrak{o}_K^\times)$. Then $|x^{\sigma_i}| = 1$ for all i. Suppose that x has characteristic equation $T^n + a_1 T^{n-1} + \cdots + a_n = 0$. Recall that the a_i's are the symmetric functions in the $\{x^{\sigma_i}\}$. Hence the a_i's are all bounded absolutely (in terms of n), and so x is a root of only a finite possible number of equations. Therefore $|\ker(L \mid \mathfrak{o}_K^\times)| < \infty$, and so $x^d = 1$ for some d, i.e. x is a root of unity. Let μ_K denote the roots of unity in K. We've shown that $\mu_K \supset \ker(L \mid \mathfrak{o}_K^\times)$. Observe by inspection of L that $\mu_K \subset (L \mid \mathfrak{o}_K^\times)$. Summing up, we have shown that $\mu_K = \ker(L \mid \mathfrak{o}_K^\times)$ is finite and cyclic.

2. Show that $L(\mathfrak{o}_K^\times)$ is discrete in $\mathbb{R}^{s+t}$. Let $\mathfrak{C}$ denote the c-hypercube in $\mathbb{R}^{s+t}$. It is required to prove that $|\Sigma \cap L(\mathfrak{o}_K^\times)| < \infty$. Suppose that $L(x) \in \mathfrak{C}$. Then $L(x) = (\ldots, \log|x^{\sigma_i}|, \ldots)$ and $|\log|x^{\sigma_i}|| \leq c$ for all i. Hence $|x^{\sigma_i}| \leq e^c$ for all i. Let x have characteristic equation $T^n + a_1 T^{n-1} + \cdots + a_n$. Then, for fixed c, the $\{a_i\}$ are bounded and in $\mathbb{Z}$. Hence there are a finite number of possible such characteristic equations and so a finite number of possible x's. Therefore $|\Sigma \cap L(\mathfrak{o}_K^\times)| < \infty$, as required.

3. What is the rank of $L(\mathfrak{o}_K^\times)$ in $\mathbb{R}^{s+t}$? We shall show that $L(\mathfrak{o}_K^\times)$ lies in a fixed hyperplane of $\mathbb{R}^{s+t}$: Let

$$H = \left\{ (\xi_1, \ldots, \xi_{s+t}) \in \mathbb{R}^{s+t} \,\middle|\, \sum_{i=1}^{s} \xi_i + 2 \sum_{i=s+1}^{s+t} \xi_i = 0 \right\}.$$

We claim that $L(\mathfrak{o}_K^\times) \subseteq H$. For $\log|\prod_{i=1}^n x^{\sigma_i}| = \sum_{i=1}^n \log|x^{\sigma_i}|$ and $\log|\prod_{i=1}^n x^{\sigma_i}| = \log|N(x)| = \log 1 = 0$. Thus

$$0 = \sum_{i=1}^{n} \log|x^{\sigma_i}| = \sum_{i=1}^{s} \log|x^{\sigma_i}| + 2 \sum_{i=s+1}^{s+t} \log|x^{\sigma_i}|,$$

i.e. $L(x) \in H$.

To prove Theorem 5.17, it is sufficient to prove that $L(\mathfrak{o}_K^\times)$ is an H-lattice.

Strategy. Let $f : H \to \mathbb{R}$ be a nonzero $\mathbb{R}$-linear function. We shall show that there exists $u \in \mathfrak{o}_K^\times$ such that $f(L(u)) \neq 0$. This implies that $L(\mathfrak{o}_K^\times)\mathbb{R} = H$. [For if not, then suppose that $L(\mathfrak{o}_K^\times)\mathbb{R} = V \neq H$. Then we may write $H = V \oplus W$. Consider the linear function $g : V \oplus W \xrightarrow{\pi} W \xrightarrow{f} \mathbb{R}$. This vanishes on $V = L(\mathfrak{o}_K^\times)\mathbb{R}$, which is a contradiction.]

Proof of Theorem 5.17 Frequently we view $H \simeq \mathbb{R}^r$ (where $r = s + t - 1$) via $(\xi_1, \ldots, \xi_{s+t}) \mapsto (\xi_1, \ldots, \xi_r)$. We may obtain an inverse by using the linear relation defining H to calculate what ξ_{s+t} is. So define $f(\boldsymbol{\xi}) = \sum_{i=1}^r c_i \xi_i$, where not all of the c_i's are 0. Once and for all, fix $\alpha \in \mathbb{R}$ such that

$$\alpha \geq \left(\frac{2}{\pi}\right)^t |d_K|^{1/2}. \tag{$*$}$$

As a convention, given $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_r) \in (\mathbb{R}^+)^r$, define $\boldsymbol{\lambda}' \in \mathbb{R}^{s+t}$ with $\boldsymbol{\lambda}' = (\lambda_1, \ldots, \lambda_r, \lambda_{s+t})$ with $\prod_{i=1}^s \lambda_i \prod_{i=s+1}^{s+t} \lambda_i^2 = \alpha$ (where α is fixed). Define

$$B_{\boldsymbol{\lambda},\alpha} = \{(y_1, \ldots, y_s, z_1, \ldots, z_t) \in \mathbb{R}^s \times \mathbb{C}^t : |y_i| \leq \lambda_i, |z_i| \leq \lambda_{s+i}\}.$$

Observe that $B_{\boldsymbol{\lambda},\alpha}$ is symmetric, compact, convex, and

$$\mathrm{Vol}(B_{\boldsymbol{\lambda},u}) = \prod_{i=1}^s 2\lambda_i \prod_{i=s+1}^{s+t} \pi\lambda_i^2 = 2^s \pi^t \alpha.$$

From $(*)$, we have $2^s\pi^t\alpha \geq 2^{s+t}|d_{K/\mathbb{Q}}|^{1/2} = 2^n \,\mathrm{Vol}(\boldsymbol{\sigma}(\mathfrak{o}_K))$. Now apply Blichfeldt (Corollary 5.10) to find $x_{\boldsymbol{\lambda}} \in \mathfrak{o}_K \setminus \{0\}$ with $\boldsymbol{\sigma}(x_{\boldsymbol{\lambda}}) \in B_{\boldsymbol{\lambda},\sigma}$. Note that, by definition of $B_{\boldsymbol{\lambda},\alpha}$, we have $|x_{\boldsymbol{\lambda}}^{\sigma_i}| \leq \lambda_i$ for all i. Also

$$\begin{aligned}
|x_{\boldsymbol{\lambda}}^{\sigma_i}| &= |N(x_{\boldsymbol{\lambda}})| \left|\prod_{j\neq i} x_{\boldsymbol{\lambda}}^{\sigma_j}\right|^{-1} \\
&\geq \prod_{j\neq i} |x_{\boldsymbol{\lambda}}^{\sigma_j}|^{-1} \\
&\geq \prod_{j\neq i} \lambda_j^{-1} \\
&= \alpha^{-1}\lambda_i.
\end{aligned}$$

To sum up: $\alpha^{-1}\lambda_i \leq |x_{\boldsymbol{\lambda}}^{\sigma_i}| \leq \lambda_i$. Take logarithms: $\log\lambda_i - \log\alpha \leq \log|x_{\boldsymbol{\lambda}}^{\sigma_i}| \leq \log\lambda_i$, so

$$0 \leq \log\lambda_i - \log|x_{\boldsymbol{\lambda}}^{\sigma_i}| \leq \log\alpha. \tag{1}$$

Now $f(L(x_{\boldsymbol{\lambda}})) = f(\ldots, \log|x_{\boldsymbol{\lambda}}^{\sigma_i}|, \ldots) = \sum_{i=1}^{r} c_i \log|x_{\boldsymbol{\lambda}}^{\sigma_i}|$. Hence

$$\left| f(L(x_{\boldsymbol{\lambda}})) = \sum_{i=1}^{r} c_i \log\lambda_i \right| = \left| \sum_{i=1}^{r} c_i(\log|x_{\boldsymbol{\lambda}}^{\sigma_i}| - \log\lambda_i) \right| \leq \left(\sum_{i=1}^{r} |c_i| \right) \log\alpha \tag{2}$$

(from (1) above). Now pick $\beta > (\sum_{i=1}^{r} |c_i|)\log\alpha$. For each $h \in \mathbb{N}$, construct a vector $\boldsymbol{\lambda}(h) = (\lambda_1(h), \ldots, \lambda_r(h)) \in (\mathbb{R}^+)^r$ such that

$$\sum_{i=1}^{r} c_i \log\lambda_i(h) = 2\beta h. \tag{3}$$

Construct as before a collection of vectors $\{x_{\boldsymbol{\lambda}(h)}\}_{h=1}^{\infty}$. Note that our previous inequalities hold for these $x_{\boldsymbol{\lambda}(h)}$. Substituting (3) into (2) gives $|f(L(x_{\boldsymbol{\lambda}(h)})) - 2\beta h| < \beta$. So

$$(2h-1)\beta < |f(L(x_{\boldsymbol{\lambda}(h)}))| < (2h+1)\beta. \tag{4}$$

Thus, in particular, the $f(L(x_{\boldsymbol{\lambda}(h)}))$ are all distinct, and so the $x_{\boldsymbol{\lambda}(h)}$ are all distinct. In addition, we have

$$|N(x_{\boldsymbol{\lambda}(h)})| \leq \prod_{i=1}^{s} \lambda_i(h) \prod_{i=s+1}^{s+t} \lambda_i(h)^2 = \alpha.$$

Recall that there are only a finite number of integral ideals $\mathfrak{a}$ such that $N\mathfrak{a} \leq \mathfrak{a}$. Hence the collection of ideals $\{x_{\boldsymbol{\lambda}(h)}\mathfrak{o}_K\}_{h=1}^{\infty}$ has repeats, say $x_{\boldsymbol{\lambda}(i)}\mathfrak{o}_K = x_{\boldsymbol{\lambda}(j)}\mathfrak{o}_K$ $(i > j)$. Then $x_{\boldsymbol{\lambda}(i)} = u x_{\boldsymbol{\lambda}(j)}$, $u \in \mathfrak{o}_K^{\times}$, so $L(x_{\boldsymbol{\lambda}(i)}) = L(u) + L(x_{\boldsymbol{\lambda}(j)})$. Since f is linear, we have

$$f(L(x_{\boldsymbol{\lambda}(i)})) = f(L(u)) + f(L(x_{\boldsymbol{\lambda}(j)})).$$

Now (4) implies that $f(L(u)) \neq 0$, as required.

Remarks and Calculations with Units.

1. **Terminology.** Let $u_1, \ldots, u_r$ be a $\mathbb{Z}$-basis of $\mathfrak{o}_K^{\times}/\mu_K$. We call $u_1, \ldots, u_r$ a **system of fundamental units** for K.

2. **Cyclotomic Unit.** Let $\zeta = e^{2\pi i/p}$ and $K = \mathbb{Q}(\zeta + \zeta^{-1})$. We have

$$\begin{array}{c} \mathbb{Q}(\zeta) \\ \Big| 2 \\ \mathbb{Q}(\zeta + \zeta^{-1}) \\ \Big| \frac{p-1}{2} \\ \mathbb{Q} \end{array}$$

Thus $v_{\mathbb{Q}(\zeta)} = \frac{p-1}{2} - 1$, $v_K = \frac{p-1}{2} - 1$. Hence $(\mathfrak{o}^\times_{\mathbb{Q}(\zeta)} : \mathfrak{o}^\times_K) < \infty$. Note that $v_i = \frac{\zeta - \zeta^{-1}}{\zeta^i - \zeta^{-i}} \in \mathfrak{o}^\times_K$ (see the Problems). Do this for $1 \leq i \leq \frac{p-1}{2}$. Then $(\mathfrak{o}^\times_K : \langle v_1, \ldots, v_{\frac{p-1}{2}} \rangle) \sim h_K$, the class number of K. We need the theory of L-functions to prove this. (See, for example, Borevich and Shafarevich, Chapter IV, or Washington's *Cyclotomic Fields*.) A theorem of Kummer says that if p is odd, then $\mathfrak{o}^\times_{\mathbb{Q}(\zeta)} = \langle \zeta \rangle \times \mathfrak{o}^\times_K$.

3. **Example.** Find a unit of infinite order in $K = \mathbb{Q}(\sqrt[3]{5})$. $s = 1$, $2t = 2$, so $r = 1$. Set $\theta = \sqrt[3]{5}$. Calculate $\mathfrak{o}_K = \mathbb{Z}[\theta]$. 3 ramifies: observe that $X^3 - 5 \equiv (X+1)^3 \pmod 3$, and so we have $(3) = \mathfrak{p}^3$. Note that $N_{K/\mathbb{Q}}(2-\theta) = 3$. (Hence $2-\theta$ is a prime element of $\mathfrak{o}_K$ above 3.) Thus $(2-\theta)$ is a prime ideal above 3. Thus $\mathfrak{p} = (2-\theta)$ and so $(3) = (2-\theta)^3$. Now $(2-\theta)^3 = (8 - 12\theta + 6\theta^2 - 5) = 3(1 - 4\theta + 2\theta^2)$. Hence it follows that $3 = 3 \cdot \text{unit} \cdot (1 - 4\theta + 2\theta^2)$, and so $1 - 4\theta + 2\theta^2$ is a unit.

4. **Quadratic imaginary field K.**

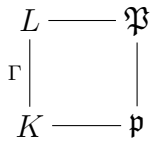
$$\mathfrak{o}^\times_K = \mu_K = \begin{cases} 6^{\text{th}} \text{ roots of unity} & \text{if } d_K = -3 \\ 4^{\text{th}} \text{ roots of unity} & \text{if } d_K = -4 \\ \pm 1 & \text{otherwise.} \end{cases}$$

5. **Real quadratic field K.** $K = \mathbb{Q}(\sqrt{d})$. If $d \not\equiv 1 \pmod 4$, then $\mathfrak{o}_K = \mathbb{Z}[\sqrt{d}]$, and $\mathfrak{o}^\times_K = \langle \pm 1 \rangle \times \langle u \rangle$, where u is a fundamental unit. Let $u = a + b\sqrt{d}$. By replacing u by $\pm u^{\pm 1}$, we may without loss of generality take $a, b > 0$. If we write $u^n = a_n + b_n\sqrt{d}$, we get a sequence $\{b_n\}$ which is monotonically increasing. Thus, to find a fundamental unit, it suffices to find u with $a, b > 0$ and b minimal. For example, in $\mathbb{Q}(\sqrt{2})$, $1 + \sqrt{2}$ is a fundamental unit.

Chapter 6

Galois Action and Prime Decomposition

Let L/K be a Galois extension of number fields with Galois group Γ.



Suppose that $\mathfrak{p}\mathfrak{o}_L = \prod_{i=1}^{g} \mathfrak{P}_i^e$. Recall (see the proof of Theorem 4.3) that Γ acts transitively on the $\{\mathfrak{P}_i\}$.

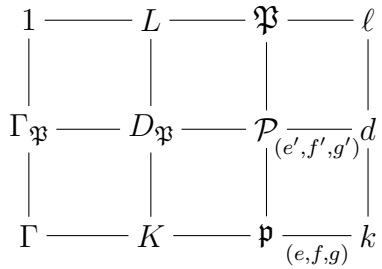
Definition 6.1

1. The **decomposition group** $\Gamma_{\mathfrak{P}}$ of $\mathfrak{P}/\mathfrak{p}$ in L/K is defined by $\Gamma_{\mathfrak{P}} = \{\gamma \in \Gamma : \mathfrak{P}^\gamma = \mathfrak{P}\}$, i.e. $\Gamma_{\mathfrak{P}}$ is the stabilizer of $\mathfrak{P}$.

2. The **inertia group** $T_{\mathfrak{P}}$ of $\mathfrak{P}/\mathfrak{p}$ in L/K is defined by $T_{\mathfrak{P}} = \{\gamma \in \Gamma : x^\gamma \equiv x \pmod{\mathfrak{P}}$ for all $x \in \mathfrak{o}_L\}$.

Alternatively, write $\mathfrak{o}_L/\mathfrak{P} = \ell$ and $\mathfrak{o}_K/\mathfrak{p} = k$. Then reduction $\pmod{\mathfrak{P}}$ induces a group homomorphism $\rho : \Gamma_{\mathfrak{P}} \to \mathrm{Gal}(\ell/k)$ by the following rule: If $x \in \mathfrak{o}_L$ and $\gamma \in \Gamma_{\mathfrak{P}}$, then $\bar{x}^{\rho(\gamma)} = \overline{x^\gamma}$. (Note that this is well-defined since $\gamma \in \Gamma_{\mathfrak{P}}$.) Then $\Gamma_{\mathfrak{P}} = \ker(\rho)$; observe that $T_{\mathfrak{P}} \lhd \Gamma_{\mathfrak{P}}$.

Definition 6.2 The **decomposition field** $D_{\mathfrak{P}} = L^{\Gamma_{\mathfrak{P}}}$ (i.e. $D_{\mathfrak{P}}$ is the subfield of L fixed by elements of $\Gamma_{\mathfrak{P}}$.) We have the following Galois-theoretic tower:



Lemma 6.3 The prime $\mathcal{P}$ is **non-split** in $L/D_{\mathfrak{P}}$ (i.e. $g' = 1$).

Proof. Suppose that $\mathcal{P}\mathfrak{o}_L = \mathfrak{P}\cdots\mathfrak{P}'$, where $\mathfrak{P} \neq \mathfrak{P}'$. By transitivity of Galois action, there exists $\gamma \in \Gamma_{\mathfrak{P}}$ such that $\mathfrak{P}^{\gamma} = \mathfrak{P}'$, which is a contradiction since $\Gamma_{\mathfrak{P}} = \mathrm{Stab}_{\Gamma}(\mathfrak{P})$.

Proposition 6.4 Let $\rho : \Gamma_{\mathfrak{P}} \to \mathrm{Gal}(\ell/k)$ be the homomorphism described above. Then ρ is surjective.

Proof. Viewing decomposition groups as stabilizers, we have $\mathrm{Gal}(L/K)_{\mathfrak{P}} = \Gamma_{\mathfrak{P}} = \mathrm{Gal}(L/D_{\mathfrak{P}})_{\mathfrak{P}}$. We also have the following diagram:

$$\begin{array}{ccc} \rho : \mathrm{Gal}(L/K)_{\mathfrak{P}} & \twoheadrightarrow & \mathrm{Gal}(\ell/k) \\ \supseteq \big| & & \big| \supseteq \\ \rho : \mathrm{Gal}(L/D_{\mathfrak{P}})_{\mathfrak{P}} & \twoheadrightarrow & \mathrm{Gal}(\ell/d) \end{array}$$

To prove the proposition, it will suffice to show that $\mathrm{Gal}(\ell/k) = \mathrm{Gal}(\ell/d)$ (i.e. $k = d$) *and* that $\rho : \mathrm{Gal}(L/D_{\mathfrak{P}})_{\mathfrak{P}} \to \mathrm{Gal}(\ell/d)$ is surjective.

First we perform reduction to $\Gamma = \Gamma_{\mathfrak{P}}$. We wish to show that $k = d$, i.e. that $f = f'$. From Galois theory, $[D_{\mathfrak{P}} : K] = [\Gamma : \Gamma_{\mathfrak{P}}] = g$ (since Γ acts transitively on the g $\mathfrak{P}_i$'s). Recall (see Theorems 4.1 and 4.3) that $[L : K] = efg$. Also,

$$[L : K] = [L : D_{\mathfrak{P}}][D_{\mathfrak{P}} : K] = e'f'g'[D_{\mathfrak{P}} : K] = e'f'[D_{\mathfrak{P}} : K] = e'f'g$$

(where the penultimate equality follows from Lemma 6.3). Putting all this together, we have $efg = e'f'g$, i.e. $ef = e'f'$. Next, we note that $f' = [\ell : d]$ and $f = [\ell : k]$, and so $f \geq f'$ since $\ell \supseteq d \supseteq k$. Now $\mathcal{P}\mathfrak{o}_L = \mathfrak{P}^{e'}$ (from Lemma 6.3). Also,

$$\mathfrak{p}\mathfrak{o}_L = (\mathfrak{p}\mathfrak{o}_{D_\mathfrak{P}})\mathfrak{o}_L = (\mathcal{P}^h \cdots)\mathfrak{o}_L = \mathfrak{P}^{he'} \cdots$$

But in addition we have $\mathfrak{p}\mathfrak{o}_L = \mathfrak{P}^e \cdots$ (by the definition of e). Comparing yields $e \geq e'$. We therefore have that $k = d$, as required.

Without loss of generality, take $\Gamma = \Gamma_\mathfrak{P}$ and $D_\mathfrak{P} = K$. Let $x \in \mathfrak{o}_L$. We want to prove that $\{\overline{x^\gamma} = \bar{x}^{\rho(\gamma)}\}_{\gamma \in \Gamma = \Gamma_\mathfrak{P}}$ runs through all Galois conjugates of $\bar{x}$ in ℓ/k. Let x have minimal polynomial $f(T)$ over K. Let $\bar{x}$ have minimal polynomial $\bar{g}(T)$ over k. Now $f(x) = 0$, and so $\bar{f}(\bar{x}) = 0$, and so $\bar{g} \mid \bar{f}$. The group Γ acts transitively on the roots of $f(T)$. Hence $\rho(\Gamma)$ acts transitively on the roots of $\bar{f}(T)$, whence on those of $\bar{g}(T)$ also.

So we now have $\rho : \Gamma_\mathfrak{P} \twoheadrightarrow \mathrm{Gal}(\ell/k)$ and $[d : k] = f$. Also $g|\Gamma_\mathfrak{P} = n = efg$, so $|\Gamma_\mathfrak{P}| = ef$. Now $|\operatorname{Gal}(\ell/k)| = f$ and $|\Gamma_\mathfrak{P}| = ef$, so $T_\mathfrak{P} = |\ker(\rho)| = e$. We have $\Gamma \supseteq \Gamma_\mathfrak{P} \supseteq T_\mathfrak{P}$.

Corollary 6.5 If $\mathfrak{p}$ is unramified in L/K, then $\Gamma_\mathfrak{P} \simeq \mathrm{Gal}(\ell/k)$.

Proof. In this case, $|T_\mathfrak{P}| = e = 1$.

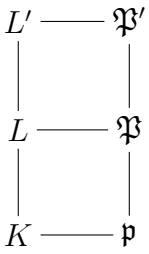
Recall that since ℓ/k is an extension of finite fields, $\mathrm{Gal}(\ell/k)$ is generated by the Frobenius automorphism $\mathrm{Frob}(\ell/k)$ given by $x \mapsto x^{|k|}$.

Definition 6.6 Let $\mathfrak{p}$ denote an unramified prime of L/K. Then there exists a unique $(\mathfrak{P}, L/K) \in \Gamma_\mathfrak{P}$ such that $\rho(\mathfrak{P}, L/K) = \mathrm{Frob}(\ell/k)$. The element $(\mathfrak{P}, L/K)$ is called the **Frobenius element** of $\mathfrak{P}$ in L/K.

6.1 Elementary Properties of the Frobenius Element

Proposition 6.7

1. $(\mathfrak{P}^\gamma, L/K) = \gamma^{-1}(\mathfrak{P}, L/K)\gamma$ for all $\gamma \in \mathrm{Gal}(L/K)$.

2. 

   Let $\mathrm{Gal}(L/K) = \Gamma$ and $\mathrm{Gal}(L'/K) = \Gamma'$. Suppose that L'/K is unramified at $\mathfrak{p}$. We have $\theta : \mathrm{Gal}(L'/K) \twoheadrightarrow \mathrm{Gal}(L/K)$ by restriction. Then $\theta(\mathfrak{P}', L'/K) = (\mathfrak{P}, L/K)$.

Proof.

1. First observe that the map $x \mapsto x^{\gamma^{-1}}$ induces an isomorphism of fields $\mathfrak{o}_L/\mathfrak{P}^\gamma \xrightarrow{\sim} \mathfrak{o}_L/\mathfrak{P}$. Let $q = N\mathfrak{p} = |k|$. Then $(x^{\gamma^{-1}})^{(\mathfrak{P},L/K)} \equiv (x^{\gamma-1})^q \pmod{\mathfrak{P}}$ for all $x \in \mathfrak{o}_L$. Apply γ to both sides. This gives

$$x^{\gamma^{-1}(\mathfrak{P},L/K)} \equiv x^q \pmod{\mathfrak{P}^\gamma}$$

   for all $x \in \mathfrak{o}_L$. Hence, by definition, $\gamma^{-1}(\mathfrak{P}, L/K)\gamma = (\mathfrak{P}^\gamma, L/K)$.

2. By definition of restriction, for $x \in \mathfrak{o}_L$, we have $x^{\theta(\gamma')} = x^{\gamma'}$ for all $\gamma' \in \Gamma'$. In particular, for $\gamma' = (\mathfrak{P}', L'/K)$, we have

$$x^{\theta(\mathfrak{P}',L'/K)} = x^{(\mathfrak{P}',L'/K)} \equiv x^q \pmod{\mathfrak{P}'} \equiv x^q \pmod{\mathfrak{P}' \cap \mathfrak{o}_L} \equiv x^q \pmod{\mathfrak{P}}.$$

   Therefore, by definition of $(\mathfrak{P}, L/K)$ and the uniqueness of the Frobenius automorphism, we have $\theta(\mathfrak{P}', L/K) = (\mathfrak{P}, L/K)$.

Example. Let $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$, where ω is a primitive cube root of unity. Then $\mathrm{Gal}(L/\mathbb{Q}) \simeq S_3$.

Claim. No prime p is totally inert in $L/\mathbb{Q}$. For if it were, then we would have $\rho : \mathrm{Gal}(L/\mathbb{Q}) \xrightarrow{\sim} \mathrm{Gal}(\ell/\mathbb{F}_p)$ (an isomorphism since there is no ramification, and $\Gamma_{\mathfrak{P}} = \mathrm{Gal}(L/\mathbb{Q})$ because p does not split). But the left side is S_3, and the right side is a Galois group of a finite extension of finite fields and so is cyclic. This is a contradiction.

Exercise. Prove the same result by considering the factorization of $x^3 - 2 \pmod{p}$.

6.2 Cyclotomic Fields

Recall from Galois theory that $(\mathbb{Z}/m\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ via $a \pmod{m} \mapsto (\sigma_a : \zeta_m \mapsto \zeta_m^a)$.

Theorem. (Kronecker-Weber) Let $K/\mathbb{Q}$ be an abelian extension. Then there exists an m such that $K \subseteq \mathbb{Q}(\zeta_m)$.

Note. If $\mathfrak{o}$ is the ring of integers of $\mathbb{Q}(\zeta_m)$, then $\mathbb{Z}[\zeta_m] \subseteq \mathfrak{o}$ (in fact, this inclusion is an equality). However, we certainly have

$$\Delta(1, \zeta, \ldots, \zeta^{\varphi(m)-1}) = \prod_{\substack{\zeta \neq \zeta' \\ m^{\text{th}} \text{ roots}}} (\zeta - \zeta'),$$

and L'Hôpital's rule gives

$$\lim_{x \to 1} \frac{x^m - 1}{x - 1} = m = \prod_{\zeta \neq 1} (1 - \zeta).$$

So if $(p) \mid (1 - \zeta)$ (where $\zeta \neq 1$), then $p \mid m$. Also, if p ramifies in $\mathbb{Q}(\zeta_m)/\mathbb{Q}$, then $p \mid m$. Also, we have $\zeta \equiv \zeta' \pmod{p}$, and so $\zeta = \zeta'$ if $p \nmid m$.

Theorem 6.8 (Decomposition in cyclotomic extensions) Let $(m,p)=1$, and let n denote the order of p in $(\mathbb{Z}.m\mathbb{Z})^\times$. Then $n=f$ (i.e. the residue class extension degree of p in $\mathbb{Q}(\zeta_m)/\mathbb{Q}$).

Proof.

$$\begin{array}{ccc} L=\mathbb{Q}(\zeta_m) & \text{——} & \mathfrak{P} \\ {\scriptstyle\Gamma}\Big| & & \Big| \\ K=\mathbb{Q} & \text{———} & p \end{array}$$

Γ is abelian, with $\Gamma \simeq (\mathbb{Z}/m\mathbb{Z})^\times$. Let $\mathfrak{P}$ be a prime in $\mathbb{Q}(\zeta_m)$ above p, and set $f=f_{\mathfrak{P}}$. We know that f is the order of $(\mathfrak{P},\mathbb{Q}(\zeta_m)/\mathbb{Q})$. Furthermore, we have $(\mathfrak{P}^\gamma, L/K) = \gamma^{-1}(\mathfrak{P},L/K)\gamma = (\mathfrak{P},L/K)$ since Γ is abelian. So we can denote this automorphism unambiguously by $(\mathfrak{P},L/K)$. Then $\zeta_m^{(\mathfrak{P},L/K)} \equiv \zeta_m^p \pmod{\mathfrak{P}}$. So $\zeta_m^{(\mathfrak{P},L/K)^n} \equiv \zeta_m^{p^n} \equiv \zeta \pmod{\mathfrak{P}}$, since n is the order of p in $(\mathbb{Z}/m\mathbb{Z})^\times$, so $(\mathfrak{P},L/K)^n = 1$ since p is unramified in L/K (and so ρ is injective), and so $f \mid n$. Now suppose for a contradiction that $f<n$. Then

$$\zeta^{(\mathfrak{P},L/K)^f} \equiv \zeta^{p^f} \equiv \zeta \pmod{\mathfrak{P}},$$

and so $\zeta^{p^f-1}-1 \in \mathfrak{P}$. Since $f<n$, $p^f \not\equiv 1 \pmod m$, and so $\zeta^{p^f-1}-1$ can be chosen to be nonzero. By the above note, $\zeta^{p^f-1}-1$ has divisors only dividing m. This is a contradiction, since $(m,p)=1$. Hence $f=n$.

Theorem 6.9 (Quadratic Reciprocity) Let p and q be distinct odd primes. Then

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

Proof. Let $q^* = (-1/q)q$. Then $L=\mathbb{Q}(\sqrt{q^*})$ is the unique quadratic subfield of $\mathbb{Q}(\zeta_q)$. There are at least two ways to see this:

1. $\Gamma = \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \simeq (\mathbb{Z}/q\mathbb{Z})^\times$, and this has a unique subgroup of index 2. Hence $\mathbb{Q}(\zeta_q)/\mathbb{Q}$ contains a unique quadratic subfield L, and q is the unique ramified prime in L. So $L=\mathbb{Q}(\sqrt{q^*})$.

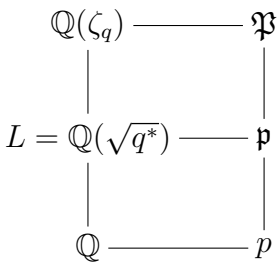
2. (See problems) Let x be the unique character of Γ of order 2, and consider the Gauß sum
$$\tau(\chi,\zeta_q) = \sum_{\gamma\in\Gamma} \chi(\gamma)\zeta_q^\gamma \in \mathbb{Q}(\zeta_q).$$

Then

$$\tau(\chi, \zeta_q)^2 = \left(\frac{-1}{q}\right) q = q^*.$$

Hence $\mathbb{Q}(\sqrt{q^*}) \subseteq \mathbb{Q}(\zeta_q)$.

Note that p does not ramify in $L/\mathbb{Q}$ (via consideration of discriminants). Kummer's criterion implies that p is split or inert in $L/\mathbb{Q}$ according as $(q^*/p) = +1$ or -1, respectively. (Consider $x^2 - q^* \equiv 0 \pmod{p}$.)



Proposition 6.7(2) implies that $(\mathfrak{P}, \mathbb{Q}(\zeta_q)/\mathbb{Q}) \mid_L = (\mathfrak{p}, L/\mathbb{Q})$. Now p is split or inert in $L/\mathbb{Q}$ according as $f_\mathfrak{p} = 1$ or 2, i.e. according as $(\mathfrak{p}, L/\mathbb{Q}) = 1$ or $\neq 1$ (since $(\mathfrak{p}, L/\mathbb{Q})$ generates $\Gamma_\mathfrak{p}$ and $|\Gamma_\mathfrak{p}| = f_\mathfrak{p}$), i.e. according as $p \pmod{q}$ is a square or nonsquare $\pmod{q}$, i.e. according as $(p/q) = +1$ or -1. Hence, equating these methods of evaluation (p/q), we see that

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

from Euler's criterion.

6.3 Quadratic Reciprocity in Totally Real Number Fields

Definition 6.10

1. Let K be a number field. We call K **totally real** if, for all field embeddings $\sigma : K \hookrightarrow \mathbb{C}$, we have $\sigma(K) \subseteq \mathbb{R}$ (i.e. $n = s$, using the notation from the geometry of numbers).

2. Let $x \in K^\times$. We call x **totally positive** if $\sigma(x) > 0$ for all real embeddings σ.

3. Let $x \in K^\times$. We call x **2-primary** if x is **odd** and if there exists $y \in K^\times$ such that $x \equiv y^2 \pmod^* 4\mathfrak{o}_K$.

Explanation.

1. x is **odd** means that no primes lying above 2 occur in the prime factorization of x.

2. The congruence is to be interpreted as follows: Suppose that $4\mathfrak{o}_K = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_m^{a_m}$. We demand that $v_{\mathfrak{p}_i}(x - y^2) \geq a_i$ for $i = 1, \ldots, n$.

Definition 6.11 Let $\mathfrak{p}$ be an odd prime; let $k = \mathfrak{o}_K/\mathfrak{p}$; let $x \in \mathfrak{o}_K \setminus \mathfrak{p}$. Then

$$\left(\frac{x}{\mathfrak{p}}\right) = \begin{cases} +1 & \text{if } x \text{ is a square} \pmod{\mathfrak{p}}, \\ -1 & \text{otherwise.} \end{cases}$$

1. If $x \equiv y \pmod{\mathfrak{p}}$, then $(x/\mathfrak{p}) = (y/\mathfrak{p})$.

2. Since $k^\times$ is cyclic, $(x/\mathfrak{p})(y/\mathfrak{p}) = (xy/\mathfrak{p})$.

3. $(x/\mathfrak{p}) \equiv x^{(N-\mathfrak{p}-1)/2}$ (à la Euler).

More generally, let $\mathfrak{n} = \mathfrak{p}_1 \cdots \mathfrak{p}_m$ (where the $\mathfrak{p}_i$'s are not necessarily distinct primes), and suppose that $(x, \mathfrak{n}) = 1$. Then set $(x/\mathfrak{n}) = \prod_{i=1}^m (x/\mathfrak{p}_i)$. We have results analogous to (1) and (2) above.

We shall aim to prove:

Theorem 6.12 Let K be totally real. Let α, β be two odd, coprime elements of $\mathfrak{o}_K$, and suppose that one of the is 2-primary. Then

$$\left(\frac{\alpha}{(\beta)}\right)\left(\frac{\beta}{(\alpha)}\right) = (-1)^{\sum_{i=1}^n \varepsilon_i(\alpha)\varepsilon_i(\beta)},$$

where $\varepsilon_i(\alpha) = \frac{\mathrm{sgn}(\sigma_i(\alpha))-1}{2}$, $\sigma_i : K \hookrightarrow \mathbb{R}$, and $\varepsilon_i(\beta)$ is defined similarly.

Exercise. Show that if $K = \mathbb{Q}$, then we recover the usual quadratic reciprocity law.

For the proof, we shall assume that $\mathfrak{o}_K$ is a PID. This is to avoid excessive technicalities.

Definition 6.13 Let V be a $\mathbb{Q}$-vector space endowed with a nondegenerate $\mathbb{Q}$-bilinear form $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{Q}$. Let $\Lambda \subseteq V$ be a lattice, i.e. Λ is finitely generated over $\mathbb{Z}$ and $\Lambda\mathbb{Q} = V$. Define the dual Λ^* of V by $\Lambda^* = \{v \in V : \langle v, \Lambda \rangle \subseteq \mathbb{Z}\}$.

Examples.

1. $V = \mathbb{Q}^n$, $\Lambda = \mathbb{Z}^n$, $\langle x, y \rangle = x \cdot y$ (the usual dot product). Then check that $\Lambda^* = \Lambda$, i.e. Λ is self-dual. If $\Lambda = m\mathbb{Z}^n$, then $\Lambda^* = \frac{1}{m}\Lambda$.
2. $V = K$, $\Lambda = \mathfrak{a}$ (initially $\mathfrak{o}_K$). $\langle x, y \rangle = \mathrm{Tr}_{K/\mathbb{Q}}(xy)$. By the problems, $\mathfrak{o}_K^\times = \{x \in K \mid \mathrm{Tr}(x\mathfrak{o}_K) \subseteq \mathbb{Z}\} = \mathscr{D}^{-1}$ (the inverse different).

Definition 6.14 (Generalized Gauß Sum.) Let $\mathscr{D} = (d)$, and let $\omega = b/ad$, where $(a, b) = 1$ and $a, b \in \mathfrak{o}_K \setminus \{0\}$. Then

$$\tau_a(\omega) := \sum_{\alpha \in \mathfrak{o}_K \pmod{a}} e(\mathrm{Tr}(\alpha^2\omega))$$

(where $e(x) = e^{2\pi i x}$).

Note. If $\alpha \equiv \beta \pmod{a}$, then $\mathrm{Tr}(\alpha^2\omega - \beta^2\omega) = \mathrm{Tr}((\alpha - \beta)(\alpha + \beta)\omega) \in \mathbb{Z}$ because $(\alpha - \beta)\omega \in \mathscr{D}^{-1}$. Hence $\tau_a(\omega)$ is well-defined.

Remark 6.15 $\mathrm{Tr}(\mathfrak{a}) \subseteq \mathbb{Z}$ iff $\mathscr{D}\mathfrak{a} \subseteq \mathfrak{o}_K$ (cf the definition of the different!). We refer to a above as the **essential denominator**.

Lemma 6.16 If $(a) \subsetneq \mathfrak{o}_K$, then $s = \sum_{\alpha \in \mathfrak{o}_K \pmod a} e(\mathrm{Tr}(\alpha\omega)) = 0$.

Proof. Recall that $\omega = b/ad$. Thus $(d\omega) \not\subseteq \mathfrak{o}_K$, and so applying Remark 6.15, we see that there exists some $\theta' \in (ba^{-1}d^{-1})$ so that $\mathrm{Tr}(\theta') \notin \mathbb{Z}$, so there is some $\theta \in \mathfrak{o}_K$ so that $\mathrm{Tr}(\theta\omega) \notin \mathbb{Z}$ (take $\theta = \theta'/\omega$). Hence we have $e(\mathrm{Tr}(\theta\omega))s = \sum e(\mathrm{Tr}(\alpha+\theta)\omega) = s$. But $e(\mathrm{Tr}(\theta\omega)) \neq 1$, and so $s = 0$.

We shall now reduce the calculation of $\tau_a(\omega)$ to the case in which a is prime. Initially, suppose that $a = a_1a_2$ with $(a_1, a_2) = 1$. Then $\mathfrak{o}_K/(a) \xrightarrow{\sim} \mathfrak{o}_K/(a_1) \times \mathfrak{o}_K/(a_2)$ given by $x \mapsto (xa_2, xa_1)$. Write $\omega = b/ad = b/a_1a_2d$. Then

$$\begin{aligned}
\tau_a(\omega) &= \sum_{x \in \mathfrak{o}_K \pmod a} e\left(\mathrm{Tr}\left(\frac{x^2 b}{a_1 a_2 d}\right)\right) \\
&= \sum_x e\left(\mathrm{Tr}\left(x^2 \frac{a_2}{a_1}\frac{b}{d} + x^2\frac{a_1}{a_2}\frac{b}{d}\right)\right) \\
&= \sum_x e\left(\mathrm{Tr}\left(x^2 \frac{a_2}{a_1}\frac{b}{d} + x^2\frac{a_1}{a_2}\frac{b}{d} + 2x^2 a_1 a_2 \frac{b}{a_1 a_2 d}\right)\right).
\end{aligned}$$

Now $2x^2a_1a_2b/d = 2x^2b/d$, and Remark 6.15 implies that the trace of this element is an integer. Thus

$$\begin{aligned}
\tau_a(\omega) &= \sum_x e\left(\mathrm{Tr}\left(x^2 \frac{a_2}{a_1}\frac{b}{d} + x^2\frac{a_1}{a_2}\frac{b}{d}\right)\right) \\
&= \sum_{x \pmod{a_1}} e\left(\mathrm{Tr}\left(x^2\frac{a_2}{a_1}\frac{b}{d}\right)\right) \sum_{x \pmod{a_2}} e\left(\mathrm{Tr}\left(x^2\frac{a_1}{a_2}\frac{b}{d}\right)\right) \\
&= \tau_{a_1}(a_2^2\omega)\tau_{a_2}(a_1^2\omega).
\end{aligned}$$

Lemma 6.17 Let π be an odd prime element of $\mathfrak{o}_K$, and let $n \geq 2$. Then if $\omega = b/\pi^n d$, we have

$$\tau_{\pi^n}(\omega) = \begin{cases} |N\pi|^{n/2} & \text{if } n \text{ is even,} \\ |N\pi|^{(n-1)/2}\tau_\pi(\pi^{n-1}\omega) & \text{if } n \text{ is odd.} \end{cases}$$

Proof. It suffices to establish the relation

$$\tau_{\pi^n}\left(\frac{b}{d\pi^n}\right) = |N\pi|\tau_{\pi^{n-2}}\left(\frac{b}{d\pi^{n-2}}\right)$$

for $n \geq 2$. Let x range through $\mathfrak{o}_K \pmod{\pi^{n-1}}$. Let y range through $\mathfrak{o}_K \pmod{\pi}$. Then

$$\begin{aligned}\tau_{\pi^n}\left(\frac{b}{d\pi^n}\right) &= \sum_{x,y} e(\mathrm{Tr}(x+\pi^{n-1}y)^2\omega) \\ &= \sum_{x,y} e(\mathrm{Tr}(x^2+2xy\pi^{n-1})\omega) \\ &= \sum_{x} e(\mathrm{Tr}(x^2\omega)) \sum_{y} e(\mathrm{Tr}(2xy\pi^{n-1}\omega)).\end{aligned}$$

Set

$$S_x = \sum_{y\in\mathfrak{o}_K \pmod{\pi}} e(\mathrm{Tr}(2xy\pi^{n-1}\omega)) = \sum_y e\left(\mathrm{Tr}\left(2xy\frac{b}{\pi d}\right)\right).$$

By Lemma 6.16, $S_x = 0$ *unless* $\pi \mid x$, in which case $S_x = |N\pi|$ (because then each term in the sum is equal to 1). So

$$\tau_{\pi^n}\left(\frac{b}{\pi^n d}\right) = |N\pi| \cdot \sum_{x\in(\pi) \pmod{\pi^{n-1}}} e(\mathrm{Tr}(x^2\omega)).$$

Set $x = \pi x'$. Then x' ranges through $\mathfrak{o}_K \pmod{\pi^{n-2}}$, and so we obtain

$$\tau_{\pi^n}\left(\frac{b}{\pi^n d}\right) = |N\pi|\tau_{\pi^{n-2}}\left(\frac{b}{d\pi^{n-2}}\right).$$

The crucial link between Gauß sums and quadratic reciprocity is given by the following result:

Theorem 6.18 Let $x \in \mathfrak{o}_K$, and suppose that a is odd, with $(x,a) = 1$. Then, with the above notation ($\omega = b/\pi d$), $\tau_a(x\omega) = \tau_a(\omega)(x/(a))$.

Proof. By the above work, we can without loss of generality take π to be prime. We have

$$\tau_\pi(x\omega) = \sum_{\alpha \in \mathfrak{o}_K \pmod{\pi}} e(\mathrm{Tr}(\alpha^2 \omega x)) = \sum_{\beta \in \mathfrak{o}_K \pmod{\pi}} e(\mathrm{Tr}(\beta \omega x)) \left\{ \left(\frac{\beta}{\pi} \right) + 1 \right\}$$

(since we are only interested in *squares*). By Lemma 6.16,

$$\sum_\beta e(\mathrm{Tr}(\beta \omega x)) = 0.$$

So we obtain

$$\tau_\pi(x\omega) = \sum_{\beta \in \mathfrak{o}_K \pmod{\pi}} e(\mathrm{Tr}(\beta \omega x)) \left(\frac{\beta}{\pi} \right). \tag{1}$$

Setting $x = 1$ yields

$$\tau_\pi(\omega) = \sum_\beta e(\mathrm{Tr}(\beta\omega)) \left(\frac{\beta}{\omega} \right).$$

So

$$\tau_\pi(\omega) \left(\frac{x}{\pi} \right) = \sum_\beta e(\mathrm{Tr}(\beta\omega)) \left(\frac{\beta x}{\pi} \right) = \sum_\beta e(\mathrm{Tr}(\beta x \omega)) \left(\frac{\beta x^2}{\pi} \right) = \tau_\pi(x\omega).$$

In order to establish generalized quadratic reciprocity, we need to show the following reciprocity relation for Gauß sums:

Theorem 6.19 Let $\omega = b/ad$ as before. For $x \in K^\times$, set $S(x) = \sum_{\sigma : K \hookrightarrow \mathbb{R}} \mathrm{sgn}(\sigma(x))$ (called the **total signature** of x). Then we have the following reciprocity law for Gauß sums:

$$\frac{\tau_a(\omega)}{|Na|^{1/2}} = \frac{1}{(\sqrt{2})^n} \frac{1}{|N(4b)|^{1/2}} e^{\frac{\pi i}{4} S(\omega)} \tau_{4b} \left(\frac{-a}{4bd} \right).$$

Proof. Needs lots of ϑ functions!!!

6.4 Theta Functions

Lemma 6.20 Let Q denote a positive definite quadratic form on $\mathbb{R}^n$. Then there exists a $c > 0$ such that $Q(\mathbf{x}) \geq c\|\mathbf{x}\|^2$ for all $\mathbf{x} \in \mathbb{R}^n$.

Proof. Consider the restriction $Q\mid_{S^n}$ of Q to S^n, the unit sphere in $\mathbb{R}^n$. As Q is continuous and S^n is compact, $Q\mid_{S^n}$ attains its bounds on S^n. Since Q is positive definite, we have $Q\mid_{S^n}(\mathbf{x}) \geq c > 0$ for all $\mathbf{x} \in S^n$. The general result now follows by scaling.

Theorem 6.21 Let Q be a positive definite quadratic form on $\mathbb{R}^n$. Define

$$T_Q(\mathbf{u}) = \sum_{\mathbf{m}\in\mathbb{Z}^n} e^{-\pi Q(\mathbf{m}+\mathbf{u})}.$$

This series is absolutely and uniformly convergent on $\mathbb{R}^n$. It is periodic on $\mathbb{Z}^n$. Furthermore, T_Q, together with all its partial derivatives, is continuous on $\mathbb{R}^n$.

Proof. Periodicity is plain. By Lemma 6.20, we have $Q(\mathbf{m}+\mathbf{u}) \geq c\|\mathbf{m}+\mathbf{u}\|^2$, so $e^{-\pi Q(\mathbf{m}+\mathbf{u})} \leq e^{-\pi c\|\mathbf{m}+\mathbf{u}\|^2}$. Suppose that C is a real positive constant, and $\mathbf{u} = (u_1, \ldots, u_n)$ with $|u_i| < C/2$. Then, by the above,

$$e^{-\pi Q(\mathbf{m}+\mathbf{u})} \leq e^{-\pi c(\sum m_i^2 - C\sum |m_i| + K)},$$

where K is a constant depending only upon C. Let $\varepsilon > 0$, and take $\mathbf{m}$ such that $\|\mathbf{m}\| > \varepsilon^{-1}$. For such $\mathbf{m}$, we have the following inequalities:

$$|m_1| + |m_2| + \cdots + |m_n| \leq \sqrt{n}\|\mathbf{m}\| \leq \sqrt{n}\varepsilon\|\mathbf{m}\|^2$$

(since $\varepsilon\|\mathbf{m}\| > 1$). So we obtain

$$e^{-\pi Q(\mathbf{m}+\mathbf{u})} \leq e^{-\pi C\|\mathbf{m}\|^2(1-C\sqrt{n}\varepsilon)-\pi CK}.$$

By choosing ε to be sufficiently small, we may assume that $a := 1 - C\sqrt{n}\varepsilon > 0$. So, with finitely many exceptions, we have that T_Q is bounded by $\sum_{\mathbf{m}} De^{\pi aC\|\mathbf{m}\|^2}$ (where $D := e^{-\pi CK}$). However, this last expression is just a product of "1-dimensional" series, which compares with a geometric series. This yields absolute and uniform convergence of our series. [The part about partial derivatives is left as an exercise, but here is a hint: Partial differentiation just introduces polynomials in $m_1, \ldots, m_n$

of even degree — easily "overcome" by $e^{-\pi a m^2}$.]

Since T_Q is $\mathbb{Z}$-periodic and C^∞, we can form the Fourier series of T_Q:

$$T_Q(\mathbf{u}) = \sum_{\mathbf{m}\in\mathbb{Z}^n} a_{\mathbf{m}} e^{2\pi i \mathbf{m}^t\cdot\mathbf{u}},$$

where

$$a_{\mathbf{m}} = \int_{\mathbf{0}}^{\mathbf{1}} T_Q(\mathbf{u}) e^{2\pi i \mathbf{m}^t\cdot\mathbf{u}}\, d\mathbf{u},$$

and we have convergence at all points.

Proposition 6.22 We have

$$a_{\mathbf{m}} = \int_{-\infty}^{\infty} e^{-\pi Q(\mathbf{u})+2\pi i \mathbf{m}^t\cdot\mathbf{u}}\, du.$$

Proof. Using the series definition of T_Q and interchanging the order of integration and summation (by absolute and uniform convergence), we obtain

$$a_{\mathbf{m}} = \sum_{\mathbf{k}} \int_{\mathbf{0}}^{\mathbf{1}} e^{-\pi Q(\mathbf{k}+\mathbf{u})+2\pi i \mathbf{m}^t\cdot\mathbf{u}}\, d\mathbf{u}.$$

Make the substitution $u_i \mapsto u_i - k_i$ (where $\mathbf{k} = (k_1, \ldots, k_n)$). Then

$$a_{\mathbf{m}} = \sum_{\mathbf{k}} \int_{\mathbf{k}}^{\mathbf{k+1}} e^{-\pi Q(\mathbf{u})+2\pi i \mathbf{m}^t\cdot\mathbf{u}}\, d\mathbf{u} = \int_{-\infty}^{\infty} e^{-\pi Q(\mathbf{u})+2\pi i \mathbf{m}^t\cdot\mathbf{u}}\, d\mathbf{u}.$$

Now we introduce some arithmetic.

Recall. $\boldsymbol{\sigma} : K \hookrightarrow \mathbb{R}^n$, $\boldsymbol{\sigma}(x) = (x^{\sigma_i}) = (\sigma_i(x))$. We now pick a $\mathbb{Z}$-basis $\alpha_1, \ldots, \alpha_n$ of a given $\mathfrak{o}_K$-ideal $\mathfrak{a}$. Let $t_1, \ldots, t_n$ denote a set of independent, real, positive variables. Let $Q = Q_{\mathbf{t},\mathfrak{a}}$ be the quadratic form given by $Q_{\mathbf{t},\mathfrak{a}}(\mathbf{u}) = \sum_{i=1}^n t_i z_i^2$, where

$z_j = \sum_q \alpha_q^{\sigma_j} u_q$. Let $A = (\sigma_i(\alpha_q))$. Then the matrix A transforms $\mathbb{Z}^n$ into $\boldsymbol{\sigma}(\mathfrak{a})$. Also, $\det(A) = |d_{K/\mathbb{Q}}|^{1/2} \cdot N\mathfrak{a} = 0$ (see Proposition 5.13). We note that $Q_{\mathbf{t},\mathfrak{a}}(\mathbf{u})$ is positive definite.

Definition 6.23

$$\vartheta(\mathbf{t}, \mathbf{z}, \mathfrak{a}) := T_{Q_{\mathbf{t},\mathfrak{a}}}(\mathbf{u}). \tag{2}$$

(Observe that this definition makes sense since $Q = Q_{\mathbf{t},\mathfrak{a}}$ is positive definite (see Theorem 6.21).) Also observe that

$$\begin{aligned}
\vartheta(\mathbf{t}, \mathbf{z}, \mathfrak{a}) &= T_{Q_{\mathbf{t},\mathfrak{a}}}(\mathbf{u}) \\
&= \sum_{\mathbf{m}\in\mathbb{Z}^n} \exp(-\pi Q(\mathbf{m}+\mathbf{u})) \\
&= \sum_{\mathbf{m}\in\mathbb{Z}^n} \exp\left(-\pi \sum_{j=1}^n t_j \left(\sum_q \alpha_q^{\sigma_j}(m_q + u_q)\right)^2\right) \\
&= \sum_{\mathbf{m}\in\mathbb{Z}^n} \exp\left(-\pi \sum_{j=1}^n t_j \left(z_j + \sum_q m_q \alpha_q^{\sigma_j}\right)^2\right).
\end{aligned}$$

Hence we have

$$\vartheta(\mathbf{t}, \mathbf{z}, \mathfrak{a}) = \sum_{\mu\in\mathfrak{a}} \exp\left(-\pi \sum_{j=1}^m t_j (\mu^{\sigma_j} + z_j)^2\right). \tag{3}$$

By previous work (see Proposition 6.22) we know that

$$a_{\mathbf{m}} = \int_{-\infty}^{\infty} \exp\left(-\pi \sum t_p z_p^2 + 2\pi i \mathbf{m}^t \cdot \mathbf{u}\right) d\mathbf{u}. \tag{4}$$

We wish to transform this into an integral in z-space.

Lemma 6.24 Let $\{\beta_1, \ldots, \beta_n\}$ denote a dual basis of K with respect to the basis $\{\alpha_1, \ldots, \alpha_n\}$. Then $\{\beta_i\}$ is a $\mathbb{Z}$-basis of the ideal $\mathfrak{a}^{-1}\mathscr{D}^{-1}$ and

$$u_k = \sum_{j=1}^n \sigma_j(\beta_k) z_j = \sum_{j=1}^n \beta_k^{\sigma_j} z_j. \tag{5}$$

Proof. We know that $\mathfrak{a}^{-1}\mathscr{D}^{-1}$ identifies as the dual $H = \mathrm{Hom}_{\mathbb{Z}}(\mathfrak{a}, \mathbb{Z})$ of $\mathfrak{a}$ (via the trace pairing). We now observe that $\mathrm{Tr}(\beta_i, -)$ are a $\mathbb{Z}$-basis for H. Thus indeed the $\{\beta_i\}$ are a $\mathbb{Z}$-basis of $\mathfrak{a}^{-1}\mathscr{D}^{-1}$.

$$\begin{aligned}\sum_{j=1}^{n} \sigma_j(\beta_k) z_j &= \sum_j \sigma_j(\beta_k) \sum_q \sigma_i(\alpha_q) u_k \\ &= \sum_q \mathrm{Tr}(\alpha_q \beta_k) u_q \\ &= \sum_q \delta_{qk} u_q \\ &= u_q.\end{aligned}$$

Next, observe that for any $\mathbf{m} \in \mathbb{Z}^n$,

$$\mathbf{m}^t \cdot \mathbf{u} = \sum_k m_k u_k = \sum_{j,k} \sigma_j(\beta_k) m_k z_j = \sum_j \sigma_j(\lambda) z_j,$$

where $\lambda = \sum_i m_i \beta_i \in \mathfrak{a}^{-1}\mathscr{D}^{-1}$. Note that as $\mathbf{m}$ ranges through all of $\mathbb{Z}^n$, λ ranges through all of $\mathfrak{a}^{-1}\mathscr{D}^{-1}$.

We now apply the Jacobian transformation in Lemma 6.24 to the integral

$$a_{\mathbf{m}} = \int_{-\infty}^{\infty} \exp\left(-\pi \sum t_p z_p^2 + 2\pi i \mathbf{m}^t \cdot \mathbf{u}\right) \, d\mathbf{u}$$

to deduce that

$$a_{\mathbf{m}} = \frac{1}{|d_K|^{1/2} N\mathfrak{a}} \int_{-\infty}^{\infty} \exp\left(-\pi \sum_j t_j z_j^2 + 2\pi i \boldsymbol{\sigma}(\lambda)^t \cdot \mathbf{z}\right) \, d\mathbf{z}. \tag{6}$$

The following is easily checked:

Lemma 6.25

$$\int_{-\infty}^{\infty} e^{-\pi t z^2 + 2\pi i \lambda z}\, dz = e^{-\pi\lambda^2/t} \int_{-\infty}^{\infty} e^{-\pi t\left(z - \frac{i\lambda}{t}\right)^2}\, dz = \frac{e^{-\pi\lambda^2/t}}{\sqrt{t}}.$$

Applying Lemma 6.25 to each variable z_j in (6), we obtain:

Theorem 6.26

$$\vartheta(\mathbf{t}, \mathbf{z}, \mathfrak{a}) = \frac{1}{\sqrt{t_1 \cdots t_n}|d_K|^{1/2} N\mathfrak{a}} \sum_{\lambda \in \mathfrak{a}^{-1}\mathscr{D}^{-1}} \exp\left(-\pi \sum_{j=1}^{n} \frac{(\lambda^{\sigma_j})^2}{t_j} + 2\pi i \mathbf{m}^t \cdot \mathbf{u}\right),$$

where $\lambda = \sum_{i=1}^{n} m_i \beta_i$.

Note. Here, and in the sequel, $\sqrt{t_1 \cdots t_n} = \sqrt{t_1}\sqrt{t_2} \cdots \sqrt{t_n}$. Originally, Theorem 6.26 is established only for real positive $\mathbf{t}$. However, the result extends to all $\mathbf{t} \in \mathbb{C}^n$ with $\Re(t_i) > 0$ $(i = 1, \ldots, n)$, and where we take the branch of the square root already chosen.

We now set $\mathbf{z} = 0$ and write $\vartheta(\mathbf{t}, \mathfrak{a}) := \vartheta(\mathbf{t}, \mathbf{0}, \mathfrak{a})$. These values are known in the literature as the ϑ-Nullwerte.

Theorem 6.26 yields the so-called ϑ-transformation formula.

Theorem 6.27 Replacing $\mathfrak{a}$ by $\mathfrak{f}$ and writing $\frac{1}{\mathbf{t}} = \left(\frac{1}{t_1}, \ldots, \frac{1}{t_n}\right)$,

$$\vartheta(\mathbf{t}, \mathfrak{f}) = \frac{1}{\sqrt{t_1 \cdots t_n}|d_K|^{1/2} N\mathfrak{f}} \vartheta\left(\frac{1}{\mathbf{t}}, \mathfrak{f}^{-1}\mathscr{D}^{-1}\right).$$

Corollary 6.28 (Poisson summation formula) Set $\mathbf{t} = \mathbf{1}$. Then

$$\sum_{\alpha \in \mathfrak{f}} e^{-\pi Q(\alpha)} = \frac{1}{|d_K|^{1/2} N\mathfrak{f}} \sum_{\beta \in \mathfrak{f}^{-1}\mathscr{D}^{-1}} e^{-\pi Q(\beta)}.$$

(See e.g. Serre, *A Course in Arithmetic*, Chapter 7, §6, Proposition 15.)

Lemma 6.29 For each i ($i = 1, \ldots, n$), let $t_i \to 0$ in such a way that $\Re(t_i^{-1}) \to +\infty$. Then

$$\lim_{\mathbf{t}\to 0} \sqrt{t_1 \cdots t_n}\vartheta(\mathbf{t}, \mathbf{z}, \mathfrak{a}) = \frac{1}{|d_K|^{1/2} N\mathfrak{a}}.$$

(Observe that the right-hand side is independent of z.)

Proof. Let $r = \min(\Re(t_i^{-1}))$. Then

$$\left| \exp\left(-\pi \sum_j \frac{(\lambda^2)^{\sigma_j}}{t_j} \right) \right| \leq \exp\left(-\pi r \sum (\lambda^2)^{\sigma_j} \right).$$

Observe that the modulus of the left-hand side is the same as the modulus of

$$\exp\left(-\pi \sum_j \frac{(\lambda^2)^{\sigma_j}}{t_j} + 2\pi i \boldsymbol{\sigma}(\lambda)^t \cdot \mathbf{z} \right).$$

Recall that $\lambda = \sum m_i \beta_i$ (with previous notation), $\mathbf{m} \in \mathbb{Z}^n$. Thus $\sum_j (\lambda^2)^{\sigma_j}$ is a positive definite quadratic form in the variables m_i. Thus Lemma 6.20 implies that there exists $c > 0$ such that $\sum_j (\lambda^2)^{\sigma_j} \geq c\|\mathbf{m}\|^2$. Thus by Theorem 6.26,

$$\begin{aligned} \left| \vartheta(\mathbf{t}, \mathbf{z}, \mathfrak{a}) \sqrt{t_1, \cdots t_n} |d_K|^{1/2} N\mathfrak{a} - 1 \right| &\leq -1 + \sum_{\mathbf{m}} e^{-\pi r c \|\mathbf{m}\|^2} \\ &= \left(\sum_{m=-\infty}^{\infty} e^{-\pi r c m^2} \right)^n - 1 \\ &\leq \left(1 + \frac{2ce^{-\pi rc}}{1 - e^{-\pi rc}} \right) - 1, \end{aligned}$$

which approaches 0 as $r \to \infty$.

We next wish to relate the Gauß sum to the ϑ functions: Let $\omega = b/ad$, $(a, d) = 1$, $\mathfrak{f} = \mathfrak{o}_K$. Fix $\mathbf{x} = (x, x, \ldots, x)$ for some $x > 0$. Then set $t_j = x - 2i\sigma_j(\omega)$. From the definitions (see Definition 6.23), we obtain

$$\vartheta(\mathbf{x} - 2i\boldsymbol{\sigma}(\omega), \mathfrak{o}_K) = \sum_{\mu \in \mathfrak{o}_K} \exp\left(-\pi \sum (x - 2i\sigma_j(\omega)) \times \sigma_j(\mu^2) \right).$$

Write $(a) = \mathfrak{a}$, $(b) = \mathfrak{b}$, etc. Let $\{\rho\}$ denote a set of representatives of $\mathfrak{o}_K \pmod{\mathfrak{a}}$. Then write $\mu = \rho + \nu$ with $\nu \in \mathfrak{a}$. We have

$$\begin{aligned}\vartheta(\mathbf{x} - 2i\boldsymbol{\sigma}(\omega), \mathfrak{o}_K) &= \sum_{\substack{\rho \text{ rep} \\ \nu \in \mathfrak{a}}} \exp(-\pi(x - 2i\sigma_j(\omega))\sigma_j(\nu+\rho)^2) \\ &= \sum_{\rho,\nu} \exp((-\pi \mathbf{x}^t \cdot \boldsymbol{\sigma}(-\nu+\rho)^2) + 2\pi i \operatorname{Tr}(\omega(\nu+\rho)^2)).\end{aligned}$$

Note that $\operatorname{Tr}(\omega(\nu^2 + 2\rho\nu)) \in \mathbb{Z}$, and so

$$\vartheta(\mathbf{x} - 2i\boldsymbol{\sigma}(\omega), \mathfrak{o}_K) = \sum_{\rho} \exp(2\pi i \operatorname{Tr}(\omega\rho^2)) \sum_{\nu \in \mathfrak{a}} \exp(-\pi \mathbf{x}^t \cdot \boldsymbol{\sigma}(\nu+\rho)^2).$$

Now apply Lemma 6.29 by multiplying both sides by $x^{n/2}$ and letting $x \to 0$. This yields

$$\lim_{x \to 0} x^{n/2} \vartheta(x - 2i\omega, \mathfrak{o}_K) = \frac{1}{|d_K|^{1/2} N\mathfrak{a}} \sum_{\rho} \exp(2\pi i \operatorname{Tr}(\omega\rho^2)) = \frac{\tau_a(\omega)}{|d_K|^{1/2} N\mathfrak{a}}.$$

We now repeat the manipulation for $\vartheta(\mathbf{t}, \mathscr{D}^{-1})$. (Hopefully, we then get our reciprocity relationship on comparing and using the ϑ-transformation formula.)

Let $b_1 = 4b$ and $(b_1) = \mathfrak{b}_1$.

Note. $\frac{a}{4b} = \frac{1}{4\omega d}$ (where $\omega = b/ad$).

Let $\mu \in \mathfrak{o}_K$ and set $\mu = \rho + \nu$, where $\nu \in \mathfrak{b}_1$ and $\{\rho\}$ is a set of representatives of $\mathfrak{o}_K \pmod{\mathfrak{b}_1}$.

Recall. $t_j = x - 2i\sigma_j(\omega)$.

Note.

$$\frac{1}{t_j} = \frac{1}{x - 2i\sigma_j(\omega)} = \frac{i}{2\sigma_j(\omega)} + y_j, \tag{7}$$

where $y_j = \frac{-ix}{2\sigma_j(\omega)(x - 2i\sigma_j(\omega))}$. Note that $\Re\left(\frac{1}{y_j}\right) = \frac{4\sigma_j(\omega^2)}{x}$.

By definition,

$$\vartheta\left(\frac{1}{\mathbf{t}}, \mathscr{D}^{-1}\right) = \sum_{\mu \in \mathfrak{o}_K} \exp\left(-\pi \sum_j \left(y_j + \frac{i}{2\sigma_j(\omega)}\right) \times \sigma_j(\mu d^{-1})^2\right).$$

Set $\mu = \rho + \nu$. As previously, we get

$$\vartheta\left(\frac{1}{\mathbf{t}}, \mathscr{D}^{-1}\right) = \sum_{\rho} \exp\left(-2\pi i \operatorname{Tr}\left(\frac{\rho^2}{4d^2\omega}\right)\right) \times \vartheta(\mathbf{r}, \boldsymbol{\sigma}(\rho), \mathfrak{b}_1),$$

where $\mathbf{r} = (r_j)$ with $r_j = \frac{y_j}{\sigma_j(d^2)}$. Observe that

$$\sum_{\rho} \exp\left(-2\pi i \operatorname{Tr}\left(\frac{\rho^2}{4d^2\omega}\right)\right) = \tau_{b_1}\left(\frac{-1}{4d^2\omega}\right).$$

Write $\tau_2 := \tau_{b_1}\left(\frac{-1}{4d^2\omega}\right)$. Applying Lemma 6.28 again yields

$$\lim_{\mathbf{r}\to 0} \sqrt{r_1 \cdots r_n}\vartheta\left(\frac{1}{\mathbf{t}}, \mathscr{D}^{-1}\right) = \frac{1}{|d_K|^{1/2} N\mathfrak{b}_1} \cdot \tau_{b_1}\left(\frac{-1}{4d^2\omega}\right). \tag{8}$$

Note that $Nd = |d_K|$ and that $\sqrt{r_1 \cdots r_n} = \frac{1}{|d_K|}\sqrt{y_1 \cdots y_n}$.

Lemma 6.30

$$\lim_{x\to 0^+} \frac{1}{x^{n/2}} \frac{\sqrt{y_1 \cdots y_n}}{(Nd)^2} = \frac{1}{N(2\omega d)}$$

(where $\omega = b/ad$).

Proof. Recall that $y_j = \frac{-ix}{2\sigma_j(\omega)(x - 2i\sigma_j(\omega))}$. Suppose that x is small, i.e. $x \sim 0$. Then

$$\frac{y_j}{x} \sim \frac{-i}{2\sigma_j(\omega)^2 \cdot 2i} \sim \frac{1}{4\sigma_j(\omega^2)} = \frac{1}{(N(2\omega))^2},$$

and now the result follows.

Then applying the definition of r_j and Lemma 6.30 to (8) yields

$$\lim_{x\to 0} x^{n/2}\vartheta(\mathbf{t}^{-1}, \mathscr{D}^{-1}) = \frac{\tau_2}{N\mathfrak{b}_1 |d_K|^{1/2}} |N(2\omega d)|. \tag{9}$$

By Theorem 6.27, we know that

$$\lim_{x\to 0} x^{n/2}\vartheta(\mathbf{t},\mathfrak{o}_K) = \frac{1}{|d_K|^{1/2}} \lim_{x\to 0} \frac{1}{\sqrt{t_1\cdots t_n}} \lim_{x\to 0} x^{n/2}\vartheta(\mathbf{t},\mathscr{D}^{-1})$$

(where $t_j = x - 2i\sigma_j(\omega)$).

Lemma 6.31

$$\lim_{x\to 0} \sqrt{\prod_j (x - 2i\sigma_j(\omega))} = |N(2\omega)|^{1/2} \times e^{-\frac{\pi i}{4}S(\omega)},$$

where $S(\omega) = \sum_j \operatorname{sgn}(\sigma_j(\omega))$.

Proof. Exercise.

So from (9) and Lemma 6.31, we obtain

$$\frac{\tau_a(\omega)}{|d_K|^{1/2}Na} = \frac{1}{|d_K|^{1/2}} \cdot \frac{e^{\frac{\pi i}{4}S(\omega)}}{|N(2\omega)|^{1/2}} \times \frac{\tau_2}{|N\mathfrak{b}_1|\ |d_K|^{1/2}} \cdot |N(2\omega d)|.$$

Here $\omega = b/ad$. Rewriting gives

$$\begin{aligned} RHS &= \frac{1}{|d_K|} e^{\frac{\pi i}{4}S(\omega)} \cdot \frac{\tau_2}{N(4b)} |N(2\omega)|^{1/2} \times |Nd| \\ &= e^{\frac{\pi i}{4}S(\omega)} \frac{\tau_2}{N(4b)} \left| N\left(\frac{2b}{ad}\right)\right|^{1/2} \\ &= e^{\frac{\pi i}{4}S(\omega)} \frac{\tau_2}{N(4)N(b)} \cdot \frac{|N(2)|^{1/2}|N(b)|^{1/2}}{|N(a)|^{1/2}|N(d)|^{1/2}}. \end{aligned}$$

So the original equation becomes

$$\frac{\tau_a(\omega)}{|d_K|^{1/2}N\mathfrak{a}} = e^{\frac{\pi i}{4}S(\omega)} \frac{|N(2)|^{1/2}}{N(4)} \cdot \frac{\tau_2}{|N(b)|^{1/2}|N(a)|^{1/2}} \times \frac{1}{|N(d)|^{1/2}},$$

i.e.

$$\frac{\tau_a(\omega)}{|Na|^{1/2}} = \frac{e^{\frac{\pi i}{4}S(\omega)}\tau_2}{(\sqrt{2})^n (N(4b))^{1/2}}$$

(where $\tau_2 := \tau_{b_1}\left(\frac{-1}{4d^2\omega}\right)$), and this is a reciprocity relation for Gauß sums (see Theorem 6.19).

Lemma 6.32 The Gauß sums τ_4 and τ_a (for a an odd algebraic integer) are both nonzero.

Proof. Consider $\tau_{4a}\left(\frac{1}{4ad}\right)$. By the remarks preceding Lemma 6.17, τ_{4a} is a product of τ_4 and τ_a. Hence it is sufficient to prove that $\tau_{4a} \neq 0$. Replace a by $4a$ and b by 1 in the above reciprocity relation for Gauß sums:

$$\tau_{4a}\left(\frac{1}{4ad}\right) = \frac{e^{\frac{\pi i}{4}S(\omega)}(N(4a))^{1/2}}{(\sqrt{2})^n N(4b)^{1/2}} \times \tau_1\left(\frac{-a}{d}\right).$$

Now $\tau_1\left(\frac{-a}{d}\right) = 1$, and so the right-hand side is nonzero. The result follows.

Proof of generalized quadratic reciprocity. Let α and β be two odd, coprime integers of $\mathfrak{o}_K$, and suppose that α is 2-primary (α is congruent to a square $\pmod{4\mathfrak{o}_K}$). Then

$$\tau_{\alpha\beta}(\omega) = \tau_\beta(\alpha^2\omega)\tau_\alpha(\beta^2\omega) = \tau_\beta\left(\frac{\alpha}{\beta d}\right)\tau_\alpha\left(\frac{\beta}{\alpha d}\right).$$

Applying Theorem 6.18 yields

$$\tau_{\alpha\beta}(\omega) = \left(\frac{\beta}{\alpha}\right)\left(\frac{\alpha}{\beta}\right)\tau_\beta\left(\frac{1}{\beta d}\right)\tau_\alpha\left(\frac{1}{\alpha d}\right).$$

Applying reciprocity to each of the three Gauß sums yields

$$\frac{e^{\frac{\pi i}{4}S(\omega)}\tau_4\left(\frac{-\alpha\beta}{4d}\right)|N(\alpha\beta)|^{1/2}}{(\sqrt{2})^n(N(4))^{1/2}} = \left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)\frac{e^{\frac{\pi i}{4}S(\beta d)}\tau_4\left(\frac{-\beta}{4d}\right)|N(\beta)|^{1/2}}{(\sqrt{2})^n(N(4))^{1/2}} \times \frac{e^{\frac{\pi i}{4}S(\alpha d)}\tau_4\left(\frac{-\alpha}{d}\right)|N(\alpha)|^{1/2}}{(\sqrt{2})^n(N(4))^{1/2}}.$$

Hence

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right) = \frac{v(\alpha,\beta)|N(8)|^{1/2}\cdot\tau_4\left(\frac{-\alpha\beta}{4d}\right)}{\tau_4\left(\frac{-\alpha}{4d}\right)\tau_4\left(\frac{-\beta}{4d}\right)}, \tag{10}$$

where $v(\alpha,\beta) = \exp\left(\frac{\pi i}{4}(S(\alpha\beta d) - S(\alpha d) - S(\beta d))\right)$. Recall that α is congruent to a square $\pmod 4$ to deduce that

$$\tau_4\left(\frac{-\alpha\beta}{4d}\right) = \tau_4\left(\frac{-\beta}{4d}\right), \tag{11}$$

$$\tau_4\left(\frac{-\alpha}{4d}\right) = \tau_4\left(\frac{-1}{4d}\right). \tag{12}$$

Setting $\alpha = \beta = 1$ in (10) yields

$$1 = e^{-\frac{\pi i}{4}S(d)}\tau_4\left(\frac{-1}{4d}\right)^{-1}|N(8)|^{1/2}. \tag{13}$$

Substitute (11) and (12) into (10) and use (13) to deduce that

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right) = \exp\left(\frac{\pi i}{4}(S(\alpha\beta d) - S(-\alpha d) - S(-\beta d) + S(d))\right).$$

Write $\lambda := S(\alpha\beta d) - S(-\alpha d) - S(-\beta d) + S(d)$. Observe that for any $\alpha, \beta, d \in \mathbb{R}^\times$,

$$\begin{aligned}\operatorname{sgn}(\alpha\beta d) - \operatorname{sgn}(\alpha d) - \operatorname{sgn}(\beta d) + \operatorname{sgn}(d) &= (\operatorname{sgn}(\alpha) - 1)(\operatorname{sgn}(\beta) - 1)\operatorname{sgn}(d) \\ &\equiv (\operatorname{sgn}(\alpha) - 1)(\operatorname{sgn}(\beta) - 1) \pmod 8\end{aligned}$$

(just consider the different possibilities to see this). Recall that we defined $\varepsilon_i(\alpha) = \frac{\operatorname{sgn}(\sigma_i(\alpha))-1}{2}$. Hence

$$e^{\frac{\pi i\lambda}{4}} = (-1)^{\sum_{i=1}^n \varepsilon_i(\alpha)\varepsilon_i(\beta)}.$$

Thus

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right) = (-1)^{\sum_{i=1}^n \varepsilon_i(\alpha)\varepsilon_i(\beta)},$$

and this is generalized quadratic reciprocity.

Highly Recommended Exercise. Set $K = \mathbb{Q}$. Determine the signs of the Gauß sums $\tau_p\left(\frac{1}{p}\right)$. We have shown in the problems that

$$\tau_p\left(\frac{1}{p}\right) = \begin{cases}\pm\sqrt{p} & \text{if } p \equiv 1 \pmod 4, \\ \pm i\sqrt{p} & \text{if } p \equiv 3 \pmod 4.\end{cases}$$

Find the signs.

Chapter 7

Absolute Values and Completions

Definition 7.1 An **absolute value** on a field K is a function $|\cdot| : K \to \mathbb{R}$ which satisfies the following properties:

1. For all $x \in K$, $|x| \geq 0$, and $|x| = 0$ iff $x = 0$.
2. $|xy| = |x| \cdot |y|$.
3. $|x + y| \leq |x| + |y|$.

(We shall exclude the trivial absolute value given by $|x| = 1$ for all $x \neq 0$.)

The absolute value $|\cdot|$ endows K with the structure of a metric space. Two absolute value on K are said to be **equivalent** if they define the same topology.

Proposition 7.2 Two absolute values $|\cdot|_1$ and $|\cdot|_2$ are equivalent iff there exists $\lambda \in \mathbb{R}$, $\lambda > 0$, such that $|\cdot|_1 = |\cdot|_2^\lambda$.

Proof. $|\cdot|_2$ and $|\cdot|_2^\lambda$ are equivalent: exercise. For the reverse direction, first note that $|\cdot|_1$ is equivalent to $|\cdot|_2$ means that $|x|_1 < 1$ iff $|x|_2 < 1$ for all $x \in K$ (since $|x| < 1$ iff $x^n \to 0$ in the $|\cdot|$ topology, for any $|\cdot|$). Take a fixed $y \in K$ with $|y|_1 > 1$ (such a y certainly exists since $|\cdot|_1$ is nontrivial). We shall show that there exists $\lambda > 0$ such that $|z|_1 = |z|_2^\lambda$ whenever $|z|_1 > 1$. This is sufficient: if $0 < |x|_1 < 1$, then $|xy^n|_1 > 1$ for some positive integer n. Hence $|xy^n|_1 = |xy^n|_2^\lambda$, so $|x|_1 \cdot |y^n|_1 = |x|_2^\lambda \cdot |y^n|_2^\lambda$, and hence $|x|_1 = |x|_2^\lambda$. So suppose that $|z|_1 > 1$. Then $|z|_1 = |y|_1^\alpha$ for some $\alpha > 0$. Hence, if m and n are positive integers with $m/n > \alpha$, then $|z|_1 < |y|_1^{m/n}$, and so $|z^n/y^m|_1 < 1$.

So $|z^n/y^m|_2 < 1$ also, and $|z|_2 < |y|_2^{m/n}$. Similarly, if $m/n < \alpha$, then $|z|_1 > |y|_1^{m/n}$, and this implies that $|z|_2 > |y|_2^{m/n}$. It follows, therefore, that $|z|_2 = |y|_2^{\alpha}$. Hence we have

$$\frac{\log|z|_2}{\log|y|_2} = \alpha = \frac{\log|z|_1}{\log|y|_1}$$

and

$$\log|z|_1 = \left(\frac{\log|y|_1}{\log|y|_2}\right)\log|z|_2.$$

So $|z|_1 = |z|_2^{\lambda}$, with $\lambda = \frac{\log|y|_1}{\log|y|_2}$, and this holds for all z with $|z|_1 > 1$ since λ is independent of z.

Theorem 7.3 (Weak Approximation Theorem) Let $|\cdot|_1, \ldots, |\cdot|_s$ be pairwise inequivalent absolute values on a field K. Suppose that $x_1, \ldots, x_2 \in K$ and $\varepsilon > 0$. Then there exists $x \in K$ such that $|x - x_i|_i < \varepsilon$ for $i = 1, \ldots, s$.

Proof. Consider first the two absolute values $|\cdot|_1$ and $|\cdot|_2$. Since they are inequivalent, there exists $\alpha \in K$ with $|\alpha|_1 < 1$ and $|\alpha|_2 \geq 1$ and $\beta \in K$ with $|\beta|_1 \geq 1$ and $|\beta|_2 < 1$. Set $y = \beta/\alpha$. Then $|y|_1 > 1$ and $|y|_2 < 1$. We claim that we can find $y \in K$ such that $|y|_1 > 1$ and $|y|_i < 1$ for $i = 2, \ldots, s$. The claim follows via induction on s; we've done the case $s = 2$. So suppose $s \geq 3$. By our inductive hypothesis, there exists $b \in K$ with $|b|_1 > 1$, $|b|_i < 1$ for $i = 2, \ldots, s-1$. Also, since $|\cdot|_1$ and $|\cdot|_s$ are inequivalent, there exists $c \in K$ such that $|c|_1 > 1$, $|c|_2 < 1$. For sufficiently large r, define y by

$$y = \begin{cases} b & \text{if } |b|_s < 1 \\ cb^r & \text{if } |b|_s = 1 \\ \frac{cb^r}{1+b^r} & \text{if } |b|_s > 1. \end{cases}$$

This establishes the claim. Hence we can choose $a_j \in K$ such that $|a_j|_j > 1$ and $|a_j|_i < 1$ for $i \neq j$. Observe that for large r, $|a_j^r(1+a_j^r)^{-1}|_i$ is very small when $i \neq j$. Also $|a_j^r(1+a_j^r)^{-1} - 1|_j$ is very small. Set

$$x = \sum_{j=1}^{s}\left(\frac{a_j^r}{1+a_j^r}\right)x_j.$$

This satisfies the conditions of the theorem for sufficiently large r.

Remark. This is an analogue of the Chinese Remainder Theorem.

Definition 7.4 The absolute value $|\cdot|$ is called **archimedian** if $|n| > 1$ for some element n of the prime subring of K; otherwise $|\cdot|$ is **non-archimedian**.

Equivalent absolute values are simultaneously archimedian or non-archimedian.

Examples.

1. Suppose that v is a discrete valuation on a field K (see Definition 2.14), and choose $\varepsilon \in \mathbb{R}$ with $0 < \varepsilon < 1$. Then $|x|_v = \varepsilon^{v(x)}$ defines an absolute value. If K is the quotient field of a Dedekind domain and v is a $\mathfrak{p}$-adic valuation, then $|\cdot|_v$ is called a **$\mathfrak{p}$-adic absolute value**. (Different values of ε give equivalent absolutes values.)
2. On $\mathbb{C}$, the ordinary absolute value $|z| = (z\bar{z})^{1/2}$ is an archimedian absolute value.
3. Let K be an algebraic number field, and let $\sigma : K \hookrightarrow \mathbb{C}$ be an embedding. Then $|x|_\sigma = |\sigma(x)|$ defines an absolute value on K.

We define the p-adic absolute value on $\mathbb{Q}$ by $|x|_p = p^{-v_p(x)}$.

Theorem 7.5 (Ostrowski) Let $|\cdot|$ denote an absolute value on $\mathbb{Q}$. Then $|\cdot|$ is equivalent to exactly one of $|\cdot|_{\mathbb{R}}$ or $|\cdot|_p$ for some prime number p.

Proof. First we deal with p-adic valuations. Suppose that $|n| \leq 1$ for all $n \in \mathbb{Z}$. Then $|p| < 1$ for at least one prime p (since $|\cdot|$ is nontrivial). If also $|q| < 1$ for some other prime q, then we can find integers a and b with $|p^a| < 1/2$, $|q^b| < 1/2$, and integers λ and μ such that $\lambda p^a + \mu q^b = 1$. Then

$$1 = |1| = |\lambda p^a + \mu q^b| < \frac{|\lambda| + |\mu|}{2} \leq 1,$$

which is a contradiction. Hence if $|p| = |p|_p^\alpha$ (i.e. if $|p| < 1$), then $|x| = |x|_p^\alpha$ for all $x \in \mathbb{Q}$. Suppose therefore that there exists a positive integer n such that $|n| > 1$ with

$|n| = n^\alpha$, say. Since $|m| \leq m$ for all $m \in \mathbb{N}$ (via the triangle inequality), we have that $0 < \alpha \leq 1$. So suppose $m \in \mathbb{N}$, and write $m = \sum_{i=0}^{k} m_i n^i$, $0 \leq m_i < n$, $m_k \neq 0$. Then

$$|m| \leq \sum_{i=0}^{k} |m_i| n^{\alpha i} \leq \sum_{i=0}^{k} m_i n^{\alpha i} \leq \frac{(n-1)n^{\alpha(k+1)}}{n^\alpha - 1} \leq \frac{n-1}{n^\alpha - 1} \cdot m^\alpha,$$

i.e. $|m| \leq Cm^\alpha$ for all $m \in \mathbb{N}$, where C is independent of m. A similar argument, with m replaced by m^r, shows that $|m| \leq C^{1/r} m^\alpha$. Hence we deduce that

$$|m| \leq |m|_{\mathbb{R}}^\alpha \qquad \forall m \in \mathbb{Z}. \tag{$\dagger$}$$

Now set $m = n^{k+1} - b$, $0 \leq b \leq n^{k+1} - n^k$. Then $|b| < |b|^\alpha \leq (n^{k+1} - n^k)^\alpha$, and so

$$\begin{aligned} |m| &\geq |n^{k+1}| - |b| \\ &\geq n^{k+1\alpha} - (n^{k+1} n^k)^\alpha \\ &\geq n^{(k+1)\alpha} \left[1 - \left(1 - \frac{1}{n} \right)^\alpha \right] \\ &= C' n^{(k+1)\alpha} \\ &\geq C' m^\alpha, \end{aligned}$$

where C' is independent of m. Again, by replacing m by m^r, we have that $|m| \geq (C')^{1/r} m^\alpha$, and so we deduce that

$$|m| \geq |m|_{\mathbb{R}}^\alpha \qquad \forall m \in \mathbb{Z}. \tag{$\ddagger$}$$

It therefore follows from ($\dagger$) and ($\ddagger$) that $|m| = |m|_{\mathbb{R}}^\alpha$ for all $m \in \mathbb{Z}$.

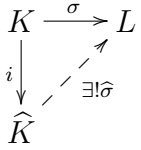
Very Easy Exercise. Show that $|\cdot|_{\mathbb{R}}$ and all the $|\cdot|_p$ are inequivalent.

7.1 Completions

$\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to the metric defined by the ordinary absolute value $|\cdot|_{\mathbb{R}}$. $\mathbb{Q}$ has other completions with respect to its other absolute values.

Theorem 7.6 Let K be a field with an absolute value $|\cdot|_1$. Then there is a field $\widehat{K}$ which is complete with respect to an absolute value $|\cdot|_1'$, and a continuous embedding $i : K \hookrightarrow \widehat{K}$ such that

1. $i(K)$ is dense in $\widehat{K}$.
2. For all $x \in K$, $|i(x)|_1' = |x|_1$.
3. If $(L, |\cdot|_2)$ is a complete field and if $\sigma : K \to L$ is a continuous embedding such that for all $x \in K$, $|x|_1 = |\sigma(x)|_2$, then there is a unique function $\widehat{\sigma} : \widehat{K} \to L$ such that $\sigma = \widehat{\sigma} \circ i$.



$(\widehat{K}, |\cdot|_1')$ is unique up to unique isomorphism, and it is referred to as the completion of K with respect to $|\cdot|_1$.

Sketch of Proof.

1. Let R be the set of $(|\cdot|_1)$-Cauchy sequences in K. Then R is a ring under the operations of pointwise addition and multiplication.
2. Let Z be the set of sequences in R which converge to zero. Then Z is the unique maximal ideal in R.
3. Thus R/Z is a field, $\widehat{K}$, say. Define an absolute value $|\cdot|_1'$ on $\widehat{K}$ by $|(a_n)|_1' = \lim_{n\to\infty} |a_n|_1$. This works.
4. Define $i : K \to \widehat{K}$ by letting $i(a)$ be the class of the constant sequence $a_n = a$. Then $|i(a)|_1' = |a|_1$.
5. $(\widehat{K}, |\cdot|_1')$ is complete, $i(K)$ is dense in $\widehat{K}$, and $(\widehat{K}, |\cdot|_1')$ satisfies the universal property (3).

[See *Local Fields* by J.-P. Serre.]

Examples 7.7

1. Let F be any field, and let $F[X]$ be the polynomial ring with coefficients in F. Fix a real number α with $0 < \alpha < 1$. Define $|\cdot| : F[X] \to \mathbb{R}$ by $\left|\sum_{i=0}^{k} a_i X^i\right| = \alpha^k$

(where $a_k \neq 0$). Extend $|\cdot|$ to $F(X)$ by $|f(X)/g(X)| = |f(X)|/|g(X)|$. Then $|\cdot|$ is an absolute value on $F(X)$. Also, $|\cdot|$ is a $\mathfrak{p}$-adic absolute value: $F[X]$ is a Dedekind domain, and $\mathfrak{p} = (X)$ is a prime ideal. The completion of $F(X)$ with respect to $|\cdot|$ is the field $F((X))$ of formal power series $\sum_{n=-\infty}^{\infty} a_n X^n$ ($a_n \in F$).

2. Let K be an extension of $\mathbb{R}$ which has an absolute value extending the ordinary one. Then $K = \mathbb{R}$ or $\mathbb{C}$. (Proof omitted.)

3. Let R be a Dedekind domain with quotient field K, and let $|\cdot| = |\cdot|_{\mathfrak{p}}$ for some prime ideal $\mathfrak{p}$. Then the completion $(\widehat{K}, |\cdot|'_{\mathfrak{p}})$ is called the **$\mathfrak{p}$-adic completion** of K. The ideals $\mathfrak{p}^n$ ($n \geq 0$) are a basis of open neighborhoods of zero in K.

Definition 7.8 Theorem 7.6 implies that $|\widehat{K}|'$ is the closure in $\mathbb{R}$ of $|K|$. An absolute value $|\cdot|$ on K is called **discrete** if $|K^\times|$ is a discrete subgroup of $\mathbb{R}^\times_{\geq 0}$.

In this case, there is a discrete valuation v on K which is related to $|\cdot|$ by the formula $|x| = \varepsilon^{v(x)}$ for some $0 < \varepsilon < 1$. (See page 63 of Fröhlich and Taylor.)

If $|\cdot|$ is discrete, then $|\widehat{K}|' = |K|$ since $|K|$ is already closed. Hence $|\cdot|'$ is also discrete.

Proposition 7.9 Let R be a discrete valuation ring, K its quotient field, π a prime element of R, and $|\cdot|$ the π-adic absolute value on K. Let $\widehat{R}$ be the closure of R in the completion $(\widehat{K}, |\cdot|')$. Then $\widehat{R}$ is a discrete valuation ring with quotient field $\widehat{K}$, π is a prime element in $\widehat{R}$, and $\widehat{R}/\pi\widehat{R} \simeq R/\pi R$.

Proof. Set $\alpha = |\pi|$. Then $|K^\times| = \widehat{K}^\times| = \langle\alpha\rangle \leq \mathbb{R}^\times_{>0}$. We claim that $\widehat{R} = \{x \in \widehat{K} : |x|' \leq 1\}$. To see this, note that if $x \in \widehat{R}$, then $x = \lim_{n\to\infty} x_n$, where $x_n \in R$. Hence $|x|' \leq 1$ since $|x_n|' \leq 1$ for all n. Conversely, suppose that $|x|' \leq 1$. Then $x = \lim_{n\to\infty} x_n$, where $x_n \in K$. Since $|\cdot|$ is discrete, we have $|x|' = |x_n|$ for all sufficiently large n, i.e. $x \in \widehat{R}$. Let $\mathfrak{a}$ be an ideal in $\widehat{R}$, and let $a \in \mathfrak{a}$ be such that $|a|' = \max\{|x|' : x \in \mathfrak{a}\}$. (This maximum is attained since $|\mathfrak{a}|'$ is discrete and bounded above by 1.) Suppose $|a|' = \alpha^n$. If $x \in \mathfrak{a}$, then $|x\pi^{-n}|' \leq 1$ ($\alpha = |\pi|$), and so $x\pi^{-n} \in \widehat{R}$, i.e. $x \in \pi^n\widehat{R}$. Now $|\pi^n a^{-1}|' = 1$, so $\pi^n a^{-1} \in \widehat{R}$, so $\pi = a(\pi^n a^{-1}) \in a\widehat{R} \subseteq \mathfrak{a}$. Hence we deduce that $\mathfrak{a} = \pi^n\widehat{R}$. It follows therefore that $\widehat{R}$ is a discrete valuation

ring with unique nonzero prime ideal $\pi\widehat{R}$ (cf Chapter 2). If $x \in \widehat{K}$, then $|\pi^n x|' \leq 1$ for sufficiently large n, and so x is a quotient of elements in $\widehat{R}$. We leave it as an exercise to show that $R/\pi R \simeq \widehat{R}/\pi\widehat{R}$.

Proposition 7.10 Let R be a complete discrete valuation ring with prime ideal πR and fraction field K. Let S be a system of representatives of $R/\pi R$ in R. Then each $r \in R$ can be written uniquely in the form $r = \sum_{n=0}^{\infty} s_n \pi^n$ $(s_n \in S)$, and each $x \in K$ can be written uniquely in the form $x = \sum_{n=-\infty}^{\infty} s_n \pi^n$ $(s_n \in S)$.

Proof. If $x \in K$, then there exists an $n \in \mathbb{N}$ such that $\pi^n x \in R$; hence the second assertion follows from the first. There exists a unique $s_0 \in S$ such that $r \equiv s_0 \pmod{\pi K}$. Hence $r = s_0 + a_1\pi$, for some $a_1 \in R$. Similarly, there exists a unique $s_1 \in S$ such that $a_1 = s_1 + a_2\pi$, and so $r = s_0 + s_1\pi + a_2\pi^2$. Continuing in this way produces an infinite series converging to r. Conversely, any series of the form $\sum_{n=0}^{\infty} s_n\pi^n$ converges to an element of R such $\left|\sum_{n=0}^{N} s_n\pi^n\right| \leq 1$ for each $N \in \mathbb{N}$.

In the case of residue characteristic p, it is easy to do more.

Proposition 7.11 Let K be a field complete with respect to a discrete valuation. Let R be the valuation ring, and let k be the residue field. Assume that k is perfect of characteristic $p > 0$. Then there is a unique system of representatives S of k in R with the property that $S^p = S$, and this system is multiplicatively closed.

Proof. Let $\mathfrak{p}$ be the maximal ideal in R. View elements of k as cosets of $\mathfrak{p}$ in R. Suppose $\alpha \in k$. Then $\alpha^{p^{-n}} \in k$ for each $n \in \mathbb{N}$, since k is perfect. Let $a_n \in R$ be any representative of $\alpha^{p^{-n}}$. Then $a_n^{p^n} \in \alpha$ for each $n \in \mathbb{N}$.

We claim that the sequence $(a_n^{p^n})$ converges in R. For a_{n+1}^p and a_n both represent $\alpha^{p^{-n}}$, and so $a_{n+1}^p \equiv a_n \pmod{\mathfrak{p}}$. Hence $a_{n+1}^{p^{n+1}} \equiv a_n^{p^n} \pmod{\mathfrak{p}^{n+1}}$. Thus $(a_n^{p^n})$ is a Cauchy sequence and so converges to a limit a, say. Since $a \equiv a_0 \pmod{\mathfrak{p}}$, it follows that $a \in \alpha$.

We must now show that the element a is independent of the choices of $a_n \in \alpha^{p^{-n}}$. If (a'_n) is another such sequence, then $a_n \equiv a'_n \pmod{\mathfrak{p}}$, and so $(a'_n)^{p^n} \equiv a_n^{p^n} \pmod{\mathfrak{p}^n}$. Hence

$$a' = \lim_{n\to\infty} (a'_n)^{p^n} = \lim_{n\to\infty} a_n^{p^n} = a.$$

Let S be the system of representatives obtained by this procedure. We first show that S is closed under multiplication. If $a = \lim_{n\to\infty} a_n^{p^n}$ and $b = \lim_{n\to\infty} b_n^{p^n}$, then $ab = \lim_{n\to\infty}(a_n b_n)^{p^n}$. Also, α^p is represented by a^p. Since $k^p = k$, it follows that $a^p = a$, and so $S^p = S$. We must now show that S is unique. Suppose that S_1 is another system of representatives of k such that $S_1^p = S$. Let $a_0 \in S_1$ represent $\alpha \in k$, and let $a_n \in S_1$ represent $\alpha^{p^{-n}}$. Since $S_1^p = S_1$, we have that $a_n^{p^n} = a_0$ for all $n \in \mathbb{N}$. So $a_0 = \lim_{n\to\infty} a_n^{p^n}$, which implies that $a_0 \in S$, and so $S_1 = S$.

Corollary 7.12 Suppose also that $\mathrm{char}(K) = p$. Then S is a subfield of K which is isomorphic to k.

Proof. Since $(a_n + b_n)^{p^n} = a_n^{p^n} + b_n^{p^n}$, it follows that S is closed under addition.

Remarks.

1. If $\mathrm{char}(K) = p$, Corollary 7.12 implies that $K \simeq k((\pi))$.
2. S is often referred to as a system of Teichmüller representatives (cf. the theory of Witt vectors in e.g. Serre's *Local Fields*).

Example 7.13 Let $\mathbb{Q}_p$ denote the completion of $\mathbb{Q}$ with respect to the p-adic absolute value given by $|x| = p^{-v_p(x)}$. $\mathbb{Q}_p$ is called the field of p-adic numbers. The closure $\mathbb{Z}_p$ of $\mathbb{Z}$ is $\mathbb{Q}_p$ is called the ring of p-adic integers.

1. Every p-adic integer has a unique representation of the form $a = \sum_{n=0}^{\infty} a_n p^n$, $0 \le a_n \le p-1$.
2. Multiplicative system of representatives: The residue field of $\mathbb{Q}_p$ is $\mathbb{F}_p$. Suppose $\zeta \in S$ represents $\alpha \in \mathbb{F}_p$, α a primitive $(p-1)^{\text{th}}$ root of unity. Then $\zeta^p = \zeta$, and so $\mu_{p-1} \subseteq \mathbb{Z}_p$. $\mu_{p-1} \cup \{0\}$ is the multiplicative system of representatives.

3. $\mathbb{Q}_p^\times = \langle p \rangle \times \mathbb{Z}_p^\times = \langle p \rangle \times \langle \zeta \rangle \times (1+p\mathbb{Z}_p)$. This has a filtration. Let $U_n = 1+p^n\mathbb{Z}_p$. Then $U_1 \supseteq U_2 \supseteq \cdots$, and $\bigcap_n U_n = 1$. We claim that $\langle 1+p \rangle$ is dense in U_1. First observe that $1+p^n \equiv (1+p)^{n+1} \pmod{p^{n+1}}$ (an easy proof by induction), and so
$$1 + bp^n \equiv (1+p)^{bp^{n-1}} \pmod{p^{n+1}}. \qquad (*)$$
Now suppose $a \in \mathbb{Z}_p$ with $a \equiv 1 \pmod{p}$, and suppose inductively that $a \equiv (1+p)^x \pmod{p^{n-1}}$ $(x \in \mathbb{Z})$. Then $a(1+p)^{-x} \equiv 1 \pmod{p^{n-1}}$, i.e.
$$a(1+p)^{-x} \equiv 1 + bp^{n-1} \pmod{p^n} \equiv (1+p)^{bp^{n-2}} \pmod{p^n}$$
(from $(*)$). Hence $a \equiv (1+p)^{x+bp^{n-2}} \pmod{p^n}$. So, given any positive integer n, there exists $y \in \mathbb{Z}$ such that $a \equiv (1+p)^y \pmod{p^n}$, i.e. $\langle 1+p \rangle$ is dense in U_1.

Terminology. We say that $1+p$ is a **topological generator** of U_1 and that U_1 is **topologically cyclic** (cf *p-Adic Numbers, p-Adic Analysis, and Zeta Functions* by N. Koblitz). See "An Introduction to the Theory of p-Adic Representations" by Laurent Berger (available at `http://www.ihes.fr/~lberger/dwork/dworksmf.pdf`).

7.2 Extensions of Absolute Values

First we need a preliminary result.

Lemma 7.14 Let K be a field which is complete with respect to an absolute value $|\cdot|_1$, and let V be a finite dimensional vector space over K. Then all norms on V are equivalent. (Two norms $\|\cdot\|_1$ and $\|\cdot\|_2$ are equivalent if there exist positive constants C_1 and C_2 such that $\|\cdot\|_1 \leq C_1\|\cdot\|_2$ and $\|\cdot\|_2 \leq C_2\|\cdot\|_1$.)

Proof. Let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis of V over K, and let $\|\cdot\|$ be the sup norm with respect to this basis. Let $|\cdot|$ be any other norm. Suppose $x = x_1\alpha_1 + \cdots + x_n\alpha_n \in V$. Then
$$|x| = |x_1\alpha_1 + \cdots + x_n\alpha_n| \leq (n \cdot \sup|\alpha_i|) \cdot \|x\| = C\|x\|,$$
say. Hence the norm $|\cdot|$ is continuous with respect to $\|\cdot\|$. The unit sphere with respect to $\|\cdot\|$ is compact, and so $|\cdot|$ has a minimum on this unit sphere, at v, say.

So $|v| \leq |x|$ for all $x \in V$ such that $\|x\| = 1$. Now suppose that $y \in V$, $y \neq 0$, and write $y = y_1\alpha_1 + \cdots + y_n\alpha_n$, $y_i \in K$. Let j be such that $|y_j|_1 = \max_i |y_i|_1 = \|y\|$. Then we may write $y = y_j x$ with $\|x\| = 1$. We have

$$|v| \leq |x| = \left|\frac{y}{y_j}\right| = \frac{|y|}{|y_j|_1} = \frac{|y|}{\|y\|}.$$

So $|v| \cdot \|y\| \leq |y|$. The result follows.

Remark. It follows that V is complete with respect to the sup norm and so is complete with respect to any norm. In particular, we may take V to be a finite extension of K.

Proposition 7.15 Let K be a field which is complete with respect to an absolute value $|\cdot|$, and let E/K be a finite extension. Then any extension of $|\cdot|$ to E is uniquely determined. In particular, if $\sigma : E \to \sigma E$ is an isomorphism of E over K, then $|\sigma\alpha| = |\alpha|$ for all $\alpha \in E$.

Proof. Lemma 7.14 implies that all extensions of $|\cdot|$ to E are equivalent. Since any two such are positive powers of each other, and since they coincide on K, it follows that they must be equal.

Now we apply this. The p-adic valuation on $\mathbb{Q}$ is given by $|p^r m/n|_p = 1/p^r$ for $r \in \mathbb{Z}$, $(mn, p) = 1$.

Recall. If $\mathfrak{o}$ is a discrete valuation ring with maximal ideal $\mathfrak{m}$ and quotient field K, then suppose that $\mathfrak{m}$ is generated by π. Every $\alpha \in K$ ($\alpha \neq 0$) can be written in the form $\alpha = \pi^r u$, $r \in \mathbb{Z}$, $u \in \mathfrak{o}^\times$. Define $|\alpha| = c^r$ (for some fixed $0 < c < 1$). This gives an absolute value on K.

Now suppose K is a number field with ring of integers $\mathfrak{o}_K$. Let $\mathfrak{p}$ be a prime ideal of $\mathfrak{o}_K$ with $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$. Let $\pi \in \mathfrak{o}_K$ have order 1 at $\mathfrak{p}$; then $p = \pi^e u$, $e > 0$, u a unit at p. Set $f = f_\mathfrak{p} = [(\mathfrak{o}_K/\mathfrak{p}) : (\mathbb{Z}/p\mathbb{Z})]$. Then $N\mathfrak{p} = |\mathfrak{o}_K/\mathfrak{p}| = p^f$. We have two absolute values on K determined by $\mathfrak{p}$:

1. $|p|_{\mathfrak{p}} = 1/p$, $|\pi|_{\mathfrak{p}} = 1/p^{1/e}$,
2. $\|\pi\|_{\mathfrak{p}} = 1/N\mathfrak{p}$.

For any $\alpha \in K$, $\alpha \neq 0$, we have $\|\alpha\|_{\mathfrak{p}} = |\alpha|_{\mathfrak{p}}^{e_{\mathfrak{p}} f_{\mathfrak{p}}}$. Of course, this can be generalized:

$$\begin{array}{ccc} L & \text{---} & \mathfrak{P} \\ | & & | \\ K & \text{---} & \mathfrak{p} \end{array}$$

Let $\Pi \in L$ be an element of order 1 at $\mathfrak{P}$. Then $\mathfrak{p}\mathfrak{o}_L = \mathfrak{P}^{e(\mathfrak{P}|\mathfrak{p})}$, and $|\pi|_{\mathfrak{P}} = |\Pi|_{\mathfrak{P}}^{e(\mathfrak{P}|\mathfrak{p})}$.

Definition 7.16 Let K be a number field. The set of absolute values consisting of the $\mathfrak{p}$-adic absolute values and of the absolute values induced by embedding K in $\mathbb{C}$ or $\mathbb{R}$ is called the **canonical set** of absolute values and is denoted by M_K. IF E/K is a finite extension, then any absolute value w on E extending an absolute value $v \in M_K$ lies in M_E, and we write $w \mid v$.

Any two distinct absolute values in M_K induce distinct topologies on K.

If $v \in M_K$, then we write K_v for the completion of K with respect to v. K_v is called a **local field**.

$$\begin{array}{ccccc} E & \text{---} & \mathfrak{o}_E & \supset & \mathfrak{P}_w \\ | & & & & | \\ K & \text{---} & \mathfrak{o}_K & \supset & \mathfrak{p}_v \end{array}$$

$$\begin{array}{ccccc} \mathfrak{o}_E & \longrightarrow & \mathfrak{o}_{E,w} & & E_w \\ \uparrow & & \uparrow & & \uparrow \\ \mathfrak{o}_K & \longrightarrow & \mathfrak{o}_{K_v} & & K_v \end{array}$$

$$\begin{array}{ccc} \mathfrak{o}_E/\mathfrak{P} & \xrightarrow{\sim} & \mathfrak{o}_{E,w}/\mathfrak{P}_w \\ \uparrow & & \uparrow \\ \mathfrak{o}_K/\mathfrak{p} & \xrightarrow{\sim} & \mathfrak{o}_{K,v}/\mathfrak{p}_v \end{array}$$

Remarks. Let K_w denote the closure of K in E_w. Then EK_w is a finite extension of K_w, and $EK_w \subseteq E_w$. Since EK_w is complete and dense in E_w, it follows that $EK_w = E_w$.

Theorem 7.17 Let E/K be a finite extension of number fields, and let $v \in M_K$. Then two K-embeddings $\sigma, \tau : E \to \bar{K}$ give rise to the same absolute value on E iff they are conjugate over K_v (i.e. iff there exists an isomorphism $\lambda : \sigma E \cdot K_v \to \tau E \cdot K_v$ such that $\lambda_{K_v} = id$).

Proof. Suppose that the two embeddings are conjugate over K_v. Then Proposition 7.15 implies that the induced absolute values on E are equal. Suppose conversely that the two absolute values are equal, and let $\lambda : \tau E \to \sigma E$ be a K-isomorphism. We show that λ extends to a K_v-isomorphism $\lambda : \tau E \cdot K_v \to \sigma E \cdot K_v$. Now suppose $x \in \tau E \cdot K_v$. Since τE is dense in $\tau E \cdot K_v$, we may write $x = \lim_{n\to\infty} \tau x_n$, where $x_n \in E$. Since the absolute values induced by σ and τ on E coincide, it follows that the sequence $\{\lambda\tau x_n\} = \{\sigma x_n\}$ converges to an element $\lambda x \in \sigma E \cdot K_v$. Then λx is independent of $\{x_n\}$, and the map $\lambda : \tau E \cdot K_v \to \sigma E \cdot K_v$, $x \mapsto \lambda x$, is an isomorphism.

Now we understand the extensions of v to E.

Corollary 7.18 Let K be a number field, and let E/K be a finite extension of degree n. Suppose $v \in M_K$. For each absolute value w on E extending v, and let n_w be the local degree, i.e. $n_w = [E_w : K_v]$. Then $\sum_{w|v} n_w = n$.

Proof. Let $E = K(\alpha)$, and let $f(X)$ be the minimal polynomial of α over K. Let $f(X) = f_1(X) \cdots f_s(X)$ be the factorization of f into irreducible polynomials over K_v. An embedding $E \to \bar{K}_v$ corresponds to a choice of root of f in $\bar{K}_v$, and two such embeddings are conjugate over K_v iff the chosen roots belong to the same factor $f_i(X)$.

Hence s is the number of distinct extensions of v to E, and $\sum_{w|v} n_w = [E : K] = n$.

Corollary 7.19 Define $\sigma : E \otimes_K K_v \to \prod_{w|v} E_w$ by $\sigma(\ell \otimes a) = (\ell a, \ell a, \ldots, \ell a)$. Then σ is an isomorphism.

Proof. The weak approximation theorem (Theorem 7.3) implies that the image of σ is dense in $\prod_{w|v} E_w$. Since the image is also closed, it follows that σ is surjective. Hence Corollary 7.18 implies that σ is an isomorphism.

Corollary 7.20 Let $v \in M_K$, and for each $w \mid v$, let $N_w : E_w \to K$ be the local norm and $\mathrm{Tr}_w : E_w \to K_v$ the local trace. Then, if $\alpha \in E$, $N_{E/K}(\alpha) = \prod_{w|v} N_w(\alpha)$ and $\mathrm{Tr}_{E/K}(\alpha) = \sum_{w|v} \mathrm{Tr}_w(\alpha)$.

Proof. Follows immediately from Corollary 7.19, together with the definitions of norm and trace.

Corollary 7.21 Notation as in Corollary 7.20. Then $\prod_{w|v} |\alpha|_w^{n_w} = |N_{E/K}(\alpha)|_v$.

Proof. Exercise.

Definition 7.22 Let K be a number field, and let E/K be a field extension of degree n. Suppose $v \in M_K$. Say that v **splits completely** in E if there exist precisely n extensions of v to E.

Remark. Theorem 7.17 implies that v splits completely in E iff every K-embedding $\sigma : E \to \bar{K}_v$ maps E into K_v, i.e. if $\sigma(E) \cdot K_v = K_v$.

Theorem 7.23 (Hensel's Lemma) Let K be a field which is complete with respect to an absolute value $|\cdot|$, and let $\mathfrak{o}_K$ denote the valuation ring of K. Let $f(X)$ be a polynomial with coefficients in $\mathfrak{o}_K$. Let $\alpha_0 \in \mathfrak{o}_K$ be such that $|f(\alpha_0)| < |f'(\alpha_0)|^2$.

Then the sequence $\alpha_{i+1} = \alpha_i - \frac{f(\alpha_i)}{f'(\alpha_i)}$ converges to a root α of $f(X)$ in $\mathfrak{o}_K$. Furthermore, $|\alpha - \alpha_0| \leq \left|\frac{f(\alpha_0)}{f'(\alpha_0)^2}\right| < 1$.

Proof. Set $c = |f(\alpha_0)/f'(\alpha_0)^2| < 1$. We show inductively that

(i) $|\alpha_i| \leq 1$.

(ii) $|\alpha_i - \alpha_0| \leq c$.

(iii) $\left|\frac{f(\alpha_i)}{f'(\alpha_i)^2}\right| \leq c^{2^i}$.

These conditions imply our proposition. If $i = 0$, the conditions are our hypotheses. By induction, assume the conditions for i.

(i)' $\left|\frac{f(\alpha_i)}{f'(\alpha_i)^2}\right| \leq c^{2^i}$ implies that $|\alpha_{i+1} - \alpha_i| \leq c^{2^i} < 1$ and so $|\alpha_{i+1}| \leq 1$.

(ii)' $|\alpha_{i+1} - \alpha_0| \leq \max\{|\alpha_{i+1} - \alpha_i|, |\alpha_i - \alpha_0|\} = c$.

(iii)' Taylor's Theorem implies that we have

$$f(\alpha_{i+1}) = f(\alpha_i) - f'(\alpha_i)\frac{f(\alpha_i)}{f'(\alpha_i)} + \beta\left(\frac{f(\alpha_i)}{f'(\alpha_i)}\right)^2,$$

$\beta \in \mathfrak{o}_K$, and so $|f(\alpha_{i+1})| \leq \left|\frac{f(\alpha_i)}{f'(\alpha_i)}\right|^2$. Also, we have, for some $\gamma \in \mathfrak{o}_K$,

$$f'(\alpha_{i+1}) = f'(\alpha_i) - \frac{f(\alpha_i)}{f'(\alpha_i)} \cdot \gamma = f'(\alpha_i)\left(1 - \frac{f(\alpha_i)}{f'(\alpha_i)^2}\gamma\right),$$

and so $|f'(\alpha_{i+1})| = |f'(\alpha_i)|$. Putting everything together gives

$$|f(\alpha_{i+1})| \leq \left|\frac{f(\alpha_i)}{f'(\alpha_i)}\right|^2 \leq |f(\alpha_i)|c^{2^i}.$$

Hence

$$\left|\frac{f(\alpha_{i+1})}{f'(\alpha_{i+1})^2}\right| \leq \left|\frac{f(\alpha_i)}{f'(\alpha_i)^2}\right| \cdot c^{2^i} \leq c^{2^{i+1}}.$$

Examples.

1. In $\mathbb{Q}_2$, the equation $x^2 + 7 = 0$ has a root. (In fact, for any $\gamma \in \mathbb{Z}_2$ with $\gamma \equiv 1 \pmod 8$, the equation $x^2 = \gamma$ has a root.) Take $\alpha_0 = 1$ in Theorem 7.23.

2. In Theorem 7.23, let $\mathfrak{p}$ denote the maximal ideal of $\mathfrak{o}_K$, and suppose that $f(\alpha_0) \equiv 0 \pmod{\mathfrak{p}}$ but $f'(\alpha_0) \not\equiv 0 \pmod{\mathfrak{p}}$. Then the theorem applies. (This is the **trivial** case of Hensel's Lemma.)

3. Every unit of $\mathfrak{o}_K$ sufficiently close to 1 has an m^{th} root if m is not divisible by the characteristic of K. ($X^n - u = 0$, $\alpha_0 = 1$ provided that $|u - 1| < |m|^2$.)

The following result is useful in determining extensions of K.

Proposition 7.24 (Krasner's Lemma) Let $\alpha, \beta \in \bar{K}$, and assume that α is separable over $K(\beta)$. Assume that for all K-isomorphism σ of $K(\alpha)$ (with $\sigma \neq id$) we have $|\beta - \alpha| < |\sigma\alpha - \alpha|$. Then $K(\alpha) \subseteq K(\beta)$.

Proof. It suffices to show that any $K(\beta)$ isomorphism τ of $K(\alpha, \beta)$ also fixes α. By Proposition 7.15, we have $|\beta - \alpha| = |\beta - \tau\alpha| < |\sigma\alpha - \alpha|$. Hence we obtain

$$|\tau\alpha - \alpha| = |\tau\alpha - \beta + \beta - \alpha| < |\sigma\alpha - \alpha|$$

for all $\sigma \neq id$. This implies that $\tau = id$, and hence $K(\alpha, \beta) = K(\beta)$.

7.3 Nonramified and Tamely Ramified Extensions

Let K be a field which is complete with respect to a discrete absolute value $|\cdot|$ associated to a valuation v_K, $\mathfrak{o}_K$ its valuation ring, and $\mathfrak{p}$ its maximal ideal. Assume $k := \mathfrak{o}_K/\mathfrak{p}$ is finite. $\pi \in \mathfrak{p}$ with $\pi\mathfrak{o}_K = \mathfrak{p}$ is a **uniformizing element**.

Suppose L/K is a finite extension.

$$\begin{array}{ccc} L & \text{——} & k_L \\ | & & | \\ K & \text{——} & k \end{array} \qquad \begin{array}{c} \mathfrak{P} \\ | \\ \mathfrak{p} \end{array}$$

We have $[L : K] = f(L/K)e(L/K)$. We say L/K is **totally ramified** if $[L : K] = e(L/K)$. Then $f(L/K) = 1$, i.e. $k_L = k$.

A monic polynomial $g(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_1X + a_0 \in \mathfrak{o}_K[X]$ is called an **Eisenstein polynomial** if $a_j \in \mathfrak{p}$ for all j and $a_0 \notin \mathfrak{p}^2$.

Theorem 7.25

(a) The following are equivalent:

  (i) $L = K(\lambda)$, where λ is a root of an Eisenstein polynomial $g(X)$.

  (ii) L/K is totally ramified.

  (iii) $\mathfrak{o}_L = \mathfrak{o}_K[\lambda]$ for a uniformizer λ of $\mathfrak{o}_L$.

(b) If (i) holds, then λ is a uniformizer of $\mathfrak{o}_L$, and $\deg(g(X)) = [L : K]$, so $g(X)$ is irreducible over K.

(c) The minimal polynomial over K of a uniformizing parameter of a totally ramified separable extension L of K is an Eisenstein polynomial over K.

Proof. We first show (i) implies (ii) and (b). Let $g(X) = X^n + b_{n-1}X^{n-1} + \cdots + b_0$. Then $\lambda \in \mathfrak{o}_L$, and so $\lambda^n = -\sum_{j=0}^{n-1} b_j\lambda^j \in \mathfrak{p}\mathfrak{o}_L$. Hence $v_L(\lambda) \geq 1$. Now $v_L(\lambda^n + b_0) = v_L\left(-\sum_{j=1}^{n-1} b_j\lambda^j\right) \geq 1 + e(L/K)$, and $v_L(b_0) = e(L/K)$, and so we must have $v_L(\lambda^n) = e(L/K)$. Therefore $[L : K] \geq e(L/K) = nv_L(\lambda) \geq n = [L : K]$. Hence all these inequalities are in fact equalities, and we have $e(L/K) = [L : K]$, so L/K is totally ramified. Since $n = [L : K]$, $g(X)$ is irreducible. Since $nv_L(\lambda) = n$, $v_L(\lambda) = 1$, i.e. λ is a uniformizer.

Now we show that (ii) implies (iii). Suppose L/K is totally ramified. Then $k_L = k$, i.e. $\mathfrak{o}/\mathfrak{P} \simeq \mathfrak{o}_K/\mathfrak{p}$. Let $S \subseteq \mathfrak{o}_K$ be a set of representatives of $\mathfrak{o}_L/\mathfrak{P}$. Suppose that λ is a uniformizer of L. For $h = i + e_j$ ($e = e(L/K)$, $0 \leq i < e$), set $\lambda_h = \lambda^i\pi^j$ (π a uniformizer of K). Then every element of $\mathfrak{o}_L$ may be written uniquely in the form $\sum_{h=0}^{\infty} s_h\lambda_h$ ($s_h \in S$) (cf the proof of Proposition 7.2). Collecting and rearranging terms, it follows that every element of $\mathfrak{o}_L$ may be written in the form $\sum_{i=0}^{e-1} a_i\lambda^i \in \mathfrak{o}_K[\lambda]$. Since $\mathfrak{o}_K[\lambda] \subseteq \mathfrak{o}_L$, we deduce that $\mathfrak{o}_K[\lambda] = \mathfrak{o}_L$.

Now we show that (iii) implies (ii). Suppose that $\mathfrak{o}_L = \mathfrak{o}_K[\lambda]$, λ a uniformizer of L. Reducing modulo $\mathfrak{P}$ gives $\mathfrak{o}_L/\mathfrak{P} \simeq \mathfrak{o}_K/\mathfrak{p}$, and so $f(L/K) = 1$, whence $e = e(L/K) = [L : K]$, i.e. L/K is totally ramified.

Finally we show that (ii) and (iii) imply (i) as well as (c). Assume (ii) and (iii). Then we may write $\lambda^e = \sum_{i=0}^{e-1} c_i \lambda^i$ with $c_i \in \mathfrak{o}_K$. Then $v_L(\lambda^e - c_0) \geq 1$, so $v_L(c_0) \geq 1$, so $v_K(c_0) \geq 1$, so $v_L(c_0) \geq e$. Similarly, $v_L(\lambda^e - c_0 c_1 \lambda) \geq 2$, so $v_K(c_1) \geq 1$. Continuing in this way, we have that $v_K(c_j) \geq 1$ for $j = 0, 1, \ldots, e-1$. Therefore $v_L(\lambda^e - c_0) \geq e+1$, and so we must have $v_L(c_0) = e$, i.e. $v_K(c_0) = 1$. Hence $g(X) = X^e - \sum_{j=0}^{e-1} c_i X^i$ is Eisenstein. Since the choice of λ in the proof of (ii) implies (iii) was arbitrary, (c) follows also.

Corollary 7.26 Let F denote an algebraic number field. Suppose that $g(X) \in \mathfrak{o}_F[X]$ is such that $g(X)$ is Eisenstein in $F_{\mathfrak{p}}[X]$ for some prime $\mathfrak{p}$ of $\mathfrak{o}_F$. Then $g(X)$ is irreducible in $F[X]$.

Proof. By Theorem 7.27, $g(X)$ is irreducible in $F_{\mathfrak{p}}[X]$. Hence $g(X)$ is irreducible in $F[X]$.

Example. Let p be a prime and $n \in \mathbb{N}$. Consider the cyclotomic polynomial in $\mathbb{Q}_p[X]$:

$$\Phi_{p^n}(X) = \frac{X^{p^n} - 1}{X^{p^{n-1}} - 1} = X^{p^{n-1}(p-1)} + X^{p^{n-1}(p-2)} + \cdots + X^{p^{n-1}} + 1.$$

The roots of $\Phi_{p^n}(X)$ are the primitive $(p^n)^{\text{th}}$ roots of unity in $\bar{\mathbb{Q}}_p$. Set $g(X) := \Phi_{p^n}(X+1)$; then $\bar{g}(X) \equiv X^{p^{n-1}(p-1)} \pmod{p}$. Since $g(0) = \Phi_{p^n}(1) = p$, it follows that $g(X)$ is Eisenstein. Set $K = \mathbb{Q}_p(\zeta)$, ζ a primitive $(p^n)^{\text{th}}$ root of unity. Then

(a) $K/\mathbb{Q}_p$ is totally ramified of degree $p^{n-1}(p-1)$.

1. $\mathfrak{o}_K = \mathbb{Z}_p[\zeta]$.
2. $1 - \zeta$ is a uniformizer of K.

7.4 Unramified Extensions

Let L/K be finite, separable, and algebraic.

Proposition 7.27

(i) Suppose L/K is unramified. Then there exists $x \in \mathfrak{o}_L$ such that $k_L = k(\bar{x})$. Suppose that x is such an element, and let $g(X)$ be its minimal polynomial over K. Then $\mathfrak{o}_L = \mathfrak{o}_K[x]$, $L = K(x)$, and $\bar{g}(X)$ is irreducible and separable over k.

(ii) Suppose that $g(X)$ is a monic polynomial in $\mathfrak{o}_K[X]$ such that $\bar{g}(X)$ is irreducible and separable over k. If x is a root of $g(X)$, then $L = K(x)$ is unramified over K, and $k_L = k(\bar{x})$.

Proof.

(i) If k_L/k is separable, then $k_L = k(\bar{x})$ for some $x \in \mathfrak{o}_L$. Let $G(X)$ be the minimal polynomial of $\bar{x}$ over k. Then $G(X)$ is separable, and we have

$$[L : K] \geq \deg g(X) \geq \deg G(X) = [k_L : k] = [L : K].$$

Hence $G(X) = \bar{g}(x)$, i.e. $\bar{g}(X)$ is irreducible and $L = K(x)$. We leave it as an exercise to show that $\mathfrak{o}_L = \mathfrak{o}_K[x]$ (cf the ideas involved in the proof of Theorem 4.10).

(ii) Observe that we have $[L : K] = \deg g(X) = [k(\bar{x}) : k] \leq [k_L : k] \leq [L : K]$. Hence

(a) $[L : K] = [k_L : k] = f(L/K)$, i.e. $e(L/K) = 1$,

(b) $k_L = k(\bar{x})$, i.e. k_L/k is separable.

Theorem 7.28 Let ℓ/k be a finite separable extension. Then there exists a finite separable extension $L = L(\ell)$ of K such that

(i) $\ell \simeq k_L$ (over k).

(ii) L/K is unramified.

(iii) The natural maps $\mathrm{Hom}_K(L, L') \to \mathrm{Hom}_k(k_L, k_{L'})$ are bijective for all L'.

Proof. We have $\ell = k(\tilde{\alpha})$. Let $G(X)$ be the minimal polynomial of $\tilde{\alpha}$ over k. Then $G(X)$ is separable. Choose any monic polynomial $g(X) \in \mathfrak{o}_K[X]$ with $\bar{g}(X) = G(X)$. Let $L = K(x)$. Then Proposition 7.27 implies that L satisfies (i) and (ii) (cf Proposition 7.27). Now consider any k-homomorphism $\alpha : k_L \to k_{L'}$. The trivial case of Hensel's Lemma implies that L' contains a *unique* element y such that $g(y) = 0$ and $\bar{y} = \alpha(\bar{x})$. Then there exists a unique homomorphism $\alpha_1 : L \to L'$ such that $\alpha_1(x) = y$, and clearly $\bar{\alpha}_1 = \alpha$. If $\bar{\beta} : k_L \to k_{L'}$ is such that $\bar{\beta}(\bar{x}) = \bar{y}$, then $\beta(x) = y$, so $\beta = \alpha_1$.

Corollary 7.29 $L(\ell)/K$ is normal iff ℓ/k is normal. If this is so, then $\mathrm{Gal}(L(\ell)/K) \simeq \mathrm{Gal}(\ell/k)$. (Of course, the point here is that we are not assuming that k is finite.)

Theorem 7.30 Let L/K be a finite extension. Then L has a subfield $L_0 \supset K$ such that the subfields $L' \supseteq K$ of L which are unramified over K are precisely the subfields of L_0. Also, $k_{L_0} = k_L^{\mathrm{sep}}$, the separable closure of k in k_L. If L/K is normal with Galois group Γ, then L_0/K is normal, and L_0 is the fixed field of $\Gamma_0 = \{\gamma \in \Gamma : v_L(\gamma(x) - x) > 0 \text{ for all } x \in \mathfrak{o}_L\}$. ($\Gamma_0$ is called the inertia group of L/K.)

Proof. Theorem 7.28 implies that there exists a subfield $L_0 \supset K$ of L with L_0/K unramified and $k_{L_0} = k_L^{\mathrm{sep}}$. All subfields of L_0 are unramified over K. Suppose conversely that L' is a subfield of L, with L'/K unramified. Setting $\ell = k_{L'}$ in Theorem 7.28, we obtain a K-homomorphism $\sigma : L' \to L_0$ so that $\bar{\sigma} : k_{L'} \hookrightarrow k_{L_0} = k_L^{\mathrm{sep}}$ is the inclusion map. Let $k_{L'} = k(\bar{x})$, with $x \in \mathfrak{o}_L$. Then x and $\sigma(x)$ are elements of L with the same residue class. Hence (by the trivial case of Hensel's Lemma) $\sigma(x) = x$, i.e. $x \in L_0$. Hence by Proposition 7.27, $L' = K(x)$, and so $L' \subseteq L_0$. Now suppose that L/K is normal. Then the conjugate fields of L_0 in L are all unramified over K. Hence they coincide with L_0, and so L_0/K is normal. Observe that, by definition, Γ_0 is the kernel of the homomorphism $\Gamma = \mathrm{Gal}(L/K) \to \mathrm{Gal}(k_{L_0}/k) \simeq \mathrm{Gal}(L_0/K)$ (from Theorem 7.28).

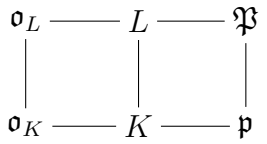
Corollary 7.31 The compositum of two unramified extensions of K in a separable closure of K is unramified.

Corollary 7.32 Let K_{unr} be the union of all unramified extensions L/K in a given separable closure of K. Then every finite extension of K in K_{unr} is unramified. We have that $\text{Gal}(K_{\text{unr}}/K) \simeq \text{Gal}(k^{\text{sep}}/k)$.

Example. Suppose that k is a finite field of characteristic p; $|k| = q = p^m$, say. Let $\widehat{\mathbb{Z}}$ be the completion of $\mathbb{Z}$ with respect to the topology defined by the subgroups $n\mathbb{Z}$ $(n > 0)$. (So $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$.) Then $\text{Gal}(k^{\text{sep}}/k) \simeq \widehat{\mathbb{Z}}$ under the map $\nu \mapsto w_q^\nu$ $(\nu \in \widehat{\mathbb{Z}})$, where $w_q(\alpha) = \alpha^q$ (for all $\alpha \in k^{\text{sep}}$). So we deduce from Theorem 7.28 that there exists a unique element $\sigma_q \in \text{Gal}(K_{\text{unr}}/K)$ with the following property: If L is a subfield of K_{unr}/K, then for all $a \in \mathfrak{o}_L$, we have $\sigma_q(a) \equiv a^q \pmod{\mathfrak{p}_L}$. The map $\nu \to \sigma_q^\nu$ is an isomorphism $\widehat{\mathbb{Z}} \xrightarrow{\sim} \text{Gal}(K_{\text{unr}}/K)$ of topological groups. Hence for each integer $n > 0$, K has exactly one unramified extension L of degree n. L/K is normal and $\text{Gal}(L/K)$ is cyclic. Furthermore, Proposition 7.27 implies that K_{unr} is the union of the fields of m^{th} roots of unity (in a given separable closure of K) for all m coprime to p.

7.5 Tamely Ramified Extensions

Definition 7.33 Let L/K be a finite extension with $\text{char}(k) = p$. We say that L/K is a **tame extension** (or that L/K is **tamely ramified**) if $p \nmid e(L/K)$.



Theorem 7.34 $\mathfrak{P}^{e-1}$ divides the different $\mathscr{D}(L/K)$. Furthermore, the following conditions are equivalent:

(a) L/K is tame.

(b) $\mathrm{Tr}_{L/K}(\mathfrak{o}_L) = \mathfrak{o}_K$.

(c) $\mathscr{D}(L/K) = \mathfrak{P}^{e-1}$.

Proof. Choose $N \supset L$ with N/K finite Galois, and let $\mathfrak{q}$ be the unique prime of N lying above $\mathfrak{P}$. Then if $a \in L$, $\mathrm{Tr}_{L/K}(a) = \sum_{\sigma: L \to N} a^\sigma$. If $a \in \mathfrak{P}$, then $\mathrm{Tr}_{L/K}(a) \in \mathfrak{q} \cap K = \mathfrak{p}$. Hence $\mathrm{Tr}_{L/K}(\mathfrak{P}) \subseteq \mathfrak{p}$. Thus we have $\mathrm{Tr}(\mathfrak{P}\mathfrak{p}^{-1}) \subseteq \mathfrak{o}_K$, and so $\mathfrak{P}\mathfrak{p}^{-1} = \mathfrak{P}^{1-e} \subseteq \mathscr{D}^{-1}(L/K)$. Hence it follows that $\mathscr{D}(L/K) \subseteq \mathfrak{P}^{e-1}$, as asserted.

We now show that (b) is equivalent to (c). Suppose that $\mathrm{Tr}_{L/K}(\mathfrak{o}_L) = \mathfrak{o}_K$. Then $\mathrm{Tr}(\mathfrak{p}^{-1}\mathfrak{o}_L) = \mathfrak{p}^{-1}$, and so we have

$$\mathfrak{p}^{-1}\mathfrak{o}_L = \mathfrak{P}^{-e} \supsetneq \mathscr{D}^{-1}(L/K) \supseteq \mathfrak{P}^{1-e}.$$

This implies that $\mathscr{D}(L/K) = \mathfrak{P}^{e-1}$, since $\mathscr{D}(L/K)$ is an $\mathfrak{o}_L$-ideal. Suppose conversely that $\mathrm{Tr}_{L/K}(\mathfrak{o}_L) \subset \mathfrak{p}$. Then $\mathrm{Tr}_{L/K}(\mathfrak{p}^{-1}\mathfrak{o}_L) \subseteq \mathfrak{o}_K$, and so $\mathfrak{p}^{-1} = \mathfrak{P}^{-e} \subseteq \mathscr{D}^{-1}(L/K)$, i.e. $\mathfrak{P}^e \mid \mathscr{D}(L/K)$.

We now show that (a) is equivalent to (b). We begin with a preliminary observation. Let M be the maximal unramified extension of K in L. Then $\mathrm{Tr}_{M/K}(\mathfrak{o}_M) \subseteq \mathfrak{o}_K$. Also if $a \in \mathfrak{o}_M$, then $\overline{\mathrm{Tr}_{M/K}(a)} = \mathrm{Tr}_{k_M/k}(\bar{a})$. Since k_M/k is separable, we have $\mathrm{Tr}_{k_M/k}(k_M) = k$. It follows from Nakayama's Lemma that $\mathrm{Tr}_{M/K}(\mathfrak{o}_M) = \mathfrak{o}_K$. Hence it suffices to prove that (a) is equivalent to (b) in the case that L/K is totally ramified. So assume L/K is totally ramified. Then $\mathfrak{o}_L = \mathfrak{o}_K + \mathfrak{P}$ (from Theorem 7.25), and hence

$$\mathrm{Tr}_{L/K}(\mathfrak{o}_L) = \mathrm{Tr}_{L/K}(\mathfrak{o}_K) + \mathrm{Tr}_{L/K}(\mathfrak{P}) = e\mathfrak{o}_K + \mathrm{Tr}_{L/K}(\mathfrak{P}) = \begin{cases} \mathfrak{o}_K & \text{if } p \nmid e, \\ \subseteq \mathfrak{p} & \text{if } p \mid e. \end{cases}$$

Corollary 7.35 If L/K is tame, $\mathrm{Tr}_{L/K}(\mathfrak{P}) = \mathfrak{p}$.

Proof. Suppose that $\mathfrak{p} = \pi\mathfrak{o}_K$. Then

$$\mathrm{Tr}_{L/K}(\mathfrak{P}) \supset \mathrm{Tr}_{L/K}(\pi\mathfrak{o}_L) = \pi\,\mathrm{Tr}_{L/K}(\mathfrak{o}_L) = \pi\mathfrak{o}_K = \mathfrak{p}.$$

Since also $\mathrm{Tr}_{L/K}(\mathfrak{P}) \subseteq \mathfrak{p}$, the result follows.

Chapter 8

Zeta Functions and L-Series

8.1 Asymptotic Estimate for the Number of Ideals in an Ideal Class

Problem. Let K be a number field, and suppose that Y is an ideal class of K. Find a formula $f(Y,t)$ for the number of integral ideals in Y of norm at most t.

Motivating Example. Let $K = \mathbb{Q}(i)$. Let R be a region in the plane, bounded by a simple smooth curve C of length L. Let A be the area of R and $a(R)$ the number of lattice points in R.

Claim. A is approximated by $a(R)$ in the sense that $|A - a(R)| \leq 4(L+1)$, i.e. $A = a(R) + O(L)$.

[**Recall.** $f = O(g)$ iff there exists a constant C such that $|f(t)| \leq Cg(t)$ for all $t \gg 0$.]

Proof. To each lattice point, associate the square of side 1 of which the point is the lower left vertex. Let $\alpha(C)$ denote the number of these squares which meet the curve C. Then $\alpha(R) - \alpha(C) \leq A \leq \alpha(R) + \alpha(C)$, so $|A - \alpha(R)| \leq \alpha(C)$. Now an arc of length 1 can meet at most four squares; hence C meets at most $4(\lfloor L \rfloor + 1) \leq 4(L+1)$ square. Thus $|A - \alpha(R)| \leq 4(L+1)$, as asserted.

Now suppose that R is the region enclosed by a circle of radius $\sqrt{t}$ centered at the origin. A lattice point (x, y) is in R iff $x^2 + y^2 < t$. Hence we have

$$\sum_{x^2+y^2<t} 1 = \pi t + O(\sqrt{t}). \qquad (*)$$

[**Remark.** In $(*)$, it doesn't matter whether we sum over $x^2 + y^2 < t$ or $x^2 + y^2 \leq t$ since the number of lattice points on the circle is $O(\sqrt{t})$.]

The left side of $(*)$ is the number of Gaussian integers $x + iy$ of norm less than t. Note that every ideal in $\mathbb{Z}[i]$ is principal, and $|\mathbb{Z}[i]^\times| = 4$. So, to count integral ideals rather than integers, we just need to divide by 4, and we obtain

$$\sum_{\{\mathfrak{a}: N\mathfrak{a} \leq t\}} 1 = \frac{\pi}{4} + O(\sqrt{t}).$$

Remarks.

1. The general case is more complicated because K may have an infinite number of units.

2. We will need to be able to approximate the volume of a domain D in $\mathbb{R}^n$ in terms of the number of lattice points in D and the volume of a fundamental parallelepiped of the lattice in question. (In the example, the lattice was the usual lattice in $\mathbb{R}^2$.) To do this, we have to show that the number of lattice points on the boundary ∂D or D has a lower order of magnitude than the number of such points in D. This works if ∂D is described by a piecewise continuously differentiable map on $[0, 1]^{n-1} \subseteq \mathbb{R}^n$ (cf the example).

Definition 8.1 Let (L_1, d_1) and (L_2, d_2) be metric spaces. A function $\phi : L_1 \to L_2$ is called a **Lipschitz map** provided that

(a) ϕ is continuous.

(b) There exists $C \in \mathbb{R}$ such that for all $x, y \in L_1$, $d_2(\phi(x), \phi(y)) \leq C d_1(x, y)$.

A subset $X \subseteq \mathbb{R}^n$ is said to be **k-Lipschitz parametrizable** if there is a finite collection of Lipschitz maps $\phi_i : [0,1]^k \to X$ such that each $x \in X$ lies in the image of at least one ϕ_j.

Notation. For any subset $D \subseteq \mathbb{R}^n$ and any $t \in \mathbb{R}$, let $tD := \{tx : x \in D\}$.

Proposition 8.2 Let D be a subset of $\mathbb{R}^n$, and let L be a lattice in $\mathbb{R}^n$. Assume that ∂D is $(n-1)$-Lipschitz parametrizable. For each t, let $\lambda(t) = |tD \cap L|$. Then

$$\lambda(t) = \left(\frac{\operatorname{Vol} D}{\operatorname{Vol} L}\right) t^n + O(t^{n-1}).$$

Proof. Let P be a fundamental parallelepiped for L. For $\ell \in L$, let $P_\ell := \{p + \ell : p \in P\}$. For $t \in \mathbb{R}$, set $b(t) = |\{\ell \in L : P_\ell \cap \partial D \neq \varnothing\}|$. Then

$$(\lambda(t) - b(t)) \operatorname{Vol}(L) \leq \operatorname{Vol}(tD) \leq (\lambda(t) + b(t)) \operatorname{Vol}(L),$$

so

$$|\lambda(t) \operatorname{Vol}(L) - \operatorname{Vol}(tD)| \leq b(t) \operatorname{Vol}(L),$$

and so it follows that

$$\left|\lambda(t) - \frac{\operatorname{Vol}(D)}{\operatorname{Vol}(L)} t^n\right| \leq b(t).$$

So we have to estimate $b(t)$ as $t \to \infty$. Let $\phi : [0,1]^{n-1} \to \mathbb{R}^n$ be one of the maps which parametrizes ∂D; then $t\phi$ parametrizes the corresponding part of $\partial(tD)$. For a given $t > 1$, divide $[0,1]^{n-1}$ into cubes of edge $1/\lfloor t \rfloor$ (so there will be $\lfloor t \rfloor^{n-1}$ such small cubes in $[0,1]^{n-1}$). Since ϕ is Lipschitz, there exists a constant C_1 such that the image of each small cube has diameter at most $C_1/\lfloor t \rfloor$. Thus the image under $t\phi$ of one of these cubes has diameter at most $tC_1/\lfloor t \rfloor \leq C_2$ for some constant C_2. The number of points ℓ in which P_ℓ can intersect a set of diameter at most C_2 is bounded by a constant C_ϕ, say. Set $C = \sum_\phi C_\phi$. Then $b(t) \leq C\lfloor t \rfloor^{n-1} \leq Ct^{n-1}$, as required.

Now recall some basic facts concerning the geometry of numbers: let K be a number field, $n = [K : \mathbb{Q}]$, $\sigma_1, \ldots, \sigma_{r_1}$ real embeddings of K, and $\sigma_{r_1+1}, \ldots, \sigma_{r_1+r_2}, \bar{\sigma}_{r_1+1}, \ldots, \bar{\sigma}_{r_1+r_2}$ complex embeddings of K. Let $\boldsymbol{\sigma} : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ be given by

$$x \mapsto (\sigma_1(x), \ldots, \sigma_{r_1}(x), \sigma_{r_1+1}(x), \ldots, \sigma_{r_1+r_2}(x)).$$

For each i, define $|\cdot|_i$ by

$$|x|_i = \begin{cases} |\sigma_i(x)| & \text{for } i = 1, \dots, r_1, \\ |\sigma_i(x)|^2 & \text{for } i = r_1+1, \dots, r_1+r_2. \end{cases}$$

There is a norm map $N : \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \to \mathbb{R}$ given by $N(\boldsymbol{\xi}) = \prod_{i=1}^{r_1+r_2} |\xi_i|_i$. Observe that we have $N(\boldsymbol{\sigma}(x)) = |N_{K/\mathbb{Q}}(x)|$ for $x \in K$. Define local degrees

$$n_i = \begin{cases} 1 & 1 \le i \le r_1, \\ 2 & r_1+1 \le i \le r_1+r_2. \end{cases}$$

Then $n = \sum n_i = r_1 + 2r_2$.

We define the **homogenized logarithm map** $\mathbf{g} : \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \to \mathbb{R}^{r_1+r_2}$ by

$$\boldsymbol{\xi} \mapsto \left(\dots, \log \left[\frac{|\xi_i|_i}{N(\boldsymbol{\xi})^{\frac{n_i}{n}}} \right], \dots \right).$$

$$\begin{array}{ccc} K^\times & \xrightarrow{\quad\boldsymbol{\sigma}\quad} & \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} := \mathscr{R} \\ & \searrow^{\boldsymbol{\ell}} & \downarrow \mathbf{g} \\ & & \mathbb{R}^{r_1+r_2} := \mathscr{L} \end{array}$$

For $\varepsilon \in \mathfrak{o}_K^\times$ we have $N(\boldsymbol{\sigma}(\varepsilon)) = 1$, and so $\boldsymbol{\ell}(\varepsilon) = (\log|\sigma_1(\varepsilon)|_1, \dots, \log|\sigma_{r_1+r_2}(\varepsilon)|_{r_1+r_2})$.

Dirichlet's Unit Theorem. $\boldsymbol{\ell}(\mathfrak{o}_K^\times)$ is a full lattice in the hyperplane

$$H = \left\{ \mathbf{x} \in \mathscr{L} : \sum_{i=1}^{r_1+r_2} x_i = 0 \right\}.$$

Let $\varepsilon_1, \dots, \varepsilon_r$ ($r = r_1 + r_2 - 1$) be a set of fundamental units of K. Set $y^{(i)} := \boldsymbol{\ell}(\varepsilon_i)$. Then $\{y^{(1)}, \dots, y^{(r)}\}$ is a basis of $\boldsymbol{\ell}(\mathfrak{o}_K^\times)$. We first calculate $\mathrm{Vol}(\boldsymbol{\ell}(\mathfrak{o}_K))$. Set $y^{(0)} =$

$((r_1+r_2)^{-1/2},\dots,(r_1+r_2)^{-1/2})$. Then $\|y^{(0)}\| = 1$, and $y^{(0)} \cdot H = 0$. Thus the r-dimensional volume of $\mathfrak{o}_K^\times$ is the $(r+1)$-dimensional volume of the lattice generated by $y^{(0)}, y^{(1)}, \dots, y^{(r)}$. Thus

$$\mathrm{Vol}(\mathfrak{o}_K^\times) = \left| \det \begin{pmatrix} (r_1+r_2)^{-1/2} & y_1^{(1)} & \cdots & y_1^{(r)} \\ \vdots & \vdots & \ddots & \vdots \\ (r_1+r_2)^{-1/2} & y_{r_1+r_2}^{(1)} & \cdots & y_{r_1+r_2}^{(r)} \end{pmatrix} \right|,$$

where $y_j^{(i)} = \log|\sigma_j(\varepsilon_i)|_j$. Add the sum of the remaining rows to the first row and use the fact that $\sum_j y_j^{(i)} = 0$. This yields $\mathrm{Vol}(\mathfrak{o}_K^\times) = (r_1+r_2)^{-1/2} R_K$, where $R_K = |\det(\log|\sigma_j(\varepsilon_i)|_j)|$.

Definition 8.3 The **regulator** R_K of K is the absolute value of the determinant of any $r \times r$ minor of the matrix $(\log|\sigma_j(\varepsilon_i)|_j)$ $(1 \le i \le r,\ 1 \le j \le r_1+r_2)$.

Now let Y be an ideal class in K, and let $f(Y,t)$ denote the number of integral ideals $\mathfrak{a} \in Y$ with $N\mathfrak{a} \le t$.

Theorem 8.4 $f(Y,t) = \rho t + O(t^{1-\frac{1}{n}})$, where

$$\rho = \frac{z^{r_1}(2\pi)^{r_2} R_K}{w|d_K|^{1/2}},$$

where $n = [K:\mathbb{Q}]$, w is the number of roots of unity in K, and d_K is the discriminant of K.

(**Note.** The result is independent of Y.)

Preliminary remarks prior to the proof.

1. Observe that $\mathfrak{o}_K^\times$ acts on $\mathscr{R}$: $u \cdot \boldsymbol{\xi} = (\sigma_1(u)\xi_1, \dots, \sigma_{r_1+r_2}(u)\xi_{r_1+r_2})$. A **fundamental domain** in $\mathscr{R}$ (for the action of $\mathfrak{o}_K^\times$) is a set of representatives of the orbits of $\mathfrak{o}_K^\times$ which is also measurable (and may be required to have other properties).

2. Suppose $\mathfrak{b} \in Y^{-1}$ ($\mathfrak{b}$ an integral ideal). Then $\mathfrak{a} \in Y$ iff $\mathfrak{b}\mathfrak{a} = (x)$, a principal ideal. $N(\mathfrak{a}) \le t$ iff $|N(x)| \le tN(\mathfrak{b})$. Suppose that D is a fundamental domain

in $\mathscr{R}$, and set $D(s) := \{\boldsymbol{\xi} \in D \mid N(\boldsymbol{\xi}) \leq s\}$. Then $f(Y,t) = |\sigma(\mathfrak{b}) \cap D(tN(\mathfrak{b}))|$, i.e. for any $\mathfrak{a} \in Y$, there exists exactly one generator x of the ideal $\mathfrak{ab}$ for which $\boldsymbol{\sigma}(x) \in D$; conversely, if $\boldsymbol{\sigma}(x) \in \boldsymbol{\sigma}(\mathfrak{b}) \cap D(tN(\mathfrak{b}))$, then $(x) = \mathfrak{ab}$ for some $\mathfrak{a} \in Y$ and $N\mathfrak{a} \leq t$.

3. Suppose we can construct D with the property that $sD = D$ for all $s > 0$. Then $D(s) = s^{1/n}D(1)$. (If $\boldsymbol{\xi} \in D$ with $N(\boldsymbol{\xi}) \leq s$, then $\boldsymbol{\xi} = s^{1/n}\boldsymbol{\eta}$, with $N(\boldsymbol{\eta}) \leq 1$, and conversely.) Set $\lambda(s) = |sD(1) \cap \sigma(\mathfrak{b})|$. Then (2) implies that $f(Y,t) = \lambda(\{tN(\mathfrak{b})\}^{1/n})$. If also ∂D is $(n-1)$-Lipschitz parametrizable, then we can apply Proposition 8.1 to express $f(Y,t)$ in terms of $\mathrm{Vol}(D(1))$ and $\mathrm{Vol}(\sigma(\mathfrak{b}))$.

4. In fact, we will construct a fundamental domain for $\langle \varepsilon_1, \ldots \varepsilon_r \rangle$, where $\varepsilon_1, \ldots, \varepsilon_r$ are a set of fundamental units of $\mathfrak{o}_K^\times$. Now $|\mathfrak{o}_K^\times : \langle \varepsilon_1, \ldots \varepsilon_r \rangle| = w$. Hence for such a D, we have

$$\begin{aligned} wf(Y,t) &= \lambda((tN(\mathfrak{b}))^{1/n}) \\ &= \frac{\mathrm{Vol}\, D(1)}{\mathrm{Vol}(\mathfrak{b})} \cdot tN(\mathfrak{b}) + O((tN(\mathfrak{b}))^{1-\frac{1}{n}}) \\ &= \frac{\mathrm{Vol}\, D(1)}{\mathrm{Vol}(\mathfrak{b})} \cdot tN(\mathfrak{b}) + O(t^{1-\frac{1}{n}}). \end{aligned}$$

So we have to construct a domain D such that $sD = D$ for all $s > 0$ *and* ∂D is $(n-1)$-Lipschitz parametrizable.

Proof of Theorem 8.4 We first construct D. Recall that $r = r_1 + r_2 - 1$. Let $\{\varepsilon_1, \ldots, \varepsilon_r\}$ be a set of fundamental units in K, $V := \langle \varepsilon_1, \ldots, \varepsilon_r \rangle$, $y^{(i)} := \boldsymbol{\ell}(\varepsilon_i) \in \mathscr{L}$, $P := \left\{\sum_{i=1}^r c_i y^{(i)} : 0 \leq c_i < 1 \text{ for all } i\right\}$. Then P is a fundamental parallelogram in H for the lattice $\boldsymbol{\ell}(\mathfrak{o}_K^\times)$. Now set $D = \mathbf{g}^{-1}(P) \cap \mathscr{R}^\times$.

We now claim that D is a fundamental domain for the action of V on $\mathscr{R}$. Suppose $\boldsymbol{\xi} \in \mathscr{R}^\times$; then $\mathbf{g}(\boldsymbol{\xi}) \in H$ (from the definition of $\mathbf{g}$ — this is why we homogenize the logarithm map!), and so $\mathbf{g}(\boldsymbol{\xi}) = \sum c_i y^{(i)}$, with the $c_i \in \mathscr{R}$ uniquely determined. Set $d_i = c_i - \lfloor c_i \rfloor$, $v = \prod \varepsilon_i^{\lfloor c_i \rfloor}$. Then $\mathbf{g}(\boldsymbol{\xi} \cdot v^{-1}) = \sum d_i y^{(i)} \in P$, i.e. $v^{-1}\boldsymbol{\xi} \in D$. So the orbit of $\boldsymbol{\xi}$ meets D. Suppose now that $\boldsymbol{\eta} \in D$, $v = \prod \varepsilon_i^{h_i}$, and $v\boldsymbol{\eta} \in D$ also. Suppose $\mathbf{g}(\boldsymbol{\eta}) = \sum a_i y^{(i)}$. Then $\mathbf{g}(v\boldsymbol{\eta}) = \sum (a_i + h_i) y^{(i)}$, and so we must have $h_i = 0$ since $h_i \in \mathbb{Z}$, $0 \leq a_i < 1$, $0 \leq a_i + h_i < 1$. Hence $v = 1$, and so D is a fundamental domain, as claimed.

We now claim that for $s \in \mathbb{R}$, $s \neq 0$, we have $sD = D$. This follows from the fact that $\mathbf{g}(s\boldsymbol{\xi}) = \mathbf{g}(\boldsymbol{\xi})$ for all $\boldsymbol{\xi} \in \mathscr{R}$.

We now claim that $D(1)$ is bounded. Suppose that $\boldsymbol{\xi} \in D(1)$. Then $\boldsymbol{\xi} = (\xi_1, \dots, \xi_{r_1+r_2})$ and $N\boldsymbol{\xi} \leq 1$. Then

$$\mathbf{g}(\boldsymbol{\xi}) = \left(\dots, \log \frac{|\xi_h|_h}{|N\boldsymbol{\xi}|^{n_h/n}}, \dots \right).$$

Write $g(\boldsymbol{\xi}) = \sum c_i y^{(i)}$, $0 \leq c_i \leq 1$, and suppose that $y^{(i)} = (y_1^{(i)}, \dots, y_{r_1+r_2}^{(i)})$. Set $M = \max\{|y_j^{(i)}| : 1 \leq i \leq r_1+r_2-1,\ 1 \leq j \leq r_1+r_2\}$. Now equate the h^{th} coefficients for $\mathbf{g}(\boldsymbol{\xi})$; this gives $\log \frac{|\xi_h|_h}{|N\boldsymbol{\xi}|^{n_h/n}} = \sum_i c_i y_h^{(i)}$, and this implies that $|\xi_h|_h \leq e^{(r_1+r_2-1)M}$. Hence $D(1)$ is bounded.

We now calculate $\operatorname{Vol} D(1)$. Let $r = r_1 + r_2 - 1$. Introduce polar coordinates on $\mathscr{R}^\times$. Let $\xi_i = (\rho_i, \theta_i)$, $(i = 1, \dots, r+1)$. Then $\rho_i \geq 0$ for all i, $\theta_i = \pm 1$ $(i = 1, \dots, r_1)$, and $0 \leq \theta_i$ $(i = r_1 + 1, \dots, r_1 + r_2)$. In these coordinates, $D(1)$ is described by the following conditions:

1. $0 \leq \prod \rho_i^{n_i} \leq 1$ (this expresses the condition $N\boldsymbol{\xi} \leq 1$).

2. $$\log \rho_j - \frac{1}{n} \prod_{i=1}^{r+1} \rho_i^{n_i} = \sum_{q=1}^{r} c_q \log |\sigma_j(\varepsilon_q)|,$$

   $0 \leq c_q < 1$, $q = 1, \dots, r$. (This expresses the condition that $\mathbf{g}(\boldsymbol{\xi}) \in P$.)

(These conditions don't involve any of the angles θ_i.) Let $F = \{(\rho_1, \dots, \rho_{r+1}) \in \mathbb{R}^{r+1} : \rho_i > 0$, and (1) and (2) hold$\}$. Then

$$\operatorname{Vol}(D(1)) = 2^{r_1}(2\pi)^{r_2} \int \cdots \int \rho_1 \cdots \rho_{r+1} F \, d\rho_1 \cdots d\rho_{r+1}.$$

To evaluate this, let S be the cube in $\mathbb{R}^{r+1}$ given by $S = \{(u, c_1, \dots, c_r) : 0 < u \leq 1,\ 0 \leq c_q < 1\}$. There is a bijection $f : S \to F$ given in one direction by

$$\rho_j(u, c_1, \dots, u_r) = c^{1/n} \exp\left(\sum_q c_q \log |\sigma_j(\varepsilon_q)| \right),$$

$j = 1, \ldots, r+1$. [In the other direction, we have $h : F \to S$ given by $h(\boldsymbol{\rho}) = (u(\boldsymbol{\rho}), c_1(\boldsymbol{\rho}), \ldots, c_r(\boldsymbol{\rho}))$, where $\boldsymbol{\rho} = (\rho_1, \ldots, \rho_{r+1}) \in F$, $u(\boldsymbol{\rho}) = \prod_{i=1}^{r+1} \rho_i^{n_i}$, and the numbers $c_q(\boldsymbol{\rho})$ are determined by the linear equations

$$\sum_{q=1}^{r} c_q(\boldsymbol{\rho}) \log |\sigma_j(\varepsilon_q)| = \log \rho_j - \frac{1}{n} \log u(\boldsymbol{\rho})$$

$(j = 1, \ldots, r+1)$.] This works because the determinant $\det(\log |\sigma_j(\varepsilon_q)|)$ does not vanish. We now compute the Jacobian J of F.

$$\frac{\partial \rho_j}{\partial u} = \frac{1}{n} \frac{\rho_j}{u}; \qquad \frac{\partial \rho_j}{\partial c_q} = \rho_j \log |\sigma_j(\varepsilon_q)|.$$

Hence we have

$$\begin{aligned} J &= \begin{vmatrix} \frac{\rho_1}{nu} & \rho_1 \log |\sigma_q(\varepsilon_1)| & \cdots & \rho_1 \log |\sigma_1(\varepsilon_r)| \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\rho_{r+1}}{nu} & \rho_{r+1} \log |\sigma_{r+1}(\varepsilon_1)| & \cdots & \rho_{r+1} \log |\sigma_{r+1}(\varepsilon_r)| \end{vmatrix} \\ &= \frac{\rho_1 \rho_2 \cdots \rho_{r+1}}{nu} \begin{vmatrix} 1 & \\ \vdots & \log |\sigma_i(\varepsilon_j)|_i \\ 1 & \end{vmatrix}, \end{aligned}$$

$1 \le i \le r+1$, $1 \le j \le r$. Multiply the i^{th} row by n_i, and then add the first r rows to the last row. The last row becomes $(n, 0, 0, \ldots, 0)$. So the determinant is $n 2^{-r_2} R_K$, and so J is $J = \frac{\rho_1 \rho_2 \cdots \rho_{r+1}}{nu} n 2^{-r_2} R_K$. Now

$$\prod_{j=1}^{r+1} \rho_j^{n_j} = u \exp\left(\sum c_q \left(\sum_{j=1}^{r+1} n_j \log |\sigma_j(\varepsilon_q)| \right) \right) = u.$$

So $J = \frac{R_K}{\rho_{r_1+1} \cdots \rho_{r+1} 2^{r_2}}$. Thus

$$\begin{aligned} \operatorname{Vol} D(1) &= 2^{r_1} (2\pi)^{r_2} \int_F \rho_{r_1+1} \cdots \rho_{r+1} \, d\boldsymbol{\rho} \\ &= 2^{r_1} (2\pi)^{r_2} \int_S \rho_{r_1+1}(s) \cdots \rho_{r+1}(s) J(s) \, ds \\ &= 2^{r_1} \pi^{r_2} R_K \int_S ds \\ &= 2^{r_1} \pi^{r_2} R_K. \end{aligned}$$

Finally, we show that $\partial D(1)$ is Lipschitz parametrizable. Recall that we have $f : S \to F$ given by

$$\rho_j(u, c_1, \ldots, c_r) = u^{1/n} \exp\left(\sum_q c_q \log|\sigma_j(\varepsilon_q)|\right)$$

$(j = 1, \ldots, r+1)$. Only $u^{1/n}$ is not continuously differentiable. Reparametrize the cube by setting $u = u_1^n$. Then we get a continuously differentiable parametrization of the closed cube onto the closure of F given by

$$\rho_j(u, c_1, \ldots, c_r) = u_1 \exp\left(\sum_q c_q \log|\sigma_j(\varepsilon_q)|\right)$$

$(j = 1, \ldots, r+1)$. Then ρ restricted to ∂S gives an $(r-1)$-Lipschitz parametrization of $\partial D(1)$. This completes the proof of the theorem.

8.2 Dirichlet Series

Definition 8.5 A Dirichlet series is an infinite series $\sum_{n=1}^{\infty} a_n e^{-\lambda_n s}$, with $a_n, s \in \mathbb{C}$, $\lambda_n \in \mathbb{R}$.

We shall be concerned with series of the form $\sum a_n n^{-s}$, i.e. $\lambda_n = \log n$.

Proposition 8.6 If the partial sums of a Dirichlet series are bounded for a particular value s_1 of s, then the series converges uniformly on compact subsets of the set $\{s : \Re(s) > \Re(s_1)\}$.

Proof. Let $\sum_{v=1}^{\infty} a_v v^{-s}$ be the Dirichlet series. Set $Q_n = \sum_{v=1}^{n} a_v v^{-s_1}$. By hypothesis, there exists a Q such that $|Q_n| \leq Q$ for all n. Let $\sigma_1 = \Re(s_1)$, and suppose $\delta > 0$.

Then, on the domain $\Re(s) = \sigma \geq \sigma_1 + \delta$, we have

$$\begin{aligned}
\sum_{v=n+1}^{n+m} a_v v^{-s} &= \sum_{v=n+1}^{n+m} a_v v^{-s_1} v^{s_1-s} \\
&= \sum_{v=n+1}^{n+m} (Q_v - Q_{v-1}) v^{s_1-s} \\
&= \sum_{v=n+1}^{n+m} Q_v v^{s_1-s} - \sum_{v=n}^{n+m-1} Q_v (v+1)^{s_1-s} \\
&= Q_{n+m}(n+m)^{s_1-s} - Q_n (n+1)^{s_1-s} + \sum_{v=n+1}^{n+m-1} Q_v (v^{s_1-s} - (v+1)^{s_1-s}).
\end{aligned}$$

Hence

$$\left| \sum_{v=n+1}^{n+m} a_v v^{-s} \right| \leq Q\left((n+m)^{\sigma_1-\sigma} + (n+1)^{\sigma_1-\sigma}\right) + Q \sum_{v=n+1}^{n+m} |v^{s_1-s} - (v+1)^{s_1-s}|.$$

Next observe that we have

$$\begin{aligned}
|v^{s_1-s} - (v+1)^{s_1-s}| &= \left| (s_1 - s) \int_v^{v+1} u^{s_1-s-1}\, du \right| \\
&\leq |s_1 - s| \int_v^{v+1} u^{-\delta-1}\, du.
\end{aligned}$$

If s remains in the domain $|s - s_1| < C$, then

$$|v^{s_1-s} - (v+1)^{s_1-s}| \leq C \int_v^{v+1} u^{-\delta-1}\, du \leq C\delta^{-1}(v^{-\delta} - (v+1)^{-\delta}).$$

Hence

$$\begin{aligned}
\left| \sum_{v=n+1}^{n+m} a_v v^{-s} \right| &\leq Q\left[(n+m)^{-\delta} + (n+1)^{-\delta}\right] + C\delta^{-1} Q \sum_{v=n+1}^{n+m} (v^{-\delta} - (v+1)^{-\delta}) \\
&< (2 + C\delta^{-1}) Q u^{-\delta} \\
&\to 0
\end{aligned}$$

as $n \to \infty$ (independently of m). Hence the result follows.

Corollary 8.7 If the Dirichlet series converges for some value of s, then there is a real number σ_0 such that the series converges for $\Re(s) > \sigma_0$ and diverges for $\Re(s) < \sigma_0$. σ_0 is called the **abscissa of convergence**.

Proposition 8.8 If the partial sums $P_n = \sum_{v=1}^{n} a_v$ of the coefficients of a Dirichlet series $\sum_v a_v v^{-s}$ have the property that $|P_n| \leq P n^{\sigma_1}$ for some P and some $\sigma_1 > 0$, then the abscissa of convergence σ_0 is less than or equal to σ_1.

Proof. Let $\Re(s) = \sigma > \sigma_1$. Then

$$\sum_{v=n+1}^{n+m} a_v v^{-s} = P_{n+m}(n+m)^{-s} - P_n(n+1)^{-s} + \sum_{v=n+1}^{n+m-1} P_v(v^{-s} - (v+1)^{-s}).$$

So (as in the proof of Proposition 8.6), we have

$$\begin{aligned}
\left| \sum_{v=n+1}^{n+m-1} a_v v^{-s} \right| &\leq P\left[(n+m)^{\sigma_1-\sigma} + (n+1)^{\sigma_1-\sigma}\right] + \sum_{v=n+1}^{n+m-1} P v^{\sigma_1} |s| \int_v^{v+1} u^{-\sigma-1}\, du \\
&\leq 2Pn^{\sigma_1-\sigma} + P|s| \sum v^{\sigma_1} \int_v^{v+1} u^{-\sigma-1}\, du \\
&\leq 2Pn^{\sigma_1-\sigma} + P|s| \sum \int_v^{v+1} u^{\sigma_1-\sigma-1}\, du \\
&\leq 2Pn^{\sigma_1-\sigma} + P|s|(\sigma_1-\sigma)^{-1} \sum_{v=n+1}^{n+m-1} ((v+1)^{\sigma_1-\sigma} - v^{\sigma_1-\sigma}) \\
&\leq 2Pn^{\sigma_1-\sigma} + |s|P(\sigma_1-\sigma)^{-1}(n+1)^{\sigma_1-\sigma} \\
&\leq (2 + |s|(\sigma-\sigma_1)^{-1}) P n^{\sigma_1-\sigma} \\
&\to 0
\end{aligned}$$

as $n \to \infty$ (independently of m).

Definition 8.9 The Riemann zeta function $\zeta(s)$ is defined by $\zeta(s) = \sum_{v=1}^{\infty} v^{-s}$.

Proposition 8.8 implies that the abscissa of $\zeta(s)$ is at most 1. However, $\zeta(s)$ does not converge at $s = 1$, and so the abscissa of convergence is 1.

Theorem 8.10 $\zeta(s)$ has an analytic continuation to $\Re(s) > 0$, except for a simple pole at $s = 1$, with residue 1.

Proof. Consider the following series:

$$\zeta_2(s) = 1 - \frac{1}{2^s} + \frac{1}{3^s} - \cdots .$$

The partial sums of the coefficients are equal to 0 or 1, and so are bounded, i.e. $\zeta_2(s)$ is analytic for $\Re(s) > 0$. For $\Re(s) > 1$, we have $\frac{2}{2^s}\zeta(s) + \zeta_2(s) = \zeta(s)$, i.e. $\zeta(s) = \frac{1}{1-2^{1-s}}\zeta_2(s)$, giving a meromorphic continuation to $\Re(s) > 0$. To see that $\zeta(s)$ has no poles for $s \neq 1$, consider the series

$$\zeta_r(s) = \frac{1}{1^s} + \frac{1}{2^s} + \cdots + \frac{1}{(r-1)^s} + \frac{1-r}{r^s} + \frac{1}{(r+1)^s} + \cdots + \frac{1-r}{(2r)^s} + \frac{1}{(2r+1)^s} + \cdots .$$

Then the partial sums of the coefficients of $\zeta_r(s)$ are bounded by r. Hence Proposition 8.8 implies that $\zeta_r(s)$ is analytic for $\Re(s) > 0$. Also, we have $\zeta(s) = \frac{1}{1-r^{1-s}}\zeta_r(s)$. Hence if $s \neq 1$ ($\Re(s) > 0$) is a pole of $\zeta(s)$, then we must have $r^{1-s} = 1$ for all r, which is a contradiction.

Theorem 8.11 Let $f(s) = \sum_{v=1}^{\infty} a_v v^{-s}$, and let $P_n = \sum_{v=1}^{n} a_v$. Suppose that for some $\rho \in \mathbb{C}$ and $\sigma_1 \in \mathbb{R}$ ($0 \leq \sigma_1 < 1$), there exists a constant C such that $|P_n - \rho n| < Cn^{\sigma_1}$ for all n. Then $f(s)$ is holomorphic for $\Re(s) > \sigma_1$, except for a simple pole of residue 1 at $s = 1$.

Proof. The sum of the first n coefficients of the Dirichlet series of $f(s) - \rho\zeta(s)$ is $P_n - \rho n$. Thus Proposition 8.8 implies that $f(s) - \rho\zeta(s)$ is holomorphic on $\Re(s) > \sigma_1$. The result now follows from Theorem 8.10.

8.3 The Zeta Function of an Algebraic Number Field

Let K be a number field and $n = [K : \mathbb{Q}]$.

Lemma 8.12 For $\Re(s) > 1$, the sum $\sum_{\mathfrak{p}} N\mathfrak{p}^{-s}$ over all prime ideals $\mathfrak{p}$ of K converges.

Proof.

$$\sum_{\mathfrak{p}} N\mathfrak{p}^{-s} = \sum_{\substack{p \in \mathbb{Z} \\ p \text{ prime}}} \sum_{\mathfrak{p}|(p)} N\mathfrak{p}^{-s} \leq n \sum_{p} p^{-s} \leq n \sum_{m=1}^{\infty} m^{-s},$$

and this last sum converges.

Remark. For $s = \sigma + it$ and $y > 0$, $y^s = e^{s \log y}$, where $\log y$ is the real logarithm.

Theorem 8.13 For $\sigma > 1$, we have

(1) $\prod_{\mathfrak{p}} (1 - N\mathfrak{p}^{-s})^{-1}$ is absolutely convergent and converges uniformly on compact subsets.

(2) The sum $\zeta_K(s) = \sum_{\mathfrak{a}} N\mathfrak{a}^{-s}$ (sum over all integral ideals $\mathfrak{a}$ of K) is absolutely convergent and converges uniformly on compact subsets. ($\zeta_K(s)$ is the zeta function of K.)

(3) $\zeta_K(s) = \prod_{\mathfrak{p}} (1 - N\mathfrak{p}^{-s})^{-1}$. (In particular, $\zeta_K(s) \neq 0$ for $\Re(s) > 1$.)

Proof.

(1) Fix $\sigma_0 > 1$, and consider the product in the domain $\sigma \geq \sigma_0$. For any $\mathfrak{p}$, we have

$$\begin{aligned} \log(1 - |N\mathfrak{p}^{-s}|)^{-1} &= \sum_{m=1}^{\infty} N\mathfrak{p}^{-\sigma m} m^{-1} \\ &\leq \sum_{m=1}^{\infty} N\mathfrak{p}^{-\sigma m} \\ &= \frac{N\mathfrak{p}^{-\sigma}}{1 - N\mathfrak{p}^{-\sigma}} \\ &\leq \frac{N\mathfrak{p}^{-\sigma_0}}{1 - N\mathfrak{p}^{-\sigma_0}} \\ &\leq 2N\mathfrak{p}^{-\sigma_0}. \end{aligned}$$

Now since $\sum_{\mathfrak{p}} N\mathfrak{p}^{-\sigma_0}$ converges, it follows that $\sum_{\mathfrak{p}} \log(1-|N\mathfrak{p}^{-s}|)^{-1}$ converges uniformly for $\sigma \geq \sigma_0$. This implies (1).

(2) and (3) Consider a finite product

$$\prod_{N\mathfrak{p}\leq t}(1-N\mathfrak{p}^{-s})^{-1} = \prod_{N\mathfrak{p}\leq t}(1+N\mathfrak{p}^{-s}+N\mathfrak{p}^{-2s}+\cdots) = \sum\nolimits' N\mathfrak{a}^{-s},$$

where $\sum'$ denotes the sum over all integral ideals $\mathfrak{a}$ whose prime factors have norm at most t. Then

$$\prod_{N\mathfrak{p}\leq t}(1-N\mathfrak{p}^{-s})^{-1} = \sum_{N\mathfrak{a}\leq t} N\mathfrak{a}^{-s} + \sum_{N\mathfrak{a}>t}{}' N\mathfrak{a}^{-s}. \qquad (\dagger)$$

Hence for $\sigma_0 > 1$ fixed, we have $\sum_{N\mathfrak{a}\leq t} N\mathfrak{a}^{-\sigma_0} < \prod_{N\mathfrak{p}\leq t}(1-N\mathfrak{p}^{-\sigma_0})^{-1}$. This implies that $\sum_{\mathfrak{a}} N\mathfrak{a}^{-s}$ is absolutely convergent for $\Re(s) > 1$. From (†), we have

$$\left|\prod_{N\mathfrak{p}\leq t}(1-N\mathfrak{p}^{-s})^{-1} - \sum_{N\mathfrak{a}\leq t} N\mathfrak{a}^{-s}\right| \leq \sum_{N\mathfrak{a}>t} N\mathfrak{a}^{-\sigma}.$$

On $\sigma \geq \sigma_0 > 1$, we have $\sum_{N\mathfrak{a}>t} N\mathfrak{a}^{-\sigma} < \sum_{N\mathfrak{a}>t} N\mathfrak{a}^{-\sigma_0} \to 0$ as $t \to \infty$ (exercise). This proves (2) and (3).

Definition 8.14 Let Y be any ideal class of K. The **partial zeta function** of Y is $\zeta_K(s;Y) = \sum_{\mathfrak{a}\in Y} N\mathfrak{a}^{-s}$ (sum over integral ideals only). So $\zeta_K(s) = \sum_Y \zeta_K(s;Y)$.

Theorem 8.15 For any ideal class Y of K, $\zeta_K(s;Y)$ is holomorphic on $\Re(s) > 1-\frac{1}{n}$, except for a simple pole at $s=1$ of residue

$$\rho_K = \frac{2^{r_1}(2\pi)^{r_2}R_K}{w|d_K|^{1/2}}.$$

Proof. We may write $\zeta_K(s;Y) = \sum_{v=1}^{\infty} a_v v^{-s}$, where $a_v = \#\{\mathfrak{a}\in Y \mid N\mathfrak{a} = v\}$. Recall that

$$f(Y,t) = \#\{\mathfrak{a}\in Y \mid N\mathfrak{a}\leq t\} = \rho_K t + O(t^{1-\frac{1}{n}}).$$

Now $P_m = a_1 + \cdots + a_m = f(Y, m)$, and so the result follows from Theorem 8.11.

Corollary 8.16 $\zeta_K(s)$ is holomorphic on $\Re(s) > 1 - \frac{1}{n}$, except for a simple pole at $s = 1$ of residue $h_K \rho_K$ (where h_K is the class number of K).

Corollary 8.17 K contains infinitely many prime ideals of degree 1 over $\mathbb{Q}$.

Proof. On $\{z : |z| < 1\}$, the branch of the logarithm for which $\log 1 = 0$ is given by $\log(1 - z) = -\sum_{v=1}^{\infty} v^{-1} z^v$. For this branch, for $\sigma > 0$ real, we have

$$\begin{aligned}
\log \zeta_K(\sigma) &= \sum_{\mathfrak{p}} \log(1 - N\mathfrak{p}^{-\sigma})^{-1} \\
&= \sum_{\mathfrak{p}} \sum_{v=1}^{\infty} (vNp^{\sigma v})^{-1} \\
&= \sum_{\mathfrak{p}} N\mathfrak{p}^{-\sigma} + \sum_{\mathfrak{p}} \sum_{v \geq 2} (vN\mathfrak{p}^{\sigma v})^{-1}.
\end{aligned}$$

We claim that $\sum_{\mathfrak{p}} \sum_{v \geq 2} (vN\mathfrak{p}^{-sv})^{-1}$ is holomorphic on any domain $\Re(s) > \sigma_0 > \frac{1}{2}$. We have

$$\begin{aligned}
\sum_{\mathfrak{p}} \sum_{v \geq 2} |vN\mathfrak{p}^{-sv}|^{-1} &< \frac{1}{2} \sum_{\mathfrak{p}} \sum_{v \geq 2} |N\mathfrak{p}^{-sv}| \\
&= \frac{1}{2} \sum_{\mathfrak{p}} |N\mathfrak{p}^{-2s}| (1 - |N\mathfrak{p}^{-s}|)^{-1} \\
&< \frac{1}{2} (1 - 2^{-\sigma_0})^{-1} \sum_{\mathfrak{p}} N\mathfrak{p}^{-2\sigma_0} \\
&\leq n \sum_{m=1}^{\infty} m^{-2\sigma_0},
\end{aligned}$$

where $n = [K : \mathbb{Q}]$, and this last sum converges for $\sigma_0 > \frac{1}{2}$.

Hence it follows that $\sum_{\mathfrak{p}} N\mathfrak{p}^{-\sigma} \to \infty$ as $\sigma \to 1^+$. Next we observe that

$$\sum_{\mathfrak{p}} N\mathfrak{p}^{-\sigma} = \sum_{f_{\mathfrak{p}}=1} N\mathfrak{p}^{-\sigma} + \sum_{f_{\mathfrak{p}}\geq 2} N\mathfrak{p}^{-\sigma},$$

and the last sum on the right converges at $\sigma = 1$. Hence $\sum_{f_{\mathfrak{p}}=1} N\mathfrak{p}^{-1}$ diverges, and so the result follows.

Corollary 8.18 $\sum_{\substack{p\in\mathbb{Z} \\ p \text{ prime}}} p^{-1}$ diverges.

8.4 Some Remarks on Characters (Extended Exercise)

Definition 8.19 Let F be a field and G a finite abelian group. An F-valued **character** χ of G is a homomorphism $\chi : G \to F^\times$. A **character** of G is a $\mathbb{C}$-valued character of G.

$\chi(G)$ is contained in S^1. We let $\widehat{G}$ denote the group of characters of G. This is a finite abelian group.

Duality Theory for Finite Abelian Groups (8.20)

(1) $\widehat{G \times H} \simeq \widehat{G} \times \widehat{H}$.

(2) $G \simeq \widehat{G}$ (non-canonically).

(3) For a subgroup $H \leq G$, let $H^\perp = \{\chi \in \widehat{G} : \chi(H) = 1\}$. Then $\widehat{H} \simeq \widehat{G}/H^\perp$ and $H = \bigcap_{\chi\in H^\perp} \ker(\chi)$.

(4) $\widehat{\widehat{G}} \simeq G$ via $g(\chi) = \chi(g)$ (so this isomorphism is canonical).

(5)

$$\sum_{g\in G} \chi(G) = \begin{cases} |G| & \text{if } \chi \text{ is trivial,} \\ 0 & \text{otherwise.} \end{cases}$$

(3') $H^{\perp} = \bigcap_{h \in H} \ker(h)$ (viewing $h \in \widehat{\widehat{G}}$).

(5')

$$\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} |G| & \text{if } g = id, \\ 0 & \text{otherwise.} \end{cases}$$

Definition 8.21 Let $m \in \mathbb{N}$. A **Dirichlet character modulo** m is a function $\chi : \mathbb{Z} \to \mathbb{C}$ such that

(i) $\chi(a) = \chi(b)$ if $a \equiv b \pmod{m}$.

(ii) $\chi(ab) = \chi(a)\chi(b)$.

(iii) $\chi(a) = 0$ iff $(a, m) \neq 1$.

Hence a Dirichlet character modulo m defines a character of $(\mathbb{Z}/m\mathbb{Z})^{\times}$.

Definition 8.22 Let χ be a Dirichlet character modulo m, and suppose that $n \mid m$. Then χ is **induced** from a Dirichlet character modulo n if $\chi(x) = \chi(y)$ whenever $x \equiv y \pmod{n}$ and $(xy, m) = 1$.

Point. If $n \mid m$, then there is a natural quotient map $\theta : (\mathbb{Z}/m\mathbb{Z})^{\times} \to (\mathbb{Z}/n\mathbb{Z})^{\times}$. Then $x \in \widehat{(\mathbb{Z}/m\mathbb{Z})^{\times}}$ is induced from $(\mathbb{Z}/n\mathbb{Z})^{\times}$ iff $\chi = \chi'\theta$ for some $\chi' \in \widehat{(\mathbb{Z}/n\mathbb{Z})^{\times}}$ (i.e. iff χ factors through $\ker(\theta)$).

Definition 8.23 A character χ is called **primitive** if it is not induced from a character modulo a proper divisor of m. In this case, m is called the **conductor** of χ.

Exercise. Suppose that χ is a Dirichlet character on $\mathbb{Z}$. If χ is induced from a character modulo m and also a character modulo n, then χ is induced from a character modulo (m, n).

Corollary 8.24 Let χ be a Dirichlet character on $\mathbb{Z}$. Then there is a unique positive integer f_χ such that χ is induced from a primitive character modulo f_χ. The number f_χ is called the conductor of χ.

8.5 L-Functions

Definition 8.25 Let χ be a primitive Dirichlet character. The (Dirichlet) L-function attached to χ is defined by

$$L(s,\chi) = \sum_{v=1}^{\infty} \chi(v) v^{-s}.$$

Theorem 8.26 Assume that $\chi \neq id$. Then $\sum_{v=1}^{\infty} \chi(v) v^{-s}$ converges absolutely on $\Re(s) > 0$, and it converges uniformly on compact subsets of this region. For $\Re(s) > 1$, we have

$$L(s,\chi) = \prod_p (1 - \chi(p) p^{-s})^{-1}.$$

Proof. Observe that the partial sums $P_n = \sum_{v=1}^{n} \chi(v)$ are bounded (independently of n) by e.g. $\phi(f_\chi)$, where ϕ is the Euler ϕ-function and f_χ is a conductor of χ. Hence the first assertion follows from Proposition 8.8 and Proposition 8.6. The second assertion is proved as in Theorem 8.13.

Remark. $L(s,\chi_0) = \zeta(s)$, where χ_0 is the trivial character.

Theorem 8.27 Let $K = \mathbb{Q}(\zeta_n)$, so $\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$. Then $\zeta_K(s) = \prod_\chi L(s,\chi)$, where the product is taken over all primitive Dirichlet characters whose conductors divide n.

Proof. It suffices to prove the equality for real values of $s > 1$. For such values of s, we have $\zeta_K(s) = \prod_{\mathfrak{p}}(1 - N\mathfrak{p}^{-s})^{-1}$,

$$\prod_{\chi} L(s,\chi) = \prod_{\chi}\prod_{p}(1-\chi(p)p^{-s})^{-1}.$$

The theorem will follow if we show that

$$\prod_{\mathfrak{p}|(p)}(1-N\mathfrak{p}^{-s}) = \prod_{\chi}(1-\chi(p)p^{-s}). \qquad (\dagger)$$

Let $n = p^r m$ ($r \geq 0$, $(m,p) = 1$).

$$\begin{array}{c} \mathbb{Q}(\zeta_n) = K \\ | \\ \mathbb{Q}(\zeta_m) \\ | \\ \mathbb{Q} \end{array}$$

We now compute the left side of (†). We have $p\mathfrak{o}_K = (\mathfrak{p}_1 \cdots \mathfrak{p}_g)^e$, $N\mathfrak{p}_i = p^f$, where f is the order of $p \pmod m$, and $efg = \phi(n)$. Thus the left side of (†) is $(1-p^{-fs})^g$.

We now compute the right side of (†). If, for some χ, $f_\chi \nmid m$, then $p \mid f_\chi$, and so $\chi(p) = 0$. So the right side is $\prod_{f_\chi | m}(1-\chi(p)p^{-s})$. Each character χ with $f_\chi \mid m$ induces a character χ on $(\mathbb{Z}/m\mathbb{Z})^\times$ (via the quotient map $(\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/f_\chi\mathbb{Z})^\times$). As χ runs over the set of primitive characters for which $f_\chi \mid m$, the induced characters χ' run over $\widehat{(\mathbb{Z}/m\mathbb{Z})^\times}$ (since every such χ' is induced from a unique primitive character χ, and for such χ, $f_\chi \mid m$). If $z \equiv p \pmod m$, then $\chi(p) = \chi'(z)$. Since z has order f in $(\mathbb{Z}/m\mathbb{Z})^\times$, $\chi'(z)$ is an f^{th} root of unity. As χ' runs over $(\mathbb{Z}/m\mathbb{Z})^\times$, $\chi'(z)$ runs over the group of f^{th} roots of unity, taking each value $\chi(m)/f = g$ times. (Think of the set $\left\{\chi'(z) : \chi' \in \widehat{(\mathbb{Z}/m\mathbb{Z})^\times}\right\}$ as being the set of values of $z \in \widehat{\widehat{(\mathbb{Z}/m\mathbb{Z})^\times}}$.) Hence the right side of (†) is

$$\prod_{w^f=1}(1-wp^{-s})^g = (1-p^{-fs})^g = (1-p^{-fs})^g,$$

which is the same as the left side.

Corollary 8.28 Let h_K be the class number of $K = \mathbb{Q}(\zeta_n)$. Then

$$\rho_K h_K = \prod_{\substack{\chi \neq \chi_0 \\ f_\chi | n}} L(1, \chi),$$

where χ_0 is the trivial character and

$$\rho_K = \frac{2^{r_1}(2\pi)^{r_2} R_K}{w|d_K|^{1/2}}.$$

Proof. Evaluate the residue at $s = 1$ of both sides of the equation $\zeta_K(s) = \prod_\chi L(s, \chi)$. For $\chi \neq \chi_0$, $L(s, \chi)$ is holomorphic at $s = 1$. $L(s, \chi_0) = \zeta(s)$ has residue 1 at $s = 1$. $\zeta_K(s)$ has residue $\rho_K h_K$ at $s = 1$.

Corollary 8.29 For any character χ, $L(1, \chi) \neq 0$.

Theorem 8.30 (Dirichlet's theorem on primes in an arithmetic progression) Let m and d be positive integers with $(m, d) = 1$. Then the arithmetic progression $\{m + nd \mid n \in \mathbb{N}\}$ contains infinitely many primes.

Proof. Write $f(s) \sim g(s)$ to mean $f(s) - g(s)$ is holomorphic in a neighborhood of $s = 1$. Let χ be a Dirichlet character with $f_\chi \mid m$. Then

$$\log L(s, \chi) = \sum_p \log(1 - \chi(p)p^{-s})^{-1} = \sum_{p,n} \frac{\chi(p)^n}{np^{ns}} \sim \sum_p \chi(p)p^{-s}$$

(since $\sum_{p,n\geq 2} \frac{1}{np^{ns}}$ is finite). Thus

$$\log L(s, \chi) \sim \sum_{p \nmid m} \chi(p)p^{-s} = \sum_{C \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(C) \sum_{p \in C} p^{-s}, \qquad (\dagger)$$

since $p \equiv q \pmod{m}$ implies $\chi(p) = \chi(q)$. Let $A \in (\mathbb{Z}/m\mathbb{Z})^\times$ be a fixed residue class. Multiply both sides of $(\dagger)$ by $\chi(A^{-1})$, and sum over $\chi \in \widehat{(\mathbb{Z}/m\mathbb{Z})^\times}$. We get

$$\sum_\chi \chi(A^{-1}) \log L(s, \chi) \sim \sum_{\chi, C} \chi(A^{-1}C) \sum_{p \in C} p^{-s} = \sum_C \left[\sum_\chi \chi(A^{-1}C) \sum_{p \in C} p^{-s} \right].$$

Now

$$\sum_C \chi(A^{-1}C) = \begin{cases} \phi(m) & \text{if } A = C, \\ 0 & \text{otherwise.} \end{cases}$$

(Exercise.) Hence

$$\sum_\chi \chi(A^{-1}) \log L(s,\chi) \sim \phi(m) \sum_{p \in A} p^{-s}.$$

Since $L(1,\chi) \neq 0$ for $\chi \neq \chi_0$, we obtain $\log \zeta(s) \sim \phi(m) \sum_{p \in A} p^{-s}$, and this implies the result.

Corollary 8.31 Given any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$, there are infinitely many primes for which σ is the Frobenius automorphism.

8.6 Abelian Extensions of $\mathbb{Q}$

Suppose that $K/\mathbb{Q}$ is an abelian extension. The Kronecker-Weber Theorem implies that $K \subseteq \mathbb{Q}(\zeta_n)$ for some n. Now $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$, and so $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/K)$ is isomorphic to a subgroup $H(K)$ of $(\mathbb{Z}/n\mathbb{Z})^\times$. Recall that

$$H(K)^\perp = \left\{ \chi \in \widehat{(\mathbb{Z}/n\mathbb{Z})^\times} : \chi(H) = 1 \right\}.$$

Then

$$H(K) \simeq \widehat{H(K)} = \left[\widehat{(\mathbb{Z}/n\mathbb{Z})^\times} / H(K)^\perp \right].$$

Then

$$H(K)^\perp \simeq \mathrm{Gal}(K/\mathbb{Q}) \simeq \widehat{\mathrm{Gal}(K/\mathbb{Q})}.$$

We refer to $H(K)^\perp$ as the **group of Dirichlet characters** belonging to K, or the **group of characters** of K.

Definition 8.32 Let $K/\mathbb{Q}$ be abelian. Then **conductor** of K is defined to be the smallest positive integer n such that $K \subseteq \mathbb{Q}(\zeta_n)$.

Exercise. Let K be a quadratic field of discriminant d. Show that the conductor of K is $|d|$.

Proposition 8.33 The conductor of K is the least common multiple of the characters of K.

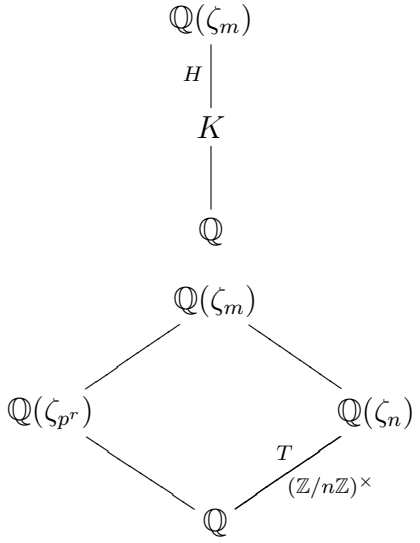
Proof. Let $K \subseteq \mathbb{Q}(\zeta_n)$, and view the characters of K as characters modulo n. Set $H = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/K)$, viewed as a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$. Then $H = \bigcap_{\chi \in H^\perp} \ker(\chi)$. If $m \mid n$, then $K \subseteq \mathbb{Q}(\zeta_m)$ iff $\{x \pmod n : x \equiv 1 \pmod m\} \subseteq H$. Hence $K \subseteq \mathbb{Q}(\zeta_m)$ iff each character of K is induced from a character of $(\mathbb{Z}/m\mathbb{Z})^\times$ iff $f_\chi \mid m$ for each $\chi \in H^\perp$.

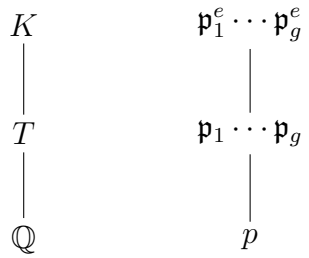
Theorem 8.34 Suppose $K/\mathbb{Q}$ is abelian. Then $\zeta_K(s) = \prod_{\chi \text{ of } K} L(s, \chi)$ (product over all characters of K).

Proof. As in the proof of Theorem 8.27, it suffices to prove that, for each rational prime p,

$$\prod_{\mathfrak{p}|(p)} (1 - N\mathfrak{p}^{-s}) = \prod_{\chi} (1 - \chi(p)p^{-s}). \qquad (\dagger)$$

The left side is equal to $(1-p^{-fs})^g$, where $(p) = (\mathfrak{p}_1 \cdots \mathfrak{p}_g)^e$, and f is the residue class degree of $\mathfrak{p}_i/\mathfrak{p}$ (any i). Fix m such that $K \subseteq \mathbb{Q}(\zeta_m)$. Set $H = \mathrm{Gal}(\mathbb{Q}(\zeta_m)/K)$, viewed as a subgroup of $(\mathbb{Z}/m\mathbb{Z})^\times$. Let $m = p^r n$ ($r \geq 0$, $p \nmid n$). Set H_0 to be the image of H in $(\mathbb{Z}/n\mathbb{Z})^\times$ under the quotient map.





Then $T := \mathbb{Q}(\zeta_n) \cap K$ is the subfield of $\mathbb{Q}(\zeta_n)$ fixed by H_0. $T/\mathbb{Q}$ is the maximal subextension of $K/\mathbb{Q}$ in which p is unramified. Suppose $z = p \pmod{n}$ in $(\mathbb{Z}/n\mathbb{Z})^\times$. Then f is the order of $z \pmod{H_0}$ since $\mathrm{Frob}(p, T/\mathbb{Q}) = \mathrm{Frob}(p, \mathbb{Q}(\zeta_n)/\mathbb{Q}) \mid_T$. We have $g = [(\mathbb{Z}/n\mathbb{Z})^\times : H_0]/f$. Now let χ be a character of K. If $p \mid f_\chi$, then $\chi(p) = 0$. Hence

$$\prod_{\chi \text{ of } K} (1 - \chi(p)p^{-s}) = \prod_{\chi \text{ of } T} (1 - \chi(p)p^{-s}).$$

The characters of T are the characters of $(\mathbb{Z}/n\mathbb{Z})^\times/H_0$. As χ runs over all such characters, $\chi(z)$ runs over the f^{th} roots of unity. Each such f^{th} root of unity occurs g times. The right side of (†) is

$$\prod_{w^f=1} (1 - p^{-s})^g = (1 - p^{-sf})^g.$$

8.7 Functional Equations

Let χ be a Dirichlet character. Let

$$\delta_\chi = \begin{cases} 0 & \text{if } \chi(-1) = 1, \text{ i.e. } \chi \text{ is } \textbf{even}, \\ 1 & \text{if } \chi(-1) = -1, \text{ i.e. } \chi \text{ is } \textbf{odd}. \end{cases}$$

Let $\tau(\chi) = \sum_{a=1}^{f_\chi} \chi(a) e^{-2\pi i a/f_\chi}$. Let $\Gamma(z) = \int_0^\infty t^{z-1} e^{-t}\, dt$, where $z \in \mathbb{C}$, $\Re(z) > 0$; this admits a meromorphic continuation to all of $\mathbb{C}$. Let

$$\Lambda(s, \chi) = (f_\chi \pi^{-1})^{s/2} \Gamma\left(\frac{s + \delta_\chi}{2}\right) L(s, \chi).$$

Theorem 8.35 $\Lambda(s,\chi)$ can be extended to a meromorphic function on $\mathbb{C}$. It satisfies the functional equation

$$\Lambda(s,\chi) = \frac{\tau(x)}{f_\chi^{1/2} i^{\delta_\chi}} \Lambda(1-s,\bar{\chi}).$$

If $\chi \neq \chi_0$, the trivial character, then $L(s,\chi)$ is entire. If $\chi = \chi_0$, then the only pole of $L(s,\chi_0) = \zeta(s)$ is at $s = 1$.

[See e.g. Lang or Tate's thesis.]

Remarks.

1. $W_\chi := \frac{\tau(\chi)}{f_\chi^{1/2} i^{\delta_\chi}}$ is called the root number.

2. If $\chi \neq \chi_0$, we know that $L(\chi, s)$ is holomorphic for $\Re(s) > 0$. The functional equation implies

$$L(s,\chi) = W_\chi (f/\pi)^{\frac{1-2s}{2}} \times \Gamma\left(\frac{1-s+\delta_\chi}{2}\right) \Gamma\left(\frac{s+\delta_\chi}{2}\right)^{-1} \times L(1-s,\bar{\chi}).$$

   Since the Γ function is never zero, any poles of $L(s,\chi)$ on the domain $\Re(s) \leq 0$ would have to arise as poles of the factor $\Gamma\left(\frac{1-s+\delta_\chi}{2}\right)$. The Γ function has poles at 0 and at the negative integers and nowhere else. Hence $L(s,\chi)$ is holomorphic for $\Re(s) \leq 0$.

3. If $\chi = \chi_0$, the functional equation of the Riemann ζ function is

$$\Gamma\left(\frac{s}{2}\right) \pi^{\frac{s}{2}} \zeta(s) = \Gamma\left(\frac{1-s}{2}\right) \pi^{-\frac{1-s}{2}} \zeta(1-s),$$

   so

$$\zeta(s) = \frac{\Gamma\left(\frac{1-s}{2}\right) \pi^{-\frac{1}{2}+s} \zeta(1-s)}{\Gamma\left(\frac{s}{2}\right)}.$$

   Hence $\zeta(s)$ has zeros at $s = -2n$ ($n \in \mathbb{N}$) ("trivial zeros"). The values $\zeta(1-2n)$ ($n \in \mathbb{N}$) are in $\mathbb{Q}$.

4. The zeta function of any algebraic number field satisfies a functional equation. Suppose that $K/\mathbb{Q}$ is a real abelian extension, with $n = [K : \mathbb{Q}]$. Set

$$Z_K(s) = |d_K|^{1/2} \left(\pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right)\right)^n \times \zeta_K(s).$$

Then $Z_K(s) = Z_K(1-s)$. Recall that $\zeta_K(s) = \prod_{\chi \text{ of } K} L(s,\chi)$ (Theorem 8.34). Comparing the functional equation of $\zeta_K(s)$ with that of $\prod_\chi L(s,\chi)$ gives

$$\left(|d_K| \prod_\chi f_\chi^{-1}\right)^{s/2} = \prod_\chi (\chi(-1) f_\chi)^{s/2} \tau(\chi)^{-1} \times \left(|d_K| \prod_\chi f_\chi^{-1}\right)^{\frac{1-s}{2}}.$$

This is possible for all s only if both sides equal 1, i.e.

$$|d_K| = \prod_\chi f_\chi \tag{$*$}$$

and

$$\prod_\chi \tau(\chi) = \prod_\chi (\chi(-1) f_\chi)^{1/2}. \tag{$**$}$$

In fact, these formulae hold for all abelian extensions $K/\mathbb{Q}$. $(*)$ is called the **conductor-discriminant formula**. It implies that p ramifies in $K/\mathbb{Q}$ iff p divides the conductor of K (cf Proposition 8.33).

Corollary 8.36 Let χ be the unique quadratic character modulo p. Then

$$\tau(\chi) = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \pmod 4, \\ i\sqrt{p} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Proof. Apply $(**)$ to K, the unique quadratic subextension of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$.

Chapter 9

Class Number Formulae

Recall. Let $K/\mathbb{Q}$ be abelian with $n = [K : \mathbb{Q}]$. Then $\zeta_K(s) = \prod_{\chi \text{ of } K} L(s, \chi)$, so

$$hR = w|d_K|^{1/2} 2^{-r_1} (2\pi)^{r_2} \prod_{\chi \neq \chi_0} L(1, \chi).$$

Either all embeddings $\sigma : K \hookrightarrow \mathbb{C}$ are real (in which case $w = 2$) or they are all complex. So

$$hR = \begin{cases} |d_K|^{1/2} 2^{1-n} \prod_{\chi \neq \chi_0} L(1, \chi) & K \text{ real}, \\ w|d_K|^{1/2} (2\pi)^{-n/2} \prod_{\chi \neq \chi_0} L(1, \chi) & K \text{ complex}. \end{cases}$$

If K is imaginary quadratic, these determine h. Otherwise we have to deal with the regulator (which is hard).

9.1 Summation of L-Series

Let $\chi \neq \chi_0$ be a primitive character, f its conductor, and $\zeta = e^{2\pi i/f}$. Then

$$L(s, \chi) = \sum_{v=1}^{\infty} \chi(v) v^{-s} = \sum_{(x,f)=1} \chi(x) \sum_{v \equiv x \pmod f} v^{-s}$$

($\Re(s) > 1$). Now $\sum_{v \equiv x \pmod f} v^{-s} = \sum_{v=1}^{\infty} c_v v^{-s}$ (a Dirichlet series), where

$$c_v = \begin{cases} 1 & \text{if } v \equiv x \pmod f, \\ 0 & \text{otherwise.} \end{cases}$$

Now

$$\sum_{k=0}^{f-1} \zeta^{rk} = \begin{cases} f & \text{if } r \equiv 0 \pmod{f}, \\ 0 & \text{otherwise,} \end{cases}$$

so

$$c_v = \frac{1}{f} \sum_{k=0}^{f-1} \zeta^{(x-v)k}.$$

Hence

$$\begin{aligned} L(s,\chi) &= \sum_{(x,f)=1} \chi(x) \sum_{v=1}^{\infty} \zeta^{(x-v)k} v^{-s} \\ &= f^{-1} \sum_{k} \left[\sum_{(x,f)=1} \chi(x) \zeta^{kx} \right] \sum_{v=1}^{\infty} \zeta^{-vk} v^{-s} \\ &= f^{-1} \sum_{k=0}^{f-1} \tau_k(\chi) \sum_{v=1}^{\infty} \zeta^{-vk} v^{-s}, \end{aligned}$$

say, where $\tau_k(\chi)$ is the Gauß sum, with $\tau_0(\chi) = 0$ for $\chi \neq \chi_0$. For $k \neq 0$, the partial sums $\sum_{v=1}^{n} \zeta^{-vk}$ are bounded. Proposition 8.8 implies that the last series is convergent for $\Re(s) > 0$ (and represents $L(s,\chi)$ by analytic continuation). Thus

$$L(1,\chi) = f^{-1} \sum_{k=1}^{f-1} \tau_k(\chi) \sum_{v=1}^{\infty} \zeta^{-vk} v^{-1}.$$

Thus

$$L(1,\chi) = -f^{-1} \sum_{k=1}^{f-1} \tau_k(\chi) \log(1 - \zeta^{-k})$$

($\chi \neq \chi_0$, $f = f_\chi$).

Exercise. If $(a, f_\chi) = 1$, then $\tau_a(\chi) = 0$.

Theorem 9.1

(a) If χ is odd (i.e. $\chi(-1) = -1$), then

$$L(1,\chi) = \frac{\pi i \tau(\chi)}{f^2} \sum_{0<k<f} \overline{\chi(k)} k.$$

(b) If χ is even ($\chi(-1) = 1$), then

$$L(1,\chi) = -\frac{\tau(\chi)}{f} \sum_{k \pmod f} \overline{\chi(k)} \log|1-\zeta^k| = -\frac{\tau(\chi)}{f} \sum_{0<k<f} \overline{\chi(k)} \log\left(\sin\frac{\pi k}{f}\right).$$

Proof. Note that $\tau_a(\chi) = \overline{\chi(a)}$ for any a. Hence

$$L(1,\chi) = -f^{-1} \sum_{k=1}^{f-1} \tau_k(\chi) \log(1-\zeta^{-k}) = -\frac{\tau(\chi)}{f} \sum_{k=1}^{f-1} \overline{\chi(k)} \log(1-\zeta^{-k}).$$

Set $S = \sum_k \overline{\chi(k)} \log(1-\zeta^{-k})$. We wish to evaluate S. First

$$\begin{aligned} 1-\zeta^{-k} &= 1 - e^{-2\pi ik/f} \\ &= e^{-\pi ik/f}(e^{\pi ik/f} - e^{-\pi ik/f}) \\ &= 2ie^{-\pi ik/f} \sin\frac{\pi k}{f} \\ &= 2e^{i\left(\frac{\pi}{2} - \frac{\pi k}{f}\right)} \sin\frac{\pi k}{f}. \end{aligned}$$

If $0 < k < f$, then $\frac{\pi}{2} - \frac{\pi k}{f}$ lies in the open interval $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$. Hence

$$\begin{aligned} \log(1-\zeta^{-k}) &= \log\left(2\sin\frac{\pi k}{f}\right) + i\pi\left(frac12 - \frac{k}{f}\right), \\ \log(1-\zeta^{k}) &= \log\left(2\sin\frac{\pi k}{f}\right) - i\pi\left(\frac{1}{2} - \frac{k}{f}\right) \end{aligned}$$

provided $0 < k < f$.

(i) Assume χ is odd. Replacing k by $-k$ in the equation defining S gives

$$S = -\sum_{k \pmod f} \overline{\chi(k)} \log(1-\zeta^k).$$

Hence

$$2S = \sum_k \overline{\chi(k)}[\log(1-\zeta^{-k}) - \log(1-\zeta^k)] = 2\sum_{0<k<f} \overline{\chi(k)} i\pi\left(\frac{1}{2} - \frac{k}{f}\right).$$

Since $\sum_k \chi(k) = 0$, this implies that

$$S = -\frac{i\pi}{f} \sum_{0<k<f} \overline{\chi(k)}k,$$

and now (a) follows.

(ii) Now assume χ is even. Replacing k by $-k$ in the equation defining S gives

$$S = \sum_{k \pmod f} \overline{\chi(k)} \log(1 - \zeta^k).$$

Hence

$$\begin{aligned} 2S &= \sum_k \overline{\chi(k)}[\log(1 - \zeta^{-k}) + \log(1 - \zeta^k)] \\ &= \sum_k \overline{\chi(k)} \log|1 - \zeta^k| \\ &= 2 \sum_{0<k<f} \overline{\chi(k)} \log\left(2 \sin \frac{\pi k}{f}\right) \\ &= 2 \sum_{0<k<f} \overline{\chi(k)} \log\left(\sin \frac{\pi k}{f}\right), \end{aligned}$$

and now (b) follows.

9.2 Quadratic Fields

Let $K/\mathbb{Q}$ be a quadratic extension of discriminant d and f the conductor of K, which is $|d|$. K has a unique nontrivial character, χ, say, and χ is primitive modulo f. If $p \nmid f$, then $\chi(p) = \left(\frac{p}{d}\right)$ (the Jacobi symbol).

$$\begin{array}{c} \mathbb{Q}(\zeta_f) \\ {\scriptstyle H}\,\big| \\ K \\ \big| \\ \mathbb{Q} \end{array}$$

The Galois group of $\mathbb{Q}(\zeta_f)/\mathbb{Q}$ is $(\mathbb{Z}/n\mathbb{Z})^\times$. Let H be the unique subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$ of index 2 which contains none of the subgroups $\ker((\mathbb{Z}/f\mathbb{Z})^\times \to (\mathbb{Z}/f'\mathbb{Z}))$ for divisors $f' \mid f$. $\sigma_{-1} : \zeta_f \mapsto \zeta_f^{-1}$ is complex conjugation. Hence χ is even iff K is real.

Theorem 9.2 Let K be a real quadratic field of discriminant d. Then the class number of K is given by

$$h = -\frac{1}{\log \varepsilon} \sum_{0<x<\frac{d}{2}} \chi(x) \log \sin \frac{\pi x}{d},$$

where $\varepsilon > 1$ is the fundamental unit, and χ is the nonprincipal character of K.

Proof. $\zeta_K(s) = \prod_{\chi \text{ of } K} L(s,\chi)$, so $hR = |d_K|^{1/2} 2^{-1} L(1,\chi)$ in this case. So Theorem 9.1 implies that

$$h = \frac{|d_K|^{1/2}}{2R} \left(\frac{-\tau(\chi)}{f}\right) \sum_{0<k<f} \overline{\chi(k)} \log \left(\sin \frac{\pi k}{f}\right)$$

(and in this case $f = d$). The conductor-discriminant formula implies that $\tau(\chi) = |d_K|^{1/2}$. We have $\chi(f-x) = \chi(-x) = \chi(x)$, and $\sin\left(\frac{\pi(f-x)}{f}\right) = \sin \frac{\pi x}{f}$. So

$$\begin{aligned} h &= \frac{|d_K|^{1/2}}{2R} \left(\frac{-\tau(\chi)}{f}\right) \sum_{0<k<f} \overline{\chi(k)} \log \left(\sin \frac{\pi k}{f}\right) \\ &= -\frac{1}{\log \varepsilon} \sum_{0<x<\frac{d}{2}} \chi(x) \log \left(\sin \frac{\pi x}{d}\right). \end{aligned}$$

Theorem 9.3 Let $K/\mathbb{Q}$ be an imaginary quadratic extension with discriminant $-d < -4$. The class number h of K is given by

$$h = -\frac{1}{d} \sum_{0<x<d} \chi(x) x = (2 - \chi(2))^{-1} \sum_{0<x<\frac{d}{2}} \chi(x),$$

where χ is the nonprincipal character of K.

Proof. Note that with our notation, $f_\chi = d$. Then

$$h = \frac{d^{1/2}w}{2\pi R} L(1,\chi).$$

$-d < -4$, so $w = 2$. We have $R = 1$ for any imaginary quadratic field. So we obtain (cf Theorem 9.1(a))

$$h = \frac{d^{1/2}}{\pi}\left(\frac{i\pi\tau(\chi)}{f^2}\right)\sum_{0<k<f}\chi(k)k.$$

Since χ is even, $\tau(\chi) = if^{1/2}$ (conductor-discriminant formula). Hence we get $h = -\frac{1}{d}\sum_{0<x<d}\chi(x)x$, which is the first equality.

We now prove the second equality. Suppose that f is even. We have $\chi(1+f/2) = -1$ since $1 + f/2 \pmod f$ generates the kernel of $(\mathbb{Z}/f\mathbb{Z})^\times \to \left(\mathbb{Z}/\frac{f}{2}\mathbb{Z}\right)^\times$. If $(y, f) = 1$, then $1 + \frac{yf}{2} \equiv 1 + \frac{f}{2} \pmod f$, and so $\chi\left(1 + \frac{yf}{2}\right) = -1$. For any x with $(x, f) = 1$, we have $x + \frac{f}{2} \equiv x\left(1 + x^{-1}\frac{f}{2}\right) \pmod f$. Thus $\chi\left(x + \frac{f}{2}\right) = -\chi(x)$ (if $2 \mid f$). So we obtain

$$\begin{aligned} hf &= -\sum_{0<x<\frac{f}{2}}\chi(x)x - \sum_{0<x<\frac{f}{2}}\chi\left(x+\frac{f}{2}\right)\left(x+\frac{f}{2}\right) \\ &= -\sum_{0<x<\frac{f}{2}}\chi(x)x + \sum_{0<x<\frac{f}{2}}\chi(x)\left(x+\frac{f}{2}\right) \\ &= \frac{f}{2}\sum_{0<x<\frac{f}{2}}\chi(x). \end{aligned}$$

Since $\chi(2) = 0$ if $2 \mid f$, this proves the second equality when f is even.

Now suppose f is odd. We have

$$\begin{aligned} hf &= -\sum_{0<x<\frac{f}{2}}\chi(x)x - \sum_{0<x<\frac{f}{2}}\chi(f-x)(f-x) \\ &= -\sum_{0<x<\frac{f}{2}}\chi(x)x + \sum_{0<x<\frac{f}{2}}\chi(x)(f-x) \qquad (*) \\ &= \sum_{0<x<\frac{f}{2}}\chi(x)(-2x+f). \end{aligned}$$

On the other hand, we may write

$$\begin{aligned} hf &= -\sum_{\substack{0<x<f \\ x \text{ even}}} [\chi(x)x + \chi(f-x)(f-x)] \\ &= -\sum_{\substack{0<x<f \\ x \text{ even}}} [\chi(x)x - \chi(x)(f-x)] \\ &= -2\sum_{0<x<\frac{f}{2}} \chi(2x)x - 2\sum_{0<x<\frac{f}{2}} \chi(2x)x + f\sum_{0<x<\frac{f}{2}} \chi(2x) \\ &= -4\sum_{0<x<\frac{f}{2}} \chi(2x)x + f\sum_{0<x<\frac{f}{2}} \chi(2x). \end{aligned}$$

Hence

$$hf = \sum_{0<x<\frac{f}{2}} \chi(x)(-4x+f). \qquad (**)$$

$-2x(*) + (**)$ gives

$$hf(-2+\chi(2)) = -f\sum_{0<x<\frac{f}{2}} \chi(x),$$

as required.

Corollary 9.4 Suppose $p \equiv 3 \pmod 4$ is prime. Let R and N denote the number of quadratic residues and nonresidues, respectively, in the interval $\left(0, \frac{p}{2}\right)$. The class number of $\mathbb{Q}(\sqrt{-p})$ is odd. If $p \equiv 7 \pmod 8$, then $h = R - N$. If $p \equiv 3 \pmod 8$, then $h = \frac{R-N}{3}$.

Proof. The nontrivial character of $\mathbb{Q}(\sqrt{-p})$ has conductor p and is given by $\chi(x) = \left(\frac{x}{p}\right)$ (Legendre symbol). Hence $\chi(2) = (-1)^{(p^2-1)/8}$, i.e.

$$\chi(2) = \begin{cases} -1 & \text{if } p \equiv 3 \pmod 8, \\ 1 & \text{if } p \equiv 7 \pmod 8. \end{cases}$$

Theorem 9.3 implies that

$$h = (2-\chi(2))^{-1} \sum_{0<x<\frac{p}{2}} \chi(x).$$

The sum is $R - N$, and it is odd because the number of terms is odd.

Remark. Corollary 9.4 implies that $R > N$, and so the quadratic residues tend to cluster in the first half of the interval $(0, p)$.

Corollary 9.5 Let K be a real quadratic field with discriminant d, class number h, and fundamental unit ε. Let

$$\eta = \left(\prod_b \sin \frac{\pi b}{d} \right) \left(\prod_a \sin \frac{\pi a}{d} \right)^{-1},$$

where a and b run over integers in $(0, d/2)$ which are coprime to d and which satisfy $\chi(a) = 1$ and $\chi(b) = -1$, respectively. Then $\varepsilon^h = \eta$.

Proof. Exponentiate Theorem 9.2.

Remark. Suppose $p \equiv 1 \pmod 4$ is prime. The nontrivial character of $\mathbb{Q}(\sqrt{p})$ is $\chi(x) = \left(\frac{x}{p}\right)$. Since $\chi(x) = \chi(-x)$, there are as many quadratic residues in $(0, p/2)$ as there are in $(p/2, p)$. However, $\eta > 1$ since η is a power of $\varepsilon > 1$. Hence $\prod_b \sin \frac{\pi b}{d} > \prod_a \sin \frac{\pi a}{d}$. Since the function $\sin t$ is increasing on the interval $(0, \pi/2)$, it follows that the quadratic residues cluster near the beginning of the interval $(0, p/2)$.

Example. Let $p = 29$. Then the quadratic residues between 1 are 14 are 1, 4, 5, 6, 7, 9, and 13. In particular, there are five between 1 and 7 but only two between 8 and 14.

Chapter 10

Artin L-Functions

10.1 A Crash Course in Representation Theory

Let G be a finite group. If $f_1, f_2 : G \to \mathbb{C}$ are $\mathbb{C}$-valued functions on G, we define their inner product by $(f_1, f_2) = \frac{1}{|G|}\sum_{g\in G} f_1(g)\overline{f_2(g)}$. If $f : G \to \mathbb{C}$ is a $\mathbb{C}$-valued function on G and $\sigma \in G$, define $f^\sigma : G \to \mathbb{C}$ by $f^\sigma(g) = f(\sigma g \sigma^{-1})$. f is said to be a **class function** if $f^\sigma = f$ for all $\sigma \in G$. Suppose $H \leq G$, and let $f : H \to \mathbb{C}$ be a class function on H. We define a class function $\mathrm{Ind}_H^G f : G \to \mathbb{C}$ as follows: Let $g_1, \ldots, g_r$ be a collection of coset representatives of H in G. Extend f to $\widehat{f}$ on G by

$$\widehat{f}(g) = \begin{cases} f(g) & g \in H, \\ 0 & g \notin H. \end{cases}$$

Then

$$(\mathrm{Ind}_H^G f)(g) = \sum_{i=1}^{r} \widehat{f}(g_i^{-1} g g_i) = \frac{1}{|H|}\sum_{s\in G} \widehat{f}(s^{-1} g s).$$

Let f_1 be a class function on H and f_2 a class function on G. The Frobenius reciprocity theorem states that $(f_1, f_2 \mid_H)_H = (\mathrm{Ind}_H^G f_1, f_2)_G$.

How do class functions arise?

A **representation** of a finite group G is an action G on a finite-dimensional $\mathbb{C}$-vector space V, i.e. a homomorphism $\rho : G \to \mathrm{GL}(V)$. The **degree** of ρ is $\dim(V)$. The representation (ρ, V) is **irreducible** if the G-module V contains no proper submodules. Two representations (ρ, V) and (ρ', V') are **equivalent** if the G-modules V

and V' are isomorphic. Every representation (ρ, V) decomposes into a direct sum $V = V_1 \oplus \cdots \oplus V_s$ of irreducible representations. If an irreducible representation (ρ_α, V_α) is equivalent to precisely r_α representations in this direct sum decomposition, we call r_α the **multiplicity** of ρ_α in ρ, and we write $\rho = \sum_\alpha r_\alpha \rho_\alpha$. The **character** χ of a representation (ρ, V) is the function $\chi : G \to \mathbb{C}$; $\chi(\sigma) = \mathrm{Tr}(\rho(\sigma))$; this is a class function on G. Two representations are equivalent iff their characters are equal.

If $\rho = \sum_\alpha r_\alpha \rho_\alpha$, then $\chi = \sum_\alpha r_\alpha \chi_\alpha$. For irreducible characters χ_α and χ_β, we have

$$(\chi_\alpha, \chi_\beta) = \begin{cases} 0 & \text{if } \alpha \neq \beta, \\ 1 \text{if } \alpha = \beta \end{cases}$$

and

$$\sum_\alpha \chi_\alpha(\sigma)\chi_\alpha(\tau) = \begin{cases} 0 & \text{if } \langle\sigma\rangle \neq \langle\tau\rangle, \\ \frac{|G|}{|\langle\sigma\rangle|} \text{if } \langle\sigma\rangle = \langle\tau\rangle, \end{cases}$$

where $\langle\sigma\rangle$ and $\langle\tau\rangle$ are the conjugacy classes of σ and τ.

Every class function on G is a $\mathbb{C}$-linear combination of characters χ of irreducible representations. A class function which is a $\mathbb{Z}$-linear combination of characters is called a **generalized character**.

For each $g \in G$, define a symbol x_g, and consider the $\mathbb{C}$-vector space $V = \bigoplus_{g \in G} \mathbb{C} x_g$. Then $\dim V = |G|$. The **regular representation** $\mathrm{reg}_G : G \to \mathrm{GL}(V)$ is defined by $\sigma \mapsto \{x_g \mapsto x_{\sigma g}\}$. Then

$$\chi_{\mathrm{reg}_G}(\sigma) = \begin{cases} |G| & \text{if } \sigma = e, \\ 0 & \text{if } \sigma \neq e. \end{cases}$$

We have $\chi_{\mathrm{reg}_G} = \sum_\alpha \chi_\alpha(1)\chi_\alpha$ and $\mathrm{reg}_G = \mathrm{Ind}_{\{e\}}^G \mathbb{1}$, where $\mathbb{1}$ denotes the trivial character on the subgroup $\{e\}$.

10.2 Induced Modules

If $H \leq G$ and V is an H-module, then we may define a G-module $W := \mathrm{Ind}_H^G(V)$ called the **induced G-module**. $W = \{f : G \to V, f(\tau x) = f(x) \text{ for all } \tau \in H\}$.

The action of $\sigma \in G$ on $f \in W$ is $(\sigma f)(x) = f(x\sigma)$. There is a canonical H-homomorphism $\pi : \mathrm{Ind}_H^G V \to V$, $\pi(f) = f(1)$. This maps the H-submodule $V' = \{f \in \mathrm{Ind}_H^G V : f(x) = 0 \text{ for all } x \notin H\}$ isomorphically onto V. Identify V' with V. Then with this identification, $\mathrm{Ind}_H^G V = \bigoplus_{\sigma \in G/H} \sigma V$. (Exercise.) ($\sigma$ runs over a system of left coset representatives of H in G.)

$$\begin{array}{ccc} L & \text{——} & \mathfrak{P} \\ {\scriptstyle G}\big| & & \big| \\ K & \text{——} & \mathfrak{p} \end{array}$$

Let L/K be Galois with $G = \mathrm{Gal}(L/K)$. Let (ρ, V) be a representation of G. For brevity, we denote the action of $\sigma \in G$ on $v \in V$ by σx rather than $\rho(\sigma)v$. Set $G_{\mathfrak{P}}$ to be the decomposition group of $\mathfrak{P}$ and $I_{\mathfrak{P}}$ the inertia group of $\mathfrak{P} \mid \mathfrak{p}$.

$$\begin{array}{ccc} L_{\mathfrak{P}} & & \ell \\ \big| {\scriptstyle G_{\mathfrak{P}}} & & \big| {\scriptstyle G_{\mathfrak{P}}/I_{\mathfrak{P}}} \\ K_{\mathfrak{p}} & & k \end{array}$$

The group $G_{\mathfrak{P}}/I_{\mathfrak{P}}$ is generated by the Frobenius automorphism $\sigma_{\mathfrak{P}}$. $\sigma_{\mathfrak{P}}$ is an endomorphism of $V^{I_{\mathfrak{P}}}$, where $V^{I_{\mathfrak{P}}} = \{v \in V \mid \tau v = v \text{ for all } \tau \in I_{\mathfrak{P}}\}$. The characteristic polynomial $\det(1 - \sigma_{\mathfrak{P}} t \mid V^{I_{\mathfrak{P}}})$ depends only on $\mathfrak{p}$, and not upon the choice of prime $\mathfrak{P}$, since any other choice $\mathfrak{P}'$ gives an endomorphism which is conjugate to $\sigma_{\mathfrak{P}}$. The determinant depends only upon the character χ of ρ, since any two representations with the same character are equivalent.

Definition 10.1 Let L/K be a Galois extension with group G, and let (ρ, V) be a representation of G with character χ. The Artin L-series of ρ (or χ) is defined by

$$L(s, \chi, L/K) = \prod_{\mathfrak{p}} \frac{1}{\det(1 - \sigma_{\mathfrak{P}}(N\mathfrak{p})^{-s} \mid V^{I_{\mathfrak{P}}})}.$$

For every $\delta > 0$, the Artin L-series converges absolutely and uniformly on the half-plane $\Re(s) \geq 1 + \delta$. This is because, in the factorization

$$\det(1 - \sigma_{\mathfrak{P}}(N\mathfrak{p})^{-s} \mid v^{I_{\mathfrak{P}}}) = \prod_{i=1}^{d} (1 - \varepsilon_i (N\mathfrak{p})^{-s}),$$

the ε_i's are roots of unity since $\sigma_{\mathfrak{P}}$ is of finite order.

Theorem 10.2

(i) For the trivial character $\chi = 1$, we obtain the Dedekind zeta function $L(s, 1, L/K) = \zeta_K(s)$.

(ii) If $L' \supseteq L \supseteq L \supseteq K$ is a larger Galois extension, then $L(s, \chi, L'/K) = L(s, \chi, L/K)$, viewing the character χ of $\mathrm{Gal}(L/K)$ as a character of $\mathrm{Gal}(L'/K)$.

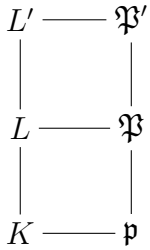
(iii) If χ_1 and χ_2 are two characters of $\mathrm{Gal}(L/K)$, then $L(s, \chi_1 + \chi_2, L/K) = L(s, \chi_1, L/K)L(s, \chi_2, L/K)$.

(iv) If M is an intermediate field $K \subseteq M \subseteq L$, ψ a character of $\mathrm{Gal}(L/M)$, and χ_ψ the induced character of $\mathrm{Gal}(L/K)$, then $L(s, \chi_\psi, L/K) = L(s, \psi, L/M)$.

Proof.

(i) Suppose that $\rho : G \to \mathrm{GL}(\mathbb{C})$ is the trivial representation $\rho(\sigma) = 1$ for all $\sigma \in G$. Then $\det(1 - \sigma_{\mathfrak{P}}(N\mathfrak{p})^{-s} \mid \mathbb{C}) = 1 - (N\mathfrak{p})^{-s}$, and so $L(s, \chi_0, L/K) = \zeta_K(s)$.

(ii)

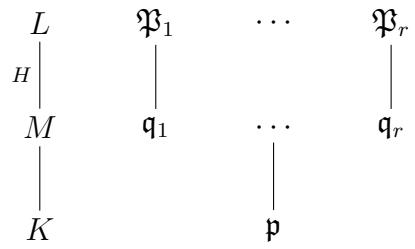


Suppose that (ρ, V) is a representation of $\mathrm{Gal}(L/K)$. Then $\mathrm{Gal}(L'/K)$ acts on that $\mathrm{Gal}(L/K)$-module V via the natural quotient map $\mathrm{Gal}(L'/K) \to \mathrm{Gal}(L/K)$. This map in turn induces homomorphisms $G_{\mathfrak{P}'} \to G_{\mathfrak{P}}$, $I_{\mathfrak{P}'} \to I_{\mathfrak{P}}$ of decomposition and inertia groups. We have $G_{\mathfrak{P}'}/I_{\mathfrak{P}'} \to G_{\mathfrak{P}}/I_{\mathfrak{P}}$, $\sigma_{\mathfrak{P}'} \mapsto \sigma_{\mathfrak{P}}$. So $(\sigma_{\mathfrak{P}'}, V^{I_{\mathfrak{P}'}}) = (\sigma_{\mathfrak{P}}, V^{I_{\mathfrak{P}}})$, i.e. $\det(1 - \sigma_{\mathfrak{P}'}t \mid V^{I_{\mathfrak{P}'}}) = \det(1 - \sigma_{\mathfrak{P}}t \mid V^{I_{\mathfrak{P}}})$, and this implies the result.

(iii) Suppose that (ρ_1, V_1) and (ρ_2, V_2) are representations of $\mathrm{Gal}(L/K)$ with characters χ_1 and χ_2. Then the direct sum $(\rho_1 \oplus \rho_2, V_1 \oplus V_2)$ is a representation with character $\chi_1 + \chi_2$ and

$$\det(1 - \sigma_{\mathfrak{P}}t \mid (V_1 \oplus V_2)^{I_{\mathfrak{P}}}) = \det(1 - \sigma_{\mathfrak{P}}t \mid V_1^{I_{\mathfrak{P}}}) \det(1 - \sigma_{\mathfrak{P}}t \mid V_2^{I_{\mathfrak{P}}}).$$

(iv) This is slightly more tricky.



Let $H = \mathrm{Gal}(L/M)$ and $G = \mathrm{Gal}(L/K)$. Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ be the distinct primes of M lying above $\mathfrak{p}$. For each $i = 1, \ldots, r$, let $\mathfrak{P}_i$ be a prime of L lying above $\mathfrak{q}_i$. Set G_i to be the decomposition group of $\mathfrak{P}_i/\mathfrak{p}$, I_i the inertia group of $\mathfrak{P}_i/\mathfrak{q}_i$. Let f_i be the degree of $\mathfrak{q}_i$ over $\mathfrak{p}$. Then $f_i = \frac{[G_i:I_i]}{[H_i:I_i]} = [G_i : H_i I_i]$. Also $N\mathfrak{q}_i = (N\mathfrak{p})^{f_i}$. Choose an element $\tau_i \in G$ such that $\mathfrak{P}_i = \mathfrak{P}_i^{\tau_i}$. Then $G_i = \tau_i^{-1} G_1 \tau_i$ and $I_i = \tau_i^{-1} I_1 \tau_i$. Let $\sigma \in G_1$ be such that $\sigma \mapsto \sigma_{\mathfrak{P}_1}$ under the map $G_1 \to G_1/I_1$. Then $\sigma_i := \tau_i^{-1}\sigma\tau_i \in G_i$ is mapped to $\sigma_{\mathfrak{P}_i} \in G_i/I_i$. The image of $\sigma_i^{f_i}$ in H_i/I_i' is the Frobenius of $\mathfrak{P}_i/\mathfrak{q}_i$. Now let $\rho : H \to \mathrm{GL}(W)$ be a representation of H with character ψ. Then χ_ψ is the character of the induced representation $\mathrm{Ind}_H^G(\rho)$ of G on $V = \mathrm{Ind}_H^G(W)$. We have to show

$$\det(1 - \sigma t \mid v^{I_1}) = \prod_{i=1}^{r} \det(1 - \sigma_i^{f_i} t^{f_i} \mid W^{I_i'}). \qquad (\dagger)$$

We now reduce to the case of $G = G_1$ and $r = 1$. Conjugation of the right side of (†) by τ_i gives

$$\det(1 - \sigma_i^{f_i} t^{f_i} \mid W^{I_i'}) = \det(1 - \sigma_i^{f_i} t^{f_i} \mid (\tau_i W)^{I_1 \cap \tau_i H \tau_i^{-1}}) \qquad (*)$$

and $f_i = [G_i : (G_i \cap \tau_i H \tau_i^{-1}) \cdot I_i]$. For each i, choose a system of left representatives φ_{ij} of G_1 modulo $G_i \cap \tau_i H \tau_i^{-1}$. Check that $\{\varphi_{ij}\tau_i\}$ is a system of left representatives of G modulo H. Hence $V = \bigoplus_{i,j} \varphi_{ij}\tau_i W$. Set $V = \bigoplus_j \varphi_{ij}\tau_i W$. This gives a decomposition $V = \bigoplus_i V_i$ of V as a G_1-module, so we have

$$\det(1 - \sigma t \mid V^{I_1}) = \prod_{i=1}^{r} \det(1 - \sigma t \mid V_i^{I_1}). \qquad (\ddagger)$$

Hence comparing (†), (∗), and (‡), it suffices to prove that

$$\det(1 - \sigma t \mid V_i^{I_1}) = \det(1 - \sigma^{f_i} t^{f_i} \mid (\tau_i W)^{I_1 \cap \tau_i H \tau_i^{-1}}).$$

We now simplify notation. Replace G_1 by G, I_1 by I, $G_1 \cap \tau_i H \tau_i^{-1}$ by H, f_i by $[G : HI]$, V_i by V, and $\tau_i W$ by W. Then again $V = \mathrm{Ind}_H^G(W)$, i.e. we are reduced to the case $r = 1$, $G_1 = G$.

We now show that we may assume that $I = \{1\}$. If we set $\bar{G} := G/I$, $\bar{H} = H/(I \cap H)$, then we have $V^I = \mathrm{Ind}_{\bar{H}}^{\bar{G}}(W^{I \cap H})$, for a function $f : G \to W$ in V is invariant under I iff $f(x\tau) = f(x)$ for all $\tau \in I$ iff f is a function on $\bar{G}$. Then f automatically takes values in $W^{I \cap H}$, since we have $\alpha f(x) = f(\alpha x) = f(x)$ for all $\alpha \in I \cap H$.

So we may assume that $I = \{1\}$. Then $G = \langle \sigma \rangle$ and $f = [G : H]$, so $V = \bigoplus_{i=0}^{f-1} \sigma_i W$. Let A be the matrix of σf with respect to a basis $w_1, \ldots, w_d$ of W. Write I for the $d \times d$ identity matrix. Then

$$B = \begin{pmatrix} 0 & I & \cdots & 0 \\ \vdots & \ddots & \cdots & \vdots \\ 0 & \ddots & \ddots & I \\ A & \cdots & \cdots & 0 \end{pmatrix}$$

is the matrix of σ with respect to the basis $\{\sigma^i w_j\}$. So now we get

$$\det(1 - \sigma t \mid V) = \det \begin{pmatrix} I & -tI & \cdots & 0 \\ 0 & 0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & -tI \\ tI & \cdots & \cdots & I \end{pmatrix} = \det(1 - \sigma^f t^f \mid W)$$

(multiply the first row by t and add to the second, then multiply the second row by t and add to the third, etc.).

Corollary 10.3 Let $\{\chi_\alpha\}$ denote the set of irreducible characters of G. Then

$$\zeta_L(s) = \zeta_K(s) \prod_{\chi_\alpha \neq 1} L(s, \chi_\alpha, L/K)^{\chi_\alpha(1)}.$$

Proof. Recall that for the regular representation reg_G of G, we have $\mathrm{reg}_G = \mathrm{Ind}_{\{1\}}^G \mathbb{1}$ and $\chi_{\mathrm{reg}_G} = \sum_\alpha \chi_\alpha(1)\chi_\alpha$. The result now follows immediately from Theorem 10.2.

$$\begin{array}{c} L \\ | \\ | G \\ | \\ K \end{array}$$

Question. (Artin) Is $\zeta_L(s)/\zeta_K(s)$ a homolorphic function on the entire complex plane?

Artin's Conjecture. For every irreducible character $\chi \neq 1$, the Artin L-series has an analytic continuation to the entire complex plane.

It is known that $L(s, \chi, L/K)$ has a meromorphic continuation to $\mathbb{C}$ and satisfies a functional equation.

10.3 Another Formula for the Artin L-Series

(This shows explicitly the pure dependence upon the character χ.)

$$\begin{array}{ccc} L & \text{——} & \mathfrak{P} \\ {\scriptstyle G}\,| & & | \\ K & \text{——} & \mathfrak{p} \end{array}$$

Consider all elements of $G_{\mathfrak{P}}$ which are mapped onto the Frobenius $\sigma_{\mathfrak{P}}$ under the map $G_{\mathfrak{P}} \to G_{\mathfrak{P}}/I_{\mathfrak{P}}$. Fix one such element σ; then the other such elements are in the coset $\sigma I_{\mathfrak{P}}$. Write

$$\rho(\mathfrak{p}^m) = \frac{1}{e}\sum_{\tau \in I_{\mathfrak{P}}} \rho(\sigma^m \tau),$$
$$\chi(\mathfrak{p}^m) = \frac{1}{e}\sum_{\tau \in I_{\mathfrak{P}}} \chi(\sigma^m \tau),$$
$$e = |I_{\mathfrak{P}}|.$$

We can think of these as "mean values."

Proposition 10.4 For $\Re(s) > 1$, we have

$$L(s, \chi, L/K) = \prod_{\mathfrak{p}} \frac{1}{\det(1 - \rho(\mathfrak{p})(N\mathfrak{p})^{-s} \mid V)} = \exp\left(\sum_{\mathfrak{p}} \sum_{m=1}^{\infty} \frac{\chi(p^m)}{m(N\mathfrak{p})^{ms}}\right).$$

Proof. Consider the exact sequence

$$0 \to V^I \to V \to V/V^I \to 0$$

($I = I_{\mathfrak{P}}$). Now $\rho(\mathfrak{p}) = \rho(\sigma_{\mathfrak{p}})$ on V^I. $\rho(\mathfrak{p}) = 0$ on V/V^I since

$$\rho(\mathfrak{p})v = \sum_{\tau \in I} \tau\sigma(v) \in V^{\perp}$$

for all $v \in V$. Hence $\det(1 - \rho(\mathfrak{p})t \mid V) = \det(1 - \rho(\sigma_{\mathfrak{p}}t \mid V^I))$, and so the first equality follows.

We now recall a general fact from linear algebra. If α is any endomorphism of a finite dimensional vector space V, then

$$\log \det(1 - \alpha t)^{-1} = \sum_{m=1}^{\infty} \operatorname{tr}(\alpha^m)\frac{t^m}{m} \qquad (\dagger)$$

(identity of formal power series), e.g. if $\dim V = 1$ and α is multiplication by a, then

$$\log(1 - at) = -\sum_{m=1}^{\infty} a^m \frac{t^m}{m}.$$

[For the general formula, choose a basis of V with respect to which α is upper triangular.] Now we apply this to $\alpha = \rho(\mathfrak{p})$.

We claim that $\alpha^m = \rho(\mathfrak{p}^m)$. For consider $J := \frac{1}{e}\sum_{\tau \in I} \rho(\tau)$. Then $J^2 = J$, and J commutes with $\rho(\sigma)$. So

$$\rho(\mathfrak{p}^m) = \rho(\sigma^m)J = \rho(\sigma)^m J^m = (\rho(\sigma)J)^m = \rho(\mathfrak{p})^m.$$

Now the second equality of the proposition follows from (†) together with the fact that $\mathrm{tr}(\alpha^m) = \mathrm{tr}(\rho(\mathfrak{p}_1^m)) = \chi(\mathfrak{p}^m)$.

Chapter 11

Introduction to Class Field Theory

Aim. Let K be a field. Determine the abelian extensions of K in terms of the arithmetic of K.

Let K be a number field with $[K : \mathbb{Q}] = n$.

Definition 11.1 A **divisor** $\mathfrak{M}$ of K is a formal product $\mathfrak{M}_0\mathfrak{M}_\infty$, where $\mathfrak{M}_0$ is an ideal of $\mathfrak{o}_K$ and $\mathfrak{M}_\infty$ is a (possibly empty) product of distinct, real, infinite places of K. $\mathfrak{M}_0$ is the **finite** part of $\mathfrak{M}$, and $\mathfrak{M}_\infty$ is the **infinite** part of $\mathfrak{M}$.

If L/K is a finite extension, then a divisor of K determines a divisor of L in a natural way.

Definition 11.2 Let $\mathfrak{M}$ be a divisor of K, $\alpha \in K^\times$. Write $\alpha \equiv 1 \bmod^* \mathfrak{M}$ to mean

(1) $v_\mathfrak{p}(\alpha - 1) \geq v_\mathfrak{p}(\mathfrak{M})$ for all finite primes dividing $\mathfrak{M}$.

(2) $\alpha > 0$ at all infinite places dividing $\mathfrak{M}$.

Let $P_\mathfrak{M}$ be the group of principal ideals of K which have a generator $\alpha \equiv 1 \bmod^* \mathfrak{M}$ and $I_\mathfrak{M}$ the group of fractional ideals coprime to $\mathfrak{M}$ (so $I_\mathfrak{M} = I_{\mathfrak{M}_0}$). Then $I_\mathfrak{M}/P_\mathfrak{M}$ is a finite group called the **mod $\mathfrak{M}$ ray class group**.

Example 11.3

(1) The mod $\mathfrak{o}_K$ ray class group is just the usual ideal class group.

(2) (a) Let $K/\mathbb{Q}$, $\mathfrak{M} = n$ $(n > 0)$. I_n is the set of ideals generated by rational integers coprime to n. Suppose $(r) \in P_n$. Then $r \equiv \pm 1 \pmod{n}$. Thus $I_n/P_n \simeq (\mathbb{Z}/n\mathbb{Z})^\times/\{\pm 1\}$.

(b) $K = \mathbb{Q}$, $\mathfrak{M} = n \cdot \infty$ $(n > 0)$. Then $I_{n\cdot\infty} = I_n$. If $(r) \in P_n$, then we need $|r| \equiv +1 \pmod{n}$. If $|r| \equiv -1 \pmod{n}$, then $(r) \notin P_n$. Thus $I_{n\cdot\infty}/P_{n\cdot\infty} \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.

Exercise. Let K be a real quadratic field.

$$\begin{array}{ccc} L & & \mathfrak{P} \\ {\scriptstyle G \atop \text{abelian}}\Big| & & \Big| \\ K & & \mathfrak{p} \end{array}$$

Suppose $\mathfrak{p}$ is unramified in L/K. Let $\sigma_{\mathfrak{P}}$ be the Frobenius element of $\mathfrak{p}$ in G. (This is unique since G is abelian.) Now let $\mathfrak{M}$ be a divisor of K which is divisible by all primes that ramify in L/K. We may define a group homomorphism called the **Artin map**: $(\cdot, L/K) : I_{K,\mathfrak{M}} \to \mathrm{Gal}(L/K)$ induced by the map $\mathfrak{p} \mapsto \sigma_{\mathfrak{p}} = (\mathfrak{p}, L/K)$. Then it may be shown that $(\cdot, L/K)$ is surjective and that its kernel contains the subgroup $N_{L/K}(I_{L,\mathfrak{M}})$.

Theorem 11.4 Let L/K be a finite abelian extension. Then there exists a divisor $\mathfrak{f}$ of K (the minimal such is called the **conductor** of L/K) such that the following hold:

(i) A prime $\mathfrak{p}$ ramifies in L/K iff $\mathfrak{p} \mid \mathfrak{f}$.

(ii) Suppose that $\mathfrak{M}$ is a divisor with $\mathfrak{f} \mid \mathfrak{M}$. Then there exists a subgroup H with $P_{\mathfrak{M}} \subseteq H \subseteq I_{\mathfrak{M}}$ such that the Artin map induces an isomorphism $I_{\mathfrak{M}}/H \simeq \mathrm{Gal}(L/K)$.

We have $H = P_{\mathfrak{M}} \cdot N_{L/K}(I_{\mathfrak{M}}(L))$.

Theorem 11.5 Suppose $\mathfrak{M}$ is a divisor of K, and let H be a subgroup of $I_{\mathfrak{M}}$ with $P_{\mathfrak{M}} \subseteq H \subseteq I_{\mathfrak{M}}$. Then there exists a unique abelian extension L/K, ramified only at primes dividing $\mathfrak{M}$, such that

1. $H = P_{\mathfrak{M}} \cdot N_{L/K}(I_{\mathfrak{M}}(L))$.

(ii) $I_{\mathfrak{M}}/H \simeq \mathrm{Gal}(L/K)$ via the Artin map.

Theorem 11.6 Suppose L_1/K and L_2/K are abelian extensions of conductors $\mathfrak{f}_1$ and $\mathfrak{f}_2$. Let $\mathfrak{M}$ be a multiple of $\mathfrak{f}_1\mathfrak{f}_2$, and let $H_1, H_2 \subseteq I_{\mathfrak{M}}$ be the corresponding subgroups. Then $H_1 \subseteq H_2$ iff $L_1 \supseteq L_2$.

Definition 11.7 The abelian extension associated to H in Theorem 11.5 is called the **class field** of H. If $H = P_{K,\mathfrak{M}}$, then $L := K(\mathfrak{M})$ is called the **ray class field** mod $\mathfrak{M}$.

Definition 11.8 Let $\mathfrak{M}$ be a divisor of K. Say that $\mathfrak{M}$ is **admissible** for L/K if

(i) $\mathfrak{M}$ is divisible by all of those primes of K which ramify in L/K,

(ii) $P_{K,\mathfrak{m}}$ is contained in the kernel of the Artin map $(\cdot, L/K) : I_{K,\mathfrak{M}} \to \mathrm{Gal}(L/K)$.

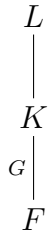
Example 11.9 Take $\mathfrak{M} = 1$ and $H = P_K$ to be the principal ideals in K. Then we obtain an abelian extension L/K with $\mathrm{Gal}(L/K) \simeq I_K/P_K$, the ideal class group of K (via the Artin map). Then Theorem 11.5 implies that L/K is everywhere unramified. Theorem 11.4 implies that any unramified extension of K has conductor $\mathfrak{f} = 1$ and corresponds to a subgroup containing $P_1 = P$. Theorem 11.6 implies that L is the maximal everywhere unramified abelian extension of K. L is called the **Hilbert class field** of K.

Consequence. Suppose $\mathfrak{p}$ is a prime ideal of K. Then $\mathfrak{p}$ splits completely in the Hilbert class field iff the decomposition group at $\mathfrak{p}$ is trivial iff $\sigma_{\mathfrak{p}} = 1$ iff $\mathfrak{p} \in P$, i.e.

$\mathfrak{p}$ is principal.

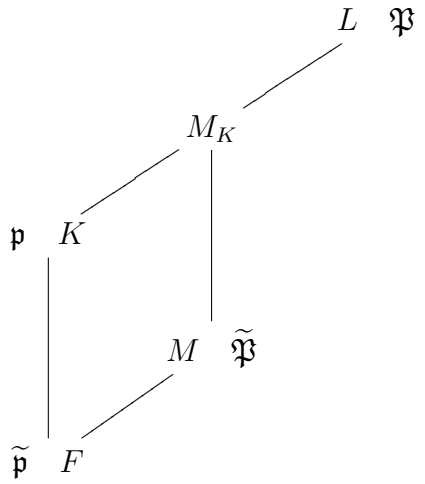
Golod and Shafarevich constructed a tower by starting with $K = \mathbb{Q}(\sqrt{-2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13})$ or $K = \mathbb{Q}(\sqrt{2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19})$.

Example 11.10 Let L/K be the Hilbert class field of K, and suppose K/F is a finite Galois extension.



We claim that G acts on $\mathrm{Gal}(L/K)$. Suppose that $\tau \in G$. Extend τ to $\widetilde{\tau} \in \mathrm{Gal}(L/F)$. Then if $\sigma \in \mathrm{Gal}(L/K)$, $\sigma^\tau = \widetilde{\tau}\sigma\widetilde{\tau}^{-1}$. (This is independent of the choice of $\widetilde{\tau}$ because $\mathrm{Gal}(L/K)$ is abelian.) Let $\mathfrak{p}$ be a prime of K. Then $\mathfrak{p} \mapsto \sigma_\mathfrak{p}$ under the Artin map $\tau\mathfrak{p} \mapsto \sigma_{\tau\mathfrak{p}} = \widetilde{\tau}\sigma_\mathfrak{p}\widetilde{\tau}^{-1} = (\sigma\mathfrak{p})^\tau$. Hence $\mathrm{Gal}(L/K)$ is isomorphic to the ideal class group of K as $\mathrm{Gal}(K/F)$-modules.

Example 11.11



Let $\mathfrak{p}$ be a prime in K unramified in L/K and $\mathfrak{P}$ a prime of L lying above $\mathfrak{p}$. $\widetilde{\mathfrak{p}}$ and $\widetilde{\mathfrak{P}}$ are the primes of F and M, respectively, lying below $\mathfrak{p}$ and $\mathfrak{P}$. Assume that $\widetilde{\mathfrak{p}}$ is unramified in M/F. Set $f = [\mathfrak{o}_K/\mathfrak{p} : \mathfrak{o}_F/\widetilde{\mathfrak{p}}]$, the residue class degree. $N_{K/F}\mathfrak{p} = \widetilde{\mathfrak{p}}^f$, $N\mathfrak{p} = (N\widetilde{\mathfrak{p}})^f$. We have $\mathfrak{o}_M \subseteq \mathfrak{o}_L$, so

$$\sigma_{\mathfrak{p}}^{L/K} \mid_M (x) \equiv x^{N\mathfrak{p}} \pmod{\widetilde{\mathfrak{P}}}$$

for all $x \in \mathfrak{o}_M$. Also

$$\sigma_{N_{K/F}(\mathfrak{p})}^{M/F} x = (\sigma_{\widetilde{\mathfrak{p}}}^{M/F})^f x \equiv x^{N\widetilde{\mathfrak{p}}^f} \pmod{\widetilde{\mathfrak{P}}} \equiv x^{N\mathfrak{p}} \pmod{\widetilde{\mathfrak{P}}}.$$

So $\sigma_{\mathfrak{p}}^{L/K} \mid_M = \sigma_{N_{K/F}(\mathfrak{p})}^{M/F}$.

Application. Suppose

(a) M is the Hilbert class field of F,

(b) L is the Hilbert class field of K.

(c) $M \cap K = F$ (e.g. K/F is totally ramified for some prime).

Then $\mathrm{Gal}(MK/K) \simeq \mathrm{Gal}(M/F)$ (via restriction). So $\mathrm{Gal}(L/K) \to \mathrm{Gal}(M/F)$ (via restriction) is surjective. We have the following diagram:

$$\begin{array}{ccc} I_K/P_K & \xrightarrow[\text{Artin}]{\sim} & \mathrm{Gal}(L/K) \\ {\scriptstyle N_{K/F}}\downarrow & & \downarrow{\scriptstyle \text{restriction}} \\ I_F/P_F & \xrightarrow{\sim} & \mathrm{Gal}(M/F) \end{array}$$

The diagram commutes (via what we proved earlier). The restriction map is surjective. Thus the norm map is surjective. Hence the class number of F divides the class number of K.

Example 11.12 (Abelian Extensions of $\mathbb{Q}$) Let $n \in \mathbb{N}$, and consider $\mathbb{Q}(\zeta_n)$. If $p \nmid n$, then $\sigma_p(\zeta_n) = \zeta_n^p$. Hence we have a map $I_n \to \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. If $(a, n) = 1$ and $a > 0$, then $(a) \mapsto \sigma_a$, and so the map is surjective.

We now wish to determine its kernel. Suppose $r \in \mathbb{Q}$, with $(r) \in I_n$. Suppose $|r| = \prod p_i^{b_i}$. Then $(r) = \prod (p_i)^{b_i}$, and so $\sigma_{(r)} = \prod \sigma_{p_i}^{b_i} = \sigma_{|r|}$, where $\sigma_{|r|}(\zeta_n) = \zeta_n^{|r|}$. $\sigma_{(r)} = 1$ iff $|r| \equiv 1 \pmod{n}$ iff $(r) \in P_{n\cdot\infty}$. Since $I_n = I_{n\cdot\infty}$, we have $I_{n\cdot\infty}/P_{n\cdot\infty} \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Now suppose that $K/\mathbb{Q}$ is abelian. Theorem 11.4 implies that there exists a divisor $\mathfrak{M}$ and a subgroup H with $P_{\mathfrak{M}} \subseteq H \subseteq I_{\mathfrak{M}}$. We may take $\mathfrak{M} = n \cdot \infty$, $n \in \mathbb{Z}$. Theorem 11.6 implies that K is contained in the field corresponding to $P_{n\cdot\infty}$, i.e. $\mathbb{Q}(\zeta_n)$.

Theorem 11.13 Let $K/\mathbb{Q}$ be an abelian extension. Then K is contained in a cyclotomic field.

Remark 11.14 Suppose that $K/\mathbb{Q}$ is abelian, and let $H \subseteq P_{n\cdot\infty}$ be the corresponding subgroup. Then the group $H/P_{n\cdot\infty}$ corresponds to a subgroup of congruence classes modulo n since $I_{n\cdot\infty}/P_{n\cdot\infty} \simeq (\mathbb{Z}/n\mathbb{Z})^\times$. Now (p) splits completely iff $\sigma_p = 1$ iff $(p) \in H$. So the primes that split completely are determined by congruence conditions modulo n.

11.1 Local Class Field Theory

Now suppose that $K/\mathbb{Q}_p$ is a finite extension. Write $K^\times = \pi^{\mathbb{Z}} \times U = \pi^{\mathbb{Z}} \times W^1 \times U_1$, where π is a local uniformizer, U is the set of local units in K, W^1 is the set of roots of unity in K of order prime to p, and $U_1 = \{x \in U : x \equiv 1 \pmod{\pi}\}$.

Theorem 11.15 Let L/K be a finite abelian extension.

(i) Then there is a map (the **local Artin map**) $K^\times \to \mathrm{Gal}(L/K)$ which induces an isomorphism $K^\times/N_{L/K}(L^\times) \simeq \mathrm{Gal}(L/K)$.

(ii) If I is the inertia subgroup of L/K, then $U_K/N_{L/K}(U_L) \simeq I$.

(iii) If L/K is unramified, then $\mathrm{Gal}(L/K)$ is cyclic (generated by the Frobenius F), and $(a, L/K) = F^{v_\pi(a)}$.

Theorem 11.16 Let $H \subseteq K^\times$ be an open subgroup of finite index. Then there exists a unique abelian extension L/K with $N_{L/K}(L^\times) = H$.

Theorem 11.17 Suppose that L_1 and L_2 are finite abelian extensions of K. Then $L_1 \subseteq L_2$ iff $N_{L_1/K}(L_1^\times) \supseteq N_{L_2/K}(L_2^\times)$.

11.2 Infinite Abelian Extensions

Let $\widehat{K}^\times$ denote the profinite completion of $K^\times$, i.e. $\varprojlim K^\times/H$. (H runs over all open subgroups of finite index.) $K^\times/H \simeq (\mathbb{Z}/m\mathbb{Z}) \times W^1 \times \frac{U_1}{U_1^{p^n}}$, for some m, n. $U_1 = \varprojlim U_1/U_1^{p^n}$, $\widehat{W} = \varprojlim W'$, $\varprojlim \mathbb{Z}/m\mathbb{Z} = \widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$. Hence $\widehat{K}^\times \simeq \pi^{\widehat{\mathbb{Z}}} \times U_1 \simeq \mathrm{Gal}(K^{\mathrm{ab}}/K)$.

11.3 Global Class Field Theory via Idèles

Now suppose K is a number field, and let $\mathfrak{p}$ be a prime of K, $K_\mathfrak{p}$ the completion of K at $\mathfrak{p}$, and $U_\mathfrak{p}$ the set of local units of $K_\mathfrak{p}$. The **idèle group** J_K of K is defined by $J_K = \{(\ldots, x_\mathfrak{p}, \ldots)\} \in \prod_\mathfrak{p} K_\mathfrak{p}^\times \mid x_\mathfrak{p} \in U_\mathfrak{p}$ for almost all $\mathfrak{p}\}$. Give $U = \prod_\mathfrak{p} U_\mathfrak{p}$ the product topology, and let U be an open subset of J_K. Then J_K becomes a locally compact group. We have $K^\times \hookrightarrow J_K$ with discrete image. The image of $K^\times$ is called the **group of principal idèles**. Define $C_K := J_K/K^\times$. C_K is called the **group of idèle classes** or the **idèle class group**.

$$\begin{array}{ccc} L & \text{---} & \mathfrak{P} \\ | & & | \\ K & \text{---} & \mathfrak{p} \end{array}$$

Suppose L/K is a finite extension. We have a norm map $N_{\mathfrak{P}/\mathfrak{p}} : L_{\mathfrak{P}} \to K_{\mathfrak{p}}$. If $x = (\ldots, x_{\mathfrak{P}}, \ldots) \in J_L$, define $N_{L/K}(x) = (\ldots, y_{\mathfrak{p}}, \ldots) \in J_K$, where $y_{\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} N_{\mathfrak{P}/\mathfrak{p}}(x_{\mathfrak{p}})$. This induces a map $N_{L/K} : C_L \to C_K$.

Theorem 11.18 Let L/K be a finite abelian extension. Then there is an isomorphism

$$\frac{J_K}{K^\times N_{L/K}(J_L)} = \frac{C_K}{N_{L/K}(C_L)} \simeq \mathrm{Gal}(L/K).$$

$\mathfrak{p}$ is unramified in L/K iff $U_{\mathfrak{p}} \subseteq K^\times N_{L/K}(J_L)$. (There is a natural embedding $U_{\mathfrak{p}} \hookrightarrow J_K$ given by $u_{\mathfrak{p}} \mapsto (1, 1, \ldots, 1, u_{\mathfrak{p}}, 1, 1, \ldots, 1).$)

Theorem 11.19 If H is an open subgroup of C_K of finite index, then there exists a unique abelian extension L/K such that $N_{L/K}(C_L) = H$.

Aliter. If $H \supseteq K^\times$ is an open subgroup of I_K of finite index, then there exists a unique abelian extension L/K such that $K^\times N_{L/K}(J_K) = H$.

Theorem 11.20 Suppose that L_1 and L_2 are finite abelian extensions of K. Then $L_1 \subseteq L_2$ iff $K^\times N_{L_1/K}(J_{L_1}) \supseteq K^\times N_{L_2/K}(J_{L_2})$.

Example. Suppose that L is the Hilbert class field of K. Since L/K is unramified everywhere, $U = \prod_{\mathfrak{p}} U_{\mathfrak{p}} \subseteq K^\times N_{L/K}(J_L)$. Since L is maximal, $K^\times U$ is the subgroup of J_K corresponding to L. We have a natural map α from J_K to the ideals of K given by

$$(\ldots, x_{\mathfrak{p}}, \ldots) \mapsto \prod_{\text{finite } \mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(x_{\mathfrak{p}})}.$$

$\ker(\alpha) = U$. Considering the induced map to the ideal class group gives $J_K/K^\times U \simeq \mathrm{Gal}(L/K)$, which is isomorphic to the ideal class group of K.

11.4 Adèles of K

$\mathbb{A}_K = \left\{(\ldots, x_{\mathfrak{p}}, \ldots) \in \prod_{\mathfrak{p}} K_{\mathfrak{p}} \mid x_{\mathfrak{p}} \in \mathfrak{o}_{K,\mathfrak{p}} \text{ for all but finitely many } \mathfrak{p}\right\}$. So $J_K = \mathbb{A}_K^{\times}$.

$$\begin{array}{ccccc} K^{\mathrm{ab}} & & & & \\ {\scriptstyle G}\big| & {\scriptstyle L} & & & \\ K & \hookrightarrow & J_K & \hookrightarrow & \mathbb{A}_K^{\times} \end{array}$$

Chapter 12

Problems

1. Which of the following numbers are algebraic integers:
   (a) $\sqrt[12]{15}(\sqrt[39]{7} + \sqrt[7]{39})$
   (b) $\frac{1+i}{\sqrt{2}}$
   (c) $\frac{1+\sqrt[3]{10}+\sqrt[3]{100}}{3}$

2. (a) Let d be a squarefree integer. Find the ring of integers of $\mathbb{Q}(\sqrt{d})$.
   (b) Let d be a squarefree integer with the property that $d \equiv 1 \pmod 4$. Show that $\mathbb{Z}(\sqrt{d})$ is not a PID.

3. Let L/K be a finite, separable extension of fields (not necessarily of characteristic 0).
   (a) Show that $\mathrm{Tr}_{L/K} : L \times L \to K$; $(x, y) \mapsto \mathrm{Tr}_{L/K}(xy)$ is a nondegenerate, symmetric, K-bilinear form on L.
   (b) Show that the map $\mathrm{Tr}_{L/K} : L \to K$; $x \mapsto \mathrm{Tr}_{L/K}(x)$ is surjective.

4. Suppose that K is a number field, and let $x \in \mathfrak{o}_K$. Show that x is a unit in $\mathfrak{o}_K$ if and only if $N_{K/\mathbb{Q}}(x) = \pm 1$.

5. Let $\zeta^n = 1$ and assume that $\alpha = \frac{1}{m}\left(\sum_{i=1}^{m} \zeta^{\kappa_i}\right)$ is an algebraic integer. Show that either $\sum_{i=1}^{m} \zeta^{\kappa_i} = 0$ or $\zeta^{\kappa_1} = \cdots = \zeta^{\kappa_m}$.

6. Find the ring of integers, and calculate the discriminant of $\mathbb{Q}(\sqrt[3]{5})$.

7. Find the ring of integers, and calculate the discriminant of $\mathbb{Q}(\sqrt{2}, \sqrt{i})$.

8. Let K be a number field of degree n over $\mathbb{Q}$, and fix algebraic integers $\alpha_1, \ldots, \alpha_n \in K$. We know that $d = D(\alpha_1, \ldots, \alpha_n)$ is in $\mathbb{Z}$; we will show that $d \equiv 0$ or $1 \pmod 4$. Letting $\sigma_1, \ldots, \sigma_n$ denote the embeddings of K in $\mathbb{C}$, we know that d is the square of the determinant $|\sigma_i(\alpha_j)|$. This determinant is the sum of $n!$ terms, one for each permutation of $\{1, \ldots, n\}$. Let P denote the sum of the terms corresponding to even permutations, and let N denote the sum of the terms (without negative signs) corresponding to odd permutations. Thus $d = (P-N)^2 = (P+N)^2 - 4PN$. Complete the proof by showing that $P+N$ and PN are in $\mathbb{Z}$. In particular, we have $d(\mathbb{A} \cap K) \equiv 0$ or $1 \pmod 4$. This is known as **Stickelberger's criterion**.

9. Let $f(x) = x^3 + ax + b$, a and $b \in \mathbb{Z}$, and assume f is irreducible over $\mathbb{Q}$. Let α be a root of f.

   (a) Show that $f'(\alpha) = -(2a\alpha + 3b)/\alpha$.

   (b) Show that $2a\alpha + 3b$ is a root of $\left(\frac{x-3b}{2a}\right)^3 + a\left(\frac{x-3b}{2a}\right) + b$. Use this to find $N_{\mathbb{Q}[\alpha]/\mathbb{Q}}(2a\alpha + 3b)$.

   (c) Show that $d(\alpha) = -(4a^3 + 27b^2)$.

   (d) Suppose $\alpha^3 = \alpha + 1$. Prove that $\{1, \alpha, \alpha^2\}$ is an integral basis for $\mathbb{A} \cap \mathbb{Q}[\alpha]$. Do the same if $\alpha^3 + \alpha = 1$.

10. Let θ be a root of the polynomial $T^3 - 2T + 2$. Calculate the ring of integers of $\mathbb{Q}(\theta)$.

11. Let K be a number field with $[K : \mathbb{Q}] = n$, and let $2t$ of the n embeddings of K into $\mathbb{C}$ have complex image. By considering the action of complex conjugation on $\Delta(K/\mathbb{Q})$, show that the sign of $d(K/\mathbb{Q})$ is equal to $(-1)^t$.

12. Let K be a number field with $[K : \mathbb{Q}] = 3$. By considering the action of various Galois embeddings on $\Delta(K/\mathbb{Q})$, show that $d(K/\mathbb{Q})$ is a square if and only if $K/\mathbb{Q}$ is Galois.

13. Let $f(T) \in \mathbb{Z}[T]$ be a monic, irreducible polynomial. Let x be a root of f, and let $K = \mathbb{Q}(x)$. By expressing $1/f(T)$ in partial fractions, show that

$$\begin{aligned} \mathrm{Tr}_{K/\mathbb{Q}}(x^i/f'(x)) &= 0 \qquad 0 \le i < n-1 \\ &= 1 \qquad i = n-1. \end{aligned}$$

   Now suppose that $\mathfrak{o}_K = \mathbb{Z}[x]$. Let D^{-1} denote the image of the dual of $\mathfrak{o}_K$ under the composite homomorphism

$$\mathrm{Hom}_{\mathbb{Z}}(\mathfrak{o}_K, \mathbb{Z}) \hookrightarrow \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{Q}) \simeq K,$$

where the isomorphism is given by the trace. Show that D^{-1} is a fractional ideal and that $N(D) = |d(K/\mathbb{Q})|$.

14. Let p be an odd prime, and let ζ_p be a primitive p^{th} root of unity. Set $\Gamma = \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, and let $\chi : \Gamma \to \mathbb{C}^*$ be a character of order $n > 1$ (i.e. χ is a group homomorphism, and n is the least integer such that χ^n is the trivial homomorphism). We define the Gauß sum $\tau(\chi, \zeta_p)$ by

$$\tau(\chi, \zeta_p) = \sum_{\gamma \in \Gamma} \chi(\gamma)\zeta_p^{\gamma}.$$

(a) Show that, for $\gamma \in \Gamma$, we have

$$\tau(\chi, \zeta_p^{\gamma}) = \chi(\gamma^{-1})\tau(\chi, \zeta_p).$$

(b) Show that

$$\tau(\chi, \zeta_p)\overline{\tau(\chi, \zeta_p)} = p.$$

(Here $\bar{z}$ denotes the complex conjugate of z.)

(c) Let χ be the unique character of Γ of order 2. From (a) and (b), deduce that

$$\tau(\chi, \zeta_p) = \pm\sqrt{\left(\frac{-1}{p}\right)p}.$$

15. Describe the factorization of ideals generated by 2, 3, 5 in $\mathbb{Q}(\sqrt[3]{6})$.

16. Let θ satisfy $\theta^3 - \theta - 1 = 0$. Describe the factorization of the ideals generated by 2, 3, 5, 23 in $\mathbb{Q}(\theta)$.

17. (a) Let f be any nonconstant polynomial over $\mathbb{Z}$. Prove that f has a root (mod p) for infinitely many primes p.

(b) Let K be any number field. Prove that there are infinitely many primes P in K such that $f(P \mid p) = 1$, where p is the prime of $\mathbb{Z}$ lying under P.

(c) Prove that for each $m \in \mathbb{Z}$ there are infinitely many primes $p \equiv 1 \pmod{m}$.

(d) Let K and L be number fields, $K \subset L$. Prove that infinitely many primes of K split completely (split into $[L : K]$ distinct factors) in L.

(e) Let f be a nonconstant monic irreducible polynomial over a number ring R. Prove that f splits into linear factors (mod p) for infinitely many primes P of R.

18. Let p be a prime and a be an integer, and let (a/p) denote the Legendre symbol. Taking a to be an integer modulo p, verify that the map from $\mathbb{F}_p^*$ to $\{\pm 1\}$ given by $a \mapsto (a/p)$ is a homomorphism. Let p be an odd prime and let z be a generator of the multiplicative group $\mathbb{F}_p^*$. Show that $z^{(p-1)/2} = -1$ and hence deduce *Euler's criterion*: For any d prime to p, $d^{(p-1)/2} \equiv (d/p) \pmod{p}$.

19. Let p and q be distinct odd primes, and let w denote a primitive p^{th} root of unity in an extension of $\mathbb{F}_q$. For any $a \in \mathbb{F}_p^*$, define the Gauß sum (in an extension of $\mathbb{F}_q$) as

$$\tau(a) = \sum_{x \in \mathbb{F}_p^*} \left(\frac{x}{p}\right) w^{ax}.$$

Prove:

(a) $\tau(a) = (a/p)\tau(1)$.
(b) $\tau(1)^q = \tau(q)$.
(c) $\tau(q)^2 = (-1)^{(p-1)/2} p$.

20. For any odd n, put $\varepsilon(n) \equiv (n-1)/2 \pmod{4}$. Use (19) above to show that $\tau(1)^{q-1} = (q/p)$. By evaluating $\tau(q)^{q-1} = [\tau(q)^2]^{(q-1)/2}$ in two ways, prove *the law of quadratic reciprocity*, viz.:

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

21. For any odd n, put $\omega(n) \equiv (n^2-1)/2 \pmod{8}$. Let α be a primitive 8^{th} root of unity in an extension of $\mathbb{F}_p$, and put $\beta = \alpha + \alpha^{-1}$. Show that $\beta^2 = 2$. Using the Frobenius endomorphism $x \mapsto x^p$ and Euler's criterion to evaluate β^{p-1} in two ways, prove that $(2/p) = (-1)^{\omega(p)}$.

22. Find the class number of $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{-6})$. Hence find all the integral solutions to

(a) $x^3 = y^2 + 2$.
(b) $x^3 = y^2 + 54$.

23. For any integer n, let ζ_n denote a primitive n^{th} root of unity.

(a) If n is not a prime power, show that $1 - \zeta_n$ is a unit of $\mathbb{Q}(\zeta_n)$.
(b) Let p be a prime, and let $(m, p) = 1$. Show that $(1-\zeta_p)/(1-\zeta_p^m)$ is a unit of $\mathbb{Q}(\zeta_p)$.

24. Calculate the class number of $K := \mathbb{Q}(\sqrt[3]{2})$. Find a unit of infinite order in K.