Franz Lemmermeyer

Class Field Theory

April 30, 2007

Franz Lemmermeyer
email franz@fen.bilkent.edu.tr
http://www.rzuser.uni-heidelberg.de/~hb3/

Preface

Class field theory has a reputation of being an extremely beautiful part of number theory and an extremely difficult subject at the same time. For someone with a good background in local fields, Galois cohomology and profinite groups there exist accounts of class field theory that reach the summit (existence theorems and Artin reciprocity) quite quickly; in fact Neukirch's books show that it is nowadays possible to cover the main theorems of class field theory in a single semester.

Students who have just finished a standard course on algebraic number theory, however, rarely have the necessary familiarity with the more advanced tools of the trade. They are looking for sources that include motivational material, routine exercises, problems, and applications.

These notes aim at serving this audience. I have chosen the classical approach to class field theory for the following reasons:

1. Zeta functions and L-series are an important tool not only in algebraic number theory, but also in algebraic geometry.
2. The analytic proof of the first inequality is very simple once you know that the Dedekind zeta function has a pole of order 1 at $s = 1$.
3. The algebraic techniques involved in the classical proof of the second inequality give us results for free that have to be derived from class field theory in the idelic approach; among the is the ambiguous class number formula, Hilbert's Theorem 94, or Furtwängler's principal genus theorem.
4. Many of the central unsolved problems in modern number theory are directly connected to analytic objects. Let me just mention the Riemann conjecture for various L-functions, the Stark conjectures, the conjecture of Birch and Swinnerton-Dyer, and the whole Langlands program.

I also have tried to approach certain central results by first treating special cases; this is not particularly elegant, but it helps students to see how some of the more technical proofs evolved from relatively simple considerations.

Table of Contents

Part I. Dirichlet's Analytic Methods

Part II. Hilbert Class Fields

Part III. Takagi's Class Field Theory

Part IV. Appendix

Part I

Dirichlet's Analytic Methods

1. Dirichlet Series for Quadratic Characters

Analytic methods occupy a central place in algebraic number theory. In this chapter we introduce the basic tools of the trade provided by Dirichlet. Most of the results proved here will be generalized step by step in subsequent chapters until we finally will have all the techniques required for the proof of the First Inequality of class field theory.

Most modern accounts of class field theory give an arithmetic proof of both the First and the Second Inequality. This approach has the additional advantage of bringing out clearly the local-global aspects of class field theory. On the other hand, class number formulas and the density theorems of Dirichlet, Kronecker, Frobenius and Chebotarev are central results of algebraic number theory which every serious student specializing in number theory must be familiar with, in particular since these analytic techniques are also needed in the theory of elliptic curves (or, more generally, abelian varieties) and modular forms. In this theory, the analog of the class number formula of Dirichlet and Dedekind is the conjecture of Birch and Swinnerton-Dyer, which – together with the Riemann hypothesis – belongs to the most important open problems in number theory.

1.1 Euler

One of the earliest outstanding results of Euler was the formula

$$\frac{\pi^2}{6} = 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \ldots . \tag{1.1}$$

This is the value $\zeta(2)$ of Riemann's zeta function

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \ldots .$$

Euler's first "proof" of (1.1) was full of holes, but very beautiful. In a nutshell, here's what he did.

Fix some $\alpha \in \mathbb{R}$ with $\sin\alpha \neq 0$, and consider the function $f(x) = 1 - \frac{\sin x}{\sin \alpha}$. This function has a Taylor expansion

$$f(x) = 1 - \frac{x}{\sin\alpha} + \frac{x^3}{3!\sin\alpha} + \frac{x^5}{5!\sin\alpha} - \dots.$$

The real roots of this function are $x = 2n\pi + \alpha$ and $x = (2n+1)\pi - \alpha$.

Euler knew that two polynomials of degree n with equal roots and equal constant term (the value at $x = 0$) must be the same. Regarding $f(x)$ as a polynomial of infinite degree, he concluded that

$$\begin{aligned} f(x) &= \prod_{n=-\infty}^{\infty} \Big(1 - \frac{x}{2n\pi+\alpha}\Big)\Big(1 - \frac{x}{(2n+1)\pi-\alpha}\Big) \\ &= \Big(1 - \frac{x}{\alpha}\Big) \prod_{n=1}^{\infty} \Big(1 - \frac{x}{(2n-1)\pi-\alpha}\Big)\Big(1 + \frac{x}{(2n-1)\pi+\alpha}\Big) \\ &\qquad \Big(1 - \frac{x}{2n\pi+\alpha}\Big)\Big(1 + \frac{x}{2n\pi-\alpha}\Big). \end{aligned}$$

Expanding the right hand side and comparing coefficients yields

$$\begin{aligned} \frac{1}{\sin\alpha} &= \frac{1}{\alpha} + \sum_{n=1}^{\infty} \Big(\frac{1}{(2n-1)\pi-\alpha} \\ &\qquad - \frac{1}{(2n-1)\pi+\alpha} + \frac{1}{2n\pi+\alpha} - \frac{1}{2n\pi-\alpha}\Big), \end{aligned} \tag{1.2}$$

$$\begin{aligned} \frac{1}{\sin^2\alpha} &= \frac{1}{\alpha^2} + \sum_{n=1}^{\infty} \Big(\frac{1}{((2n-1)\pi-\alpha)^2} \\ &\qquad - \frac{1}{((2n-1)\pi+\alpha)^2} + \frac{1}{(2n\pi+\alpha)^2} - \frac{1}{(2n\pi-\alpha)^2}\Big). \end{aligned} \tag{1.3}$$

Putting $\alpha = \frac{\pi}{2}$ in (1.2) gives Leibniz's series

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} \pm \dots.$$

For $\alpha = \frac{\pi}{4}$, (1.2) produces

$$\frac{\pi}{2\sqrt{2}} = 1 + \frac{1}{3} - \frac{1}{5} - \frac{1}{7} + \frac{1}{9} + \dots,$$

which Euler credits to Newton; in fact, this formula appears in a letter from Newton to Oldenberg from October 24, 1676.

Plugging $\alpha = \frac{\pi}{2}$ into (1.3) gives

$$1 + \frac{1}{3^2} + \frac{1}{5^2} + \dots = \frac{\pi^2}{8}.$$

Euler then observes that

$$\zeta(2) = \Big(1 + \frac{1}{3^2} + \frac{1}{5^2} + \dots\Big) + \frac{1}{4}\zeta(2), \tag{1.4}$$

and this then implies $\zeta(2) = \frac{\pi^2}{6}$.

Euler's arguments for the product expansion of $f(x)$ are not convincing for two reasons: first, he only considered real roots of f; second, the functions $f(x)$ and $e^x f(x)$ have the same roots and the same constant term, so these properties do not determine f.

Euler found the formula $\zeta(2) = \frac{\pi^2}{6}$ by comparing the coefficients of x^2 in the expansions of $f(x)$; by comparing the coefficients of x^{2k}, he was able to come up with the formula

$$\zeta(2k) = (-1)^{k-1}\frac{(2\pi)^{2k}}{2(2k)!}B_{2k},$$

where the Bernoulli numbers B_k are defined by

$$\frac{xe^x}{e^x - 1} = \sum_{k=0}^{\infty} B_k \frac{x^k}{k!}.$$

Euler also found that $\zeta(s)$ has a product decomposition, which he wrote in the form

$$\zeta(s) = \frac{2^s \cdot 3^s \cdot 5^s \cdot 7^s \cdot 11^s \cdots}{(2^s-1)(3^s-1)(5^s-1)(7^s-1)(11^s-1)\cdots}.$$

Let us now introduce the functions

$$\zeta_2(s) = 1 - 2^{-s} + 3^{-s} - 4^{-s} \pm \ldots;$$

and

$$\theta(s) = 1 + 3^{-s} + 5^{-s} + 7^{-s} + \ldots;$$

then $2^{1-s}\zeta(s) = 2(2^{-s} + 4^{-s} + 6^{-s} + \ldots)$ shows that $\zeta_2(s) + 2^{1-s}\zeta(s) = \zeta(s)$, and similarly we find $\theta(s) = (1 - 2^{-s})\zeta(s)$. Euler "computed" the values of $\zeta_2(s)$ at the negative integers as follows. He started with the geometric series

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + x^4 + \ldots;$$

applying the operator $x\frac{d}{dx}$ he found

$$\frac{x}{(1-x)^2} = x + 2x^2 + 3x^3 + 4x^4 + \ldots,$$

and similarly

$$\frac{x(1+x)}{(1-x)^3} = x + 2^2x^2 + 3^2x^2 + 4^2x^4 + \ldots.$$

These expansions converge for $|x| < 1$; boldly evaluating them at $x = -1$, Euler finds

$$\begin{aligned}
\zeta_2(0) &= 1 - 1 + 1 - 1 + \ldots = \frac{1}{2}, \\
\zeta_2(-1) &= 1 - 2 + 3 - 4 + \ldots = \frac{1}{4}, \\
\zeta_2(-2) &= 1 - 2^2 + 3^2 - 4^2 + \ldots = 0, \\
\zeta_2(-3) &= 1 - 2^3 + 3^3 - 4^3 + \ldots = -\frac{1}{8}, \\
\zeta_2(-5) &= 1 - 2^5 + 3^5 - 4^5 + \ldots = -\frac{1}{4}, \\
\zeta_2(-7) &= 1 - 2^7 + 3^7 - 4^7 + \ldots = -\frac{17}{16}
\end{aligned}$$

etc. Comparing the formulas above with the values of $\theta(2k)$ resulting from (1.4), Euler found

$$\zeta_2(-1) = \frac{2 \cdot 1}{\pi^2}\,\theta(2), \qquad \zeta_2(-3) = -\frac{2 \cdot 3!}{\pi^4}\,\theta(4), \qquad \zeta_2(-5) = \frac{2 \cdot 5!}{\pi^6}\,\theta(6);$$

we remark in passing that expressing $\zeta_2(s)$ and $\theta(s)$ in terms of $\zeta(s)$, these formulas lead to the beautiful formula

$$\zeta(-k) = -\frac{B_{k+1}}{k+1}. \tag{1.5}$$

Since $B_3 = B_5 = B_7 = \ldots = 0$, the zeta function has zeros at the even negative integers; these are called the trivial zeros of the zeta function.

Euler's observations led him to the general result

$$\theta(1-2k) = (-1)^{k-1}\frac{2 \cdot (2k-1)!}{\pi^{2k}}\zeta_2(2k)$$

for all $k \in \mathbb{N}$; Euler also saw that $\theta(-2k) = 0$ for integers $k \geq 1$. Expressing these formulas in terms of the function $\zeta_2(s)$ alone, Euler found

$$\zeta_2(1-2k) = (-1)^{k-1}\frac{(2^{2k}-1)(2k-1)!}{(2^{2k-1}-1)\pi^{2k}}\zeta_2(2k).$$

Euler then made the even bolder conjecture that this formula can be "interpolated":

$$\zeta_2(1-s) = -\Gamma(s)\frac{2^s-1}{(2^{2s}-1)\pi^s}\cos\frac{\pi s}{2}\zeta_2(s)$$

for all s. Here $\Gamma(s)$ denotes the gamma function

$$\Gamma(s) = \int_0^\infty x^{s-1}e^{-x}dx$$

defined for $s > 0$, which satisfies the functional equation $\Gamma(s+1) = s\Gamma(s)$, and which has the property that $\Gamma(n+1) = n!$ for integers $n \geq 0$. We remark in passing that the gamma function was found by Euler.[1]

Rewriting Euler's conjecture in terms of the Riemann zeta function shows that this equation is equivalent to

$$\zeta(1-s) = \pi^{-s} 2^{1-s} \Gamma(s) \cos\frac{\pi s}{2} \zeta(s).$$

This functional equation was first proved by Riemann.

Euler used the product decomposition of the zeta function to improve Euclid's theorem concerning the infinitude of prime numbers by showing that $\sum_p \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \ldots$ diverges. In the next section, we will give rigorous proofs for some of Euler's results on the zeta function.

1.2 Basic Properties of the Riemann Zeta Function

The integral test immediately shows that $\zeta(s)$ converges (pointwise) for all $s > 1$. If $s = \sigma + it$ is a complex number, then $|n^s| = n^\sigma |n^{s-\sigma}| = n^\sigma |n^{it}| = n^\sigma$ shows that if a Dirichlet series $f(s) = \sum a_n n^{-s}$ converges absolutely for all real $s > \sigma$, then it converges absolutely for all $s \in \mathbb{C}$ with $\operatorname{Re} s > \sigma$.

The most important property from a number theorists point of view is Euler's product formula:

Theorem 1.1. *For all $s > 1$ we have*

$$\zeta(s) = \prod_p \frac{1}{1-p^{-s}}, \tag{1.6}$$

where the product is over all primes p.

Proof. For $s > 1$ and a fixed natural number N we have

$$Z_N(s) := \prod_{p \leq N} \frac{1}{1-p^{-s}} = \prod_{p \leq N} \sum_{k=0}^{\infty} p^{-ks} = \sum_{n \in \mathbb{N}^*} n^{-s},$$

where N^* denotes the set of natural numbers without prime factors $> N$. Thus

$$0 < \zeta(s) - Z_N(s) \leq \sum_{n > N} n^{-s},$$

and the right hand side goes to 0 as $N \longrightarrow \infty$. □

[1] In a lecture by Serre called "How to write mathematics badly" which you can find on youtube, Serre stressed that it is important to choose a title that says as little as possible about the content of the manuscript, and suggested "On a theorem of Euler" as an example.

Since the harmonic series $1 + \frac{1}{2} + \frac{1}{3} + \ldots$ diverges, the function $\zeta(s)$ goes to ∞ as $s \to 1$. In fact, the behaviour of $\zeta(s)$ in a vicinity of $s = 1$ can be described quite precisely:

Proposition 1.2. *We have* $0 < \zeta(s) - \frac{1}{s-1} < 1$ *for* $s > 1$.

Proof. For all $n \ge 2$ we have

$$\int_n^{n+1} \frac{dx}{x^s} < \frac{1}{n^s} < \int_{n-1}^{n} \frac{dx}{x^s}$$

hence

$$\int_1^{\infty} \frac{dx}{x^s} < \sum_{n=1}^{\infty} \frac{1}{n^s} < 1 + \int_1^{\infty} \frac{dx}{x^s}$$

and therefore

$$\frac{1}{s-1} < \zeta(s) < 1 + \frac{1}{s-1}.$$

This proves the claim. □

Together with Euler's product formula this immediately implies that there must be infinitely many primes: if there only were finitely many, there would be only finitely many products in Euler's formula, and this would clearly converge at $s = 1$. As Euler showed, however, the product formula implies a lot more:

Theorem 1.3. *The series* $\sum_p \frac{1}{p}$ *diverges.*

Thus not only are there infinitely many primes, there are so many that the sum over all their inverses diverges; in particular, there are "more" primes than squares.

Proof. Since $\zeta(s)$ diverges for $s \longrightarrow 1$, so does $\log \zeta(s)$. We find

$$\begin{aligned}\log \zeta(s) &= \log \prod_p \frac{1}{1-p^{-s}} = \sum_p \log \frac{1}{1-p^{-s}} = -\sum_p \log(1-p^{-s}) \\ &= \sum_p \sum_{n\ge1} \frac{1}{n} p^{-ns} = \sum_p p^{-s} + \sum_p \sum_{n\ge2} \frac{1}{n} p^{-ns}.\end{aligned}$$

We now claim that the second sum converges; in fact,

$$\begin{aligned}\sum_p \sum_{n\ge2} \frac{1}{n} p^{-ns} &< \sum_p \sum_{n\ge2} p^{-ns} = \sum_p \frac{p^{-2s}}{1-p^{-s}} = \sum_p \frac{1}{p^s(p^s-1)} \\ &\le \sum_p \frac{1}{p(p-1)} \le \sum_{n=2}^{\infty} \frac{1}{n(n-1)} = 1.\end{aligned}$$

Thus $\sum_p p^{-s} \to \infty$ as $s \to 1$. One might be tempted to think that this implies the claim, but $\lim\limits_{s\to 1+0} \sum_p p^{-s} = \sum \frac{1}{p}$ can only be derived using the continuity of $\zeta(s)$ at $s = 1$, i.e., at a place where the series for $\zeta(s)$ is not even converging. A more careful approach is the following: replace $\zeta(s)$ by $Z_N(s)$ in the proof above. Then we can form the limit for $s \to 1$ and get

$$0 \le \log Z_N(1) - \sum_p \frac{1}{p} \le 1.$$

Now letting N go to ∞ and observing that $\lim_{N\to\infty} Z_N(1) = \infty$ implies the claim. □

A different way of making the estimate above exact is the following: we have found

$$0 < \log \zeta(s) - \sum p^{-s} < 1$$

for $s > 1$. This shows that $\log \zeta(s) - \sum p^{-s}$ is bounded, i.e., that $\sum p^{-s} = \log \zeta(s) + O(1)$, where we have used Landau's big-O notation (we say that $f = g + O(h)$ is there is a constant c such that $|f(x) - g(x)| \le c \cdot h(x)$ for all x under consideration). The inequalitites $\frac{1}{s-1} < \zeta(s) < \frac{s}{s-1}$ for $s > 1$ imply $\log \zeta(s) = \log \frac{1}{s-1} + O(1)$ for all $s \in (1, 2)$, say. Thus we get

Proposition 1.4. *For all real s with $1 < s < 2$ we have*

$$\sum p^{-s} = \log \frac{1}{s-1} + O(1).$$

We will also show that the zeta function can be extended meromorphically to the half plane $\operatorname{Re} s > 0$. By Lemma 1.7 below, $\zeta_2(s)$ is analytic for $\operatorname{Re} s > 0$. Similarly we can show $\zeta_3(s) + (1 - 3^{1-s})\zeta(s)$ for

$$\zeta_3(s) = 1 + \frac{1}{2^s} - \frac{2}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} - \frac{2}{6^s} \ldots .$$

These formulas give an analytic continuation of $\zeta(s)$ for all s with $\operatorname{Re} s > 0$, except possibly where $1 - 2^{1-s} = 1 - 3^{1-s} = 0$. This happens if and only if $(1 - s)\log 2 = 2\pi i m$ and $(1 - s)\log 3 = 2\pi i n$ for integers m, n, which in turn implies $2^n = 3^m$ and hence $m = n = 0$. We have proved:

Proposition 1.5. *The Riemann zeta function $\zeta(s)$ can be extended to a meromorphic function in the half plane $\operatorname{Re} s > 0$, with a simple pole at $s = 1$.*

We next prove a couple of results concerning the convergence of Dirichlet series $f(s) = \sum_{n=1}^\infty a_n n^{-s}$. These proofs use the concept of uniform convergence. Recall that if a sequence of real-valued functions $f_1, f_2, \ldots$ converges pointwise to a function f, then f need not be continuous even if the f_i are infinitely often differentiable. If we want to transfer properties like continuity and differentiability from the f_n to the limit function f, we need something stronger than pointwise convergence. We say that a sequence of complex-valued functions $f_n : D \longrightarrow \mathbb{C}$ converges uniformly to f on D (and write $f_n \Longrightarrow f$) if for every $\varepsilon > 0$ there is an $N \in \mathbb{N}$ such that for all $x \in D$ and all $n > N$ we have $|f_n(x) - f(x)| < \varepsilon$. Thus uniform convergence means that the difference $f_n(x) - f(x)$ can be made small for all $x \in D$ at the same time.

In real analysis, we have the following classical results:

1. If $f_n \Longrightarrow f$ and the f_n are continuous, then so is f.
2. If $f_n \Longrightarrow f$, the f_n are differentiable, and if $f_n' \Longrightarrow g$, then f is differentiable and $f' = g$.

In complex analysis, things are as usual a little bit simpler: If the f_n converge uniformly to f on all compacta inside a domain D, and if the f_n are analytic, then so is f. This result justifies the introduction of the term "converges almost uniformly" for a sequence of functions on a domain D that converges uniformly on each compact subset of D.

Proposition 1.6. *If the partial sums of a Dirichlet series $f(s)$ are bounded for a specific value $s_0 \in \mathbb{C}$, then the series converges almost uniformly for* $\operatorname{Re} s > \operatorname{Re} s_0$.

Proof. Consider the partial sums $f_m(s) = \sum_{n=1}^m a_n n^{-s}$. By assumption, there is a constant $c > 0$ such that $|f_n(s_0)| < c$ for all n. Let $\sigma_0 = \operatorname{Re} s_0$, and pick a $\delta > 0$. On the half plane $\operatorname{Re} s = \sigma \ge \sigma_0 + \delta$, we have

$$\begin{aligned}\sum_{n=m+1}^{m+N} a_n n^{-s} &= \sum_{n=m+1}^{m+N} a_n n^{-s_0} n^{s_0-s} = \sum_{n=m+1}^{m+N} (f_n(s_0) - f_{n-1}(s_0)) n^{s_0-s} \\ &= \sum_{n=m+1}^{m+N} f_n(s_0) n^{s_0-s} - \sum_{n=m}^{m+N-1} f_n(s_0)(n+1)^{s_0-s} \\ &= f_{m+N}(s_0)(m+N)^{s_0-s} - f_m(s_0)(m+1)^{s_0-s} \\ &\qquad + \sum_{n=m+1}^{m+N-1} f_n(s_0)\big(n^{s_0-s} - (n+1)^{s_0-s}\big).\end{aligned}$$

Taking absolute values and using $|f_n(s_0)| < c$ we find

$$\begin{aligned}\Big|\sum_{n=m+1}^{m+N} a_n n^{-s}\Big| &\le c(m+N)^{\sigma_0-\sigma} + c(m+1)^{\sigma_0-\sigma} \\ &\qquad + c \sum_{n=m+1}^{m+N-1} \big|n^{s_0-s} - (n+1)^{s_0-s}\big|.\end{aligned}$$

In order to give a bound for the last sum, observe that $\int x^{-t-1} dx = -\frac{1}{t} x^{-t}$ for $t \ne 0$, hence $x^{-t} = -t \int x^{-t-1} dx$. Now we find

$$\begin{aligned}\left|n^{s_0-s}-(n+1)^{s_0-s}\right| &= \left|(s-s_0)\int_n^{n+1} x^{s_0-s-1}dx\right| \\ &\le |s-s_0|\int_n^{n+1} |x^{s_0-s-1}|dx \\ &\le |s-s_0|\int_n^{n+1} x^{-1-\delta}dx \\ &\le \frac{|s-s_0|}{\delta}\big[(n+1)^{-\delta}-n^{-\delta}\big].\end{aligned}$$

For all s with $|s-s_0|<C$ this then implies

$$\Big|\sum_{n=m+1}^{m+N} a_n n^{-s}\Big| \le c((m+N)^{-\delta}+(N+1)^{-\delta}) + \frac{cC}{\delta}\sum_{n=m+1}^{m+N-1}(n^{-\delta}-(n+1)^{-\delta}).$$

The last sum is a telescope sum and equals $(m+1)^{-\delta}-(m+N)^{-\delta}$, and we see

$$\Big|\sum_{n=m+1}^{m+N} a_n n^{-s}\Big| < 2cn^{-\delta} + \frac{cC}{\delta}n^{-\delta} = c\Big(2+\frac{C}{\delta}\Big)n^{-\delta}.$$

The last expression does not depend on N and tends to 0 for $n \to \infty$; this proves our claim. □

A Dirichlet series $f(s)$ need not converge anywhere; if it does converge for some $s_0 \in \mathbb{C}$, then we have just seen that it converges for all $s \in \mathbb{C}$ with $\operatorname{Re} s > \sigma = \operatorname{Re} s_0$. The minimal $\sigma \in \mathbb{R}$ with this property is called the abscissa of convergence; $f(s)$ converges for $\operatorname{Re} s > \sigma$, and does not converge for $\operatorname{Re} s < \sigma$.

Lemma 1.7. *Consider the Dirichlet series $f(s) = \sum a_n n^{-s}$. If the partial sums $A(m) = \sum_{n=1}^m a_n$ of the coefficients have the property that $|A(m)| \le cm^{\sigma_0}$ for some constants $c, \sigma_0 > 0$, then $f(s)$ is an analytic function in the half plane* $\operatorname{Re} s > \sigma_0$.

Proof. Let $\operatorname{Re} s = \sigma > \sigma_0$; then

$$\begin{aligned}\sum_{n=m+1}^{m+N} a_n n^{-s} &= A(m+N)(m+N)^{-s} - A(n)(n+1)^{-s} \\ &\quad + \sum_{n=m+1}^{m+N-1} a_n n^{-s} A(n)(n^{-s}-(n+1)^{-s}).\end{aligned}$$

The estimate involving the integral in the proof of Prop. 1.6 shows

$$\begin{aligned}
\sum_{n=m+1}^{m+N} a_n n^{-s} &\le c\big((m+N)^{\sigma_0-\sigma} + (m+1)^{\sigma_0-\sigma}\big) + c\sum_{n=m+1}^{m+N-1} n^{\sigma_0}|s| \int_n^{n+1} x^{-\sigma-1}dx \\
&\le 2cm^{\sigma_0-\sigma} + c|s|\sum n^{\sigma_0}\int_n^{n+1} x^{-\sigma-1}dx \\
&\le 2cm^{\sigma_0-\sigma} + c|s|\sum \int_n^{n+1} x^{\sigma_0-\sigma-1}dx \\
&\le 2cm^{\sigma_0-\sigma} + c|s|(\sigma_0-\sigma)^{-1}\sum_{n=m+1}^{m+N-1}\big((n+1)^{\sigma_0-\sigma} - n^{\sigma_0-\sigma}\big) \\
&\le 2cm^{\sigma_0-\sigma} + c|s|(\sigma_0-\sigma)^{-1}(n+1)^{\sigma_0-\sigma} \\
&\le c\Big(2 + \frac{|s|}{\sigma-\sigma_0}\Big)m^{\sigma_0-\sigma}.
\end{aligned}$$

This tends to 0 independently of N as $m \to \infty$. □

1.3 Quadratic Number Fields

A quadratic number field is a quadratic extension K of $\mathbb{Q}$. They all have the form $K = \mathbb{Q}(\sqrt{m}\,)$ for some squarefree integer $m \in \mathbb{Z}$. The elements of K are $a + b\sqrt{m}$ with $a, b \in \mathbb{Q}$. The conjugate of $\alpha = a + b\sqrt{m}$ is $\alpha = a - b\sqrt{m}$, and the map $\sigma : K \longrightarrow K; \alpha \longmapsto \sigma(\alpha) = \alpha'$ is the nontrivial automorphism of $K/\mathbb{Q}$. The rational numbers $N\alpha = \alpha\alpha'$ and $\operatorname{Tr}\alpha = \alpha + \alpha'$ are called the norm and the trace of α, respectively.

The ring of integers $\mathfrak{O}_K$ has the form $\mathfrak{O}_K = \mathbb{Z} \oplus \mathbb{Z}\omega$, where

$$\omega = \begin{cases} \frac{1+\sqrt{m}}{2} & \text{if } m \equiv 1 \bmod 4, \\ \sqrt{m} & \text{if } m \equiv 2, 3 \bmod 4. \end{cases}$$

The set $\{1, \omega\}$ is called an integral basis of K, and

$$\begin{vmatrix} 1 & \omega \\ 1 & \omega' \end{vmatrix}^2 = (\omega - \omega')^2$$

is called the discriminant of K. We find

$$\operatorname{disc} K = \begin{cases} m & \text{if } m \equiv 1 \bmod 4, \\ 4m & \text{if } m \equiv 2, 3 \bmod 4. \end{cases}$$

The prime ideal decomposition is governed by the Kronecker symbol $(\frac{d}{p})$ for $d = \operatorname{disc} K$; this is the usual Legendre symbol if p is an odd prime, and is defined by

$$\Big(\frac{d}{2}\Big) = \begin{cases} +1 & \text{if } d \equiv 1 \bmod 8, \\ -1 & \text{if } d \equiv 5 \bmod 8, \\ 0 & \text{if } d \equiv 0 \bmod 4. \end{cases}$$

Every prime ideal $\mathfrak{p} \neq (0)$ in $\mathfrak{O}_K$ contains a unique rational prime p, and we say that $\mathfrak{p}$ lies above p. The prime p splits, is inert, or ramifies in K according as $p\mathfrak{O}_K = \mathfrak{p}\mathfrak{p}'$ for distinct prime ideals $\mathfrak{p} \neq \mathfrak{p}'$, $p\mathfrak{O}_K$ remains prime, or $p\mathfrak{O}_K = \mathfrak{p}^2$ becomes a square.

Theorem 1.8 (Decomposition Law in Quadratic Number Fields)**.** *Let K be a quadratic number field with discriminant d. Then a prime number p*

- *splits if and only if $(\frac{d}{p}) = +1$;*
- *is inert if and only if $(\frac{d}{p}) = -1$;*
- *ramifies if and only if $p \mid d$.*

The norm $N\mathfrak{a}$ of an ideal $\mathfrak{a}$ is by definition the cardinality of the residue class group $\mathfrak{O}_K/\mathfrak{a}$. For prime ideals we have $N\mathfrak{p} = p^f$, where $f = 1$ if p splits or ramifies, and $f = 2$ if p is inert. Note that in Dedekind rings such as $\mathfrak{O}_K$, all nonzero prime ideals are maximal, hence the $\mathfrak{O}_K/\mathfrak{p}$ is a finite field. It is easily seen to contain $\mathbb{F}_p$, and we have $(\mathfrak{O}_K/\mathfrak{p} : \mathbb{F}_p) = f$.

1.4 Gauss

Riemann's zeta function can be interpreted as the sum of $N\mathfrak{a}^{-s}$ over all (principal) ideals $\mathfrak{a} = (n)$ of $\mathbb{Z}$; recall that $N(n) = \#\mathbb{Z}/n\mathbb{Z} = |n|$, and that summation over ideals means that n and $-n$ (for $n \in \mathbb{N}$) only contribute n^{-s}.

If we do the same in $K = \mathbb{Q}(i)$ and the ring of Gaussian integers $\mathbb{Z}[i]$, and if we observe that each ideal $(x + iy)$ has a unique representative in the first quadrant, then we find

$$\zeta_K(s) = \sum_{\mathfrak{a} \neq 0} N\mathfrak{a}^{-s} = \sum_{x,y \geq 0, (x,y) \neq (0,0)} \frac{1}{(x^2 + y^2)^s}.$$

Unique Factorization in $\mathbb{Z}[i]$ implies that the zeta function of $\mathbb{Z}[i]$ admits the Euler factorization

$$\zeta_K(s) = \prod_{\pi} \frac{1}{1 - N\pi^{-s}},$$

where the product is over all primes π in the first quadrant. For $\pi = 1 + i$ we get $N\pi = 2$; there are exactly two primes π above primes $p \equiv 1 \bmod 4$, and their contribution to the Euler product is $\prod\limits_{p \equiv 1 \bmod 4} \frac{1}{(1-p^{-s})^2}$. Finally, the primes $p \equiv 3 \bmod 4$ remain inert in $\mathbb{Z}[i]$ and have norm p^2, so they contribute $\prod\limits_{p \equiv 3 \bmod 4} \frac{1}{1-p^{-2s}}$. Thus we have

$$\begin{aligned}\zeta_K(s) &= \frac{1}{1-2^{-s}} \prod_{p\equiv 1 \bmod 4} \frac{1}{(1-p^{-s})^2} \prod_{p\equiv 3 \bmod 4} \frac{1}{1-p^{-2s}} \\ &= \zeta(s) \prod_{p\equiv 1 \bmod 4} \frac{1}{1-p^{-s}} \prod_{p\equiv 3 \bmod 4} \frac{1}{1+p^{-s}} \\ &= \zeta(s)L(s,\chi).\end{aligned}$$

Here Dirichlet's L-series $L(s,\chi)$ for the character $\chi = (\frac{-4}{\cdot})$ is defined, for all $s > 1$, via its Euler product

$$L(s,\chi) = \prod_p \frac{1}{1-\chi(p)p^{-s}}.$$

Since χ is a multiplicative function, it is easily shown that

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

In particular,

$$L(1,\chi) = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} \pm \ldots = \frac{\pi}{4}$$

since

$$\frac{\pi}{4} = \int_0^1 \frac{dx}{x^2+1} = \int_0^1 (1 - x^2 + x^4 - x^6 \pm \ldots)dx = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} \pm \ldots.$$

Thus not only does $L(s,\chi)$ converge for $s = 1$, it converges to some nonzero limit. Multiplying $\zeta_K(s) = \zeta(s)L(s,\chi)$ through by $s-1$ and taking limits we see

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{\pi}{4}$$

for $K = \mathbb{Q}(i)$.

The pole of the zeta function of K at $s = 1$ immediately implies that there are infinitely many prime ideals in $\mathbb{Z}[i]$, but this is of course a trivial consequence of the infinitude of primes in $\mathbb{Z}$ since there is at least one prime ideal above every rational prime.

But we can also, exactly as before, deduce that the sum $\sum \frac{1}{N\pi}$ over all primes π in $\mathbb{Z}[i]$ diverges; since the sum for primes $\pi \equiv 3 \bmod 4$ obviously converges (it is majorized by $\sum_{n\geq 9} n^{-2}$), we deduce that $\sum \frac{1}{N\pi}$ diverges, where the sum is over all odd primes of degree 1. Since there are exactly two primes of norm $p \equiv 1 \bmod 4$, we find

$$\sum \frac{1}{N\pi} = 2 \sum_{p\equiv 1 \bmod 4} \frac{1}{p},$$

and thus we conclude

$$\sum_{p \equiv 1 \bmod 4} \frac{1}{p} = \infty.$$

That the divergence of $\sum N\mathfrak{p}^{-1}$ implies a stronger result is a consequence of the fact that the divergence must result from primes of degree 1; primes of degree ≥ 2 contribute only a finite amount to $\sum N\mathfrak{p}^{-1}$. Generalizing Dirichlet's technique to arbitrary number fields will therefore imply that each number field has infinitely many prime ideals of degree 1.

1.5 Dirichlet's *L*-series

Let us now see how Dirichlet generalized this to quadratic number fields. To be precise, Dirichlet worked not with quadratic number fields, but with binary quadratic forms. Dedekind later showed that these two languages were essentially isomorphic, and gave the defnition of the zeta function of a general number field K:

$$\zeta_K(s) = \sum_{\mathfrak{a} \neq (0)} N\mathfrak{a}^{-s}$$

for all $s \in \mathbb{C}$ with $\operatorname{Re} s > 1$. Unique factorization into prime ideals implies

$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1 - N\mathfrak{p}^{-s}},$$

where the product is over all prime ideals $\mathfrak{p} \neq (0)$.

Now let $K = \mathbb{Q}(\sqrt{d}\,)$ be a quadratic number field with discriminant d, and let $\chi = (\frac{d}{\cdot})$ be its associated quadratic character; recall that $\chi(n) = 0$ if $\gcd(d, n) \neq 1)$. Define Dirichlet's L-series $L(s, \chi) = \sum \frac{\chi(n)}{n^s}$ for all $s > 1$.

Lemma 1.9. *Let ψ be a multiplicative function defined on $\mathbb{N}$. Then*

$$L(s, \psi) = \sum \frac{\psi(n)}{n^s} = \prod_p \frac{1}{1 - \psi(p)p^{-s}}$$

wherever $L(s, \psi)$ converges.

Proof. Exactly as for Riemann's zeta function. □

Now we claim

Theorem 1.10. *The Dirichlet L-series has an Euler factorization*

$$L(s, \chi) = \sum \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1 - \chi(p)p^{-s}}.$$

Moreover, we have

$$\zeta_K(s) = \zeta(s)L(s, \chi). \tag{1.7}$$

Note that $L(s,\chi) = \frac{\zeta_K(s)}{\zeta_{\mathbb{Q}}(s)}$ is the quotient of the zeta functions of K and its subfield $\mathbb{Q}$. It can be shown that these zeta functions can be extended to meromorphic functions on the whole complex plane, and that their only singularity is a simple pole at $s = 1$. Thus their quotient $L(s,\chi)$ is an entire function on the whole complex plane.

Proof. Exactly as for $\operatorname{disc} K = -4$; just use the decomposition law in quadratic number fields. □

It remains to show that $L(1,\chi)$ converges to a nonzero limit. This can be done easily with a little bit of complex analysis, and there are also quite elementary proofs using only real analysis. Our goal is a lot bigger: not only will we show that $L(1,\chi) \neq 0$, we will compute its exact value. In the next section we will present an elementary proof of $L(1,\chi) \neq 0$, then show how Dirichlet succeeded in computing the exact value of $L(1,\chi)$, and finally explain how to derive the classical class number formulas for quadratic number fields.

Consequences of the Nonvanishing of $L(1,\chi)$

Assume now that $L(1,\chi) \neq 0$ for $\chi(n) = (\frac{d}{n})$, where d is the discriminant of a quadratic number field. Imitating Euler's proof in the case $K = \mathbb{Q}$, we easily find

$$\log \zeta_K(s) = \sum N\mathfrak{p}^{-s} + O(1)$$

for $s > 1$. On the other hand, taking the log of the fundamental equation (1.7) shows that

$$\log \zeta_K(s) = \log \zeta(s) + \log L(s,\chi).$$

If $L(1,\chi) \neq 0$, then we can bound $\log L(s,\chi)$ on some interval like $(1,2)$, and get

$$\log \zeta_K(s) = \log \zeta(s) + O(1),$$

which in turn implies

$$\log \zeta_K(s) = \log \frac{1}{s-1} + O(1).$$

Finally, the contribution of primes of degree 2 to the sum $\sum N\mathfrak{p}^{-s}$ is bounded, and since there are two prime ideals above every prime p that splits in K we have

$$\sum N\mathfrak{p}^{-s} = 2 \sum_{(\frac{d}{p})=1} p^{-s} + O(1),$$

which implies

$$\sum_{(\frac{d}{p})=1} p^{-s} = \frac{1}{2} \log \frac{1}{s-1} + O(1).$$

Let P be a set of positive integers such that $\sum_{p\in P}\frac{1}{p}$ diverges. Then a subset S of P is said to have Dirichlet density δ if

$$\lim_{s\to 1+0}\frac{\sum_{p\in S}p^{-s}}{\sum_{p\in P}p^{-s}}=\delta.$$

The following properties are easy to prove:

- Finite sets have Dirichlet density 0.
- P has Dirichlet density 1.
- If S and S' are disjoint sets with Dirichlet densities δ and δ', respectively, then $S\cup S'$ has Dirichlet density $\delta+\delta'$.
- If S and S' have Dirichlet density δ and δ', respectively, and if $S\subseteq S'$, then $\delta\le\delta'$.
- If S has Dirichlet density δ, then $P\setminus S$ has Dirichlet density $1-\delta$.

If P is the set of all primes in $\mathbb{N}$, then a subset S will have Dirichlet density δ if and only if

$$\sum_{p\in S}p^{-s}\sim\delta\log\frac{1}{s-1}$$

as $s\to 1+0$. Here $f(s)\sim g(s)$ if $\lim\limits_{s\to 1+0}f(s)/g(s)=1$.

These properties then imply the following

Theorem 1.11. *Let d be the discriminant of a quadratic number fields. Then the sets of primes p with $(\frac{d}{p})=+1$ and $(\frac{d}{p})=-1$ have Dirichlet density $\frac{1}{2}$.*

Notes

Observe that we have not used the quadratic reciprocity law for the proof of Theorem 1.11; thus this result may be used to prove quadratic reciprocity if the nonvanishing of $L(1,\chi)$ also can be proved without quadratic reciprocity. In the next chapter we will give three proofs for $L(1,\chi)\neq 0$; the one that is only valid for prime discriminants uses the reciprocity law, the other two do not. This has some relevance for the history of mathematics: Legendre's attempt at proving the reciprocity law was incomplete since he had to assume the existence of certain primes p with $(\frac{d}{p})=-1$ for suitable values of d.

The proof given in Section 1.4 can be found in [Ga1889, 655–677].

I would also like to say a few things about the distinction between analytic and algebraic number theory. Nontrivial results about the distribution of primes are encoded in the behavior of the zeta function:

$$\zeta(s) \text{ has a pole at } s = 1 \Longrightarrow \sum_p p^{-s} \sim \frac{1}{s-1}$$
$$\zeta(s) \neq 0 \text{ for } \operatorname{Re} s = 1 \Longrightarrow \pi(x) \sim \frac{x}{\log x}$$
$$\zeta(s) \neq 0 \text{ for } \operatorname{Re} s > \frac{1}{2} \Longrightarrow \pi(x) = \frac{x}{\log x} + O(x^{\frac{1}{2}+\varepsilon}) \text{ for all } \varepsilon > 0.$$

Here $\pi(x)$ denotes the number of primes $p \le x$. For me, the watershed between algebraic and analytic number theory lies between the first and the second statement, and the last two statements are analytic because they deal with the distribution of zeros (more exactly they require knowledge about zero-free regions of zeta functions). Of course zeta functions and L-series are analytic objects, but they encode unique factorization into prime ideals (Euler product) and decomposition laws of prime ideals in extensions (equation (1.7)), which are algebraic objects, and their residues at poles are connected with arithmetic invariants (class numbers, units, discriminants).

Let me also remark that the convergence of the Euler product of $\zeta(s)$ for $\operatorname{Re} s > 1$ implies that $\zeta(s) \neq 0$ for all $s \in \mathbb{C}$ with $\operatorname{Re} s > 1$. In particular, $1/\zeta(s)$ is an entire function on this halfplane, and in fact Euler (who else?) found that $1/\zeta(s) = \sum \mu(n)n^{-s}$, where μ is the Moebius function.

Equation (1.7) is a special case of a conjecture of Dedekind, according to which the zeta function $\zeta_k(s)$ divides $\zeta_K(s)$ for any extension K/k of number fields; by this we mean that the quotient $\zeta_K(s)/\zeta_k(s)$ should be an entire function on the whole complex plane. This was proved for normal extensions K/k by Aramata and Brauer, and for extensions whose normal closure is solvable by Uchida and van der Waall.

The algebraic number theory that we need in this course can be found in Marcus [Ma1977]; this is an excellent book with lots of exercises. A modern and very concise introduction to algebraic number theory is Swinnerton-Dyer's [Sw2001]; it also presents the main theorems of class field theory and discusses local fields. The best introduction to local fields is probably Cassels' [Ca1986]; he also develops the theory of algebraic number fields, and studying [Ca1986] may be followed up by looking at more advanced texts like Serre's excellent [Se1980]. Finally, Davenport's [Da1980] contains a good introduction to Dirichlet series.

Exercises

1.1 Plug $\alpha = \frac{\pi}{3}$ and $\alpha = \frac{\pi}{6}$ into Euler's formula (1.2), and simplify the results as much as possible.

1.2 Show that $\lim\limits_{s \to 1+0} \cos \frac{\pi}{2} s \zeta(s) = -\frac{\pi}{2}$ (Hint: you know what happens for $(s-1)\zeta(s)$). Show that the functional equation then implies that $\zeta(0) = -\frac{1}{2}$.

1.3 Every factor on the right hand side of the Euler product (1.6) has a pole at $s = 0$, whereas the functional equation predicts $\zeta(0) = -\frac{1}{2}$. Explain.

1.4 Show that if $f(s) = \sum a_n n^{-s}$, where $a_n \in \mathbb{R}$, converges absolutely for some real number σ, then it converges absolutely for all $s \in \mathbb{C}$ with $\operatorname{Re} s > \sigma$.

1.5 Let ψ be a multiplicative function such that $|\psi(n)| < C$ for some constant $C > 0$. Show that

$$\sum_{n \geq 1} \frac{\psi(n)}{n^s} = \prod_p \frac{1}{1 - \psi(p)p^{-s}}$$

for all $s \in \mathbb{C}$ with $\operatorname{Re} s > 1$.

1.6 Let K be a number field. Show that the number of integral ideals of norm $\leq n$ is $O(n)$, and deduce that the Dedekind zeta function $\zeta_K(s) = \sum N\mathfrak{a}^{-s}$ converges for all $s \in \mathbb{C}$ with $\operatorname{Re} s > 1$.

1.7 Let K be a number field. Use unique factorization into prime ideals to show that Dedekind's zeta function admits an Euler factorization:

$$\zeta_K(s) = \sum N\mathfrak{a}^{-s} = \prod_{\mathfrak{p}} \frac{1}{1 - N\mathfrak{p}^{-s}}.$$

1.8 Let K be a quadratic number field with discriminant d. Let χ be the associated character defined by

$$\chi(n) = \begin{cases} (\frac{d}{n}) & \text{if } \gcd(d,n) = 1, \\ 0 & \text{if } \gcd(d,n) \neq 1. \end{cases}$$

Use the decomposition law in K to show that

$$\zeta_K(s) = \zeta(s)L(s,\chi)$$

for all $s \in \mathbb{C}$ with $\operatorname{Re} s > 1$.

1.9 For this exercise you need some knowledge about the decomposition of prime ideals in normal extensions. Consider the biquadratic number field $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$. It contains three quadratic subfields $k_j = \mathbb{Q}(\sqrt{d_j})$ with discriminants d_1, d_2, and d_3.

1. Show that $d_1 d_2 = d_3 m^2$ for some integer m.
2. Show that p splits completely if and only if $(d_1/p) = (d_2/p) = +1$.
3. Show that primes $p \nmid d_1 d_2$ have inertia degree 2 if and only if $(d_j/p) = +1$ for exactly one index j.
4. Show that no prime can remain inert in $K/\mathbb{Q}$.
5. Show that if $p \mid d_j$ for every j, then $p = 2$. Deduce that if p ramifies completely, then $p = 2$.
6. Discuss the possible decompositions $p\mathfrak{O}_K = \mathfrak{P}^4$, $\mathfrak{P}^2$, $\mathfrak{P}_1^2\mathfrak{P}_2^2$ in terms of the Kronecker symbols (d_j/p).

1.10 (continued) Let $\chi_j = (d_j/\cdot)$ be the quadratic character attached to the quadratic number field k_j. Show that

$$\zeta_K(s) = \zeta(s)L(s,\chi_1)L(s,\chi_2)L(s,\chi_3)$$

for all $s > 1$, and that the right hand side represents an analytic function for all $s \in \mathbb{C}$ with $\operatorname{Re} s > 0$, with a simple pole of order 1 at $s = 1$.

1.11 (continued) Show that the primes p with $(d_1/p) = (d_2/p) = +1$ have Dirichlet density $\frac{1}{4}$, and then deduce the same thing for primes with $(d_1/p) = +1$, $(d_2/p) = -1$, as well as for primes with $(d_1/p) = (d_2/p) = -1$.

1.12 (continued) Show that there are infinitely many primes in each of the residue classes $a \equiv 1, 3, 5, 7 \bmod 8$. Do the same for $a \equiv 1, 5, 7, 11 \bmod 12$.

1.13 (continued) Sketch a proof for the existence of infinitely many primes p with $(d_1/p) = (d_2/p) = (d_3/p) = +1$, where d_1, d_2, d_3 are independent (i.e., do not differ just by square factors) quadratic discriminants.

1.14 Show that (1.7) implies the decomposition law in quadratic extensions.

2. The Nonvanishing of $L(1, \chi)$ for Quadratic Characters

In this chapter I will present various techniques for showing that $L(1, \chi) > 0$ for quadratic characters $\chi = (\frac{d}{\cdot})$. Since $L(s, \chi) \geq 0$ for all $s \geq 0$, this is equivalent to showing $L(1, \chi) \neq 0$.

2.1 Dirichlet's Proof for Prime Discriminants

Let $d = \operatorname{disc} K$ be the discriminant of a quadratic number field, and let $\chi = (\frac{d}{\cdot})$ be the corresponding character. In his attempts to prove that $L(1, \chi) \neq 0$, Dirichlet computed $L(1, \chi)$ more or less explicitly. For doing so he observed that $(\frac{d}{\cdot})$ is periodic with period $m = |d|$ since $(\frac{d}{a}) = (\frac{d}{a+m})$ for all positive integers a. This follows easily from the quadratic reciprocity law (see Exercise 8).

The computation of $L(1, \chi)$ will allow us to prove that $L(1, \chi) \neq 0$ only in special cases; the calculation is, however, also indispensible for the derivation of Dirichlet's class number formula. We will now give a simplified approach to Dirichlet's calculations, and will discuss Dirichlet's original proof in the Notes.

Let us now deal with the problem of computing $L(x, \chi)$ for a general character $\chi = (\frac{d}{\cdot})$ with period $m = |d|$. The periodicity implies

$$\begin{aligned} L(1, \chi) &= \sum \chi(n) n^{-1} \\ &= \chi(1) + \chi(2) 2^{-1} + \ldots + \chi(m) m^{-1} \\ &\ + \chi(1)(m+1)^{-1} + \ldots + \chi(m)(2m)^{-1} + \ldots \\ &= \sum_{k=1}^{m} \chi(k) \sum_{n \equiv k \bmod m} n^{-1}. \end{aligned}$$

Let ζ denote a primitive m-th root of unity. Since $\sum_{a=0}^{m-1} \zeta^{ra} = \begin{cases} m & \text{if } m \mid r, \\ 0 & \text{if } m \nmid r, \end{cases}$

we can write $\sum_{n \equiv k \bmod m} n^{-1} = \frac{1}{m} \sum_{a=0}^{m-1} \zeta^{(n-k)a}$, and find

$$\begin{aligned} L(1,\chi) &= \frac{1}{m} \sum_{k \bmod m} \chi(a) \sum_{a=0}^{m-1} \zeta^{(k-n)a} n^{-1} \\ &= \frac{1}{m} \sum_{a=0}^{m-1} \Big(\sum_{k \bmod m} \chi(k) \zeta^{ak} \Big) \sum_{n=1}^{\infty} \zeta^{-na} n^{-1} \end{aligned}$$

The sum $\tau_a(\chi) = \sum_{k \bmod m} \chi(k)\zeta^{ak}$ is called a quadratic Gauss sum for the character χ. A simple calculation[1] shows that $\tau_a(\chi) = \chi(a)\tau_1(\chi)$, and we put $\tau = \tau_1(\chi)$. Another straightforward computation reveals that $\tau^2 = p^*$ for $p^* = (\frac{-1}{p})p$; in particular, $\tau \neq 0$.

The sum $\sum_{n=1}^{\infty} z^n n^{-1}$ converges for all $z \neq 1$ inside the unit disc to $-\log(1-z)$, where we have to choose the principal branch of the logarithm (the one that vanishes at $z = 0$); thus $\sum_{n=1}^{\infty} \zeta^{-na} n^{-1} = -\log(1-\zeta^a)$, and we get

$$L(1,\chi) = -\frac{\tau}{m} \sum_{a=0}^{m-1} \chi(a) \log(1-\zeta^a). \tag{2.1}$$

Evaluation of (2.1)

It remains to evaluate $\sum \chi(a) \log(1-\zeta^{-a})$. As a runs through a coprime system of residue classes, so does $-a$, hence

$$\sum_{a=1}^{m-1} \chi(a) \log(1-\zeta^{-a}) = \chi(-1) \sum_{a=1}^{m-1} \chi(a) \log(1-\zeta^a).$$

For evaluating the expression $\log(1-\zeta^a)$, we fix the primitive m-th root of unity by setting $\zeta = \exp(\frac{2\pi i}{m})$. With $\xi = \exp(\frac{\pi i}{m})$ we find $\xi^2 = \zeta$ and $1-\zeta^a = -\xi^a(\xi^a - \xi^{-a}) = -2i\xi^a \sin\frac{\pi a}{m}$. This implies $\log(1-\zeta^a) = \log(-2i\xi^a) + \log\sin\frac{\pi a}{m}$. Thus for $0 < a < m$ we get $\log(1-\zeta^a) = \log 2 + (\frac{a}{m} - \frac{1}{2})\pi i + \log\sin\frac{\pi a}{m}$ (observe that $-i = e^{-\pi i/2}$). Collecting everything we see

$$L(1,\chi) = -\chi(-1)\frac{\tau}{p} \sum_{a=1}^{p-1} \chi(a) \Big(\log\sin\frac{a\pi}{m} + \frac{a\pi i}{m} \Big)$$

where we have used $\sum \chi(a) = 0$ (see Exercise 1).

Let us pause for a moment to discuss a subtle point. The complex log function is, as you know, multivalued since $\exp(z) = \exp(z + 2\pi i)$. On the positive real axis, however, we can fix the value of log by demanding that Im $\log z = 0$ for real $z > 0$; this is also the value that is produced by the Taylor expansion of $\log(1-z)$ for real z with $|z| < 1$.

In order to select a well defined value $\log z$ for complex values of z we remove the negative real axis (including the origin); if we write $\log(1-z) =$

[1] I will provide proofs for these basic facts in an appendix.

$x + iy$ for such z with $|z| \le 1$ and $z \ne \pm 1$, then $-\pi < y < \pi$. These values of $\log(1-z)$ are said to form the principal branch of the complex log function, and by analytic continuation this holds for all z outside the negative axis. In our case, the value of $\log(1-\zeta^a)$ came from an integration, that is, from the Taylor expansion of $\log(1-z)$, hence we have to take the principal value. The imaginary part of $\log(1-\zeta^a)$ computed above is $(\frac{a}{m} - \frac{1}{2})\pi$, and this is the principal value if we choose $0 < a < m$. Thus everything involving $\log(1-\zeta^a)$ below is only valid for this particular choice of representatives of $a \bmod m$.

Next we invoke the following

Lemma 2.1. *Let χ be a quadratic character modulo m. Then*

$$\begin{cases} \sum \chi(a)a = 0 & \textit{if } \chi(-1) = 1, \\ \sum \chi(a) \log \sin \frac{a\pi}{p} = 0 & \textit{if } \chi(-1) = -1, \end{cases}$$

where the sums are over all $a \in (\mathbb{Z}/m\mathbb{Z})^\times$.

Proof. If $\chi(-1) = 1$, then $\sum \chi(a)a = \sum \chi(m-a)(m-a) = -\sum \chi(a)a$ since $\sum \chi(a) = 0$; this implies $\sum \chi(a)a = 0$.

If $\chi(-1) = -1$, then $\sum \chi(a) \log \sin \frac{a\pi}{m} = \sum \chi(m-a) \log \sin \frac{(m-a)\pi}{m} = -\sum \chi(a) \log \sin \frac{a\pi}{m}$, hence this sum vanishes. □

A character χ is called odd or even according as $\chi(-1) = -1$ or $\chi(-1) = +1$. Using this lemma, our expression for $L(1,\chi)$ simplifies to

$$L(1,\chi) = \begin{cases} \frac{\pi i \tau}{m^2} \sum\limits_{a=1}^{m-1} \chi(a)a & \text{if } \chi \text{ is odd,} \\ -\frac{\tau}{m} \sum\limits_{a=1}^{m-1} \chi(a) \log \sin \frac{a\pi}{m} & \text{if } \chi \text{ is even.} \end{cases} \tag{2.2}$$

With this equation we have expressed $L(1,\chi)$ as a finite sum that can be computed for a given character χ. In the special case where $d = p \equiv 3 \bmod 4$ is prime, the first formula immediately implies that $L(1,\chi) \ne 0$: this is because in this case, $\sum \chi(a)a \equiv \sum a = \frac{p(p-1)}{2} \equiv 1 \bmod 2$ is an odd integer and therefore $\ne 0$.

Theorem 2.2. *Let $p \equiv 3 \bmod 4$ be an odd prime and $\chi = (\frac{\cdot}{p})$. Then $L(1,\chi) > 0$.*

Simplifying (2.2) for Odd Characters

In the special case $d = -3$, we have $\tau = \zeta - \zeta^2 = \frac{-1-i\sqrt{3}}{2} - \frac{-1+i\sqrt{3}}{2} = i\sqrt{3}$, hence $L(1,\chi) = \frac{\pi i^2 \sqrt{3}}{9}(1-2) = \frac{\pi}{3\sqrt{3}} \approx 0.604599788$. Here is a table with the partial sums $L_m = \sum_{n=1}^m \chi(n)n^{-s}$ for a few values of m:

m	L_m	m	L_m
10	0.66785	11	0.57694
100	0.61123	101	0.60133
1000	0.60526	1001	0.60426
10000	0.60466	10001	0.60456

If $d = -4$, then $\tau = i - i^3 = 2i$, hence $L(1,\chi) = \frac{\pi}{4}$

Now consider discriminants $d < -4$; we would like to simplify the expression

$$h = -\frac{1}{m}\sum \chi(a)a,$$

where the sum is over all $1 \le a < m = |d|$ with $\gcd(a,d) = 1$. We have to distinguish a few cases:

1. $m = |d|$ is even. Then $\chi(a + \frac{m}{2}) = -\chi(a)$ (see Exercise 9). Then

$$\begin{aligned} hm &= -\sum_{0<a<m/2} \chi(a)a - \sum_{0<a<m/2} \chi(a+\tfrac{m}{2})(a+\tfrac{m}{2}) \\ &= -\sum_{0<a<m/2} \chi(a)a + \sum_{0<a<m/2} \chi(a)(a+\tfrac{m}{2}) \\ &= \frac{m}{2}\sum_{0<a<m/2} \chi(a), \end{aligned}$$

   hence $h = \frac{1}{2}\sum_{0<a<m/2}\chi(a)$.
2. $m = |d|$ is odd. Then $m \equiv 3 \bmod 4$, hence $\chi(-1) = -1$ by Exercise 8. This time we find

$$\begin{aligned} hm &= -\sum_{0<a<m/2} \chi(a)a - \sum_{0<a<m/2} \chi(m-a)(m-a) \\ &= -2\sum_{0<a<m/2} \chi(a)a + m\sum_{0<a<m/2} \chi(a), \end{aligned}$$

   as well as

$$\begin{aligned} hm &= -\sum_{2\mid a} \chi(a)a - \sum_{2\mid a} \chi(m-a)(m-a) \\ &= -4\sum_{0<a<m/2} \chi(2a)a + m\sum_{0<a<m/2} \chi(2a) \\ &= -4\chi(2)\sum_{0<a<m/2} \chi(a)a + m\chi(2)\sum_{0<a<m/2} \chi(a). \end{aligned}$$

   Combining these formulas shows

$$(2-\chi(2))h = \sum_{0<a<m/2} \chi(a).$$

Thus, in both cases, we have proved the following formula:

Theorem 2.3. *Let $d < -4$ denote the discriminant of a complex quadratic number field. Then*

$$h = -\frac{1}{m}\sum \chi(a)a = \frac{1}{2-\chi(2)} \sum_{0<a<m/2} \chi(a).$$

The value of the quadratic Gauss sum can be determined explicitly:

Theorem 2.4 (Gauss)**.** *For $\chi = (\frac{d}{\cdot})$, the value of the Gauss sum $\tau = \tau_1(\chi)$ is given by*

$$\tau = \begin{cases} \sqrt{d} & \text{if } d > 0, \\ i\sqrt{-d} & \text{if } d < 0. \end{cases}$$

In particular, we have

Theorem 2.5. *Let d be the discriminant of a complex quadratic number field. Then*

$$L(1,\chi) = \frac{\pi}{\sqrt{|d|}}h.$$

Since $h \geq 1$, this gives us the lower bound $L(1,\chi) \geq \frac{\pi}{\sqrt{|d|}}$ for the values of $L(1,\chi)$. If we could show that there is an $\varepsilon > 0$ such that $L(1,\chi) > \varepsilon$ for all quadratic characters χ, we could deduce that there are only finitely many complex quadratic number fields with given class number.

Specializing Theorem 2.3 to fields $\mathbb{Q}(\sqrt{-p}\,)$ for odd primes $p > 3$ we immediately get

Corollary 2.6. *Let $p \equiv 3 \bmod 4$ be prime > 3, and let R and N denote the sum of the quadratic residues and nonresidues in the interval $[1, \frac{p-1}{2}]$. Then*

$$h = \begin{cases} R - N & \text{if } p \equiv 7 \bmod 8, \\ \frac{1}{3}(R-N) & \text{if } p \equiv 3 \bmod 8. \end{cases}$$

Computing these numbers for a few small primes produces the following table:

d	-3	-4	-7	-8	-11	-15	-19	-20	-23
h	1	1	1	1	1	2	1	2	3

Dirichlet knew this numbers h: these are the class numbers of the quadratic forms with discriminant d. In fact, Jacobi had earlier conjectured (in connection with calculations involving Jacobi sums) that the class number of the complex quadratic number field $\mathbb{Q}(\sqrt{-p}\,)$ is given by the formula in Cor. 2.6.

This surprising connection between the values $L(1,\chi)$ and the class numbers of complex quadratic fields made Dirichlet look for a proof that would explain this mystery. Eventually, Dirichlet found such a proof, and we will present it in Section 2.3 below.

Note that Cor. 2.6 implies that $R > N$ (since h has the same sign as $L(1,\chi)$, hence is positive), i.e., that there are more residues than nonresidues in the interval $[1, \frac{p-1}{2}]$. The only known proofs of this elementary fact are analytic.

Simplifying (2.2) for Even Characters

The case of even characters χ is a great deal more complicated. For showing that $L(1,\chi) \neq 0$ we have to show that the expression

$$\sum_{(a,d)=1} \chi(a) \log \sin \frac{\pi a}{m}$$

does not vanish. Since $\chi(a) = \chi(m-a)$ and $\sin x = \sin(\pi - x)$, this sum can also be written in the form

$$\sum_{1 \le a < m/2} \chi(a) \log \sin \frac{\pi a}{m}.$$

Now we observe that

$$\sum \chi(a) \log \sin \frac{a\pi}{m} = \log \eta \quad \text{for} \quad \eta = \frac{\prod \sin \frac{\pi n}{m}}{\prod \sin \frac{\pi r}{m}},$$

where n and r run through the integers from 1 to $\frac{m}{2}$ with $\chi(n) = -1$ and $\chi(r) = 1$. Clearly $L(1,\chi) \neq 0$ if and only if $\eta \neq 1$.

We will now study η using Galois theory applied to cyclotomic fields. Dirichlet was able to do this using Gauss's results on cyclotomy (in modern terms, Gauss developed the Galois theory of cyclotomic extensions in Chapter VII of his Disquisitiones; general Galois theory had not yet been invented).

Lemma 2.7. *η is a unit in $\mathbb{Q}(\sqrt{d}\,)$.*

Proof. η is a product of terms of the form $\frac{\xi^n - \xi^{-n}}{\xi^r - \xi^{-r}}$, where $\xi = \exp(\frac{\pi i}{m})$, and where n and r satisfy $\chi(n) = -1$ and $\chi(r) = 1$. We will show first that each such factor is a unit in $\mathbb{Q}(\xi)$, and then show that η lies in $\mathbb{Q}(\sqrt{d}\,)$.

Now $\frac{\xi^n - \xi^{-n}}{\xi^r - \xi^{-r}} = \xi^{n-r} \frac{1-\zeta^{-n}}{1-\zeta^{-r}}$. Let s be an integer with $rs \equiv 1 \bmod m$, and let σ_s denote the automorphism of $\mathbb{Q}(\zeta)$ with $\sigma_s(\zeta) = \zeta^s$. Then $\sigma_s\big(\frac{1-\zeta^{-n}}{1-\zeta^{-r}}\big) = \frac{1-\zeta^{-ns}}{1-\zeta}$, which clearly is an algebraic integer in $\mathbb{Q}(\zeta)$. Thus $\frac{1-\zeta^{-n}}{1-\zeta^{-r}}$ is integral, and a similar argument shows that so is $\frac{1-\zeta^{-r}}{1-\zeta^{-n}}$; thus this element is a unit in $\mathbb{Q}(\zeta)$.

The root of unity ξ^{n-r} also lies in $\mathbb{Q}(\zeta)$: if d is even, then n and r must be odd, hence $\xi^{n-r} = \zeta^{(n-r)/2}$. If d is odd, then $\xi \in \mathbb{Q}(\zeta)$.

The equation $\tau^2 = d$ shows that $k = \mathbb{Q}(\tau) = \mathbb{Q}(\sqrt{d}\,)$ is a subfield of $K = \mathbb{Q}(\zeta)$. The Galois group of $K/\mathbb{Q}$ consists of all automorphisms σ_a with $\gcd(a, m) = 1$. In order to show that k is the fixed field of the group of all σ_a with $\chi(a) = +1$, we only need to show that these σ_a fix k. But this follows immediately from $\sigma_a(\tau) = \tau_a = \chi(a)\tau$.

Thus η will be a unit in k if we can show that $\sigma_a(\eta) = \eta$ for all a with $\chi(a) = +1$. The proof involves a variant of Gauss's lemma from the elementary theory of quadratic reciprocity and will be added soon. □

Lemma 2.8. *Let d be a positive discriminant, χ the corresponding character, and $\varepsilon > 1$ the fundamental unit of $\mathbb{Q}(\sqrt{d}\,)$. Then there is an integer $h \ge 0$ such that $\eta = \varepsilon^h$.*

Proof. This follows immediately from the fact that $\eta \ge 1$, i.e., that $\log \eta \ge 0$, which in turn is a consequence of $L(1, \chi) \ge 0$. □

Lemma 2.9. *assume that $d = p \equiv 1 \bmod 4$ is prime. Then $N\eta = -1$, hence the fundamental unit ε of $\mathbb{Q}(\sqrt{p}\,)$ has negative norm, and the integer h in Lemma 2.8 is odd.*

Proof. To be added soon. □

We have proved:

Theorem 2.10. *Let p be an odd prime and $\chi = (\frac{\cdot}{p})$. Then $L(1, \chi) > 0$.*

In Section 2.3 below we will show that $\sum (\frac{a}{p})a = hp$ for all primes $p \equiv 3 \bmod 4$ with $p > 3$, where h is the class number of $\mathbb{Q}(\sqrt{-p}\,)$, and that the unit η is equal to $\eta = \varepsilon^{2h}$, where ε is the fundamental unit and h the class number of $\mathbb{Q}(\sqrt{p}\,)$.

The miracle that the explicit value $L(1, \chi)$ of Dirichlet's L-function for the characters $(\frac{\cdot}{p})$ at $s = 1$ is connected to deep arithmetic invariants of the fields $\mathbb{Q}(\sqrt{p^*}\,)$ such as their class number and fundamental unit will be explained in Section 2.3 below.

2.2 Nonvanishing of Dirichlet's *L*-functions

In this section I will present an elementary proof that $L(1, \chi) \ne 0$ for quadratic Dirichlet characters χ. The idea behind it is due to Gelfond [GL1965, pp. 47–49], with some simplifications thrown in by Monsky [Mo1993].

We start by putting

$$c_n = c_\chi(n) = \sum_{d \mid n} \chi(d).$$

The function c_χ has the following properties:

Lemma 2.11. *We have*

1. $c_\chi(m)c_\chi(n) = c_\chi(mn)$ *whenever* $\gcd(m,n) = 1$*;*
2. $c_\chi(p^a) \ge 0$ *for all prime powers* p^a*;*
3. $c_\chi(n) \ge 0$ *for all integers* $n \ge 1$*;*
4. $c_\chi(n^2) \ge 1$.

Proof. 1. We have $c_\chi(mn) = \sum\limits_{d|mn} \chi(d) = \sum\limits_{e|m}\sum\limits_{f|n} \chi(ef) = c_\chi(m)c_\chi(n)$.

2. Clearly $c_\chi(p^a) = \chi(1) + \chi(p) + \chi(p^2) + \ldots + \chi(p^a) \ge 0$ since $\chi(r^2) = 1$.
3. This follows immediately from (1) and (2).
4. Observe that $c_\chi(p^k) = 0$ or $= 1$ according as k is odd or even. Now use multiplicativity.

□

The series $f(t) = \sum\limits_{n\ge1} \chi(t)\frac{t^n}{1-t^n}$ converges absolutely in $[0,1)$.

Lemma 2.12. *1. We have* $f(t) = \sum\limits_{n\ge1} c_\chi(n)t^n$.

2. $\lim\limits_{t\to1^-} f(t) = \infty$.

Proof. 1. $f(t) = \sum\limits_{n\ge1} \chi(t)\frac{t^n}{1-t^n} = \sum\limits_{n\ge1} \chi(t)\sum_{m=1}^\infty t^{mn} = \sum\limits_{N=1}^{\infty} c_\chi(N)t^N$.

2. Clearly $f(t) \ge \sum\limits_{n=1}^{\infty} t^{n^2}$, and the right hand side diverges as $t \to 1^-$.

□

Now let us see why $L(1,\chi) \ne 0$ for quadratic characters $\chi \ne 1$. Assume that $0 = L(1,\chi) = \sum \frac{\chi(n)}{n}$; then

$$-f(t) = \sum_{n\ge1} \chi(n)\Big(\frac{1}{n(1-t)} - \frac{t^n}{1-t^n}\Big) =: \sum_{n\ge1} b_n\chi(n).$$

Lemma 2.13. *We have* $b_1(t) \ge b_2(t) \ge b_3(t) \ge \ldots$ *for all* $t \in [0,1)$.

Proof. Observe that

$$\begin{aligned}(1-t)(b_n - b_{n+1}) &= \frac{1}{n} - \frac{1}{n+1} - \frac{t^n}{1+t+\ldots+t^{n-1}} + \frac{t^{n+1}}{1+t+\ldots+t^n}\\ &= \frac{1}{n(n+1)} - \frac{t^n}{(1+t+\ldots+t^{n-1})(1+t+\ldots+t^n)}\\ &\ge \frac{1}{n(n+1)} - \frac{1}{n(n+1)} = 0,\end{aligned}$$

where we have used the inequality between arithmetic and geometric means:

$$\begin{aligned} 1+t+\ldots+t^{n-1} &\ge nt^{(n-1)/2} \ge nt^{n/2}, \\ 1+t+\ldots+t^{n} &\ge (n+1)t^{n/2}. \end{aligned}$$

The claim now follows. □

Observe that χ is defined modulo d, and that $\sum_{n=1}^{d}\chi(d) = 0$. Now we use a trick called Abel summation: we have

$$\begin{aligned} \sum_{n=1}^{k}\chi(n)b_n = \chi(1)(b_1-b_2) &+ (\chi(1)+\chi(2))(b_2-b_3) \\ &+ (\chi(1)+\chi(2)+\chi(3))(b_3-b_4)+\ldots \\ &+ (\chi(1)+\ldots+\chi(k))(b_k-b_{k+1}) + (\chi(1)+\ldots+\chi(k))b_{k+1}. \end{aligned}$$

Taking absolute values, applying the triangle inequality and observing that $|\chi(1)+\ldots+\chi(m)| \le d$ and $b_m - b_{m-1} \ge 0$ yields

$$\begin{aligned} \Big|\sum_{n=1}^{k}\chi(n)b_n\Big| &\le d(b_1-b_2)+d(b_2-b-3)+\ldots+d(b_k-b_{k+1})+d|b_{k+1}| \\ &= db_1 + d(|b_{k+1}|-b_{k+1}). \end{aligned}$$

Since $\lim b_n = 0$, the last term is bounded, hence $-f(t) = \sum\chi(n)b_n$ is bounded as well, and this contradiction proves the claim.

2.3 Computation of $L(1,\chi)$

Our starting point is the basic equation

$$\zeta_K(s) = \zeta(s)L(s,\chi),$$

where $\chi(n) = (\frac{d}{n})$ and $d = \operatorname{disc} K$ is the discriminant of the quadratic number field K. Multiplying through by $s-1$ and taking limits we see that

$$\lim_{s\to 1+0}(s-1)\zeta_K(s) = \lim_{s\to 1+0}(s-1)\zeta(s)L(s,\chi) = L(1,\chi).$$

Thus if we can show that $\lim_{s\to 1+0}(s-1)\zeta_K(s)$ exists and is nonzero, we will have proved that $L(1,\chi) \ne 0$.

Gaussian Integers

In order to understand the basic idea, let us first consider the case $K = \mathbb{Q}(i)$. Let a_m denote the number of ideals of norm m; then $\zeta_K(s) = \sum a_n n^{-s}$. Put $A_m = a_1 + \ldots + a_m$; then A_m is the number of nonzero ideals of norm $\le m$.

Since K has class number 1, every ideal is principal, and since the unit group has 4 elements, $a_m = \frac{1}{4}b_m$, where b_m is the number of *elements* with norm m. Similarly, $B_m = b_1 + \ldots + b_m$ is the number of nonzero elements with norm $\leq m$.

If we represent $\mathbb{Z}[i]$ as a lattice in $\mathbb{C}$, then $B_m + 1$ is the number of lattice points inside a circle of radius $\sqrt{m}$. If m is large, this number can be approximated by the area $m\pi$ of the circle (put a unit square around each lattice point), and in fact we will show below that $|B_m - m\pi| = O(\sqrt{m}\,)$. Dividing through by 4 gives $|A_m - m\frac{\pi}{4}| = O(\sqrt{m}\,)$.

Now define a Dirichlet function

$$f(s) = \zeta_K(s) - \frac{\pi}{4}\zeta(s) = \sum_{n\geq 1}\Big(a_n - \frac{\pi}{4}\Big)n^{-s}.$$

Since the partial sums of the coefficients are $O(n^{1/2})$, $f(s)$ converges for $s > \frac{1}{2}$, and we get

$$\lim_{s\to 1+0}(s-1)\zeta_K(s) = \lim_{s\to 1+0}(s-1)f(s) + \frac{\pi}{4}\lim_{s\to 1+0}(s-1)\zeta(s) = \frac{\pi}{4}.$$

Thus we have proved that $L(1,\chi) = \frac{\pi}{4}$ is a consequence of unique factorization of $\mathbb{Z}[i]$.

Remark. Let N_t denote the number of lattice points inside a circle of radius t; we have shown above that $|N_t - \pi t^2| = O(t)$. It is believed that the error term can be improved to $O(t^{\frac{1}{2}+\varepsilon})$ for any $\varepsilon > 0$; the result is known to be false for $\varepsilon = 0$. The best known result in this direction is due to Iwaniec (1989), who proved $|N_t - \pi t^2| = O(t^{7/11})$.

Complex Quadratic Number Fields

Let K be a complex quadratic number field with discriminant $d < 0$, and let w denote the number of roots of unity in K (thus $w = 6, 4, 2$ according as $d = -3, -4$, or $d < -4$). As before, let a_m denote the number of ideals of norm m, and put $A_m = a_1 + \ldots + a_m$; then A_m is the number of nonzero ideals of norm $\leq m$.

For an ideal class $c \in \mathrm{Cl}(K)$, let $a_m(c)$ denote the number of ideals of norm m in c, and put $A_m(c) = a_1(c) + \ldots + a_m(c)$. Pick an integral ideal $\mathfrak{b} \in c^{-1}$; then for any ideal $\mathfrak{a} \in c$ with norm m, the ideal $\mathfrak{ab} = (\alpha)$ is principal and has norm $mN\mathfrak{b}$. Conversely, if $\alpha \in \mathfrak{b}$ has norm $mN\mathfrak{b}$, then $(\alpha) = \mathfrak{ab}$ for some $\mathfrak{a} \in c$ with norm m. Thus ideals of norm m in c correspond bijectively to principal ideals (α) of norm $mN\mathfrak{b}$ with $\alpha \in \mathfrak{b}$.

Let b_m denote the number of elements of $\mathfrak{b}$ with norm $mN\mathfrak{b}$, and put $B_m = b_1 + \ldots + b_m$ as before; then $A_m(c) = \frac{1}{w}B_m$. The elements of $\mathfrak{b}$ form a lattice in $\mathbb{C}$, and B_m is the number of lattice points α with $|\alpha| \leq \sqrt{mN\mathfrak{b}}$.

A (full) lattice Λ in $\mathbb{C}$ is an additive subgroup of $\mathbb{C}$ of the form $\mathbb{Z}\alpha \oplus \mathbb{Z}\beta$; the fundamental parallelogram P_Λ is the parallelogram with vertices 0, α, β, and $\alpha+\beta$. The area of P_Λ does not depend on the choice of the basis.

For counting the number of lattice points inside some circle we use the following

Lemma 2.14. *Let Λ be a lattice in $\mathbb{C}$, and let A denote the area of its fundamental parallelogram. Let C_t denote the circle with radius t around the origin. Then there is a constant $C > 0$ such that the number $N(t)$ of lattice points inside C_t satisfies*

$$\Big| N(t) - \frac{\pi t^2}{A} \Big| \le Ct$$

for all $t > 1$.

Proof. For each $\lambda \in \Lambda$ let P_λ denote the parallelogram you get by shifting the fundamental parallelogram by λ. We introduce the following numbers:

- $N_1(t)$ denotes the number of lattice points such that P_λ lies inside C_t.
- $N_2(t)$ denotes the number of lattice points such that P_λ intersects C_t.

Then we obviously have

$$N_1(t) \le N(t) \le N_2(t).$$

Since the circle contains $N_1(t)$ parallelograms P_λ, we clearly have

$$N_1(t) \cdot A \le \pi t^2,$$

and since the parallelograms counted by $N_2(t)$ cover the circle, it is also clear that

$$N_2(t) \ge \pi t^2.$$

This gives

$$N_1(t) \le \frac{\pi t^2}{A}, \quad N_2(t) \ge \frac{\pi t^2}{A}.$$

Unfortunately, these inequalities go in the wrong direction. Luckily, we can turn things around as follows.

Let δ denote the length of the long diagonal of the fundamental parallelogram (this does depend on the choice of the basis). Then for any lattice point λ inside C_t we see that $P_\lambda \subset C_{t+\delta}$, which gives

$$N(t) \le N_1(t+\delta) \le \frac{\pi(t+\delta)^2}{A}.$$

Similarly, if P_λ intersects $C_{t-\delta}$, then $P_\lambda \subset C_t$, hence

$$\frac{\pi(t-\delta)^2}{A} \le N_2(t-\delta) \le N(t).$$

Combining these inequalities we see

$$-\frac{2\pi\delta}{A}t+\frac{\pi\delta^2}{A}\le N(t)-\frac{\pi t^2}{A}\le\frac{2\pi\delta}{A}t+\frac{\pi\delta^2}{A}.$$

Thus for all $t>1$ we get

$$\Big|N(t)-\frac{\pi t^2}{A}\Big|\le Ct$$

for $C=\frac{\pi}{A}(2\delta+\delta^2)$. □

It remains to compute the area A of the fundamental parallelogram. Clearly $A=1$ for the lattice $\Lambda=\mathbb{Z}[i]$, and, more generally, $A=\sqrt{m}$ for $\Lambda=\mathbb{Z}[\sqrt{-m}\,]$.

To deal with the general case, observe first that we may choose $\mathfrak{b}$ primitive, i.e., not divisible by a rational prime ($\mathfrak{b}$ was chosen as an integral ideal in c^{-1}; but if $\mathfrak{b}=n\mathfrak{c}$ for some $n\in\mathbb{N}$ with $\mathfrak{c}$ primitive, then $\mathfrak{c}$ is an integral ideal in the same class). Let $\{1,\omega\}$ denote the standard integral basis of $\mathfrak{O}_K$ and recall that if $\alpha_1=a+b\omega$ and $\alpha_2=c+d\omega$ form a basis of $\mathfrak{b}$, then the area of the triangle spanned by 0, α_1 and α_2 is $\left|\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right|=ad-bc$ times the area of the triangle spanned by 0, 1 and ω. Since every primitive integral ideal has the form $\mathfrak{b}=a\mathbb{Z}\oplus(b+\omega)\mathbb{Z}$ for $a=N\mathfrak{b}$, we find that the area of its fundamental parallelogram is $\left|\begin{smallmatrix}a&0\\b&1\end{smallmatrix}\right|=a=N\mathfrak{b}$ times the volume of the parallelogram spanned by 0, 1 and ω; the latter is easily seen to be $\frac12\sqrt{-d}$, and this shows

Lemma 2.15. *The area of the fundamental parallelogram of Λ is $A=\frac12\sqrt{|d|}$.*

This shows that $\frac{\pi t^2}{A}=\frac{2\pi mN\mathfrak{b}}{\sqrt{-d}N\mathfrak{b}}=\frac{2\pi m}{\sqrt{-d}}$ for a circle with radius $t=\sqrt{mN\mathfrak{b}}$; thus $B_m=\frac{2\pi m}{\sqrt{-d}}+O(\sqrt{m}\,)$ and $|A_m(c)-\frac{2\pi m}{w\sqrt{-d}}|\le k_c\sqrt{m}$ for a constant k_c depending on c (and the choice of $\mathfrak{b}$ and its basis). Now we set $k=\max k_c$ as c runs through the finitely many ideal classes; then $|A_m-\frac{2\pi h}{w\sqrt{-d}}m|\le k\sqrt{m}$.

Imitating the argument from $d=-4$ we now set

$$f(s)=\zeta_K(s)-\frac{2\pi h}{w\sqrt{-d}}\zeta(s)=\sum_{n\ge1}\Big(a_n-\frac{2\pi h}{w\sqrt{-d}}\Big)n^{-s}.$$

Since the partial sums of the coefficients are $O(n^{1/2})$, $f(s)$ converges for $s>\frac12$, and we get

$$\lim_{s\to1+0}(s-1)\zeta_K(s)=\lim_{s\to1+0}(s-1)f(s)+\frac{2\pi h}{w\sqrt{-d}}\lim_{s\to1+0}(s-1)\zeta(s)=\frac{2\pi h}{w\sqrt{-d}}.$$

Thus we have proved

Theorem 2.16. *Let $d < 0$ be the discriminant of a complex quadratic number field K; let w denote the number of roots of unity in K, and h the class number of K. Then*

$$L(1,\chi) = \frac{2\pi h}{w\sqrt{-d}} \tag{2.3}$$

for $\chi = (\frac{d}{\cdot})$. In particular, we have $L(1,\chi) \neq 0$.

In the special cases $d = -4$ and $d = -8$ give us back the series of Leibniz and Newton we have come across in Chapter 1.

Dirichlet's computation of $L(1,\chi)$ for characters $\chi = (\frac{\cdot}{p})$ easily extends to all quadratic Dirichlet characters $\chi = (\frac{d}{\cdot})$ and shows

Theorem 2.17. *Let $d < 0$ be the discriminant of a complex quadratic number field K, and let $\tau = \sum \chi(a)\zeta_{|d|}^a$ be the corresponding Gauss sum. Then*

$$L(1,\chi) = \frac{\pi i \tau}{d^2} \sum_{a=1}^{|d|-1} \chi(a)a. \tag{2.4}$$

Comparing (2.3) and (2.4) yields the following class number formula:

$$h = \frac{wi\tau\sqrt{|d|}}{d^2} \sum \chi(a)a.$$

Thus in our case we get

Theorem 2.18 (Dirichlet's Class Number Formula)**.** *Let $d < 0$ be the discriminant of a complex quadratic number field K, let w denote the number of roots of unity in K, and h its class number. Then*

$$h = \frac{w}{2d} \sum_{a=1}^{|d|-1} \chi(a)a.$$

For $d = -3$ we have $w = 6$, hence $h = -\frac{3}{3}(1-2) = 1$; for $d = -4$ we have $w = 4$, hence $h = -\frac{2}{4}(1-3) = 1$. For all other quadratic fields, we have $w = 2$ and therefore

$$h = \frac{1}{d} \sum_{a=1}^{|d|-1} \chi(a)a.$$

Although this is a very beautiful formula, its practical value is small: for computing the class number of a field whose discriminant has 10 digits, you already need to compute 10^{10} Legendre symbols.

Real Quadratic Number Fields

For real quadratic number fields there is an additional difficulty coming from the existence of infinitely many units. Fortunately this problem is easily dealt with:

Lemma 2.19. *Let K be a real quadratic number field with fundamental unit $\varepsilon > 1$. Then every $\alpha \in K^\times$ has a unique associate β with the properties $\beta > 0$ and $\varepsilon^{-2} < |\beta'/\beta| \le 1$.*

Proof. Every associate of α has the form $\beta = \pm\alpha\varepsilon^m$ for some $m \in \mathbb{Z}$. The condition $\beta > 0$ determines the sign. Now $N\varepsilon = \varepsilon\varepsilon' = \pm 1$ shows that $|\varepsilon'| = 1/|\varepsilon|$, hence $|\beta'/\beta| = \varepsilon^{-2m}|\alpha'/\alpha|$; this clearly implies that there is a unique choice of m for which this expression lies between ε^{-2} and 1. □

Next we embed K into $\mathbb{R}^2$ by sending $\alpha \in K$ to the point $(\alpha, \alpha') \in \mathbb{R}^2$. Since $N\alpha = \alpha\alpha'$, elements of norm n will lie on the hyperbola $xy = n$ in $\mathbb{R}^2$. The elements β satisfying the conditions of Lemma 2.19 lie inside a domain in the right half plane ($\beta > 0$), and those in the first quadrant lie between the lines through $(1,1)$ and $(\varepsilon, \frac{1}{\varepsilon})$.

As before, pick a primitive ideal $\mathfrak{b}$ in the inverse of the ideal class c; then every integral ideal $\mathfrak{a}$ in c with norm m corresponds to a unique principal ideal (α) with $\alpha \in \mathfrak{b}$ and $|N\alpha| = mN\mathfrak{b}$. Each such principal ideal has a unique representative in the domain D constructed above.

This shows that $N(m) = A_m(c) + 1$ is the number of lattice points inside the domain $D_m = \{mP \in \mathbb{R}^2 : m > 1, P \in D\}$. For real $t > 1$, the domain D_t is bounded and has a "nice" (piecewise differentiable) boundary; thus we can argue as before and find that the number $N(t)$ of lattice points inside D_t is approximately equal to $\frac{1}{A}$ times the area of D_t, where A denotes the area of the fundamental parallelogram of the lattice $\Lambda_{\mathfrak{b}}$ attached to $\mathfrak{b}$. Clearly D_t is t^2 times the area of $D_1 = D$, hence it remains to compute A and the area of D.

The fundamental parallelogram P of $\Lambda_{\mathfrak{b}}$ is spanned by the vectors pointing from $(0,0)$ to $(1,1)$ and (ω, ω'), respectively. If $\omega = \sqrt{m}$, then P is a rectangle with sides $\sqrt{2}$ and $\sqrt{2m}$, hence has area $2\sqrt{m} = \sqrt{d}$. If $\omega = \frac{1+\sqrt{m}}{2}$, recall that the area T of a triangle with (positively oriented) vertices (x_j, y_j) is given by

$$T = \frac{1}{2}\begin{vmatrix} 1 & x_1 & y_1 \\ 1 & x_2 & y_2 \\ 1 & x_3 & y_3 \end{vmatrix},$$

so in our case we find that the area of the fundamental parallelogram is

$$\begin{vmatrix} 1 & 0 & 0 \\ 1 & \omega & \omega' \\ 1 & 1 & 1 \end{vmatrix} = \omega - \omega' = \sqrt{m}.$$

Since A is $N\mathfrak{b}$ times this area, we find $A = (\operatorname{disc} K)N\mathfrak{b}$.

The area of the part of D lying in the first quadrant consists of the triangle with vertices $(0,0)$, $(1,1)$, and $(1, \varepsilon^{-2})$, as well as of the area bounded by the lines $x = 1$, $x = \varepsilon$, the line $y = \varepsilon^{-2}x$ from below and $y = \frac{1}{x}$ from above. Thus we find

$$\begin{aligned}\frac{1}{2}\text{area}(D) &= \int_0^1 \int_{x/\varepsilon^2}^{x} dydx + \int_1^{\varepsilon} \int_{x/\varepsilon^2}^{1/x} dydx \\ &= \int_0^1 (1-\varepsilon^{-2})xdx + \int_1^{\varepsilon} \Big(\frac{1}{x} - \frac{x}{\varepsilon^2}\Big)x\,dx \\ &= \log\varepsilon.\end{aligned}$$

In exactly the same way as for negative discriminant we now get

Theorem 2.20. *Let $d > 0$ be the discriminant of a real quadratic number field K; let $\varepsilon > 1$ denote the fundamental unit, and h the class number of K. Then*

$$L(1,\chi) = \frac{2h\log\varepsilon}{\sqrt{d}} \tag{2.5}$$

for $\chi = (\frac{d}{\cdot})$. In particular, we have $L(1,\chi) \neq 0$.

Dirichlet's direct evaluation of $L(1,\chi)$ shows

Theorem 2.21. *Let $d > 0$ be the discriminant of a real quadratic number field K. Then*

$$L(1,\chi) = -\frac{1}{\sqrt{d}} \sum_{(a,d)=1} \chi(a)\log\sin\frac{\pi a}{d}. \tag{2.6}$$

Comparing (2.5) and (2.6) yields the following class number formula:

$$h = -\frac{1}{2\log\varepsilon} \sum_{(a,d)=1} \chi(a)\log\sin\frac{\pi a}{d}.$$

Since $(\frac{d}{a}) = (\frac{d}{d-a})$ and $\sin x = \sin(\pi - x)$, this formula can be simplified slightly:

$$h = -\frac{1}{\log\varepsilon} \sum_{1\le a<d/2} \chi(a)\log\sin\frac{\pi a}{d}.$$

Notes

Dirichlet originally only considered prime discriminants d (these are discriminants of the form $d = p$ ($p \equiv 1 \bmod 4$) or $d = -p$ ($p \equiv 3 \bmod 4$)). He started with the simple observation[2]

$$n^{-1} = \int_0^1 x^{n-1}dx. \tag{2.7}$$

Plugging this into $L(1,\chi)$ and exchanging integration and summation, we get

[2] Actually this is how Dedekind presented Dirichlet's proof in his edition of Dirichlet's lectures on number theory.

$$L(1,\chi) = \int_0^1 \sum_{n=1}^{\infty} \Big(\frac{n}{p}\Big) x^{n-1} dx. \tag{2.8}$$

Now $(\frac{n}{p})$ is a periodic function of n; this implies that

$$\sum_{n\ge1} \Big(\frac{n}{p}\Big) x^{n-1} = (1+x^p+x^{2p}+\ldots) \sum_{a=1}^{p-1} \Big(\frac{a}{p}\Big) x^{a-1} = -\frac{f(x)}{x^p-1}$$

for $f(x) = \sum\limits_{a=1}^{p-1} (\frac{a}{p}) x^{a-1}$.

In order to compute the integral we split $\frac{f(x)}{x^p-1}$ into partial fractions. Let $\zeta = e^{2\pi i/p}$ denote a primitive p-th root of unity; then we try to determine complex numbers h_a such that

$$\frac{f(x)}{x^p-1} = \sum \frac{h_a}{x-\zeta^a}.$$

Multiplying through by x^p-1 and setting $x=\zeta^b$ we find $f(\zeta^b) = h_b \frac{x^p-1}{x-\zeta^b}\big|_{\zeta^b}$. Now

$$\frac{x^p-1}{x-\zeta^b}\bigg|_{\zeta^b} = \prod_{j\ne b} (\zeta^b - \zeta^j) = \zeta^{a(p-1)} \prod_{j=1}^{p-1} (1-\zeta^j) = \zeta^{-a} p$$

since $\prod(1-\zeta^j) = \prod(x-\zeta^j)|_1 = 1+x+x^2+\ldots+x^{p-1}|_1 = p$. Thus

$$\frac{f(x)}{x^p-1} = \frac{1}{p} \sum_{a=0}^{p-1} \zeta^a \frac{f(\zeta^a)}{x-\zeta^a}.$$

Substituting this into (2.8) we find

$$L(1,\chi) = -\frac{1}{p} \sum_{a=1}^{p-1} \zeta^a f(\zeta^a) \int_0^1 \frac{dx}{x-\zeta^a}.$$

The integral is computed easily:

$$\int_0^1 \frac{dx}{x-\zeta^a} = \log(x-\zeta^a)\Big|_0^1 = \log(1-\zeta^a) - \log(-\zeta^a) = \log(1-\zeta^{-a}).$$

The expression

$$\tau_a(p) = \zeta^a f(\zeta^a) = \sum_{k=1}^{p-1} \Big(\frac{k}{p}\Big) \zeta^{ak}$$

is a quadratic Gauss sum, and with $\tau_a(p) = (\frac{a}{p})\tau$ we get

$$L(1,\chi) = -\frac{\tau}{p} \sum_{a=1}^{p-1} \Big(\frac{a}{p}\Big) \log(1-\zeta^{-a}). \tag{2.9}$$

This is a special case of (2.1).

Remark. Instead of using (2.7), Dirichlet actually used the definition of the Gamma function

$$\Gamma(s) = \int_0^\infty x^{s-1}e^{-x}dx.$$

The substitution $x \longmapsto n\log\frac{1}{x}$ then shows that

$$\Gamma(s) = n^s \int_0^1 \Big(\log\frac{1}{x}\Big)^{s-1} x^{n-1}dx,$$

hence

$$n^{-s} = \frac{1}{\Gamma(s)}\int_0^1 x^{n-1}\Big(\log\frac{1}{x}\Big)^{s-1}dx.$$

Plugging this into $L(s,\chi)$ we get

$$\Gamma(s)L(s,\chi) = \int_0^1 \Big(\log\frac{1}{x}\Big)^{s-1}\sum_{n=1}^\infty \Big(\frac{n}{p}\Big)x^{n-1}dx.$$

This formula can then be used to extend $L(s,\chi)$ to an entire function in the whole complex plane.

Just as the Riemann zeta function, the L-series $L(s,\chi)$ satisfy a functional equation connecting its values at s and $1-s$; putting $s=1$ in the functional equation shows that

$$L(0,\chi) = \begin{cases} 0 & \text{if } d>0,\\ h & \text{if } d<0. \end{cases}$$

Thus the value of $L(s,\chi)$ is a lot "simpler" than that at $s=0$, and it seems that, once the L-series is extended to the left of $\operatorname{Re} s = 0$, it is even easier to derive (see Stark [St1993]). On the other hand, it seems that we have lost all information in the real case; this is, however, not true: if $d>0$, then $L(s,\chi)$ has a zero of order 1 at $s=0$, and the information on the class number and the fundamental unit of $\mathbb{Q}(\sqrt{d}\,)$ is contained in the derivative $L'(0,\chi)$. Explanations for the values of L-functions and their derivatives at $s=0$ are provided by the Stark conjectures (which can be proved in the abelian case, but are wide open in general).

Exercises

2.1 Show that $\sum\limits_{a=1}^{p-1}(\frac{a}{p}) = 0$.

2.2 For primes $p \equiv 1 \bmod 4$, show that the sum of the quadratic residues is equal to the sum of the quadratic nonresidues modulo p.

2.3 Compute the Gauss sums attached to the quadratic characters $(\frac{d}{\cdot})$ directly from the definition for $d = -3$, $d = -4$, $d = -8$, and $d = 8$.

2.4 Use `pari` or a pocket calculator to compute η (or rather its real approximation) and compare it with ε^2, where $\varepsilon = \frac{1+\sqrt{5}}{2}$ is the fundamental unit of $\mathbb{Q}(\sqrt{5}\,)$.

2.5 In the proof of Theorem 2.16 we have used that the class number of a complex quadratic number field is finite. The following idea allows us to actually *prove* the finiteness of the class number using this approach. As a first step, show that, for an arbitrary number field K, the Dedekind zeta function $\zeta_K(s)$ converges for $\operatorname{Re} s > 1$.
Hints: start with the Euler product $\prod_{\mathfrak{p}}(1 - N\mathfrak{p}^{-s})^{-1}$ and show that this converges for $\operatorname{Re} s > 1$. To this end, observe that $\frac{1}{1-N\mathfrak{p}^{-s}} \le \frac{1}{1-p^{-s}}$, and that there are at most $n = (K : \mathbb{Q})$ primes $\mathfrak{p}$ above p. Thus $\zeta_K(s) \le \zeta(s)^n$.

2.6 (continued) Let $\mathcal{C} = \{c_1, \ldots, c_r\}$ be a set of ideal classes, and let b_n denote the number of ideals with norm n from one of the classes in $\mathcal{C}$. Let $\zeta_{\mathcal{C}}(s) = \sum b_n n^{-s}$ and show that $\zeta_K(s) \ge \zeta_{\mathcal{C}}(s)$. Multiply through by $s-1$; conclude that $(s-1)\zeta_K(s) \to \infty$ if there are infinitely many ideal classes, and derive a contradiction.

2.7 Is it possible to give an analytic proof of the finiteness of the class number and the solvability of the Pell equation for real discriminants in a way analogous to that of the preceding exercises?

2.8 We have defined the Kronecker symbol $\chi = (\frac{d}{p})$ for all positive primes, and therefore for all $n \in \mathbb{N}$ coprime to $m = |d|$. Show that the quadratic reciprocity law implies that, for positive a coprime to d, we always have $\chi(a) = \chi(a+m)$. Use this relation to extend χ to all integers coprime to d, and then show that

$$\chi(-1) = \begin{cases} +1 & \text{if } d > 0, \\ -1 & \text{if } d < 0, \end{cases}$$

by observing $\chi(-1) = (\frac{d}{2m-1})$.

2.9 Let $d < 0$ be an even discriminant and put $\chi = (\frac{d}{\cdot})$ and $m = |d|$. Show that $\chi(a + \frac{m}{2}) = -\chi(a)$ for all positive a coprime to d.
Hints: First write $d = 8k$ for some odd $k < 0$; then $(\frac{d}{a+4k}) = (\frac{2}{a+4k})(\frac{k}{a+4k})$ and $(\frac{d}{a}) = (\frac{2}{a})(\frac{k}{a})$. Now show that $(\frac{2}{a+4k})(\frac{2}{a}) = -1$ and $(\frac{k}{a+4k})(\frac{k}{a})$ (here you should multiply and invert the Jacobi symbol, observing that $a(a+4k) \equiv 1 \bmod 4$). Now consider the case $d = 4k$ for $k \equiv 3 \bmod 4$.

2.10 This is an exercise from an old trigonometry textbook by Hobson (A treatise on plane geometry, Chap. XV, Ex. 22; 7th ed. CUP 1928; the first edition appeared in 1891): show that

$$\frac{\pi}{4} + \frac{\sqrt{3}}{4}\log\frac{2+\sqrt{3}}{2-\sqrt{3}} = 3\Big(1 - \frac{1}{7} + \frac{1}{13} - \frac{1}{19} + \frac{1}{25} - \ldots\Big).$$

Actually, the problem also asked you to show that this sum equals

$$\frac{\tan^{-1}\alpha}{\alpha} + \frac{\tan^{-1}\beta}{\beta} + \frac{\tan^{-1}\gamma}{\gamma},$$

where α, β, γ denote the three cube roots of unity.

2.11 Use the class number formula to show that the class number $h(p)$ of $\mathbb{Q}(\sqrt{-p}\,)$, where $p \equiv 1 \bmod 4$ is prime, is even, and that in fact $h(p) \equiv \frac{p-1}{2} \bmod 4$.

2.12 Use the class number formula to show that the class number $h(pq)$ of $\mathbb{Q}(\sqrt{pq}\,)$, where $p \equiv q \equiv 3 \bmod 4$ primes, is odd.

3. Primes in Arithmetic Progression

We have seen so far how to prove the existence of infinitely many primes of the form $(\frac{d}{p}) = +1$ using L-series of quadratic characters. These techniques, however, do not seem to allow us to "separate" the residue classes $\pm 2 \bmod 5$ and prove that there are e.g. infinitely many primes $p \equiv 2 \bmod 5$. The reason for this failure is that $(\frac{2}{5}) = (\frac{3}{5})$, so quadratic characters cannot see the difference between these classes. In order to make progress, we have to define more general characters. Consider e.g. the map $\psi : (\mathbb{Z}/5\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$ defined by $\psi(a \bmod 5) = 1, i, -1, -i$ according as $a \equiv 1, 2, 3, 4 \bmod 5$. Such characters ψ can distinguish between the residue classes $2 \bmod 5$ and $3 \bmod 5$ since $\psi(2 \bmod 5) = i$ and $\psi(3 \bmod 5) = -1$. Dirichlet's approach to the Theorem on primes in arithmetic progression was to show that the L-series $L(s, \chi)$ defined with these more general characters also satisfy $L(1, \chi) \neq 0$. In this chapter, we will present his proof.

In order to motivate the following discussion, let us briefly go through Dirichlet's proof that there are infinitely many primes in each of the residue classes $1 \bmod 4$ and $3 \bmod 4$. Consider the Dirichlet characters on $(\mathbb{Z}/4\mathbb{Z})^\times$ defined by $\chi_4(n) = (\frac{-4}{n})$ and the unit character χ_1. Then

$$\begin{aligned} L(s, \chi_4) &= \prod_p \frac{1}{1 - \chi(p)p^{-s}}, \\ L(s, \chi_1) &= (1 - 2^{-s})\zeta(s), \end{aligned}$$

because $\chi_1(n) = 0$ for even integers n. Taking logs we find

$$\begin{aligned} \log L(s, \chi_4) &= \sum_{p \equiv 1 \ (4)} p^{-s} - \sum_{p \equiv 3 \ (4)} p^{-s} + O(1), \\ \log L(s, \chi_1) &= \sum_{p \equiv 1 \ (4)} p^{-s} + \sum_{p \equiv 3 \ (4)} p^{-s} + O(1), \end{aligned}$$

hence

$$\begin{aligned} \sum_{p \equiv 1 \ (4)} p^{-s} &\equiv \frac{1}{2}(\log L(s, \chi_1) + \log L(s, \chi_4)) + O(1), \\ \sum_{p \equiv 3 \ (4)} p^{-s} &\equiv \frac{1}{2}(\log L(s, \chi_1) - \log L(s, \chi_4)) + O(1). \end{aligned}$$

Since $\log L(s,\chi_4)$ remains bounded as $s \to 1$, we find that the primes in each residue class have Dirichlet density $\frac{1}{2}$.

Thus the two characters χ_1 and χ_4 on $(\mathbb{Z}/4\mathbb{Z})^\times$ allow us to seperate the residue classes $p \equiv 1 \bmod 4$ and $p \equiv 3 \bmod 4$. This example is not typical in the sense that it was sufficient to look at quadratic characters, that is, characters with values ±1. The reason for this is the fact that the group $(\mathbb{Z}/4\mathbb{Z})^\times$ has exponent 2. In the next few sections, we will introduce general Dirichlet characters, study their L-series, and give a full proof of Dirichlet's theorem on primes in arithmetic progressions.

3.1 Characters

A Dirichlet character defined mod m is a homomorphism $(\mathbb{Z}/m\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$; more generally, a character on a finite abelian group G is a homomorphism $G \longrightarrow \mathbb{C}^\times$. If $g \in G$ has order f, then $\chi(g)^f = \chi(g^f) = \chi(1) = 1$, hence the image of ϕ consists of roots of unity. The characters of an abelian group G form a group $\widehat{G}$ with respect to the multiplication of values; this group $X(G) = \widehat{G}$ is called the character group of G.

Dirichlet's Lemma

The principal character $\mathbb{1}$ is the character that sends every element of G to 1. Examples for nontrivial characters modulo m for odd integers m are given by Legendre symbols $\chi = (\frac{\cdot}{m})$. These are Dirichlet characters mod m since $\chi(a)$ only depends on $a \bmod m$, and since $\chi(ab) = \chi(a)\chi(b)$.

The only nontrivial Dirichlet character χ defined modulo 4 must satsify $\chi(3) = -1$; thus we have $\chi(a) = (\frac{-4}{a})$ for $a > 0$. More generally, for any discriminant $d = \operatorname{disc} K$ of a quadratic number field, the map $\chi(a) = (\frac{d}{a})$ for $a > 0$ defines a Dirichlet character defined mod $|d|$ since the quadratic reciprocity law implies $\chi(a) = \chi(a + |d|)$.

We can also define a character ψ modulo 5 by demanding $\chi(2) = i$; then $\chi(4) = \chi(2)^2 = -1$, $\chi(3) = \chi(2)^3 = -i$, and of course $\chi(1) = \chi(2)^4 = 1$. This is of course not a character induced by a Kronecker symbol since it has nonreal values. Dirichlet's Lemma now characterizes all Dirichlet characters coming from Kronecker symbols:

Lemma 3.1 (Dirichlet's Lemma)**.** *Let $m > 1$ be an integer, and χ a nontrivial Dirichlet character defined modulo m. Then there is a discriminant d with $\chi(a) = (\frac{d}{a})$ for all $a > 0$ if and only if χ is a quadratic character.*

Proof. Let us first prove this for prime powers $m = p^r$. If p is odd, this is a cyclic group; every quadratic character χ is trivial on squares since $\chi(a^2) = \chi(a)^2 = 1$. Thus $\ker\chi$ has index ≤ 2; since $\chi \ne \mathbb{1}$, the kernel $\ker\chi$ must consist only of the squares mod p^r, and we must have $\chi(n) = -1$ for all nonsquares n. Now $a \in (\mathbb{Z}/p^r\mathbb{Z})^\times$ is a square if and only if a is a square mod p: this is due to the fact that $(\mathbb{Z}/p^r\mathbb{Z})^\times \simeq (\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}/p^{r-1}\mathbb{Z}$, and that every element in the second component is a square since this group has odd order. Thus $\chi(a) = (\frac{a}{p})$ for all $a \in (\mathbb{Z}/p^r\mathbb{Z})^\times$.

The case $p = 2$ is different, since the group $(\mathbb{Z}/2^r\mathbb{Z})^\times$ is, in general, not cyclic; in fact, $(\mathbb{Z}/2^r\mathbb{Z})^\times \simeq \langle -1 \rangle \times \langle 5 \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{r-2}\mathbb{Z}$ for $r \geq 3$. Since χ is determined by its images on -1 and 5, there are exactly four quadratic characters mod 2^r. One of them is the trivial character, the other three are given by the formulas $\chi_4(a) = (\frac{-4}{a})$, $\chi_8(a) = (\frac{8}{a})$, and $\chi_4\chi_8(a) = (\frac{-8}{a})$ for $a > 0$.

The claim now follows from the Chinese Remainder Theorem. □

Basic Properties of the Character Group

The set of characters $X(G) = \widehat{G}$ (we will use both notations) of G is an abelian group with respect to the multiplication $(\psi\chi)(a) = \psi(a)\chi(a)$. If A and B are finite abelian groups, then we obviously have $X(A \oplus B) \simeq X(A) \oplus XB)$. Now we claim

Proposition 3.2. *If G is a finite abelian group, then $G \simeq X(G)$ (non-canonically) and $G \simeq X(X(G))$ (canonically).*

Proof. Since G is the direct sum of cyclic groups, and since $X(A \oplus B) \simeq X(A) \oplus X(B)$, it is sufficient to prove $G \simeq X(G)$ for cyclic groups G. Let $G = \langle g \rangle$; then any character $\chi \in \widehat{G}$ is determined by the value of $\chi(g)$, since we have $\chi(g^a) = \chi(g)^a$. Now $\chi(g)$ must be a $\#G$-th root of unity; there are exactly $\#G$ of them, and they are all powers of a primitive $\#G$-th root of unity. Therefore, each character $\in X(G)$ is a power of the character χ which maps g to a primitive $\#G$-th root of unity. This shows that $\widehat{G}$ is a cyclic group of order $\#G$, and in particular, we find $G \simeq X(G)$.

In order to prove that $G \simeq X(X(G))$ we observe that every $g \in G$ induces a map $\gamma_g : \widehat{G} \longrightarrow \mathbb{C}^\times : \gamma_g(\chi) = \chi(g)$. The map $\psi : g \longmapsto \gamma_g$ defines a homomorphism $G \longrightarrow \widehat{\widehat{G}}$ with $\ker \psi = 1$; it must be onto since $\#G = \#X(G) = \#X(X(G))$. □

An important property of characters are the orthogonality relations:

Proposition 3.3. *Let G be a finite abelian group with character group X. Then*

$$\sum_{x \in G} \chi(x) = \begin{cases} \#G & \text{if } \chi = \mathbb{1} \\ 0 & \text{if } \chi \neq \mathbb{1} \end{cases} \quad \text{and} \quad \sum_{\chi \in X} \chi(x) = \begin{cases} \#G & \text{if } x = 1 \\ 0 & \text{if } x \neq 1 \end{cases} .$$

Proof. The first assertion is clear if $\chi = \mathbb{1}$. If $\chi \neq \mathbb{1}$, then there must be a $y \in G$ such that $\chi(y) \neq 1$. But now

$$\chi(y)\sum_{x\in G}\chi(x) = \sum_{x\in G}\chi(xy) = \sum_{x\in G}\chi(x),$$

proving our claim. The 'dual' assertion is reduced to the first case by identifying G and $X(X(G))$. □

Primitive Characters and Conductors

Let χ be a Dirichlet character on $(\mathbb{Z}/n\mathbb{Z})^\times$; every integer $m \in \mathbb{N}$ such that

$$a \equiv b \bmod m \Longrightarrow \chi(a) = \chi(b)$$

whenever a, b are prime to n is called a *defining modulus* for χ.

Consider e.g. the character χ modulo 8 which has values $+1$ for the residue classes $1, 5 \bmod 8$ and -1 for $3, 7 \bmod 8$. Then this character is also defined modulo 4 since it agrees with the character sending the residue classes $\pm 1 \bmod 4$ to ± 1. It is, however, not defined modulo 2 since $1 \equiv 3 \bmod 2$, whereas $\chi(1 \bmod 8) = 1$ and $\chi(3 \bmod 8) = -1$.

If m_1 and m_2 are defining moduli, then so is their greatest common divisor (this is easily seen by using a Bezout representation $d = m_1x + m_2y$ of $d = \gcd(m_1, m_2)$), hence there exists a smallest defining modulus $\mathfrak{f}$, which is called the *conductor* of χ. A Dirichlet character χ defined modulo m is called primitive if m is the conductor of χ.

Let us now compute the conductors of the Dirichlet characters defined mod 15. Since $(\mathbb{Z}/15\mathbb{Z})^\times \simeq \langle -1\rangle \times \langle 2\rangle$, such characters are defined by their values on the residue classes -1 and 2 mod 15.

Define χ by $\chi(-1) = 1$, $\chi(2) = i$, and ψ by $\psi(-1) = -1$ and $\psi(2) = 2$. It is then easily checked that the eight characters $\chi^r\psi^s$ for $0 \le r \le 3$ and $0 \le s \le 1$ are pairwise distinct; thus we have found all $8 = \phi(15)$ characters mod 15. Here is a table with all these characters, their values, and their conductors :

	1	2	4	7	8	11	13	14	f
$1\!\!1$	$+1$	$+1$	$+1$	$+1$	$+1$	$+1$	$+1$	$+1$	1
χ	$+1$	$+i$	-1	$-i$	$-i$	-1	$+i$	$+1$	15
χ^2	$+1$	-1	$+1$	-1	-1	$+1$	-1	$+1$	5
χ^3	$+1$	$-i$	-1	$+i$	$+i$	-1	$-i$	$+1$	15
ψ	$+1$	$+1$	$+1$	-1	$+1$	-1	-1	-1	15
$\chi\psi$	$+1$	$+i$	-1	$+i$	$-i$	$+1$	$-i$	-1	5
$\chi^2\psi$	$+1$	-1	$+1$	$+1$	-1	-1	$+1$	-1	3
$\chi^3\psi$	$+1$	$-i$	-1	$-i$	$+i$	$+1$	$+i$	-1	5

The table also shows that the three quadratic characters are induced by Legendre symbols: $\psi = (\frac{\cdot}{15})$, $\chi^2 = (\frac{\cdot}{5})$, and $\chi^2\psi = (\frac{\cdot}{3})$.

3.2 Primes in Arithmetic Progression

For each character χ on $(\mathbb{Z}/m\mathbb{Z})^\times$ we now can define its L-series in the usual way, and observe that the multiplicativity of χ implies that we have an Euler factorization for all s with $\operatorname{Re} s > 1$:

$$L(s,\chi) = \sum \chi(n)n^{-s} = \prod_p \frac{1}{1-\chi(p)p^{-s}}.$$

If $\chi \neq \mathbb{1}$, this L-series actually converges for $\operatorname{Re} s > 0$: in fact, we have $\sum\limits_{a=1}^{m} \chi(a) = 0$, and this implies that $\sum\limits_{a=1}^{\mu} \chi(a) = \sum\limits_{a=1}^{\nu} \chi(a)$ for $\mu \equiv \nu \bmod m$ for some $\nu < m$. Thus

$$|A(N)| = \Big|\sum_{a=1}^{N} \chi(a)\Big| = \Big|\sum_{a=1}^{\nu} \chi(a)\Big| \le \sum_{a=1}^{\nu} |\chi(a)| = \nu < m,$$

and so the partial sums of the coefficients of $L(s,\chi)$ are bounded. Lemma 1.7 then implies that $L(s,\chi)$ converges to an analytic function for $\operatorname{Re} s > 0$.

Assuming for the moment that $L(1,\chi) \neq 1$ whenever $\chi \neq 1$, we can prove Dirichlet's theorem as follows. For a Dirichlet character χ we have

$$\begin{aligned}
\log L(s,\chi) &= \sum_p \log \frac{1}{1-\chi(p)p^{-s}} \\
&= \sum_p \sum_{n\ge 1} \frac{1}{n}\chi(p^n)p^{-ns} \\
&= \sum_p \chi(p)p^{-s} + \sum_p \sum_{n\ge 2} \frac{1}{n}\chi(p^n)p^{-ns} \\
&= \sum_p \chi(p)p^{-s} + O(1)
\end{aligned}$$

by a now standard argument. Setting $f_\chi(s) = \sum_p \chi(p)p^{-s}$, we therefore have $\log L(s,\chi) = f_\chi(s) + O(1)$.

Next we fix an integer a coprime to n, set $G = (\mathbb{Z}/m)^\times$, and compute $\sum_\chi \overline{\chi}(a) f_\chi(s)$ in two different ways. On the one hand, we have

$$\begin{aligned}
\frac{1}{\phi(m)} \sum_\chi \overline{\chi}(a) f_\chi(s) &= \frac{1}{\#G} \sum_\chi \overline{\chi}(a) \sum_p \chi(p)p^{-s} \\
&= \frac{1}{\#G} \sum_p p^{-s} \sum_\chi \overline{\chi}(a)\chi(p) \\
&= \sum_p p^{-s} \frac{1}{\#G} \sum_\chi \chi(p/a).
\end{aligned}$$

The inner sum here is 0 unless $p \equiv a \bmod m$, when it equals $\#G$; thus we get

$$\frac{1}{\phi(m)} \sum_{\chi} \overline{\chi}(a) f_{\chi}(s) = \sum_{p \equiv a \bmod m} p^{-s}.$$

On the other hand we know

$$\frac{1}{\phi(m)} \sum_{\chi} \overline{\chi}(a) f_{\chi}(s) = \frac{1}{\phi(m)} \log \frac{1}{s-1} + O(1)$$

for small $s > 1$. Combining these equations we get

$$\sum_{p \equiv a \bmod m} p^{-s} = \frac{1}{\phi(m)} \log \frac{1}{s-1} + O(1),$$

and this shows

Theorem 3.4 (Dirichlet's Theorem). *For any integer $m > 1$ and any a coprime to m, the set of primes $p \equiv a \bmod m$ has Dirichlet density $\frac{1}{\phi(m)}$. In particular, there are infinitely many such primes.*

To complete the proof, we have to show that $L(1, \chi) \neq 0$ for every Dirichlet character modulo m different from the trivial character.

The Nonvanishing of $L(1, \chi)$

Next we will give the first of two proofs for fact that $L(1, \chi) \neq 0$ for nonprincipal Dirichlet characters χ. We start with the following simple observation:

Lemma 3.5. *Fix an integer $m > 1$ and let $G = (\mathbb{Z}/m\mathbb{Z})^{\times}$. Then*

$$\sum_{\chi \in \widehat{G}} \log L(s, \chi) > 0$$

for all $s < 1$.

Proof. This is a straightforward calculation:

$$\begin{aligned} \sum_{\chi \in \widehat{G}} \log L(s, \chi) &= \sum_{\chi} \log \prod_{p} \frac{1}{1 - \chi(p) p^{-s}} \\ &= \sum_{\chi} \sum_{p} \sum_{n \geq 1} \frac{1}{n} \chi(p)^n p^{-ns} \\ &= \sum_{n \geq 1} \frac{1}{n} \sum_{p} p^{-ns} \sum_{\chi} \chi(p^n). \end{aligned}$$

The last sum is 0 unless $p^n \equiv 1 \bmod m$; thus

$$\sum_{\chi \in \widehat{G}} \log L(s,\chi) = \sum_{n \geq 1} \frac{1}{n} \sum_{p^n \equiv 1} p^{-ns} > 0$$

as claimed. □

Now recall that $\log L(s, \mathbb{1}) = -\log(s-1) + O(1)$ for small $s > 1$. If $\chi \neq \mathbb{1}$, then $L(s,\chi)$ is analytic in a vicinity of $s = 1$, and there are two cases.

1. If $L(1,\chi) \neq 0$, then $\log L(s,\chi) = O(1)$ in some vicinity of 1.
2. If $L(1,\chi) = 0$, then $L(s,\chi) = (s-1)^{a(\chi)} f(s)$ for some integer $a(\chi) \geq 1$ and a function f that is analytic around $s = 1$ with $f(s) \neq 0$. Thus $\log L(s,\chi) = a(\chi)\log(s-1) + O(1)$.

This implies

$$\sum_{\chi \in \widehat{G}} \log L(s,\chi) = -\log(s-1) + \sum_{\chi \neq 1} a(\chi)\log(s-1) + O(1) \tag{3.1}$$

for $s > 1$. If $\sum_\chi a(\chi) \geq 2$, then the right hand side of (3.1) goes to $-\infty$ for $s \longrightarrow 1$; but the left hand side is > 0 by Lemma 3.5, and this contradiction shows that $\sum a(\chi) \leq 1$.

Thus there is at most one character $\chi \neq \mathbb{1}$ with $L(1,\chi) = 0$ (and if there is one, the order of the zero is 1). This immediately implies that χ must be real: for if χ is a nonreal character, then so is $\overline{\chi} = \chi^{-1}$; but then $L(1,\overline{\chi}) = \overline{L(1,\chi)} = 0$, so there would be at least two characters for which $L(1,\chi)$ vanishes.

So if there is any character χ at all for which $L(1,\chi) = 0$, then χ must be a real character. By Dirichlet's Lemma, we have $\chi = (\frac{d}{\cdot})$ for some quadratic discriminant d; but for such characters we have already seen in Chapter 2 that $L(1,\chi) \neq 0$.

We have proved:

Theorem 3.6. *If $\chi \neq \mathbb{1}$ is a Dirichlet character modulo m, then $L(1,\chi) \neq 0$.*

3.3 Cyclotomic Number Fields

The second proof of Dirichlet's Theorem, or rather of the nonvanishing of the L-series, will employ the arithmetic of $K = \mathbb{Q}(\zeta_m)$. This is quite a natural field to look at in this connection since the decomposition of a prime p in $K/\mathbb{Q}$ only depends on the residue class $p \bmod m$. In the following, we will briefly recall the basic properties of these cyclotomic fields.

For any $m \in \mathbb{N}$, let $\zeta = \zeta_m$ denote a primitive m-th root of unity. The cyclotomic field $K = \mathbb{Q}(\zeta_m)$ has degree $n = \phi(m)$; it is an abelian extension of $\mathbb{Q}$ with Galois group $G \simeq (\mathbb{Z}/m\mathbb{Z})^\times$; the residue class $a \bmod m$ corresponds to the automorphism $\sigma_a : \zeta_m \longmapsto \zeta_m^a$.

The following result will eventually turn out to be a special case of a general theorem in class field theory, and can be proved by quite elementary means:

Theorem 3.7 (Kronecker-Weber)**.** *Every abelian extension of $\mathbb{Q}$ is contained in some cyclotomic extension $\mathbb{Q}(\zeta)$.*

The ring of integers of K is $\mathfrak{O}_K = \mathbb{Z}[\zeta]$, and the elements $1, \zeta, \zeta^2, \ldots \zeta^{\phi(m)-1}$ form an integral basis.

Theorem 3.8 (Decomposition Law in Cyclotomic fields)**.** *Let ζ be a primitive m-th root of unity, and let $K = \mathbb{Q}(\zeta)$ denote the field of m-th roots of unity. If $p \nmid m$ is a prime, then $p\mathfrak{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_g$ for prime ideals $\mathfrak{p}_i$ with inertia degree f, where f is the smallest integer $f > 0$ with $p^f \equiv 1 \bmod m$, and g is determined by $fg = (K : \mathbb{Q}) = \phi(m)$.*

Thus the decomposition type of a prime p only depends on its residue class modulo m; we will later see that such fields are class fields, and that cyclotomic fields are the simplest examples.

For example, primes $p \equiv 1 \bmod 3$ split completely in $\mathbb{Q}(\zeta_3)$, and primes $p \equiv 2 \bmod 3$ have inertia degree 2 (that is, they are inert since $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3}\,)$ is a quadratic extension). The decomposition law for quadratic extensions, on the other hand, tells us that p will split completely in $\mathbb{Q}(\sqrt{-3}\,)$ if and only if $(\frac{-3}{p}) = +1$; comparing the two statements implies that $(\frac{-3}{p}) = (\frac{p}{3})$, and this is a special case of the quadratic reciprocity law. In fact, the general reciprocity laws (not just the quadratic ones) can be derived by comparing the decomposition law in class fields and Kummer extensions.

Recall that the fundamental equation $\zeta_K(s) = \zeta(s)L(s,\chi)$ for quadratic Dirichlet characters was basically equivalent to the decomposition law for primes in quadratic extensions $K/\mathbb{Q}$. We will now prove the following cyclotomic analog:

Theorem 3.9. *Let $K = \mathbb{Q}(\zeta_m)$ be the field of m-th roots of unity, and let $G \simeq (\mathbb{Z}/m\mathbb{Z})^\times$ denote its Galois group. The decomposition law in cyclotomic fields implies that the Euler factors for primes $p \nmid m$ in $\zeta_K(s)$ and $\prod_{\chi \in \widehat{G}} L(s,\chi)$ are the same.*

Proof. We have $p\mathfrak{O}_K = \mathfrak{p}_1 \ldots \mathfrak{p}_g$ for $fg = \phi(m)$, where f is the order of the residue class $p \bmod m$ in $(\mathbb{Z}/m\mathbb{Z})^\times$. Since $N\mathfrak{p}_j = p^f$, the Euler factor for each prime above p in the product expansion of $\zeta_K(s)$ is $(1 - p^{-fs})^{-1}$, and since there are g of them, we find that p contributes the factor

$$\Big(\frac{1}{1 - p^{-fs}}\Big)^g$$

to the product expansion of $\zeta_K(s)$.

From the factorization

$$1 - x^f = \prod_{j=0}^{f-1} (1 - \zeta^k x)$$

we deduce

$$1 - p^{-fs} = \prod_{j=0}^{f-1} \Big(1 - \frac{\zeta^j}{p^s}\Big),$$

where ζ is a primitive f-th root of unity.

Let $\langle \overline{p} \rangle$ denote the subgroup of $G = (\mathbb{Z}/m\mathbb{Z})^\times$ generated by p. Since $\overline{p}$ has order f, the quotient $G/\langle p \rangle$ has order g. Since $X(\langle \overline{p} \rangle)$ is isomorphic to the group of f-th roots of unity, we have

$$\prod_{\chi \in X(\langle \overline{p} \rangle)} (1 - \chi(p)X) = \prod_{j=0}^{f-1} (1 - \zeta^j X),$$

since $\chi(p)$ runs through the f-th roots of unity as χ runs through $X(\langle \overline{p} \rangle)$.

The dual of the exact sequence

$$1 \longrightarrow \langle \overline{p} \rangle \longrightarrow G \longrightarrow G/\langle \overline{p} \rangle \longrightarrow 1$$

is the exact sequence

$$1 \longrightarrow X(G/\langle \overline{p} \rangle) \longrightarrow X(G) \longrightarrow X(\langle \overline{p} \rangle) \longrightarrow 1.$$

This shows that each character on $\langle \overline{p} \rangle$ lifts to exactly g characters on G, hence we have

$$\prod_{\chi \in X(G)} (1 - \chi(p)X) = \prod_{j=0}^{f-1} (1 - \zeta^j X)^g,$$

and this implies the claim. □

In the next chapter we will prove that the Dedekind zeta function $\zeta_K(s)$ has a pole of order 1 at $s = 1$ for any number field K, and compute its residue. Taking this for granted and using the fact that $\zeta_K(s)$ and $\prod_\chi L(s, \chi)$ differ only by finitely many Euler factors, we see that $\prod_\chi L(s, \chi)$ has a pole of order 1 at $s = 1$. But this pole comes from the factor $L(s, \mathbb{1})$, since this is, up to finitely many Euler factors, just the Riemann zeta function. This implies that $L(1, \chi) \neq 0$ for all characters $\chi \neq 1$.

The statement in Theorem 3.9 can be given a slightly more satisfying form. In fact, consider a character χ defined modulo m, and let f be its conductor. Then there is a unique (primitive) character $\widetilde{\chi}$ defined modulo f such that $\chi(a) = \widetilde{\chi}(a)$ for all a coprime to m. The L-series $L(s, \chi)$ and $L(s, \widetilde{\chi})$ differ by at most the Euler factors for the primes dividing m/f. For example, the unit character χ modulo 4 and $\widetilde{\chi}$ have L-series

$$\begin{aligned} L(s,\chi) &= 1 + 3^{-s} + 5^{-s} + 7^{-s} + \ldots, \\ L(s,\widetilde{\chi}) &= 1 + 2^{-s} + 3^{-s} + 4^{-s} + \ldots = \zeta(s). \end{aligned}$$

We now claim

Theorem 3.10. *Let $K = \mathbb{Q}(\zeta_m)$ be the field of m-th roots of unity, and let $G \simeq (\mathbb{Z}/m\mathbb{Z})^\times$ denote its Galois group. The decomposition law in cyclotomic fields implies*

$$\zeta_K(s) = \prod_{\chi \in \widehat{G}} L(s,\widetilde{\chi}).$$

Proof. There are two things to show: first, that the Euler factors for the prime p in $L(s,\chi)$ and $L(s,\widetilde{\chi})$ are the same if p is unramified, and second that the Euler factors for all primes $p \mid m$ in $\zeta_K(s)$ and $\prod_\chi L(s,\widetilde{\chi})$ are the same.

For the first point, consider Dirichlet characters as homomorphisms $\chi : G \longrightarrow \mathbb{C}^\times$ for $G = \mathrm{Gal}\,(K/\mathbb{Q})$; then $G_\chi = \ker \chi$ is a subgroup of G, and we say that χ is unramified at p if p is unramified in the fixed field of G_χ. Clearly every χ is unramified at the primes $p \nmid m$, and the principal character $1\!\!1$ is unramified everywhere since its fixed field is $\mathbb{Q}$. The key to the proof is the observation that χ is ramified at p if and only of $\widetilde{\chi}(p) = 0$.

Details will be added later. □

Notes

The conjecture that every arithmetic progression $a + mb$ for coprime integers a and m contains infinitely many primes goes back to Euler. Legendre needed such a result in his proof of the quadratic reciprocity law; he eventually even sketched a proof of his conjecture, but its key lemma later turned out to be false. Dirichlet tried to repair Legendre's arguments, but succeeded in proving his theorem only by using Euler's techniques.

Some cases of Dirichlet's theorem can be proved by elementary techniques à la Euclid; it can even be shown that Euclidean proofs for the infinitude of primes in the arithmetic progression $a + mb$ exist if and only if $a^2 \equiv 1 \bmod m$. In particular, there are such proofs for the residue classes $a \equiv 1 \bmod m$ and $a \equiv -1 \bmod m$.

Exercises

3.1 Let A and B be abelian groups. Show that $X(A \oplus B) \simeq X(A) \oplus X(B)$.

3.2 Let

$$\begin{tikzcd} 1 \arrow[r] & A \arrow[r] & B \arrow[r] & C \arrow[r] & 1 \end{tikzcd}$$

be an exact sequence of finite abelian groups. Show that there is an exact sequence

$$1 \longrightarrow \widehat{C} \longrightarrow \widehat{B} \longrightarrow \widehat{A} \longrightarrow 1.$$

3.3 Let χ and ψ be Dirichlet characters defined modulo m, and with conductors f_χ and f_ψ. Show that if $\gcd(f_\chi, f_\psi) = 1$, then the character $\chi\psi$ has conductor $f_\chi f_\psi$.

3.4 List all Dirichlet characters modulo 24, determine their conductors, and identify them with Kronecker symbols.

4. Dirichlet

This chapter is devoted to other results that Dirichlet obtained using his analytic techniques, as well as to results that were obtained later using methods available to Dirichlet.

4.1 Dirichlet's *L*-series for Quadratic Forms

Dirichlet obtained his class number formula using the language of quadratic forms: ideals had not yet been invented. In the following, we will explain the connection between the two approaches.

A binary quadratic form is an expression $Q(X,Y) = AX^2 + BXY + CY^2$; we will often denote this form by $Q = (A,B,C)$. Its discriminant is $\Delta = B^2 - 4AC$. A form (A,B,C) is called primitive if $\gcd(A,B,C) = 1$, and positive definite if $\Delta < 0$ and $A > 0$. The group $\mathrm{SL}_2(\mathbb{Z})$ of 2×2-matrices with integral entries and determinant 1 acts on these forms as follows: for $M = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$, we set $Q|_M(X,Y) = Q(rX+sY, tX+uY)$. Two forms Q, Q' are called equivalent if $Q' = Q|_M$ for some $M \in \mathrm{SL}_2(\mathbb{Z})$. It is easy to see that equivalent forms have the same discriminant and represent the same integers. The set of equivalence classes of primitive (and, if $\Delta < 0$, positive definite) forms is a finite abelian group $\mathrm{Cl}(\Delta)$ with respect to "composition"

In order to keep things as simple as possible, we will only consider the easier case of negative discriminants. To each positive definite form $Q = (A,B,C)$ we associate the ideal $\mathfrak{b} = (A, \frac{B-\sqrt{\Delta}}{2})$ in the ring of integers of the quadratic number field with discriminant Δ. Equivalent ideals correspond to ideals in the same ideal class, so the map sending forms to ideals induces an isomorphism between the class group $\mathrm{Cl}(\Delta)$ of forms and the ideal class group $\mathrm{Cl}(K)$. Conversely, given an ideal $\mathfrak{a}$ we write $\mathfrak{a} = \alpha\mathbb{Z} \oplus \beta\mathbb{Z}$ and set

$$Q(x,y) = \frac{N(\alpha x + \beta y)}{N\mathfrak{a}}.$$

Now let $c \in \mathrm{Cl}(\Delta)$ be a class of forms; pick a form $Q \in c$ and define the L-series

$$L(s,c) = \frac{1}{w} \sum_{x,y} \frac{1}{Q(x,y)},$$

where the sum is over all integers $x, y \geq 0$ with $(x, y) \neq (0, 0)$, and where w is the number of roots of unity in K (or, in the language of quadratic forms, the number of automorphs of a quadratic form of discriminant Δ). Since equivalent forms represent the same integers, this does not depend on the choice of Q. It is easy to see that the integers represented by Q are exactly the integers n for which there is an $\alpha \in \mathfrak{b}$ with $nN\mathfrak{b} = N\alpha$. To each principal ideal (α) of this form there correspond w values of α; moreover we have already seen that these principal ideals are in bijection with the ideals $\mathfrak{a} \in c^{-1}$ of norm m such that $\mathfrak{ab} = (\alpha)$ is principal.

Lemma 4.1. *Let $Q = (A, B, C)$ be a quadratic form associated to the ideal $\mathfrak{a}$. Then a natural number n is represented by Q if and only if there is an integral ideal $\mathfrak{b} \in [\mathfrak{a}]^{-1}$ with $N\mathfrak{b} = n$.*

Proof. If $\mathfrak{b} \in [\mathfrak{a}]^{-1}$ with $N\mathfrak{b} = n$, then $\mathfrak{ab} = (\alpha)$ □

4.2 Genus Theory for Quadratic Number Fields

In this section we will review genus theory for quadratic number fields, and give Dirichlet's analytic proof for the existence of genera.

4.3 Primes with Prescribed Residue Characters

In this section we will generalize Theorem 1.11. Dirichlet apparently never bothered proving this result, since it is an immediate consequence of his density result and quadratic reciprocity. Research by Kummer and Hilbert on reciprocity laws in number fields, however, required results that did not depend on reciprocity. Remarks made by Kummer in one of his proofs of quadratic reciprocity show that Kummer was aware of these applications, and Hilbert later generalized them to arbitrary number fields and used them to prove the quadratic reciprocity law in totally complex number fields with odd class number.

Let $a_1, \ldots, a_t$ be squarefree integers; we will call them independent modulo squares if any relation $\prod a_j^{e_j} = a^2$ for an integer a and exponents $e_j = 0, 1$ implies $e_1 = \ldots = e_t = 0$. Distinct primes, for example, are always independent modulo squares, whereas the integers 6, 10, 15 are not because $6 \cdot 10 \cdot 15 = 2^2 3^2 5^2$ is a square.

Theorem 4.2. *Assume that $a_1, \ldots, a_t \in \mathbb{Z}$ are independent modulo squares. Then for any choice $c = (c_1, \ldots, c_t)$ of signs $c_j = \pm 1$, the set S_c of primes p satisfying*

$$\Big(\frac{a_1}{p}\Big) = c_1, \quad \ldots, \quad \Big(\frac{a_t}{p}\Big) = c_t$$

has Dirichlet density $\delta(S) = 2^{-t}$.

If we choose $c_1 = \ldots = c_t = +1$, then $S = \operatorname{Spl}(K/\mathbb{Q})$ for the multiquadratic number field $K = \mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_t}\,)$. Since the independence modulo squares of the a_j is equivalent to $(K : \mathbb{Q}) = 2^t$, we find that the set of primes splitting completely in $K/\mathbb{Q}$ has Dirichlet density $\frac{1}{(K:\mathbb{Q})}$.

Our proof of Theorem 4.2 will be modeled after Dirichlet's proof of his density theorem. For showing that, for coprime integers a and m, there are infinitely many primes $p \equiv a \bmod m$ we introduced Dirichlet characters

$$\chi : \operatorname{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times;$$

here we have to consider characters

$$\chi : \operatorname{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^t \longrightarrow \mathbb{C}^\times.$$

Every $\sigma \in \operatorname{Gal}(K/\mathbb{Q})$ defines a vector $(e_1, \ldots, e_t) \in (\mathbb{Z}/2\mathbb{Z})^t$ via

$$\sigma(\sqrt{a_1}\,) = (-1)^{e_1}\sqrt{a_1}, \quad \ldots, \quad \sigma(\sqrt{a_t}\,) = (-1)^{e_t}\sqrt{a_t},$$

and we will identify σ with the sign vector

$$\big((-1)^{e_1}, \ldots, (-1)^{e_t}\big) = \big(\sqrt{a_1}^{\,\sigma-1}, \ldots, \sqrt{a_t}^{\,\sigma-1}\big),$$

and therefore $\operatorname{Gal}(K/\mathbb{Q})$ with μ_2^t, where μ_2 is the group of 2nd roots of unity.

Every prime $p \nmid a_1 \cdots a_t$ defines an automorphism σ_p via

$$\sigma_p = \Big(\Big(\frac{a_1}{p}\Big), \ldots \Big(\frac{a_t}{p}\Big) \Big).$$

Now we are ready for the

Proof of Thm. 4.2. Set $f_\chi(s) = \sum_p \chi(\sigma_p) p^{-s}$, where the sum is over all primes $p \nmid a = a_1 \cdots a_t$. Since χ is a quadratic character, $f_\chi(s) = O(1)$ as $s \longrightarrow 1$ unless $\chi = \mathbb{1}$; this follows by taking logs of the corresponding L-function $L(s,\chi)$ and observing that $L(1,\chi) \neq 0$.

Now

$$\sum_\chi \chi(c)\chi(\sigma_p) = \sum_\chi \chi(\sigma_p/c) = \begin{cases} 0 & \text{if } \sigma_p = c, \\ 2^t & \text{if } \sigma_p \neq c \end{cases}$$

by the orthogonality relations, hence

$$\begin{aligned} 2^{-t} \sum_\chi \chi(c) f_\chi(s) &= 2^{-t} \sum \chi(c) \sum_p \chi(\sigma_p) p^{-s} \\ &= 2^{-t} \sum_p p^{-s} \sum_\chi \chi(c)\chi(\sigma_p) \\ &= \sum_{p:\ \sigma_p = c} p^{-s}. \end{aligned}$$

On the other hand,

$$2^{-t} \sum_\chi \chi(c) f_\chi(s) = 2^{-t} \log \frac{1}{s-1} + O(1),$$

because all $f_\chi(s)$ with $\chi \neq \mathbb{1}$ are bounded as $s \to 1$, whereas $f_\chi(s) = \log \frac{1}{s-1} + O(1)$ for $\chi = \mathbb{1}$ (in this case, $f_\chi(s) = \sum_{p \nmid a} p^{-s}$). The claim now follows. □

4.4 Primes Represented by Binary Quadratic Forms

The odd primes represented by the quadratic form $Q(X,Y) = X^2 + Y^2$ are exactly the primes $p \equiv 1 \bmod 4$, hence have Dirichlet density $\frac{1}{2}$. Do primes represented by a general quadratic form $Q(X,Y) = AX^2 + BXY + CY^2$ (we will often denote this form by $Q = (A,B,C)$) also have a Dirichlet density? The problem is trivial if $\gcd(A,B,C) \neq 1$: the form $2X^2 + 2Y^2$, for example, represents only 2. Let us therefore assume that Q is primitive, i.e., that $\gcd(A,B,C) = 1$. Then Dirichlet claimed

Theorem 4.3. *Let $Q = (A,B,C)$ be a quadratic form with discriminant $\Delta = B^2 - 4AC$. Then the set S_Q of primes represented by Q has Dirichlet density*

$$\delta(S_Q) = \begin{cases} \frac{1}{h} & \text{if } Q \not\sim (A,-B,C), \\ \frac{1}{2h} & \text{if } Q \sim (A,-B,C), \end{cases}$$

where h is the class number of forms of discriminant Δ.

Actually Dirichlet's claims were slightly different, since he worked with forms $Q = (A,2B,C)$ with even middle coefficients. If $Q = (1,0,1)$, then $h = 1$, hence Thm. 4.3 tells us that primes represented by Q have Dirichlet density $\frac{1}{2}$.

Exercises

5. Algebraic Number Fields

The purpose of this chapter is to present the results from algebraic number theory that we will assume to be known. We will also derive several results on the decomposition of primes that we will need later on.

5.1 Archimedean Valuations of a Number Field

Let K be an algebraic number field; we can write $K = \mathbb{Q}(\alpha)$, where α is a root of an irreducible polyonmial $f \in \mathbb{Q}[x]$. Actually, it is sometimes better to think of K as a purely algebraic object, namely $K = \mathbb{Q}[X]/(f)$; in this interpretation, $\alpha = X + (f)$ is a root of f, but it does not make sense to ask e.g. what $|\alpha|$ is. We can, however, define $\mathbb{Q}$-homomorphisms $\kappa_j : K \longrightarrow \mathbb{C}$ as follows: over the complex numbers, f factors into n distinct linear factors:

$$f(X) = (X - \alpha_1) \cdots (X - \alpha_n).$$

We now put $\kappa_j(\alpha) = \alpha_j$ and extend this linearly to K by demanding

$$\kappa_j\Big(\sum_{t=0}^{n-1} a_t\alpha^t\Big) = \sum_{t=0}^{n-1} a_t\kappa_j(\alpha)^t.$$

These maps $\kappa_1, \ldots, \kappa_n : K \longrightarrow \mathbb{C}$ are called embeddings of K into $\mathbb{C}$. They are $\mathbb{Q}$-homomorphism, that is, they respect the ring structure of K and are $\mathbb{Q}$-linear.

If $\kappa_j(K) \subset \mathbb{R}$, the embedding κ_j is called a real embedding, and a complex embedding otherwise. The number field $K = \mathbb{Q}(\sqrt[3]{2}\,)$, for example, has one real embedding sending $\alpha = X + (X^3 - 2)$ to $\sqrt[3]{2} \in \mathbb{R}$, and two complex embeddings sending α to $\rho\sqrt[3]{2}$ and $\rho^2\sqrt[3]{2}$, respectively, where ρ is a primitive cube root of unity. If κ_j is a complex embedding, then so is $\overline{\kappa_j}$ defined by $\overline{\kappa_j}(\alpha) = \overline{\kappa_j(\alpha)}$. Thus complex embeddings come in pairs. If we denote the number of real embeddings of K by r, and the number of complex embeddings by $2s$, then we always have $n = (K : \mathbb{Q}) = r + 2s$. The pair of natural numbers (r, s) is often called the signature of K.

Using these emebddings we now can define "archimedean valuations" on K as follows. For each $j = 1, \ldots, n$ set $|\alpha|_j = |\sigma_j(\alpha)|$, where the absolute value on the right hand side is the usual absolute value in $\mathbb{R}$ or $\mathbb{C}$. Since pairs $\kappa_j, \overline{\kappa_j}$ of complex embeddings give rise to the same valuation, this provides us with $r+s$ valuations $|\cdot|_1, \ldots, |\cdot|_{r+s}$.

Now assume that all the fields $\kappa_j(K)$ coincide. Then we can define $\sigma_j(\alpha) := \kappa_1^{-1}(\kappa_j(\alpha))$ and get endomorphisms $\sigma_j : K \longrightarrow K$. For $a \in \mathbb{Q}$, we clearly have $\sigma_j(a) = a$, and this shows that the σ_j are $\mathbb{Q}$-automorphisms of K. Thus in this case, the extension $K/\mathbb{Q}$ is normal, and we have $\operatorname{Gal}(K/\mathbb{Q}) = \{\sigma_1 = \mathrm{id}, \sigma_2, \ldots, \sigma_n\}$.

Conversely, if $K/\mathbb{Q}$ is Galois with Galois group $\operatorname{Gal}(K/\mathbb{Q}) = \{\sigma_1 = \mathrm{id}, \sigma_2, \ldots, \sigma_n\}$, and if κ_1 a fixed embedding of K, then the maps $\kappa_j := \kappa_1 \circ \sigma_j$ define distinct embeddings of K into $\mathbb{C}$. Thus in this case, we get all embeddings by twisting one of them with elements of $\operatorname{Gal}(K\mathbb{Q})$.

Trace and Norm

For any $\alpha \in K$, multiplication by α is a $\mathbb{Q}$-linear endomorphism $\mu_\alpha : K \longrightarrow K$ of the $\mathbb{Q}$-vector space K. With respect to some $\mathbb{Q}$-basis such as $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$, this linear map can be described by an $n \times n$-matrix M_α. The trace and the determinant of this matrix M_α are rational numbers that do not depend on the choice of the basis, and are called the trace $\operatorname{Tr}\alpha$ and the norm $N\alpha$ of α. It follows immediately that $\operatorname{Tr}(\alpha+\beta) = \operatorname{Tr}\alpha + \operatorname{Tr}\beta$ and $N(\alpha\beta) = N\alpha \cdot N\beta$.

Trace and norm can also be defined using the embeddings of K into $\mathbb{C}$: we have

$$\begin{aligned} \operatorname{Tr}\alpha &= \sigma_1(\alpha) + \ldots + \sigma_n(\alpha), \\ N\alpha &= \sigma_1(\alpha) \cdots \sigma_n(\alpha). \end{aligned}$$

5.2 Arithmetic of Number Fields

Ring of Integers

Algebraic integers are roots of monic polynomials with integral coefficients. If f is the minimal polynomial of an algebraic integer (the monic polynomial f with minimal degree such that $f(\alpha) = 0$), then f has integral coefficients.

The set $\mathbb{A}$ of algebraic integers forms a ring. The ring $\mathfrak{O}_K$ of integers in a number field K is defined by $\mathfrak{O}_K = \mathbb{A} \cap K$. Since traces and norms of algebraic integers are coefficients of their minimal polynomial, they are integers.

Algebraic integers $\alpha_1, \ldots, \alpha_n \in \mathfrak{O}_K$ are called an integral basis if every $\alpha \in \mathfrak{O}_K$ can be written as a $\mathbb{Z}$-linear combination of the α_i. It is not difficult to prove

Theorem 5.1. *Every number field has an integral basis.*

Proof. Among all $\mathbb{Q}$-bases $\alpha_1, \ldots, \alpha_n$ with $\alpha_j \in \mathfrak{O}_K$ choose one for which the natural number $|\operatorname{disc}(\alpha_1, \ldots, \alpha_n)|$ is minimal. It is then an easy matter to show that every $\alpha \in \mathfrak{O}_K$ is a $\mathbb{Z}$-linear combination of these α_j. □

More generally, each ideal $\mathfrak{a}$ in $\mathfrak{O}_K$ has a $\mathbb{Z}$-basis $\{\alpha_1, \ldots, \alpha_n\}$, and

$$\operatorname{disc}\mathfrak{a} = \operatorname{disc}(\alpha_1, \ldots, \alpha_n)$$

is independent of the choice of the integral basis, and is called the discriminant of $\mathfrak{a}$. If $\mathfrak{a} = \mathfrak{O}_K$ is the unit ideal, $\operatorname{disc} K := \operatorname{disc} \mathfrak{O}_K$ is called the discriminant of the field K.

Proposition 5.2. *For any integral ideal* $\mathfrak{a}$ *we have*

$$\operatorname{disc}\mathfrak{a} = N\mathfrak{a}^2 \cdot \operatorname{disc} K. \tag{5.1}$$

Proof. Instead of giving the proof, let me sketch the idea behind one of them. The result is almost obvious if $\mathfrak{a} = (\alpha)$ is a principal ideal, since then $\mathfrak{a}$ has a $\mathbb{Z}$-basis of the form $\alpha\omega_1, \ldots, \alpha\omega_n$, where $\omega_1, \ldots, \omega_n$ is an integral basis of K; equation (5.1) then follows immediately.

The problem now is that the Dedekind rings $\mathfrak{O}_K$ do not necessarily have class number 1. The solution to this problem is localization: let R be a domain and S a multiplicatively closed set not containing 0; then R_S is the set of all "fractions" $\frac{r}{s}$ with $r \in R$ and $s \in S$. If P is a prime ideal, then $S = R \setminus P$ is multiplicatively closed, and we call $R_P = R_S$ the localization of R at P. If $R = \mathfrak{O}_K$, the ring $R_\mathfrak{p}$ for a prime ideal $\mathfrak{p}$ has a unique nonzero prime ideal, namely $\mathfrak{p}R_\mathfrak{p}$, and is a principal ideal domain. In commutative algebra, this technique (it is completely elementary) is studied in detail, and it allows us to reduce the proof of (5.1) to a proof in all the localizations of $\mathfrak{O}_K$; but since these are PIDs, the proof given above applies. □

If f is the minimal polynomial of $\alpha \in \mathfrak{O}_K$, then $\operatorname{disc} K \mid \operatorname{disc} f$; in fact, these discriminants differ by a perfect square.

In quadratic number fields $\mathbb{Q}(\sqrt{m}\,)$ with squarefree $m \in \mathbb{Z}$, we can pick the integral basis $\{1, \sqrt{m}\,\}$ and $\{1, \frac{1}{2}(1+\sqrt{m}\,)\}$ according as $m \equiv 2, 3 \bmod 4$ or $m \equiv 1 \bmod 4$; the discriminant of K is $4m$ and m in these cases.

Let $\zeta = \zeta_p$ be a primitive p-th root of unity, i.e., a root of the cyclotomic polynomial

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + \ldots + X + 1.$$

The cyclotomic field $\mathbb{Q}(\zeta)$ has an integral basis $\{1, \zeta, \zeta^2, \ldots, \zeta^{p-2}\,\}$ and discriminant $(-1)^{(p-1)/2}p^{p-2}$.

The discriminant satisfies congruences modulo 4 and "modulo ∞":

Proposition 5.3. *Let K be a number field. Then*

1. $\operatorname{disc} K \equiv 0, 1 \bmod 4$ *(Stickelberger);*
2. $\operatorname{disc} K$ *has sign* $(-1)^s$.

Arithmetic of Ideals

The basic result here is

Theorem 5.4. *The ring of integers $\mathfrak{O}_K$ of a number field is a Dedekind domain.*

Recall that a domain R is a Dedekind domain if the following conditions hold:

1. R is integrally closed;
2. R is Noetherian;
3. every nonzero prime ideal of R is maximal.

These conditions are equivalent to the statement that every nonzero ideal in R can be written uniquely as a product of prime ideals.

Thus, in the number field case, for every rational prime p there are prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ with

$$p\mathfrak{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g};$$

the exponent e_j is called the ramification index of $\mathfrak{p}_j$. Since prime ideals are maximal, the residue class rings $\mathfrak{O}_K/\mathfrak{p}_j$ are finite fields; their cardinality is called the norm $N\mathfrak{p}_j$ of the prime ideal $\mathfrak{p}_j$. Moreover, $\mathfrak{O}_K/\mathfrak{p}_j$ has characteristic p, hence is an extension of the finite field $\mathbb{F}_p$ (in fact, the map sending a mod p to a mod $\mathfrak{p}_j$ is an injective ring homomorphism sending $\mathbb{F}_p$ to a subfield isomorphic to $\mathbb{F}_p$ inside $\mathfrak{O}_K/\mathfrak{p}_j$). Thus $\mathfrak{O}_K/\mathfrak{p}_j$ is a finite field with p^{f_j} elements (where $f_j = (\mathfrak{O}_K/\mathfrak{p}_j : \mathbb{F}_p)$ is the degree of the extension), and f_j is called the inertia degree of $\mathfrak{p}_j$. These numbers satisfy the relation $e_1f_1 + \ldots + e_gf_g = n$.

The actual decomposition of a prime p is computed as follows: let K be a number field of degree n; for every $\alpha \in \mathfrak{O}_K$, put $\operatorname{disc}(\alpha) = \operatorname{disc}(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$. Then $\operatorname{disc}(\alpha) = j^2 \operatorname{disc} K$ for an integer $j = j_\alpha$ that measures how far the subring $\mathbb{Z}[\alpha] = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \ldots \oplus \mathbb{Z}\alpha^{n-1}$ of $\mathfrak{O}_K$ differs from $\mathfrak{O}_K$: we have $j = (\mathfrak{O}_K : \mathbb{Z}[\alpha])$. A prime p dividing this index j for every choice of α is called an inessential discriminant divisor, and Dedekind showed that we always have $p < n$.

Theorem 5.5. *Assume that $K = \mathbb{Q}(\alpha)$, and let $f \in \mathbb{Z}[X]$ denote the minimal polynomial of α. We can decompose $f(X)$ into irreducible factors over $\mathbb{F}_p[X]$:*

$$f(X) = P_1(X)^{e_1} \cdots P_g(X)^{e_g}.$$

If $p \nmid j_\alpha$, then $p\mathfrak{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ for prime ideals $\mathfrak{P}_i = (p, P_i(\alpha))$ with inertia degrees $f_i = \deg P_i$.

Observe that this immediately implies $n = e_1f_1 + \ldots + e_gf_g$ since $n = \deg f = e_1 \deg P_1 + \ldots + e_g \deg P_g$. Also note that in quadratic fields and in cyclotomic fields we can always find an α with $j_\alpha = 1$.

5.3 Prime Decomposition in Relative Extensions

So far we have studied number fields K mostly as extensions of $\mathbb{Q}$. In class field theory, we will almost always deal with extensions L/K of number fields.

Some of the definitions we have given can be applied directly to the relative situation: for example, the relative trace $\operatorname{Tr}_{L/K}$ and the relative norm $N_{L/k}$ can be defined in a completely analogous way: multiplication by $\alpha \in L$ is a K-linear map etc. Again the trace is additive and the norm multiplicative; moreover, if $L/F/K$ is a tower of number fields, then it is easily checked that $\operatorname{Tr}_{L/K}\alpha = \operatorname{Tr}_{F/K}(\operatorname{Tr}_{L/F}\alpha)$ and $N_{L/K}\alpha = N_{F/K}(N_{L/F}\alpha)$. Moreover, if $\alpha \in F$, then $\operatorname{Tr}_{L/K}\alpha = (L:F)\cdot\operatorname{Tr}_{F/K}\alpha$ and $N_{L/K}\alpha = (N_{F/K}\alpha)^{(L:F)}$.

We can also extend the norm to ideals: if $\mathfrak{A}$ is an ideal in $\mathfrak{O}_L$, then the ideal generated by the norms $N_{L/K}\alpha$, where α runs through $\mathfrak{A}$, is an ideal in $\mathfrak{O}_K$ denoted by $\mathbb{N}_{L/K}\mathfrak{A}$. If $\sigma_1, \ldots, \sigma_n$ are the $n = (L:K)$ embeddings of L into $\mathbb{C}$ that fix K elementwise, then there is a unique ideal $\mathfrak{a}$ in $\mathfrak{O}_K$ such that $\mathfrak{a}\mathfrak{O}_N = \sigma_1(\mathfrak{A})\cdots\sigma_n(\mathfrak{A})$, where the product of the ideals is formed inside the normal closure N of L/K, and we have $\mathfrak{a} = N_{L/K}\mathfrak{A}$.

If a prime ideal $\mathfrak{p}$ in $\mathfrak{O}_K$ splits as $\mathfrak{p}\mathfrak{O}_L = \mathfrak{P}_1^{e_1}\cdots\mathfrak{P}_g^{e_g}$, then the prime ideals $\mathfrak{P}_j$ are said to lie above $\mathfrak{p}$; the exponents $e_j = e(\mathfrak{P}_j|\mathfrak{p}) = e_{K/k}(\mathfrak{P}_j)$ are called the relative ramification indices, and the relative degrees $f_j = f(\mathfrak{P}_j|\mathfrak{p})$ of the extensions $(\mathfrak{O}_K/\mathfrak{P}_j)/(\mathfrak{O}_k/\mathfrak{p})$ are called the relative inertia degrees. As before, we have $n = (L:K) = e_1f_1 + \ldots + e_gf_g$.

The prime ideal $\mathfrak{P}_j$ is said to be ramified in L/K if $e_j > 1$; the prime ideal $\mathfrak{p}$ is said to be ramified in L/K if at least one of the e_j is > 1. The same remarks apply to infinite primes.

If L/K has degree n, we also can define the relative discriminant of elements $\alpha_1, \ldots, \alpha_n$ as before. But the definition of the discriminant of a number field cannot be transferred directly to relative extensions, since in general a number field L does not have a relative integral basis (that is, there do not exist $\alpha_1, \ldots, \alpha_n \in \mathfrak{O}_L$ such that every $\alpha \in \mathfrak{O}_L$ is an $\mathfrak{O}_K$-linear combination of the α_j). The reason for this failure is that the proof of the existence of an integral basis over $\mathbb{Q}$ uses the fact that $\mathbb{Q}$ has class number 1. Thus we have to proceed differently.

First recall the definition of fractional ideals in $\mathfrak{O}_K$: these are $\mathbb{Z}$-modules $\mathfrak{a} \subseteq K$ with the property that there is an $\alpha \in K^\times$ such that $\alpha\mathfrak{a}$ is an integral ideal. For example, the set $\mathfrak{a} = \{\frac{3a}{2} : a \in \mathbb{Z}\}$ is a fractional ideal in $\mathbb{Z}$ since $2\mathfrak{a} = (3)$. If $\mathfrak{a}$ is a nonzero fractional ideal, we put $\mathfrak{a}^{-1} = \{\alpha \in K : \alpha\mathfrak{a} \subseteq \mathfrak{O}_K\}$. If $\mathfrak{a}$ has the prime ideal factorization $\mathfrak{a} = \mathfrak{p}_1^{a_1}\cdots\mathfrak{p}_r^{a_r}$ (where the exponents are integers, i.e., may be negative), then $\mathfrak{a}^{-1} = \mathfrak{p}_1^{-a_1}\cdots\mathfrak{p}_r^{-a_r}$.

It is now easy to check that, for extensions L/K of number fields, the set

$$\mathfrak{O}_L^* = \{\alpha \in K : \operatorname{Tr}_{L/K}\alpha\omega \in \mathfrak{O}_k \text{ for all } \omega \in \mathfrak{O}_L\}$$

is a fractional ideal; since $\mathfrak{O}_L \subset \mathfrak{O}_L^*$, its inverse $(\mathfrak{O}_L^*)^{-1} =: \operatorname{diff}(L/K)$ is an *integral* ideal in $\mathfrak{O}_L$ called the (relative) different of the extension L/K.

The relative discriminant of L/K is simply the relative norm of the different: $\operatorname{disc}(L/K) = N_{L/K}\operatorname{diff}(L/K)$. The different is an important invariant of an extension L/K, and is multiplicative in towers $L/F/K$ of number fields:

Proposition 5.6. *The different and the discriminant have the following properties:*

1. $\operatorname{diff}(L/K) = \operatorname{diff}(L/F) \cdot \operatorname{diff}(F/K)$*;*
2. $\operatorname{disc}(L/K) = N_{F/K}\operatorname{disc}(L/F) \cdot \operatorname{disc}(F/K)^{(L:F)}$*;*
3. $\operatorname{disc}(K/\mathbb{Q}) = (\operatorname{disc} K)$*.*

The second claim follows immediately from the first by taking norms.

The most important property of the different and the discriminant is contained in the following

Theorem 5.7. *A prime ideal $\mathfrak{P}$ in $\mathfrak{O}_L$ above the prime ideal $\mathfrak{p}$ in $\mathfrak{O}_K$ is ramified if and only if $\mathfrak{P} \mid \operatorname{diff}(L/K)$; the prime ideal $\mathfrak{p}$ is ramified in L/K if and only if $\mathfrak{p} \mid \operatorname{disc}(L/K)$.*

Valuations

Every rational prime p defines a valuation on $\mathbb{Q}$: in fact, let $v_p(a)$ denote the exponent of p in the prime factorization of $a \in \mathbb{Q}^\times$ (for example, $v_2(\frac{3}{4}) = -2$, $v_3(\frac{3}{4}) = 1$, and $v_p(\frac{3}{4}) = 0$ for all primes $p \geq 5$); extend this map to all of $\mathbb{Q}$ by setting $v_p(0) = \infty$ (observe that 0 is infinitely often divisible by p). Then $v_p : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{\infty\}$ is a map with the following properties:

1. $v_p(a) = \infty$ if and only if $a = 0$;
2. $v_p(ab) = v_p(a) + v_p(b)$;
3. $v_p(a + b) \geq \min\{v_p(a), v_p(b)\}$.

If we put $|a|_p = p^{-v_p(a)}$, we get a new map $v_p : \mathbb{Q} \longrightarrow \mathbb{R}$ with the following properties:

1. $|a|_p \geq 0$, with equality if and only if $a = 0$;
2. $|ab|_p = |a|_p|b|_p$;
3. $|a + b|_p \leq \max\{|a|_p, |b|_p\}$.

Thus the maps $|\cdot|_p$ are valuations, that is, maps $v : \mathbb{Q} \longrightarrow \mathbb{R}$ with the properties

1. $|a| = 0$, with equality if and only if $a = 0$;
2. $|ab| = |a| \cdot |b|$;
3. $|a + b| \leq |a| + |b|$.

Note, however, that the $|\cdot|_p$ satisfy a stronger triangle inequality (they are called non-archimedean valuations). In addition to these valuations attached to primes p, there is the archimedean valuation $|\cdot|$ given by the usual absolute value. It can be shown that, up to rescaling, the valuations $|\cdot|_p$, $|\cdot|$, and the trivial valuation sending nonzero numbers to 1 are the only valuations on $\mathbb{Q}$.

Note that the integers can be characterized as the set of all rational numbers z with $|z|_p \le 1$ for all primes p.

All this generalizes to number fields: every prime ideal $\mathfrak{p}$ defines an additive valuation $v_{\mathfrak{p}}$ on K by sending $\alpha \in K^\times$ to the exponent of $\mathfrak{p}$ in the prime ideal factorization of the ideal (α), and then the function $|\alpha|_{\mathfrak{p}} = N\mathfrak{p}^{-v_{\mathfrak{p}}(\alpha)}$ gives us a non-archimedean valuation.

An extension L/K is called *unramified* outside ∞ if no prime ideal from K is ramified in L; this is the case if and only if $\operatorname{disc}(L/K) = (1)$. We say that L/K is unramified (everywhere) if it is unramified outside ∞, and if no infinite prime is ramified in L/K.

5.4 Prime Ideals in Galois Extensions

In the following, let L/K be a finite Galois extension of number fields with Galois group $G = \operatorname{Gal}(L/K)$. Let $\mathfrak{O} = \mathfrak{O}_L$ and $\mathfrak{o} = \mathfrak{O}_K$ denote the corresponding rings of integers, $\mathfrak{p}$ a prime ideal in $\mathfrak{o}$, and

$$\mathfrak{p}\mathfrak{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g} \tag{5.2}$$

its prime ideal factorization in L. We will also denote the residue class field of a prime ideal by κ; thus e.g. $\kappa(\mathfrak{P}) = \mathfrak{O}/\mathfrak{P}$ and $\kappa(\mathfrak{p}) = \mathfrak{o}/\mathfrak{p}$.

Since $\mathfrak{P}_j \mid \mathfrak{p}\mathfrak{O}$, we clearly have $\mathfrak{p} \subseteq \mathfrak{P}_j \cap \mathfrak{o}$ (here we have used $\mathfrak{p}\mathfrak{O} \cap \mathfrak{o} = \mathfrak{p}$; prove this!); on the other hand, $\mathfrak{p}$ is a maximal ideal, so either $\mathfrak{P}_j \cap \mathfrak{o} = \mathfrak{p}$ or $\mathfrak{P}_j \cap \mathfrak{o} = \mathfrak{o}$; in the last case, we find the contradiction $1 \in \mathfrak{P}_j$, hence we must have $\mathfrak{P}_j \cap \mathfrak{o} = \mathfrak{p}$.

We have proved

Lemma 5.8. *If $\mathfrak{P}$ is a prime ideal above $\mathfrak{p}$ in L, then $\mathfrak{p} = \mathfrak{P} \cap \mathfrak{o}$.*

Note that since $\mathfrak{P} \subset \mathfrak{O}$, we also have $\mathfrak{P} \cap K \subseteq \mathfrak{P} \cap K \cap \mathfrak{O} = \mathfrak{P} \cap \mathfrak{o}$, and since the inverse inclusion is trivial, we conclude that $\mathfrak{p} = \mathfrak{P} \cap K$.

Recall the the absolute norm $N_L\mathfrak{P}$ of a prime ideal $\mathfrak{P}$ is the cardinality of the residue class field $\mathfrak{O}/\mathfrak{P}$. This immediately implies that $N_L\mathfrak{P} = (N_K\mathfrak{p})^{f(\mathfrak{P}|\mathfrak{p})}$. Moreover, $N_{L/\mathbb{Q}}\mathfrak{P}$ is known to be the ideal generated by $N_L\mathfrak{P}$, and this shows that $N_{L/K}\mathfrak{P} = \mathfrak{p}^{f(\mathfrak{P}|\mathfrak{p})}$.

Now we claim

Proposition 5.9. *The Galois group acts transitively on the prime ideals above $\mathfrak{p}$.*

This means that if $\mathfrak{P}_i$ and $\mathfrak{P}_j$ are two prime ideals above $\mathfrak{p}$, then there is a $\sigma \in G$ such that $\mathfrak{P}_j = \mathfrak{P}_i^\sigma$.

Proof. We use the Chinese Remainder Theorem. Let $\mathfrak{P} = \mathfrak{P}_i$ and $\mathfrak{P}' = \mathfrak{P}_j$ denote two distinct prime ideals above $\mathfrak{p}$. Then we can find an $\alpha \in \mathfrak{O}$ with $\alpha \equiv 0 \bmod \mathfrak{P}$ and $\alpha \equiv 1 \bmod \mathfrak{P}_j$ for all $j \ne i$.

Now $N_{L/K}\alpha \in \mathfrak{o} \cap \mathfrak{P} = \mathfrak{p}$, and from $\mathfrak{p} \subset \mathfrak{P}_j$ we conclude that $N_{L/K}\alpha \in \mathfrak{P}_j$. Thus $\mathfrak{P}_j \mid \prod_{\sigma \in G} \alpha^\sigma$, and since $\mathfrak{P}_j$ is prime, we must have $\mathfrak{P}_j \mid \alpha^\sigma$ for a suitable $\sigma \in G$. But then $\alpha \in \sigma^{-1}(\mathfrak{P}_j)$, and our construction implies that we must have $\sigma^{-1}(\mathfrak{P}_j) = \mathfrak{P}$, that is, $\mathfrak{P}^\sigma = \mathfrak{P}_j$. □

Now consider the factorization (5.2). Then e_1 is the exponent of $\mathfrak{P}_1$ in the prime ideal factorization of $\mathfrak{p}\mathfrak{O}$. Let σ denote an automorphism that maps $\mathfrak{P}_1$ to $\mathfrak{P}_j$; then e_1 is the exponent of $\mathfrak{P}_j$ in the prime ideal factorization of $\mathfrak{p}\mathfrak{O}$. The theorem of unique factorization into prime ideals then implies that we must have $e_j = e_1$. Thus in Galois extensions, all ramification indices coincide, and we can write $e_1 = \ldots = e_g =: e$.

Since $\mathfrak{O}^\sigma = \mathfrak{O}$, the automorphism σ of L/K induces an isomorphism $\kappa(\mathfrak{P}_1) \longrightarrow \kappa(\mathfrak{P}_j)$ by sending a residue class $\alpha + \mathfrak{P}_1$ to $\alpha^\sigma + \mathfrak{P}_j$; this map leaves the elements of $\kappa(\mathfrak{p})$ fixed, hence is a $\kappa(\mathfrak{p})$-isomorphism $\kappa(\mathfrak{P}_1) \longrightarrow \kappa(\mathfrak{P}_j)$. In particular, these extensions must have the same degree over $\kappa(\mathfrak{p})$, and we conclude that $f_1 = \ldots = f_g =: f$. We have proved:

Proposition 5.10. *In Galois extensions L/K, a prime $\mathfrak{p}$ in k splits as*

$$\mathfrak{p}\mathfrak{O} = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e,$$

where each $\mathfrak{P}_i$ has inertia degree f, and we have $efg = n = (L : K)$.

The Decomposition Group

Let $\mathfrak{P}$ denote a prime ideal in $\mathfrak{O}$ above $\mathfrak{p}$, and recall that $\mathfrak{p}\mathfrak{O} = (\mathcal{P}_1 \cdots \mathcal{P}_g)^e$. Define the decomposition group $Z(\mathfrak{P}|\mathfrak{p})$ by

$$Z(\mathfrak{P}|\mathfrak{p}) = \{\sigma \in G : \mathfrak{P}^\sigma = \mathfrak{P}\}.$$

This is the stabiliser group of $\mathfrak{P}$. The fixed field of $Z(\mathfrak{P}|\mathfrak{p})$ is a subfield L_Z of K/k and is called the decomposition field of $\mathfrak{P}|\mathfrak{p}$.

For a quadratic extension L/K with Galois group G of order 2, there are only three possibilities:

decomposition	$Z(\mathfrak{P}\|\mathfrak{p})$
$\mathfrak{p}$ splits	1
$\mathfrak{p}$ is inert	G
$\mathfrak{p}$ ramifies	G

For finding the order of $Z(\mathfrak{P}|\mathfrak{p})$ in general, we consider the following abstract situation: a finite group G acts transitively on a set $X = \{x_1, \ldots, x_g\}$; let $G_x = \{\sigma \in G : \sigma x = x\}$ denote the stabiliser of x. Define a map ϕ from the cosets of G/G_x to the elements of X by sending σG_x to σx. Since G acts transitively, ϕ is surjective. Moreover ϕ is injective: if $\sigma x = \tau x$, then $\tau^{-1}\sigma \in G_x$ and hence $\tau G_x = \tau\tau^{-1}\sigma G_x = \sigma G_x$. Thus there is a bijection between the cosets of G/G_x and the elements of X:

Lemma 5.11. *Assume that a group G acts transitively on a finite set X. Let G_x denote the stabiliser of $x \in X$. Then $(G : G_x) = \#X$.*

When we apply this lemma to our situation, we find

Corollary 5.12. *We have $(G : Z(\mathfrak{P}|\mathfrak{p})) = g$.*

Since the decomposition group has index g in G, Galois theory tells us that the degree of the decomposition field L_Z over K is also equal to g.

Note that this result is already nontrivial: the group G has order efg, and we have just proved the existence of a subgroup of order g. Recall that, for arbitrary finite groups, it is not true that for every divisor n of the group order there is a subgroup of order n.

We will now study how the prime ideal $\mathfrak{p}$ splits in the intermediate fields of L/K as we go from K to L.

Lemma 5.13. *Let $\mathfrak{q} = \mathfrak{P} \cap L_Z$ be the prime ideal below $\mathfrak{P}$ in L_Z.*

1. *$\mathfrak{q}$ does not split in L/L_Z; in other words, $\mathfrak{P}$ is the only prime ideal above $\mathfrak{q}$ in $\mathfrak{O}$.*
2. *$e(\mathfrak{P}|\mathfrak{q}) = e$ and $f(\mathfrak{P}|\mathfrak{q}) = f$.*
3. *$e(\mathfrak{q}|\mathfrak{p}) = f(\mathfrak{q}|\mathfrak{p}) = 1$.*

Proof. We have

$$Z(\mathfrak{P}|\mathfrak{q}) = \{\sigma \in \operatorname{Gal}(L/L_Z) : \mathfrak{P}^\sigma = \mathfrak{P}\} = Z(\mathfrak{P}|\mathfrak{p}) = \operatorname{Gal}(L/L_Z),$$

hence $g(\mathfrak{P}|\mathfrak{q}) = (\operatorname{Gal}(L/L_Z) : Z(\mathfrak{P}|\mathfrak{q}) = 1$. This proves the first claim. Next

$$e = e(\mathfrak{P}|\mathfrak{p}) = e(\mathfrak{P}|\mathfrak{q}) \cdot e(\mathfrak{q}|\mathfrak{p}) \quad \text{and} \quad f = f(\mathfrak{P}|\mathfrak{p}) = f(\mathfrak{P}|\mathfrak{q}) \cdot f(\mathfrak{q}|\mathfrak{p}).$$

Moreover, from 1, we see that $e(\mathfrak{P}|\mathfrak{q}) \cdot f(\mathfrak{P}|\mathfrak{q}) \cdot 1 = (L : L_Z) = ef$. Since $e(\mathfrak{P}|\mathfrak{q}) \le e$ and $f(\mathfrak{P}|\mathfrak{q}) \le f$, we must have equality. The third claim now follows, too. □

Theorem 5.14. *Let L/K be a normal extension and $\mathfrak{P}$ a prime ideal above $\mathfrak{p}$ in L. Then L_Z is the largest intermediate field F such that $e(\mathfrak{q}|\mathfrak{p}) = f(\mathfrak{q}|\mathfrak{p}) = 1$.*

Corollary 5.15. *A prime ideal that splits completely in two extensions L_1/K and L_2/K splits completely in the compositum L_1L_2K.*

Corollary 5.16. *Let L/K be an extension of number field. A prime that splits completely in L/K splits completely in the normal closure of L/K.*

Decomposition Groups for Infinite Primes

Let us set up the notation. If σ is an embedding of K and τ an embedding of L restricting to σ, then all the embeddings of L restricting to τ are given by $\tau\sigma_j$ as σ_j runs through $G = \mathrm{Gal}\,(L/K)$. If v is the valuation on K defined by τ and w the valuation on L defined by σ, then the embeddings $\tau\sigma_j$ induce the valuations of L restricting to v. If the infinite prime ∞ attached to v does not ramify, then these valuations are pairwise different. If ∞ ramifies (this happens if $\sigma(K)$ is real, but $\tau(L)$ is complex), however, then $\sigma_w(\alpha) := \tau^{-1}(\overline{\tau(\alpha)})$ defines an element $\sigma_w \in G$ (in fact, if $\alpha \in K$, then $\tau(\alpha) = \sigma(\alpha)$ is real, hence $\sigma_w(\alpha) = \tau^{-1}(\overline{\tau(\alpha)}) = \tau^{-1}\tau(\alpha) = \alpha$) that fixes the subfield $L_w := \tau^{-1}(L^\tau \cap \mathbb{R})$; since $\tau(\sigma_w^2(\alpha)) = \overline{\tau(\sigma_w(\alpha))} = \overline{\overline{\tau(\alpha)}} = \tau(\alpha)$, the element σ_w has order 2. Note that $\tau\sigma_j$ and $\tau\sigma_w\sigma_j$ both induce the same valuation since $|\tau\sigma_w\sigma_j(\alpha)| = |\overline{\tau(\sigma_j(\alpha))}| = |\tau(\sigma_j(\alpha))|$.

The group $Z(w|v) = \{1, \sigma_w\}$ is called the decomposition group of w, and its fixed field L_w the corresponding decomposition field.

5.5 Minkowski Bounds

The geometric techniques introduced by Minkowski allow us to give rather simple proofs of the two fundamental finiteness results of algebraic number theory: the finiteness of the class number and Dirichlet's unit theorem, according to which the unit group of the rings $\mathfrak{O}_K$ are finitely generated.

Theorem 5.17 (Minkowski Bounds). *Let K be a number field with degree $n = r + 2s$. Then every ideal class contains an integral ideal $\mathfrak{a}$ with norm*

$$N\mathfrak{a} \le \frac{n!}{n^n}\Big(\frac{4}{\pi}\Big)^s \sqrt{|\mathrm{disc}\,K|}.$$

Since $N\mathfrak{a} \ge 1$, the Minkowski bounds imply that $|\mathrm{disc}\,K| \ge \big(\frac{n^n}{n!}(\frac{\pi}{4})^s\big)^2$. It is easy to show that the expression on the right hand side is > 1 for all number fields of degree $n > 1$; this implies the following result conjectured by Kronecker:

Corollary 5.18. *Let K be a number field $\ne \mathbb{Q}$; then* $\mathrm{disc}\,K > 1$. *In particular, in every number field $\ne \mathbb{Q}$ at least one prime ramifies.*

Let $\sigma_1, \ldots, \sigma_n$ denote the embeddings of K into $\mathbb{R}$ and $\mathbb{C}$ and order them in such a way that $\sigma_1, \ldots, \sigma_r$ are the real embeddings, and that the σ_{r+s+j} are the complex conjugate of σ_{r+j}. Let $K_\mathbb{R} = \mathbb{R}^r \times \mathbb{C}^s$ denote the tensor product[1] of K with $\mathbb{R}$; then set

$$\iota(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_r(\alpha), \sigma_{r+1}(\alpha), \ldots, \sigma_{r+s}(\alpha)).$$

[1] This is easily verified as follows: write $K = \mathbb{Q}\alpha_1 \oplus \ldots \oplus \mathbb{Q}\alpha_n$; then $K \otimes_\mathbb{Q} \mathbb{R} = \mathbb{R}\alpha_1 \oplus \ldots \oplus \mathbb{R}\alpha_n$. But $\mathbb{R}\alpha = \mathbb{R}$ if α is real, and $\mathbb{R}\alpha = \mathbb{C}$ otherwise.

The map $\iota : K \longrightarrow K_{\mathbb{R}}$ is a group homomorphism of the additive group (in fact, it even respects multiplication, but we will not need that at the moment), and it is obviously injective (already $\sigma_1(\alpha) = 0$ implies $\alpha = 0$).

If, for $x = (x_1, \ldots, x_{r+s}) \in \mathbb{R}^r \times \mathbb{C}^s$, we define

$$N(x) = |x_1 \cdots x_r (x_{r+1} \cdots x_{r+s})^2|,$$

then clearly $N(\iota(\alpha)) = |N\alpha|$ for all $\alpha \in K$, hence the following diagram commutes:

$$\begin{tikzcd}
K \arrow[r, "\iota"] \arrow[d, "N^K_{\mathbb{Q}}"'] & K_{\mathbb{R}} \arrow[d, "N"] \\
\mathbb{Q} \arrow[r] & \mathbb{R}
\end{tikzcd}$$

The map at the bottom is the usual embedding of $\mathbb{Q}$ into $\mathbb{R}$. By the way, the point of using these commutative diagrams is not preparing the application of homological methods; their only purpose is helping you “see” what’s going on.

For computing volumes it is desirable to work in $\mathbb{R}^n$; the isomorphism $\mathbb{C} \simeq \mathbb{R}^2$ of vector spaces allows us to replace $K_{\mathbb{R}}$ by $\mathbb{R}^n$ via the linear map

$$(x_1, \ldots, x_{r+s}) \longmapsto (x_1, \ldots, x_r, \operatorname{Re} x_{r+1}, \operatorname{Im} x_{r+1}, \ldots, \operatorname{Re} x_{r+s}, \operatorname{Im} x_{r+s}).$$

For example, the element $1 + i \in \mathbb{C}$ corresponds to the vector $(1, 1) \in \mathbb{R}^2$.

The composition of ι with this isomorphism gives us an embedding $\iota^* : K \longrightarrow \mathbb{R}^n$. If we give both $\mathbb{Q}$-vector spaces their natural topology, the image of ι^* is dense in $\mathbb{R}^n$. Note that ι^* is still a group homomorphism from the additive group of K to that of $\mathbb{R}^n$, but that multiplicativity has been destroyed by the isomorphism $\mathbb{R}^r \times \mathbb{C}^s \simeq \mathbb{R}^n$.

The extension of the norm function to $\mathbb{R}^n$ is defined by

$$N(x) = |x_1 \cdots x_r (x_{r+1}^2 + x_{r+2}^2) \cdots (x_{n-1}^2 + x_n^2)|,$$

and we get a commutative diagram of $\mathbb{Q}$-vector spaces

$$\begin{tikzcd}
K \arrow[r, "\iota"] \arrow[d, "N^K_{\mathbb{Q}}"'] & K_{\mathbb{R}} \arrow[r, "\simeq"] \arrow[d, "N"] & \mathbb{R}^n \arrow[d, "N"] \\
\mathbb{Q} \arrow[r] & \mathbb{R} \arrow[r, "id"] & \mathbb{R}
\end{tikzcd}$$

A lattice Λ is a discrete additive subgroup of $\mathbb{R}^n$; each lattice has the form $\Lambda = \mathbb{Z}\xi_1 \oplus \ldots \oplus \mathbb{Z}\xi_t$ for some real numbers $\xi_1, \ldots, \xi_t$ and $t \le n$; lattices with maximal rank n are called full lattices. The elements $\xi_1, \ldots, \xi_t$ are called a basis of the lattice, and the set

$$P_\Lambda = \{x \in \mathbb{R}^n : x = \sum a_j \xi_j, 0 \le a_j < 1\}$$

is called a fundamental domain of Λ (P_Λ depends on the choice of the basis).

Let $\{\alpha_1, \ldots, \alpha_n\}$ be a $\mathbb{Q}$-basis of K; then their discriminant, which is the square of the determinant

$$D = \begin{vmatrix} \sigma_1(\alpha_1) & \ldots & \sigma_n(\alpha_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(\alpha_n) & \ldots & \sigma_n(\alpha_n), \end{vmatrix},$$

is nonzero. Assume we have ordered the embeddings in the following way: the embeddings $\sigma_1, \ldots, \sigma_r$ are real, and the complex embeddings are σ_{r+1}, $\sigma_{r+2} = \overline{\sigma_{r+1}}, \ldots$. Adding the columns with index $r+2$, $r+4$, etc. to those preceding them and factoring out the resulting factor 2 from s columns shows that

$$D = 2^s \begin{vmatrix} \sigma_1(\alpha_1) & \ldots & \operatorname{Re}\sigma_r(\alpha_1) & \overline{\sigma}_r(\alpha_1) & \ldots \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ \sigma_1(\alpha_n) & \ldots & \operatorname{Re}\sigma_r(\alpha_n) & \overline{\sigma}_r(\alpha_n) & \ldots \end{vmatrix}.$$

Subtracting the columns with index $r+1$, $r+3$ etc. from those following them and pulling out the resulting factors i from s of the columns shows that

$$D = (2i)^s \det(\iota^*(\alpha_j)). \tag{5.3}$$

If the α_j form an integral basis of K, then their discriminant is $\operatorname{disc} K$, and we find $\det(\iota^*(\alpha_j))^2 = (-4)^{-s} \operatorname{disc} K$.

Lemma 5.19. *$\iota^*(\mathfrak{O}_K)$ is a full lattice in $\mathbb{R}^n$.*

Proof. Clearly $\iota^*(\mathfrak{O}_K)$ is an additive subgroup of $\mathbb{R}^n$, so we only have to show that $\iota^*(\mathfrak{O}_K)$ is discrete. To this end, let C_t denote the hypercube in $\mathbb{R}^n$ defined by the inequalities $|x_j| \le t$. If $\iota^*(\alpha) \in C_t$, then $|\sigma_j(\alpha)| \le t$ for $j = 1, \ldots, r$, and $|\sigma_j(\alpha)| \le \sqrt{2}\,t$ for $j = r+1, \ldots, n$. This implies that the coefficients of the minimal polynomial $f(X) = \prod(X - \sigma_j(\alpha))$ are bounded, hence there can only be finitely many such α. □

The volume of P_Λ can be expressed as a determinant:

Lemma 5.20. *Let Λ be a full lattice in $\mathbb{R}^n$ with fundamental domain P_Λ. Let $\xi_1, \ldots, \xi_n$ be a $\mathbb{Z}$-basis of Λ, and write $\xi_j = \sum a_{ij} e_i$, where the e_i form the standard basis of* $\mathbb{R}^n$. *Then* $\operatorname{vol}(P_\Lambda) = |\det(a_{ij})|$.

Proof. The volume of P_Λ is the absolute value of the integral $\int_{P_\Lambda} dx_1 \cdots dx_n$. Consider the the linear map T with $T(e_i) = \xi_i$, and define the change of variables $T(u_1, \ldots, u_n) = (x_1, \ldots, x_n)$. This maps the "unit cube" P_E, that is, the fundamental domain of the lattice E with the standard basis $\{e_1, \ldots, e_n\}$, to P_Λ, and the Jacobian transformation formula gives us

$$\left| \int_{P_\Lambda} dx_1 \cdots dx_n \right| = \left| \int_{P_E} (\det a_{ij}) du_1 \cdots du_n \right| = |\det a_{ij}|.$$

□

Thus $\mathrm{vol}\,(\Lambda) := \mathrm{vol}\,(P_\Lambda)$ does not depend on the choice of the basis, and (5.3) tells us that

$$\mathrm{vol}\,(\iota^*(\mathfrak{O}_K)) = 2^{-s}|\mathrm{disc}\,K|.$$

If Λ' is a full sublattice of Λ, then the index $(\Lambda : \Lambda')$ is finite, and it is easily checked that

$$\mathrm{vol}\,(\Lambda') = (\Lambda : \Lambda')\mathrm{vol}\,(\Lambda).$$

Thus if $\mathfrak{a}$ is an ideal in $\mathfrak{O}_K$, then

$$\mathrm{vol}\,(\iota^*(\mathfrak{a})) = 2^{-s}N\mathfrak{a}\,\sqrt{|\mathrm{disc}\,K|}.$$

We now have to invoke Minkowski's geometry of numbers. The basic result we need is

Theorem 5.21. *Let Λ be a full lattice in $\mathbb{R}^n$, and let S be a convex, compact, measurable, centrally symmetric subset of $\mathbb{R}^n$ with*

$$\mathrm{vol}\,(S) \geq 2^n \mathrm{vol}\,(\Lambda).$$

Then S contains a nonzero lattice point.

A set S is convex if it has the property that for all $x, y \in S$, the whole line segment joining x and y is in S. The term measurable refers to the Lebesgue measure in $\mathbb{R}^n$ and basically means that we can attach a volume to S. Finally, S is centrally symmetric if $x \in S$ implies $-x \in S$.

Minkowski's result is intuitively clear in small dimensions, and giving a rigorous proof is quite easy.

Corollary 5.22. *Assume S is a convex, compact, measurable, centrally symmetric subset of $\mathbb{R}^n$ with the property that $|N(x)| \leq 1$ for all $x \in X$. Then every full lattice Λ in $\mathbb{R}^n$ contains a nonzero point x with*

$$|N(x)| \leq \frac{2^n}{\mathrm{vol}\,(X)}\mathrm{vol}\,(\Lambda).$$

This follows easily by applying Theorem 5.21 to the set $S = tX$ for a real number t with

$$t^n = \frac{2^n}{\mathrm{vol}\,(X)}\mathrm{vol}\,(\Lambda).$$

The whole point of getting good bounds such as Minkowski's is finding a set S with the required properties that is as large as possible. The choice $S = \{(x_1, \ldots, x_n)\}$, where the x_j satisfy the inequalities

$$|x_1|, \ldots, |x_r| \leq 1, x_{r+1}^2 + x_{r+2}^2, \ldots, x_{n-1}^2 + x_n^2 \leq 1,$$

obviously has the properties we need, and its volume is easily seen to be $\mathrm{vol}\,(S) = 2^r\pi^s$. This leads to the existence of a point $x \in \Lambda \setminus \{0\}$ with $|N(x)| \leq (\frac{4}{\pi})^s\mathrm{vol}\,(\Lambda)$.

A better choice is the set T consisting of points satisfying

$$|x_1| + \ldots + |x_r| + 2\sqrt{x_{r+1}^2 + x_{r+2}^2} + \ldots + 2\sqrt{x_{n-1}^2 + x_n^2} \le n.$$

Showing that T has all the required properties is not very difficult, and a computation via double induction on r and s readily shows that

$$\operatorname{vol}(T) = \frac{n^n}{n!} 2^r \Big(\frac{\pi}{2}\Big)^s.$$

With this choice of $X = T$, Cor. 5.22 gives

Theorem 5.23. *Let Λ be a full lattice in $\mathbb{R}^n$. Then there is an $x \in \Lambda \setminus \{0\}$ with*

$$N(x) \le \frac{n!}{n^n} \Big(\frac{8}{\pi}\Big)^s \operatorname{vol}(\Lambda).$$

If we apply this to the lattice $\iota^*(\mathfrak{a})$ for some nonzero ideal $\mathfrak{a}$ we get

Corollary 5.24. *Every nonzero ideal $\mathfrak{a}$ in $\mathfrak{O}_K$ contains a nonzero element α with*

$$|N_{K/\mathbb{Q}}(\alpha)| \le \frac{n!}{n^n} \Big(\frac{4}{\pi}\Big)^s \sqrt{|\operatorname{disc} K|} \cdot N\mathfrak{a}. \tag{5.4}$$

The Minkowski bounds follow from this by applying a trick we have seen before: let $c \in \operatorname{Cl}(K)$ be an ideal class, and pick an integral ideal $\mathfrak{a} \in c^{-1}$; by Corollary 5.24, the ideal $\mathfrak{a}$ contains an element α satisfying (5.4). Thus $\mathfrak{a}\mathfrak{b} = (\alpha)$, and $\mathfrak{b} \in c$ has norm $N\mathfrak{b} = |N\alpha|/N\mathfrak{a}$.

Exercises

5.1 Show that quadratic number fields $\mathbb{Q}(\sqrt{m}\,)$ have $(r, s) = (2, 0)$ or $(r, s) = (0, 1)$ according as $m > 0$ or $m < 0$.

5.2 Show that pure cubic fields $K = \mathbb{Q}(\sqrt[3]{m}\,)$ have $(r, s) = (1, 1)$.

5.3 Determine (r, s) for pure quartic fields $\mathbb{Q}(\sqrt[4]{m}\,)$.

5.4 Show that r and s do not depend on the choice of α or f: if $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$, show that the minimal polynomials of α and β have the same number of real roots.

5.5 Show that if K is a number field of degree n and $a \in \mathbb{Q}$, then $\operatorname{Tr}(a) = na$ and $N(a) = a^n$. More generally, show that $\operatorname{Tr}(a\alpha) = a\operatorname{Tr}(\alpha)$ and $N(a\alpha) = a^n N(\alpha)$ for all $\alpha \in K$.

5.6 Let $\omega = \sqrt[3]{m}$; compute $\operatorname{Tr}(a + b\omega + c\omega^2)$ and $N(a + b\omega)$. Find a unit $\ne \pm 1$ in $\mathbb{Q}(\sqrt[3]{2}\,)$.

5.7 Show that $\operatorname{disc}(1, \sqrt{m}\,) = 4m$ and $\operatorname{disc}(1, \sqrt[3]{m}, \sqrt[3]{m}^2) = -27m^2$.

5.8 Compute $|1 + \sqrt[3]{2}\,|_1$ and $|1 + \sqrt[3]{2}\,|_2$ for the two archimedean valuations of $\mathbb{Q}(\sqrt[3]{2}\,)$.

5.9 Deduce from Theorem 5.5 how primes p split in quadratic extensions.

5.10 Use the Minkowski bounds to show that the field $\mathbb{Q}(\sqrt[3]{2})$ has class number 1. Show directly that 3 ramifies completely by verifying that $(1+\sqrt[3]{2})^3 = (3)$, and show that this relation provides you with a unit.

5.11 Draw a lattice in $\mathbb{R}^2$ and sketch an example that shows why we need the condition “centrally symmetric” in the statement of Thm. 5.21.

5.12 Show that the set T that occurred in the proof of the Minkowski bounds is convex, centrally symmetric, and compact.

6. Dirichlet's Unit Theorem

Let K be an algebraic number field with ring of integers $\mathfrak{O}_K$. The units in this ring form a group $E_K = \mathfrak{O}_K^\times$, which is often called the unit group of K (this is an abuse of language, since the unit group of the field K is actually $K^\times$). For $K = \mathbb{Q}$, the unit group has order 2 since $E_{\mathbb{Q}} = \{-1, +1\}$. For a general number field, Dirichlet proved (in modern terms) that E_K is a finitely generated abelian group, and in fact determined its abstract structure.

The unit group plays an important role in class field theory. This might seem surprising at first, but we will see over and over again that questions concerning the ideal class group are tied intricately to properties of the unit group. One manifestation of this link is the fact that Dedekind's class number formula will give us a formula for the product hR, where h is the class number of K and R its regulator, a number that does for units what the discriminant does for rings of integers.

6.1 Units in Quadratic Number Fields

It is easy to see that $\alpha \in \mathfrak{O}_K$ is a unit if and only if $N_{K/\mathbb{Q}}\alpha = \pm 1$. For quadratic number fields with discriminant d, this boils down to the solvability of the Pell equation $T^2 - dU^2 = \pm 4$. It is then easy to check that, for complex quadratic number fields, the unit groups are given by

$$E_K = \begin{cases} \langle -\rho \rangle \simeq \mathbb{Z}/6\mathbb{Z} & \text{if } d = -3; \quad \text{here } \rho^2 + \rho + 1 = 0. \\ \quad \langle i \rangle \;\simeq \mathbb{Z}/4\mathbb{Z} & \text{if } d = -4; \quad \text{here } i^2 = -1. \\ \langle -1 \rangle \simeq \mathbb{Z}/2\mathbb{Z} & \text{otherwise.} \end{cases}$$

For positive d, however, the Pell equation always has a nontrivial solution. This was known to Fermat and Euler, but it was Lagrange who first found a proof. We will next present a proof for the solvability of the Pell equation going back to Dirichlet, and then give his proof of the unit theorem in general number fields.

Theorem 6.1. *Let $K = \mathbb{Q}(\sqrt{m}\,)$ be a real quadratic number field with $m > 0$ squarefree. Then*

$$E_K = \mathfrak{O}_K^\times \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}. \tag{6.1}$$

In other words, there exists a unit $\eta \in E_K$ such that every unit $\varepsilon \in E_K$ can be written uniquely in the form $\varepsilon = (-1)^a\eta^b$ with $a \in \mathbb{Z}/2\mathbb{Z}$ and $b \in \mathbb{Z}$.

The idea behind the proof is the following: there are only finitely many integral ideals of bounded norm in $\mathbb{Q}(\sqrt{m}\,)$; if we can construct sufficiently many elements with bounded norm, then there must be two that generate the same ideal. But if $(\alpha) = (\beta)$, then $\varepsilon = \frac{\alpha}{\beta}$ is a unit. In order to make sure that ε has infinite order, we observe

Lemma 6.2. *Let $K = \mathbb{Q}(\sqrt{m}\,)$ be a real quadratic number field. Then $\varepsilon \in \mathfrak{O}_K$ has infinite order if and only if $|\varepsilon| \ne 1$.*

Proof. If $|\varepsilon| = 1$, then $\varepsilon = a + b\sqrt{m} = \pm 1$. The irrationality of $\sqrt{m}$ then implies $a = \pm 1$ and $b = 0$, that is, $\varepsilon = \pm 1$.

If $|\varepsilon| \ne 1$, then ε cannot have finite order: in fact, $\varepsilon^m = 1$ implies $|\varepsilon|^m = 1$, hence $|eps| = 1$. □

The idea is to construct a sequence of algebraic integers $\alpha_j = x_j + y_j\sqrt{m}$ (m a positive squarefree integer) with $|N\alpha_j| < B$. Eventually there will be two elements α_i and α_j generating the same ideal, and their quotient $\varepsilon = \alpha_i/\alpha_j$ will then be a unit. In order to make sure that $\varepsilon \ne \pm 1$ we construct the α_j in such a way that $\alpha_1 > \alpha_2 > \ldots > \alpha_k > \ldots$.

This is achieved in exactly the same way as above for $m = 11$: we consider the sequence $y = 0, 1, \ldots, N$ and let x denote the smallest integer $> y\sqrt{m}$; then $0 < x - y\sqrt{m} \le 1$ and $x + y\sqrt{m} < BN$ for $B = \lceil 2\sqrt{m}\,\rceil$. Since there are $N + 1$ such numbers $x - y\sqrt{m}$ in the interval $(0, 1)$, Dirichlet's box principle guarantees the existence of pairs (a, b) and (a', b') with $0 < (a - b\sqrt{m}) - (a' - b'\sqrt{m}\,) < \frac{1}{N}$. Putting $x = a - a'$ and $y = b - b'$ we find $0 < x - y\sqrt{m} < \frac{1}{N}$ and $0 < |x + y\sqrt{m}\,| < BN$. Thus we can find numbers $x - y\sqrt{m}$ with positive absolute value as small as we wish, but in such a way that $N(x - y\sqrt{m}\,) < B$ is bounded.

Now we can construct our sequence of α_j. We start with $\alpha_1 = 1$. Assume we have already found α_i for $i = 1, \ldots, k - 1$ with

$$\alpha_1 > \alpha_2 > \ldots > \alpha_{k-1} > 0$$

and $|N(\alpha_i)| < B$. By the argument above we can find $\alpha_k = x - y\sqrt{m}$ with $0 < \alpha_k < \alpha_{k-1}$ and $|N(\alpha_k)| < B$.

Since there are only finitely many integral ideals with norm $< B$, there must exist $i < j$ with $(\alpha_i) = (\alpha_j)$. But then $\varepsilon = \alpha_i/\alpha_j > 1$ is a unit, and we have proved that every real quadratic field has units $\ne \pm 1$. In particular, the Pell equation $X^2 - mY^2 = 1$, where $m > 1$ is an integer, has integral solutions with $y > 0$.

In order to prove (6.1), we first show that there is a smallest unit $\eta > 1$. If not, then there is a sequence of units $\eta_1 > \eta_2 > \ldots > 1$; then $0 < |\eta_i'| = 1/\varepsilon_i < 1$, hence if we write $\eta_j = x_j + y_j\sqrt{m}$, we find $2|x_j| = |\eta_j + \eta_j'| \le |\eta_j| + |\eta_j'| < \eta_1 + 1$: this shows that there are only finitely many choices for x, and the same argument with η_j' replaced by $-\eta_j'$ shows that the same holds for y_j. This is a contradiction.

Now let $\varepsilon > 1$ be any unit. If $\varepsilon = \eta^n$ for some integer n we are done; if not, then there is some $n \in \mathbb{N}$ with $\eta^n < \varepsilon < \eta^{n+1}$. But then $\upsilon = \varepsilon\eta^{-n}$ is a unit in $\mathfrak{O}_K$ with $1 < \upsilon < \eta$, contradicting the choice of η.

Thus every unit > 1 has the form η^n for some $n \in \mathbb{N}$. If $0 < \varepsilon < 1$, then $1/\varepsilon > 1$, hence $\varepsilon = \eta^n$ for some integer $m < 0$. Finally, if $\varepsilon < 0$, then $-\varepsilon > 0$ has the form η^n. This proves that every unit can be written as $\pm\eta^n$.

6.2 Dirichlet's Unit Theorem

The structure of the unit group of rings $\mathfrak{O}_K$ was determined by Dirichlet (to be honest, Dirichlet did not know the definition of an algebraic integer, and worked with rings of the form $\mathbb{Z}[\alpha]$ for roots α of monic polynomials with integral coefficients; it is not hard to see that the unit group of $\mathfrak{O}_K$ and that of its subring $\mathbb{Z}[\alpha]$ have the same abstract structure) . The set W_K of the roots of unity contained in a number field K is a finite cyclic group, which can easily be determined. In fact, if $W_K = \langle\zeta\rangle$ is generated by a primitive w-th root of unity, then we must have $\mathbb{Q}(\zeta_w) \subseteq K$; this already shows that W_K is finite. Moreover, if $w > 2$, then K contains a totally complex number field as a subfield, hence is totally complex; this shows that if K has $r > 0$ real embeddings, then we necessarily have $W_K = \{\pm 1\}$.

Theorem 6.3 (Dirichlet's Unit Theorem)**.** *Let K be a number field of degree $n = r + 2s$, and let ζ be a generator of W_K. Then there exist units $\varepsilon_1, \ldots, e_{r+s-1} \in \mathfrak{O}_K^\times$ such that every unit $\eta \in \mathfrak{O}_K^\times$ can be written uniquely in the form*

$$\eta = \zeta^a \varepsilon_1^{a_1} \cdots \varepsilon_{r+s-1}^{a_{r+s-1}},$$

where the a_i are integers, and where a is determined modulo the order w of ζ. In particular, the unit group of $\mathfrak{O}_K$ is finitely generated, and we have

$$\mathfrak{O}_K^\times \simeq \mathbb{Z}/w\mathbb{Z} \oplus \mathbb{Z}^{r+s-1}.$$

In order to be able to apply Minkowski's techniques, we need a map (actually a homomorphism) from the unit group to some lattice in a finite dimensional real vector space. It should not come as a big surprise that the construction of a homomorphism from a multiplicative to an additive group involves logarithms.

In fact, we get a "logarithmic" embedding $\lambda : K^\times \longrightarrow \mathbb{R}^{r+s}$ by setting

$$\lambda(\alpha) = (\log|\sigma_1(\alpha)|, \ldots, \log|\sigma_r(\alpha)|, 2\log|\sigma_{r+1}(\alpha)|, \ldots, 2\log|\sigma_{r+1}(\alpha)|).$$

Clearly the sum of the coordinates of $\lambda(\alpha)$ is equal to

$$\sum_{j=1}^{n} \log|\sigma_j(\alpha)| = \log|N\alpha|$$

since $|\sigma_{r+1}(\alpha)| = |\overline{\sigma_{r+1}}(\alpha)|$. In particular, the image of the unit group $\mathfrak{O}_K^\times$ lies in the hyperplane

$$\mathcal{H}: \quad x_1 + \ldots + x_{r+s} = 0 \tag{6.2}$$

of $\mathbb{R}^{r+s}$. Since the image of the homomorphism λ is a free abelian group, the torsion subgroup of $\mathfrak{O}_K^\times$, namely the group of roots of unity in K, must be in the kernel. In fact, it is the kernel:

Lemma 6.4 (Kronecker)**.** *We have an exact sequence*

$$1 \longrightarrow W_K \longrightarrow \mathfrak{O}_K^\times \xrightarrow{\lambda} \mathbb{R}^{r+s},$$

where W_K denotes the group of roots of unity contained in K.

Proof. The kernel of λ consists of all units ε with $|\sigma_j(\varepsilon)| = 1$. These units form a subgroup of $\mathfrak{O}_K^\times$, and since their images under ι^* lie in a bounded domain in $\mathbb{R}^n$, the coefficients of their minimal polynomials are bounded, too. Thus the group of these units must be finite, and hence each such unit has finite order. i.e., is a root of unity. □

The same type of argument shows that $\lambda(\mathfrak{O}_K^\times)$ is a discrete subgroup of the hyperplane (6.2) in $\mathbb{R}^{r+s}$, hence that the free abelian group group $\mathfrak{O}_K^\times/W_K$ has at most $r+s-1$ independent generators.

The heart of Dirichlet's proof is showing the existence of $r+s-1$ independent units, or, in other words, showing that $\lambda(\mathfrak{O}_K^\times)$ is a full lattice in the hyperplane $\mathcal{H}$ defined by (6.2).

The idea is to construct units ε_j with the property that

$$\lambda(\varepsilon_j) = (x_1, \ldots, x_{r+s}), \quad x_i < 0 \text{ for all } i \neq j,$$

(and, since $\lambda(\varepsilon_j)$ lies in (6.2), $x_j > 0$). A simple lemma from linear algebra[1] will then immediately show that any selection of $r+s-1$ out of these $r+s$ units are independent. In fact, if we delete the last row (corresponding to the unit ε_{r+s} and the last column (giving the logs of the valuation $|\cdot|_{r+s}$, then the sums of the entries in each row will be positive (before the deletion they added up to 0, and then we have deleted a negative entry), and all entries except those on the main diagonal will be negative. The lemma below shows that such matrices have nonzero determinant, and this means that their rows must be linearly independent.

[1] This result is due to Minkowski; the special case $n = 3$ was used as a problem in the 7th IMO in 1965. The proof given below is a simplification of a proof due to Furtwängler and communicated by Artin to Hasse in a letter from Oct. 27, 1927; it was published in Artin's article [Ar1932].

Lemma 6.5. *Let $A = (a_{ij})$ be a real $n \times n$-matrix with the following properties:*

i) $a_{ii} > 0$ for all $1 \le i \le n$;
ii) $a_{ij} \le 0$ for all $i \ne j$;
iii) the column sums $\sum_{i=1}^n a_{ij}$ are positive for $j = 1, 2, \ldots, n$.

Then $\det A \ne 0$.

Proof. Suppose that $\det A = 0$. Then the system of equations $\sum_{i=1}^n a_{ij}x_i = 0$, $i = 1, \ldots, n$ has a nontrivial solution $x = (x_1, \ldots, x_n) \ne 0$.

Assume that $|x_k|$ is maximal among all $|x_j|$; without loss of generality we may assume that $x_k > 0$ (otherwise replace x by $-x$). Then $x_k \ge x_j$ for all j. Now we find

$$0 = \sum_{i=1}^n a_{ik}x_i \ge \sum_{i=1}^n a_{ik}x_k = x_k \sum_{i=1}^n a_{ik} > 0.$$

Here we have used that $a_{ik} \le 0$ for $i \ne k$ implies $a_{ik}x_i \ge a_{ik}x_k$. □

The construction of the unit ε_j is done by finding a sequence of elements $\alpha_1, \alpha_2, \ldots$ of *bounded norm* with the property that all coordinates $x_i \ne x_j$ of $\lambda(\alpha_n)$ are strictly smaller than those of $\lambda(\alpha_{n-1})$. Since there are only finitely many ideals with bounded norm, there must be two such α_i that generate the same ideal, and then their quotient is the desired unit.

The construction of this sequence of α_j finally is done via the following

Lemma 6.6. *Fix an index j with $1 \le j \le r + s$; then for every nonzero $\alpha \in \mathfrak{O}_K$ there is a nonzero $\beta \in \mathfrak{O}_K$ such that*

$$N_{K/\mathbb{Q}}(\beta) < \Big(\frac{2}{\pi}\Big)\sqrt{|\mathrm{disc}\, K|},$$

as well as $\lambda(\alpha) = (a_1, \ldots, a_{r+s})$, $\lambda(\beta) = (b_1, \ldots, b_{r+s})$, and $b_i < a_i$ for all $i \ne j$.

Proof. Choose constants c_i with $0 < c_i < e^{a_i}$ for $i \ne j$ and determine c_k from the equation

$$c_1 c_2 \cdots c_{r+s} = \Big(\frac{2}{\pi}\Big)\sqrt{|\mathrm{disc}\, K|}.$$

Consider the set S of points $(x_1, \ldots, x_n) \in \mathbb{R}^n$ satisfying

$$|x_1| \le c_1, \ldots, |x_r| \le c_r, x_{r+1}^2 + x_{r+2}^2 \le x_{r+1}, \ldots, x_{n-1}^2 + x_n^2 \le c_{r+s}.$$

Then $\mathrm{vol}\,(S) = 2^r \pi^s c_1 \cdots c_{r+s} = 2^n \mathrm{vol}\,(\Lambda)$, where $\Lambda = \iota^*(\mathfrak{O}_K)$. By Minkowski, S contains some nonzero lattice point $\iota^*(\beta)$, and this $\beta \in \mathfrak{O}_K$ has the desired properties. □

6.3 The Unit Theorems of Minkowski and Herbrand

Minkowski's Unit Theorem

For computing the Herbrand quotient of the unit group E_L, we need to understand how the Galois group acts on E_L. Unfortunately, the Galois action on E_L is too difficult to be understood properly. The best we can hope for is to find a subgroup of finite index in E_L on which the Galois group acts in a way that can be described explicitly. The first such result was proved by Minkowski and deals with the unit group in normal extensions $L/\mathbb{Q}$. Such extensions are either totally real or totally complex; in the second case, complex conjugation fixes a subfield F with $(L:F) = 2$, which, in general, will not be normal (nor totally real): in fact, the extension $L = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}\,)$ is normal over $\mathbb{Q}$ with Galois group S_3, and the real subfield fixed by complex conjugation is the field $\mathbb{Q}(\sqrt[3]{2}\,)$. In each of these cases, observe that the unit rank of L is $(F:\mathbb{Q}) - 1$.

Theorem 6.7 (Minkowski's Unit Theorem)**.** *Let $L/\mathbb{Q}$ be a normal extension, and F its real subfield of degree $\rho+1 = r+s$. Then there exists a unit $\varepsilon \in E_F$ such that any ρ units among the $\rho+1$ conjugates of ε generate a subgroup of finite index in E_L.*

This result can be seen as the analog of the normal basis theorem in Galois theory: if L/K is a finite Galois extension, then there is an element $\alpha \in L$ whose conjugates form a K-basis for L. A normal basis for quadratic extensions $L = K(\sqrt{\mu}\,)$ is e.g. given by $\{1+\sqrt{\mu}, 1-\sqrt{\mu}\,\}$, and $\{\zeta, \zeta^2, \ldots, \zeta^{p-1}\}$ is a normal basis for $L = \mathbb{Q}(\zeta)$, where ζ is a primitive p-th root of unity (this is even a normal integral basis). Minkowski's result states that it is always possible to choose an independent system of units consisting of conjugate elements.

Minkowski's unit theorem is trivial for quadratic extensions, where we can take ε to be a fundamental unit. If $L = \mathbb{Q}(\sqrt{a}, \sqrt{b}\,)$ is a totally complex biquadratic extension (say with $a > 0$ and $b < 0$), then we can take ε to be the fundamental unit of $\mathbb{Q}(\sqrt{a}\,)$. If L is totally real, the fundamental units $\varepsilon_1, \varepsilon_2, \varepsilon_3$ of the three real quadratic subfields of L generate a subgroup of finite index; here it can be shown that we can take $\varepsilon = \varepsilon_1\varepsilon_2\varepsilon_3$.

Proof of Thm. 6.7. Assume first that L is totally real, and let $|\cdot|_1, \ldots, |\cdot|_n$ denote the $n = (L:K)$ archimedean valuations attached to each of the real embeddings $\sigma_1, \ldots, \sigma_r$ via $|\alpha|_j = |\sigma_j(\alpha)|$. In the proof of Dirichlet's unit theorem we have seen that there exists a unit ε with the property $|\varepsilon|_1 > 1$, $|\varepsilon|_2, \ldots, |\varepsilon|_n < 1$.

Since $L/\mathbb{Q}$ is normal, the real embeddings σ_j are the elements of $G = \operatorname{Gal}(L/\mathbb{Q})$, hence the unit $\varepsilon_i = \sigma_i^{-1}(\varepsilon) \in E_L$ has the property

$$|\varepsilon_i|_j = |\sigma_j(\varepsilon_i)| = |\sigma_j(\sigma_i^{-1}(\varepsilon))|, \quad \text{hence} \quad \begin{cases} |\varepsilon_i|_i > 1 & \\ |\varepsilon_i|_j < 1 & \text{if } j \neq i. \end{cases}$$

In the proof of Dirichlet's Unit Theorem we have seen that such units are independent, and this concludes the proof of Minkowski's Unit Theorem in the case where L is totally real.

Now assume that L is totally complex of degree $n = 2m$, and let K be the fixed field of complex conjugation σ. From each pair of complex embeddings pick one; then $\sigma_1, \ldots, \sigma_m$ give rise to the m archimedean valuations $|\cdot|_1, \ldots, |\cdot|_m$ of L. As above, Dirichlet's unit theorem provides us with a unit $\eta \in E_L$ such that $|\eta|_1 > 1$, $|\eta|_2, \ldots, |\eta|_m < 1$. Now we claim that $\varepsilon = \eta^{1+\sigma}$ has the desired properties. First of all, $\varepsilon \in E_F$ since ε is fixed by complex conjugation σ. Next $|\varepsilon|_1 > 1$, $|\varepsilon|_2, \ldots, |\varepsilon|_m < 1$ because $|\varepsilon|_j = |\eta|_j |\eta^\sigma|_j = |\eta|_j^2$. Finally we check that the units $\varepsilon_i = \sigma_i^{-1}(\varepsilon)$ have the same properties as in the totally real case. □

Herbrand's Unit Theorem

For normal extensions $L/\mathbb{Q}$, Minkowski's Unit Theorem guarantees the existence of a unit whose set of conjugates contains an independent system of units. If L is normal over some number field K, then there are fewer conjugates of units, so we cannot expect that the conjugates of a single unit generate a subgroup of finite index in the unit group.

How many units do we need then? Assume that $(K : \mathbb{Q}) = r_K + 2s_K$, where r_K and s_K are the number of real and pairs of complex embeddings. The unit rank of K is, by Dirichlet's unit theorem, $\rho = r_K + s_K - 1$. If $n = (L : K)$ denotes the relative degree of the extension L/K, then clearly each of the s_K pairs of complex embeddings lifts to n complex embeddings of L (in fact, if κ is a complex embedding of K, then each $\sigma \in G = \mathrm{Gal}\,(L/K)$ induces a co,plex embedding $\kappa\sigma$). Let d denote the number of real embedding of K that lift to complex embeddings of L; since n is even if $d > 0$, this gives rise to $d\frac{n}{2}$ pairs of complex embeddings of L. Each of the remaining $r_K - d$ real embeddings lifts to n real embeddings of L.

Thus we find $r_L = (n-d)r_K$ and $s_L = ns_K + \frac{n}{2}dr_K$. The degree of L then becomes $r_L + 2s_L = (n-d)r_K + 2ns_K + dr_K = n(r_K + 2s_K) = n(K : \mathbb{Q})$ as expected. In particular, the unit rank of L is given by $\rho_L = r_L + s_L - 1 = (n-d)r_K + ns_K + \frac{n}{2}dr_K - 1 = n(r_k + s_K) - \frac{n}{2}d - 1$.

Lemma 6.8. *Let L/K be a normal extension, and assume that d real primes ramify in L/K. Then the following formulas hold:*

$$\begin{aligned} r_L &= (r_K - d)n, \\ s_L &= ns_K + \frac{n}{2}dn \\ \rho_L &= n(r_k + s_K) - \frac{n}{2}d - 1. \end{aligned}$$

We can rewrite these equations by invoking the ramification indices $e(\mathfrak{p}_\infty)$ of infinite primes (this number equals 2 or 1 according as $\mathfrak{p}_\infty$ is ramified or not). In fact, we have

$$\sum_{\mathfrak{p}|\infty} \frac{n}{e(\mathfrak{p})} = (r_K + s_K - d)n + \frac{n}{2}d = n(r_K + s_K) - \frac{n}{2}d$$

since $\frac{n}{e(\mathfrak{p})} = n$ if $\mathfrak{p}$ is unramified (this happens for $r_K - d$ real and s_K complex primes), and $\frac{n}{e(\mathfrak{p})} = \frac{n}{2}$ otherwise (this happens d times). This shows

Lemma 6.9. *Let L/K be a normal extension. Then L has $\sum\limits_{\mathfrak{p}|\infty} \frac{n}{e(\mathfrak{p})}$ infinite primes.*

This is of course not very surprising since each infinite prime $\mathfrak{p}$ in K splits into $\frac{n}{e(\mathfrak{p})}$ infinite primes in L.

Herbrand's Unit Theorem

Our task now is to find a generalization of Minkowski's unit theorem to relative extensions. We will use the notation from Section ??; let us denote the valuations in K by $v_1, \ldots, v_{r+s}$, and let $\mathfrak{p}_j$ denote the attached infinite primes. Choose lifts $w_1, \ldots, w_{r+s}$ to L. If for each such j we can find a unit ε_j lying in the decomposition field of $w_j|v_j$, then each such unit will have at most $\frac{n}{e(\mathfrak{p}_j)}$ conjugates, and the set of conjugates of all such units will be $\sum_{\mathfrak{p}|\infty} \frac{n}{e(\mathfrak{p})} = r_L + s_L$, and if we choose the units carefully, we can make sure that any subset of $r_L + s_L - 1$ among these conjugates form an independent system of units.

Theorem 6.10 (Herbrand's Unit Theorem (I))**.** *Let K be a number field with $r + s$ archimedean valuations, and let L/K be a normal extension with Galois group n. Then there exist $r + s$ independent units $\eta_1, \ldots, \eta_{r+s}$ in E_L such that the only relations between their conjugates are*

- *$\sigma_j \eta_j = \eta_j$, where σ_j generates the decomposition group of $w_j|v_j$;*
- *$\prod_{j,\sigma} \sigma(\eta_j) = 1$.*

Proof. Let $\sigma_1, \ldots, \sigma_{\rho+1}$ denote generators of the decomposition groups of $w_j|v_j$. Choose units $\eta_j \in E_L$ with $w_j(\eta_j) > 1$ and $w_i(\eta_j) < 1$ for $i \neq j$. If $\sigma_j \neq 1$, observe that

- $w_j(\eta_j^{1+\sigma_j}) = w_j(\eta_j^2) > 1$;
-

Replacing η_j by $\eta_j^{1+\sigma_j} \in L_{w_j}$ produces units η_j with $w_j\sigma(\eta_j) > 1$, and $w_j\sigma(\eta_i) < 1$ for $i \neq j$, where σ runs through a set of representatives for $G/\langle\sigma_j ra$. Omitting any unit from the set of $r_L + s_L$ conjugates will therefore produce an independent system of units. This implies that we must have a relation

$$\prod_{j,\sigma} \sigma(\eta_j)^{m(j,\sigma)} = 1$$

in which none of the exponents can vanish (since every conjugate of a unit can be expressed by the others). Applying $\tau \in G$ to this relation produces another one; since we only can have one independent relation, this implies that the exponents $m_j = m(j, \sigma)$ do not depend on σ. Replacing each unit η_j by $\eta_j^1 m_j$ the produces a system of units with the same properties as before, and with the single relation

$$\prod_{j,\sigma} \sigma(\eta_j) = 1.$$

This concludes the proof. □

In the special case of cyclic extensions, this result can be stated in the following form:

Theorem 6.11 (Herbrand's Unit Theorem (II))**.** *Let L/K be a cyclic extension with Galois group $G = \langle \sigma \rangle$, and let ρ denote the $\mathbb{Z}$-rank of E_K. Then there exist $\rho + 1$ units $\eta_1, \ldots, \eta_{\rho+1}$ (one for each infinite prime ∞_j of K) with the following properties:*

- *The η_j and their conjugates, together with a system of fundamental units $\varepsilon_1, \ldots, \varepsilon_\rho$ of K, generate a subgroup of finite index in E_L.*
- *The only relations between the η_j are the following:*

$$\eta_j^{1+\sigma+\ldots+\sigma^{n_j-1}} = 1, \quad \textit{where} \quad n_j = \frac{n}{e(\infty_j)}, \quad j = 1, \ldots, \rho + 1.$$

The version of Herbrand's Unit Theorem can be derived easily from Thm. 6.10: let N_j denote the norm from the decomposition field of $w_j | v_j$ down to K and put $\varepsilon_j = N_j(\eta_j)$. The relation $\prod_{j,\sigma} \sigma(\eta_j) = 1$ then becomes

$$\varepsilon_1 \cdots \varepsilon_{\rho+1} = 1. \tag{6.3}$$

Since every relation between the ε_j is also a relation between the η_j, (6.3) is the only relation among the ε_j, and in particular $\varepsilon_1, \ldots, \varepsilon_\rho$ is an independent system of units in E_K. If we put $H_j = E_j^{n_j}/\eta_j$, then $N_j(\eta_j) = \varepsilon_j$ implies $N_j H_j = 1$.

Notes

The original proofs of the unit theorems of Minkowski and Herbrand can be found in Minkowski [Mi1900], Herbrand [He1930, He1931], and Artin [Ar1932]. A nontrivial upper bound for the finite index $(E_L : U_L)$ was derived by Odai [Od1994].

Exercises

6.1 Let $K/\mathbb{Q}$ be a real biquadratic extension, and let $\varepsilon \in E_K$ be the product of the fundamental units of the quadratic subfields. Show that the conjugates of ε generate a subgroup of finite index in E_L.

7. Dedekind's Zeta Function

In this chapter we will prove that the zeta function of any number field K has a simple pole of order 1 at $s = 1$, and compute its residue; we will find

Theorem 7.1. *Let K be a number field with r real and $2s$ complex embeddings. Then*

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2^{r+s}\pi^s R_K}{w\sqrt{|\operatorname{disc} K|}} \cdot h_K,$$

where R_K is the regulator, w the number of roots of unity, and h_K the class number of K.

The general theory of Dirichlet series tells us exactly what we will have to do to prove this result. Recall that $\zeta_K(s) = \sum a_n n^{-s}$, where a_n denotes the number of ideals with norm n. In particular, $\zeta_K(s)$ is a Dirichlet series with nonnegative coefficients a_n. Landau proved the following

Theorem 7.2. *Let $f(s) = \sum a_n n^{-s}$ be a Dirichlet series with real coefficients $a_n \geq 0$, and assume that f has abscissa of convergence σ_0. Then f has a singularity at $s = \sigma_0$.*

We would like to show that $\zeta_K(s)$ has a pole at $s = 1$, so we need to be able to compute its abscissa of convergence:

Theorem 7.3. *Let $\sum a_n n^{-s}$ be a Dirichlet series for which $\sum a_n$ diverges. Then the abscissa of convergence σ_0 is given by*

$$\sigma_0 = \limsup \frac{\log |A(m)|}{\log m},$$

where $A(m) = a_1 + \ldots + a_m$.

Landau's theorem can be made more precise in the special case we need:

Theorem 7.4. *Let $f(s) = \sum a_n n^{-s}$, and assume that there is some $\kappa \in \mathbb{C}$, a σ_1 with $0 \leq \sigma_1 < 1$, and a constant c such that $|A(m) - \kappa m| < cm^{\sigma_1}$ for all $m \geq 1$. Then $f(s)$ is holomorphic in the half plane $\operatorname{Re} s > \sigma_1$ except for a simple pole at $s = 1$ with residue κ.*

Proof. Consider the Dirichlet series $f(s) - \kappa\zeta(s)$; Lemma 1.7 shows that this is holomorphic in the half plane $\operatorname{Re} s > \sigma_1$. But then $\lim(s-1)f(s) =$

$\kappa \lim(s-1)\zeta(s) = \kappa \neq 0$ shows that f has a simple pole at $s = 1$ with residue κ, and that it is holomorphic everywhere else in the half plane $\operatorname{Re} s > \sigma_1$. □

Thus if we want to show that $\zeta_K(s) \to \infty$ as $s \to 1$, we need to show that the number $A(m) = a_1 + \ldots + a_m$ of ideals with norm $\leq m$ satisfies $\lim \frac{\log A(m)}{\log m} = 1$, which is easily seen to follow from $A(m) = \kappa m + O(m^{1-\varepsilon})$ for some $\varepsilon > 0$. In order to show that $\zeta_K(s)$ has a pole at $s = 1$, we are therefore almost forced to count the number of ideals in K with norm $\leq m$.

In fact, if we can show that $A(m) = \kappa m + O(m^{1-\varepsilon})$ for some $\varepsilon > 0$, then we will also know that the Dedekind zeta function $\zeta_K(s)$ can be extended holomorphically to $\operatorname{Re} s > 1 - \varepsilon$ with the exception of a simple pole with residue κ at $s = 1$.

It should be clear how to achieve this. Let K be a number field with ideal class group $\operatorname{Cl}(K)$, and fix an ideal class $c \in \operatorname{Cl}(K)$. Choose an integral ideal $\mathfrak{b} \in c^{-1}$; then for every $\mathfrak{a} \in c$, we can write $\mathfrak{a}\mathfrak{b} = (\alpha)$ for some $\alpha \in \mathfrak{b}$ with $|N\alpha| = N\mathfrak{a}N\mathfrak{b}$. Thus the ideals in c with norm $\leq m$ correspond to principal ideals (α) for $\alpha \in \mathfrak{b}$ with $|N\alpha| \leq mN\mathfrak{b}$.

7.1 Distribution of Ideals

Recall the situation we are in: let K be a number field with ideal class group $\operatorname{Cl}(K)$, and fix an ideal class $c \in \operatorname{Cl}(K)$. Choose an integral ideal $\mathfrak{b} \in c^{-1}$; then for every $\mathfrak{a} \in c$, we can write $\mathfrak{a}\mathfrak{b} = (\alpha)$ for some $\alpha \in \mathfrak{b}$ with $|N\alpha| = N\mathfrak{a}N\mathfrak{b}$. Thus the ideals in c with norm $\leq m$ correspond to principal ideals (α) for $\alpha \in \mathfrak{b}$ with $|N\alpha| \leq mN\mathfrak{b}$.

Our next job is constructing a fundamental domain D with the property that every $\alpha \in \mathfrak{b}$ is associated to exactly one element in D. To this end, let us introduce the following maps:

1. Let ι denote the restriction of the embedding $K \hookrightarrow \mathbb{R}^r \times \mathbb{C}^s$ to $K^\times$; this gives us an embedding $\iota : K^\times \longrightarrow \mathbb{R}^{\times\, r} \times \mathbb{C}^{\times\, s}$.
2. Define the norm map $N : \mathbb{R}^r \times \mathbb{C}^s$ as before via
$$N(x) = |x_1 \cdots x_r x_{r+1}^2 \cdots x_{r+s}^2| \quad \text{for} \quad x = (x_1, \ldots, xr + s).$$
Then $|N_{K/\mathbb{Q}}(\alpha)| = N(\iota(\alpha))$.
3. Define the logarithmic map $\ell : \mathbb{R}^{\times\, r} \times \mathbb{C}^{\times\, s} \longrightarrow \mathbb{R}^{r+s}$ by
$$\ell(x_1, \ldots, x_{r+s}) = (\log|x_1|, \ldots, \log|x_r|, 2\log|x_{r+s}|, \ldots, 2\log|x_{r+s}|).$$
Clearly $\lambda = \ell \circ \iota$.
4. Observe that $\log N(\alpha) = \xi_1 + \ldots + \xi_{r+s}$ for $(\xi_1, \ldots, \xi_{r+s}) = \lambda(\alpha)$, and that $\lambda(\mathfrak{O}_K^\times)$ is a full lattice in the hyperplane $\mathcal{H}$ defined by $x_1 + \ldots + x_{r+s} = 0$.

Now let $\varepsilon_1, \ldots, \varepsilon_\rho$ ($\rho = r + s - 1$) denote a system of fundamental units of $\mathfrak{O}_K$. Then the vectors $\lambda(\varepsilon_1)$, …, $\lambda(\varepsilon_\rho)$ form a basis of the hyperplane $\mathcal{H}$. The fundamental domain of this lattice $\lambda(\mathfrak{O}_K^\times)$ is

$$F = \{x = a_1\lambda(\varepsilon_1) + \ldots + a_\rho\lambda(\varepsilon_\rho) \in \mathcal{H} : 0 \le a_i < 1\}.$$

Since $u = (1, \ldots, 1, 2, \ldots, 2)$ (the first r coordinates are 1, the other s are 2) does not lie in $\mathcal{H}$ (its coordinates do not add up to 0), the elements $\lambda(\varepsilon_j)$ and u form a basis of $\mathbb{R}^{r+s}$. The reason for this particular choice will become clear below.

Now define a subset $D \subseteq \mathbb{R}^{\times\, r} \times \mathbb{C}^{\times\, s}$ by

$$D = \{x \in \mathbb{R}^{\times\, r} \times \mathbb{C}^{\times\, s} : \log(x) \in F \oplus \mathbb{R}u\}.$$

This condition means that we can write

$$\ell(x) = a_1\lambda(\varepsilon_1) + \ldots + a_\rho\lambda(\varepsilon_\rho) + au$$

for real numbers $0 \le a_i < 1$ (there is no condition on $a \in \mathbb{R}$).

Example: Real Quadratic Number Fields

Consider a real quadratic number field $K = \mathbb{Q}(\sqrt{m}\,)$; here $r = 2$ and $s = 0$, hence $u = (1, 1)$. We have $\iota(\alpha) = (\alpha, \alpha')$ and $\ell(x, y) = (\log|x|, \log|y|)$, hence $\lambda(\alpha) = (\log|\alpha|, \log|\alpha'|)$. Let $\varepsilon > 1$ denote the fundamental unit; then $\varepsilon\varepsilon' = N(\varepsilon) = \pm 1$ implies $\log|\varepsilon'| = -\log|\varepsilon|$, hence $\lambda(\varepsilon) = (\log|\varepsilon|, -\log|\varepsilon|)$. The condition $\ell(x, y) \in F + \mathbb{R}u$ means

$$\ell(x, y) = (a_1 \log\varepsilon + au, -a_1\log\varepsilon + au)$$

for some $a_1 \in \mathbb{R}$ with $0 \le a_1 < 1$. This implies $\log\frac{|y|}{|x|} = -2a_1\log\varepsilon$, and the inequalities $0 \le a_1 < 1$ then show that $-2\log\varepsilon \le \log\frac{|y|}{|x|} < 0$. Applying exp gives $\varepsilon^{-2} \le \frac{|y|}{|x|} < 1$, and for $(x, y) = \iota(\alpha) = (\alpha, \alpha')$ this gives us back the condition $\varepsilon^{-2} \le \left|\frac{\alpha'}{\alpha}\right| < 1$ we have used for constructing a fundamental domain for real quadratic fields in Chapter 2.

Basic Properties of D

We now list a couple of basic properties of the set D defined above.

Lemma 7.5. *For every $\alpha \in K^\times$ there are exactly w units $\eta \in \mathfrak{O}_K^\times$ such that $\iota(\alpha\eta) \in D$.*

Proof. Write $\lambda(\alpha) = \sum b_i\lambda(\varepsilon_i) + au$ and set $a_i = b_i - \lfloor b_i \rfloor$, as well as $\eta = \varepsilon_1^{-\lfloor b_1 \rfloor} \cdots \varepsilon_\rho^{-\lfloor b_\rho \rfloor}$. Then $\lambda(\alpha\eta) = \sum a_i\lambda(\varepsilon_i) + au$ for real numbers $0 \le a_i < 1$, hence $\iota(\alpha\eta) \in D$. In fact, replacing η by $\zeta^m\eta$ for some root of unity $\zeta \in$

W_K does not change $\lambda(\alpha\eta)$, hence we have found w units with the desired property.

Conversely, if η_1 and η_2 are units such that both $\iota(\alpha\eta_1)$ and $\iota(\alpha\eta_2)$ are in D, then it is easily seen that $\lambda(\eta_1/\eta_2) = 0$, and since $\ker\lambda = W_K$, it follows that η_1 and η_2 differ by a root of unity. □

The next property explains our choice of u:

Lemma 7.6. *D is a cone: if $x \in D$, then $tx \in D$ for all $t \in \mathbb{R}^\times$.*

Proof. Write $x = (x_1, \ldots, x_r)$; then

$$\ell(x) = (\log|x_1|, \ldots, \log|x_r|, 2\log|x_{r+1}|, \ldots, 2\log|x_{r+s}|),$$

hence

$$\begin{aligned}\ell(tx) &= (\log|tx_1|, \ldots, \log|tx_r|, 2\log|tx_{r+1}|, \ldots, 2\log|tx_{r+s}|)\\ &= (\log|t|, \ldots, 2\log|t|) + (\log|x_1|, \ldots, 2\log|x_{r+s}|)\\ &= (\log t)u + \ell(x).\end{aligned}$$

Thus if $x \in D$, then $\ell(x) = \sum a_i\lambda(\varepsilon_i) + au$ with $0 \le a_i < 1$, and this implies $\ell(tx) \sum a_i\lambda(\varepsilon_i) + (a + \log|t|)u$. The claim follows. □

Next we have to discuss the connection between the coordinates of $\ell(x)$ and the norm of $x = (x_1, \ldots, x_{r+s})$. We know that $\log N(x)$ is the sum of the coordingates of $\ell(x)$ with respect to the standard basis of $\mathbb{R}^{r+s}$. If we write $\ell(x) = \sum a_i\lambda(\varepsilon_i) + au$, then the sum of the coordinates of each $\lambda(\varepsilon_i)$ is 0, since the images of units lie in the hyperplane $\mathcal{H}$; thus the sum of the coordinates of $\ell(x)$ is a times the sum of the coordinates of u, which is $r\cdot 1 + s\cdot 2 = r + 2s = n$. We have proved

Lemma 7.7. *If $\ell(x) = \sum a_i\lambda(\varepsilon_i) + au$, then $\log N(x) = na$.*

As an immediate corollary we get

Corollary 7.8. *Write $\ell(x) = \sum a_i\lambda(\varepsilon_i) + au$ for $x \in D$. Then $N(x) \le 1$ if and only if $a \le 0$.*

Now set $D_1 = \{x \in D : N(x) \le 1\}$.

Lemma 7.9. *The set D_1 is bounded.*

Proof. If $x \in D_1$, then $\ell(x) \in F \oplus (-\infty, 0]u$. Since the fundamental domain F of the lattice $\lambda(\mathfrak{O}_K^\times)$ is bounded, the coordinates of $\ell(x)$ are bounded from above. Applying exp we see that the coordinates of x are bounded, and the claim follows. □

The Fundamental Lemma

For counting lattice points inside some domain X we need a somewhat technical lemma. If we want a good error term on the cardinality of lattice points inside X it is clear that the boundary of X has to be "nice". For the applications we have in mind it suffices to assume that ∂X is covered by finitely many differentiable functions; in the proof we will actually use something slightly weaker. We call a map $f : L_1 \longrightarrow L_2$ between two metric spaces (L_1, d_1) and (L_2, d_2) a Lipschitz map if it is continuous and if there is a real $c > 0$ such that $d_2(f(x), f(y)) \le cd_1(x, y)$ for all $x, y \in L_1$. Note that differentiable functions are Lipschitz. Next we will call a subset $X \subseteq \mathbb{R}^n$ k-Lipschitz parametrizable if there are finitely many Lipschitz maps $f_i : I^k \longrightarrow X$ (here $I = [0, 1]$) such that each $x \in X$ is in the image of at least one f_i.

Lemma 7.10. *Let X be a subset of $\mathbb{R}^n$, let Λ be a full lattice in $\mathbb{R}^n$, and let $N_t = \#(tX \cap \Lambda)$ denote the number of lattice points inside tX for real $t > 1$. If ∂X is $(n-1)$-Lipschitz parametrizable, then*

$$N_t = \frac{\mathrm{vol}\,(X)}{\mathrm{vol}\,(\Lambda)} t^n + O(t^{n-1}).$$

Proof. Let P denote a fundamental domain of the lattice Λ, and let n_t denote the number of $\lambda \in \Lambda$ for which $\lambda + P$ intersects the boundary ∂X. Then

$$(N_t - n_t)\mathrm{vol}\,(\Lambda) \le \mathrm{vol}\,(tX) \le (N_t + n_t)\mathrm{vol}\,(\Lambda)$$

hence

$$|N_t \mathrm{vol}\,(\Lambda) - \mathrm{vol}\,(tX)| \le n_t \mathrm{vol}\,(\Lambda),$$

and

$$\left| N_t - \frac{\mathrm{vol}\,(X)}{\mathrm{vol}\,(\Lambda)} t^n \right| \le n_t.$$

Thus it remains to show that $n_t = O(t^{n-1})$.

Since ∂X is covered by finitely many f_i, it is sufficient to consider the image of one of them, say f, and show that the number ν_t of lattice points λ for which $\lambda + P \cap \mathrm{im}\, f \neq \varnothing$ is $O(t^{n-1})$. To this end, we cut the interval I into $\lfloor t \rfloor$ equally long subintervals, hence I^{n-1} into $\lfloor t \rfloor^{n-1}$ little cubes. Since f is Lipschitz, there is a constant $c > 0$ such that $|f(x) - f(y)| \le c|x - y| < c_1 = c\sqrt{n}$ for all $x, y \in I^{n-1}$. Let W denote one of the little cubes; then $f(W)$ has diameter $\le c_1/\lfloor t \rfloor$ (in other words: it is contained in a ball with diameter $c_1/\lfloor t \rfloor$), and $tf(W)$ has diameter $\le c_1 t/\lfloor t \rfloor < 2c_1$. Since a ball with radius c_1 contains only finitely many lattice points, there is a constant c_2 such that $|tf(W) \cap \Lambda| \le c_3$, and this implies $|tf(I^{n-1}) \cap \Lambda| \le c_3 t^{n-1}$. □

The Regulator

We next compute the volume of the fundamental domain F of the lattice $\lambda(\mathfrak{O}_K^\times)$ in $\mathcal{H}$. Before we do that, we prove the following

Lemma 7.11. *Let (a_{ij}) be an $\rho \times (\rho+1)$-matrix with real entries and with the property that $\sum\limits_{i=1}^{\rho+1} a_{ij} = 0$. Let $v = (v_1, \ldots, v_{\rho+1})$ be a real vector with $\sum v_i = 1$. Then the determinant*

$$\begin{vmatrix} a_{11} & \ldots & a_{1,\rho+1} \\ \vdots & \ddots & \vdots \\ a_{\rho,1} & \ldots & a_{\rho,\rho+1} \\ v_1 & \ldots & v_{\rho+1} \end{vmatrix}$$

only depends on the a_{ij} and not on the v_i.

Proof. Add all columns of this determinant to the last; then we get

$$\begin{vmatrix} a_{11} & \ldots & a_{1,\rho} & 0 \\ \vdots & \ddots & \vdots & \vdots \\ a_{\rho,1} & \ldots & a_{\rho,\rho} & 0 \\ v_1 & \ldots & v_\rho & 1 \end{vmatrix}$$

Developing with respect to the last line shows that the determinant in question equals

$$\begin{vmatrix} a_{11} & \ldots & a_{1,\rho} \\ \vdots & \ddots & \vdots \\ a_{\rho,1} & \ldots & a_{\rho,\rho} \end{vmatrix}.$$

Note that the determinant also equals any other $\rho \times \rho$-minor of (a_{ij}). □

If we apply this lemma to the minors of the determinant whose rows are the $\lambda(\varepsilon_j)$ we find that the determinant

$$R_K = \begin{vmatrix} \log|\sigma_1(\varepsilon_1)| & \ldots & 2\log|\sigma_\rho(\varepsilon_1)| \\ \vdots & \ddots & \vdots \\ \log|\sigma_1(\varepsilon_\rho)| & \ldots & 2\log|\sigma_\rho(\varepsilon_\rho)| \end{vmatrix}$$

does not depend on the choice of the embeddings (the factor 2 is only attached to the logarithms of the nonreal embeddings). In particular, the regulator of a real quadratic number field K with fundamental unit $\varepsilon > 1$ is $R_K = \log\varepsilon$.

Next we compute $\operatorname{vol}(F)$. To that end we observe that the unit vector $v = \frac{1}{\sqrt{r+s}}(1, \ldots, 1)$ is perpendicular to $\mathcal{H}$; thus the volume of the fundamental domain F of $\lambda(\mathfrak{O}_K^\times)$ in $\mathcal{H}$ is the same as the volume V of the fundamental domain of the lattice $\lambda(\mathfrak{O}_K^\times \oplus \mathbb{Z}v)$ in $\mathbb{R}^{r+s}$. The latter is given by the absolute value of the determinant

$$\frac{1}{\sqrt{r+s}} \begin{vmatrix} \log|\sigma_1(\varepsilon_1)| & \dots & 2\log|\sigma_{r+s}(\varepsilon_1)| \\ \vdots & \ddots & \vdots \\ \log|\sigma_1(\varepsilon_\rho)| & \dots & 2\log|\sigma_{r+s}(\varepsilon_\rho)| \\ 1 & \dots & 1 \end{vmatrix},$$

which equals $\frac{1}{\sqrt{r+s}} R_K$. We have proved

Lemma 7.12. *The volume of the fundamental domain of the lattice $\lambda(\mathfrak{O}_K^\times)$ in $\mathcal{H}$ is $\frac{1}{\sqrt{r+s}} R_K$. In particular, R_K does not depend on the choice of the fundamental units.*

The Volume of D_1

The most technical part of the proof is the computation of $\mathrm{vol}\,(D_1)$.

Lemma 7.13. *We have*

$$\mathrm{vol}\,(D_1) = 2^{r+s}\pi^s R_K.$$

First let D_1^+ denote the subset of D_1 for which $x_1, \dots, x_r \ge 0$; then clearly $\mathrm{vol}\,(D_1) = 2^r \mathrm{vol}\,(D_1^+)$.

Next we introduce polar coordinates. We set $x_j = \rho_j e^{i\phi_j}$ (with $\phi_j = 0$ for $j = 1, \dots, r$) and map

$$(x_1, \dots, x_{r+s}) \longmapsto (\rho_1, \dots, \rho_r, \rho_{r+1}, \phi_{r+1}, \dots, \rho_{r+s}, \phi_{r+s}). \tag{7.1}$$

The Jacobian of this transformation is $\rho_{r+1} \cdots \rho_{r+s}$. The subset D_1^+ is described in these coordinates by the equations

1. $\rho_1, \dots, \rho_{r+s} > 0$;
2. $\prod \rho_j^{b_j} \le 1$, where $b_1 = \ldots = b_r = 1$ and $b_{r+1} = \ldots = b_{r+s} = 2$.
3. $\log \rho_j^{b_j} = \frac{b_j}{n} \sum_{i=1}^{r+s} b_i \log(\rho_i) + \sum_{i=1}^{r} a_i \lambda_j(\varepsilon_i)$ with $0 \le a_i < 1$ for $i = 1, \dots, r+s$.

The last equation comes from the fact that $x = (x_1, \dots, x_{r+s}) \in D_1$ satisfies $\ell(x) = \sum a_j \lambda(\varepsilon_j) + au$ with $0 \le a_j < 1$ and $na = N(x)$.

The variables $\phi_{r+1}, \dots, \phi_{r+s}$ independently run through the interval $[0, 2\pi)$; this shows that

$$\mathrm{vol}\,(D_1^+) = (2\pi)^s \int_{\widetilde{D}_1^+} \rho_{r+1} \cdots \rho_{r+s} d\rho_1 \cdots d\rho_{r+s},$$

where $\widetilde{D}_1^+$ is described by the inequalities above.

We now introduce new variables $a, a_1, \dots, a_{r+s}$ using the equations

$$\log \rho_j^{b_j} = \frac{b_j}{n} \log(a) + \sum a_i \lambda_j(\varepsilon_i),$$

where $a = \prod \rho_i^{a_i} = N(x)$. The equations for the ρ_j now become $0 < a \le 1$, $0 \le a_i < 1$ for $i = 1, \ldots, r+s$. These equations describe the unit cube, whose volume is 1. Thus all we have to do is compute the Jacobian of this transformation.

To this end observe that

$$\frac{\partial \rho_j}{\partial a} = \frac{\rho_j}{na}, \qquad \frac{\partial \rho_j}{\partial a_i} = \frac{\rho_j}{b_i} \lambda_j(\varepsilon_i).$$

Thus the Jacobian is given by

$$\begin{aligned} J &= \begin{vmatrix} \frac{\rho_1}{na} & \frac{\rho_1}{b_1}\lambda_1(\varepsilon_1) & \ldots & \frac{\rho_1}{b_1}\lambda_1(\varepsilon_\rho) \\ \frac{\rho_2}{na} & \frac{\rho_2}{b_2}\lambda_2(\varepsilon_1) & \ldots & \frac{\rho_2}{b_2}\lambda_2(\varepsilon_\rho) \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\rho_{r+s}}{na} & \frac{\rho_{r+s}}{b_{r+s}}\lambda_{r+s}(\varepsilon_1) & \ldots & \frac{\rho_{r+s}}{a_{r+s}}\lambda_{r+s}(\varepsilon_\rho) \end{vmatrix} \\ &= \frac{\rho_1 \cdots \rho_{r+s}}{na2^s} \begin{vmatrix} b_1 & \lambda_1(\varepsilon_1) & \ldots & \lambda_1(\varepsilon_\rho) \\ b_2 & \lambda_2(\varepsilon_1) & \ldots & \lambda_2(\varepsilon_\rho) \\ \vdots & \vdots & \ddots & \vdots \\ b_{r+s} & \lambda_{r+s}(\varepsilon_1) & \ldots & \lambda_{r+s}(\varepsilon_\rho) \end{vmatrix} \\ &= \frac{\rho_1 \cdots \rho_{r+s}}{a2^s} R_K = \frac{R_K}{2^s \rho_{r+1} \cdots \rho_{r+s}}. \end{aligned}$$

Putting everything together we see that

$$\operatorname{vol}(D_1) = 2^r (2\pi)^s 2^{-s} R_K = 2^r \pi^s R_K.$$

It remains to show that the boundary ∂D_1 is $(n-1)$-Lipschitz parametrizable.

Recall that we have to count the number of lattice points in D_t, where the lattice Λ is the image of the ideal $\mathfrak{b}$. We know that $\operatorname{vol}(\Lambda) = 2^{-s}\sqrt{|\operatorname{disc} K|} N\mathfrak{b}$, and that each principal ideal (α) with $\alpha \in \Lambda$ and norm $|N\alpha| \le mN\mathfrak{b}$ (where $m = N\mathfrak{a}$) corresponds to exactly w lattice points in D_t for the real number $t = \sqrt[n]{mN\mathfrak{b}}$.

Thus Lemma 7.10 shows that

$$\begin{aligned} wN_t &= \frac{\mathrm{vol}\,(D_t)}{\mathrm{vol}\,(\Lambda)} t^n + O(t^{n-1}) \\ &= \frac{\mathrm{vol}\,(D_1) N\mathfrak{b}}{\mathrm{vol}\,(\Lambda)} m + O(m^{1-\frac{1}{n}}) \\ &= \frac{2^r \pi^s R_K N\mathfrak{b}}{2^{-s}\sqrt{|\mathrm{disc}\,K|} N\mathfrak{b}} m + O(m^{1-\frac{1}{n}}) \\ &= \frac{2^{r+s}\pi^s R_K}{\sqrt{|\mathrm{disc}\,K|}} m + O(m^{1-\frac{1}{n}}). \end{aligned}$$

In particular, the number of integral ideals in an ideal class grows linearly with the norm, and does not depend on the ideal class. This finally finishes, by the same argument we used in the quadratic case, the proof of Theorem 7.1.

7.2 Dirichlet's Class Number Formula

Dirichlet was the first to study binary quadratic forms whose coefficients are Gaussian integers, and discovered a class number formula, which, in modern terms, boils down to a statement of the following form: let $k_1 = \mathbb{Q}(i)$, $k_2 = \mathbb{Q}(\sqrt{m}\,)$ and $k_3 = \mathbb{Q}(\sqrt{-m}\,)$ three quadratic number fields with class numbers $h_1 = 1$, h_2 and h_3, respectively; also assume that $m > 1$. Then the class number h_K of the compositum $K = k_1k_2k_3 = \mathbb{Q}(i, \sqrt{m}\,)$ is given by $h_K = \frac{1}{2} q h_m h_-$ for some index $q \in \{1, 2\}$. A little later, Eisenstein proved a similar formula for fields $\mathbb{Q}(\sqrt{-3}, \sqrt{m}, \sqrt{-3m}\,)$. Once Dedekind's ideal theory was available, these formulas were quickly generalized to the following general result:

Theorem 7.14. *Let k_1, k_2 and k_3 be the three quadratic subfields of a biquadratic extension $K/\mathbb{Q}$, and let h_1, h_2, h_3, h_K denote the class numbers of these fields. Then*

$$h_K = \begin{cases} \frac{1}{2} q(K) h_1 h_2 h_3 & \text{if } K \text{ is complex,} \\ \frac{1}{4} q(K) h_1 h_2 h_3 & \text{if } K \text{ is real.} \end{cases}$$

Here $q(K) = (E_K : E_1E_2E_3)$ is the unit index, which measures to which extent the unit group E_K of K is generated by the unit groups E_1, E_2, E_3 of the three quadratic subfields. Moreover, we have $q(K) \mid 2$ if K is complex, and $q(K) \mid 4$ if K is real.

It is not difficult to see how to prove such a result: using the factorization

$$\zeta_K(s) = \zeta(s) L(s, \chi_1) L(s, \chi_2) L(s, \chi_3)$$

of the Dedekind zeta function into the Riemann zeta function and the three L-series attached to the quadratic characters χ_j belonging to the quadratic subfields k_j, we immediately get the following formula for the residues at $s = 1$ by multiplying through by $s-1$ and taking limits $s \to 1$:

$$h_K \kappa_K = h_1 h_2 h_3 \kappa_1 \kappa_2 \kappa_3,$$

where $\kappa_K = \frac{2^4 R_K}{w_K \sqrt{\operatorname{disc} K}}$, $\kappa_j = \frac{2^2 R_j}{w_j \sqrt{\operatorname{disc} k_j}}$ if K is real (here w_j denotes the numbers of roots of unity in k_j, and R_j is the regulator of k_j), and $\kappa_K = \frac{\pi^2 R_K}{w_K \sqrt{\operatorname{disc} K}}$, $\kappa_1 = \frac{2^2 R_1}{w_1 \sqrt{\operatorname{disc} k_1}}$ for the real quadratic subfield k_1, and $\kappa_j = \frac{2\pi}{w_j \sqrt{|\operatorname{disc} k_j|}}$ for the two complex quadratic subfields k_2, k_3 if K is complex.

Assume first that K is real; then

$$h_K = h_1 h_2 h_3 \frac{1}{4} \frac{R_1 R_2 R_3}{R_K} \frac{w_1 w_2 w_3}{w_K} \frac{d_1 d_2 d_3}{\operatorname{disc} K},$$

where $d_j = \operatorname{disc} k_j$. Since K is real, the only roots of unity in K are ± 1, hence $w_1 = w_2 = w_3 = w_K = 2$.

7.3 Cyclotomic Fields

Exercises

7.1 Show that the Jacobian of the transformation (7.1) is $\rho_{r+1} \cdots \rho_{r+s}$. Hint: write $x_j = u_j + iv_j$ for $r+1 \le j \le r+s$, and compute $\frac{\partial x_j}{\partial \rho_i}$ and $\frac{\partial x_j}{\partial \phi_i}$. Then write down the Jacobian matrix and compute the absolute value of its determinant.

8. Density Theorems

In this chapter we will discuss a few consequences of the fact (proved in the last chapter) that the Dedekind zeta function $\zeta_K(s)$ of a number field K has a pole of order 1 at $s = 1$. We will derive the density theorems of Kronecker, Frobenius (for abelian extensions), as well as Kummer and Hilbert (in this connection we also have to study prime decomposition in Kummer extensions).

8.1 Kronecker's Density Theorem

Kronecker's starting point was his observation

Proposition 8.1. *Let $f \in \mathbb{Z}[x]$ be a polynomial with g irreducible factors. For primes p, let n_p denote the number of roots of f in $\mathbb{F}_p[x]$, counted with multiplicity. Then*

$$\sum_p n_p p^{-s} \sim g \log \frac{1}{s-1} \tag{8.1}$$

as $s \to 1$.

Here are a few very simple examples:

1. If f is the product of g linear factors, then $n_p = g$, and the statement is equivalent to $\sum p^{-s} \sim \log \frac{1}{s-1}$.
2. If $f(x) = x^2 + 1$, then $g = 1$, and we have
$$n_p = \begin{cases} 2 & \text{if } p \equiv 1 \bmod 4, \\ 0 & \text{if } p \equiv 3 \bmod 4, \end{cases}$$
hence primes $p \equiv 1 \bmod 4$ have Dirichlet density $\frac{1}{2}$.
3. If $f(x) = \Phi_m(x)$ is the m-th cyclotomic polynomial, then $g = 1$, and as above we find
$$n_p = \begin{cases} \phi(m) & \text{if } p \equiv 1 \bmod m, \\ 0 & \text{otherwise;} \end{cases}$$
this implies that primes $p \equiv 1 \bmod m$ have Dirichlet density $\frac{1}{\phi(m)}$.

The Dirichlet series on the left hand side of (8.1) can be split up as follows. Let $S_j = S_j(f)$ denote the set of primes p for which $f(x)$ has exactly p roots (counted with multiplicity). If $\deg f = n$, then

$$\sum_p n_p p^{-s} = \sum_{p \in S_1} p^{-s} + 2 \sum_{p \in S_2} p^{-s} + 3 \sum_{p \in S_3} p^{-s} + \ldots + n \sum_{p \in S_n} p^{-s}. \tag{8.2}$$

Kronecker conjectured that each of these sets S_j has a Dirichlet density $D_j = \delta(S_j)$; combining (8.1) and (8.2) then immediately implies the relation

$$D_1 + 2D_2 + 3D_3 + \ldots + nD_n = 1 \tag{8.3}$$

for irreducible polynomials. Observe that $D_{n-1} = 0$, since a polynomial with $n-1$ roots has n of them.

The existence of these densities has quite strong consequences: D_n is the density of primes for which the polynomial f (assumed to be irreducible over $\mathbb{Q}$) splits into linear factors over $\mathbb{F}_p$; according to Thm. 5.5, these are the primes that split completely in the number field $K = \mathbb{Q}(\alpha)$, where α is any root of f. Equation (8.3) immediately implies that $nD_n \le 1$, i.e. that $D_n \le \frac{1}{n}$. If $K/\mathbb{Q}$ is normal, then all the degrees of the factors of f over $\mathbb{F}_p$ must be the same, which implies $D_1 = \ldots = D_{n-1} = 0$. Kronecker's conjecture therefore implies

Theorem 8.2 (Kronecker's Density Theorem)**.** *The primes p that split completely in a normal extension $K/\mathbb{Q}$ have Dirichlet density $\frac{1}{(K:\mathbb{Q})}$.*

For certain special cases we have already seen a proof of this result:

1. the primes p that split in a quadratic extension $K/\mathbb{Q}$ have Dirichlet density $\frac{1}{2}$;
2. the primes p that split completely in a cyclotomic extension $K = \mathbb{Q}(\zeta_m)$ have Dirichlet density $\frac{1}{\phi(m)}$;
3. the primes p that split in a multiquadratic extension $K = \mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_t}\,)$ of degree 2^t have Dirichlet density 2^{-t}.

Kronecker's density theorem follows easily from the fact that Dedekind's zeta function $\zeta_K(s)$ has a pole of order 1 at $s = 1$:

Proof of Thm. 8.2. Assume that $\lim_{s \to 1}(s-1)\zeta_K(s) = \kappa \ne 0$. Then $\log \zeta_K(s) \sim \log \frac{1}{s-1}$. Using the Euler product of the zeta function we find as usual

$$\log \frac{1}{s-1} = \sum_{\mathfrak{p}} N\mathfrak{p}^{-s} + O(1).$$

In a normal extension, we have $p\mathfrak{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_g$ for all unramified primes p, with $fg = (K : \mathbb{Q})$. Thus either p splits completely into $(K : \mathbb{Q})$ prime ideals of degree 1 (i.e., norm p), or all primes above p have inertia degree ≥ 2. Since $\sum N\mathfrak{p}^{-1} = O(1)$ for primes not splitting completely, we find

$$\log \frac{1}{s-1} = \sum_{f(\mathfrak{p})=1} N\mathfrak{p}^{-s} + O(1).$$

Finally, since there are exactly $(K:\mathbb{Q})$ prime ideals of norm p above each p splitting completely, we find

$$\log \frac{1}{s-1} = (K:\mathbb{Q}) \sum_{\mathfrak{p}\in \mathrm{Spl}(K/\mathbb{Q})} p^{-s} + O(1).$$

But this says that primes splitting completely have Dirichlet density $\frac{1}{(K:\mathbb{Q})}$ as claimed. □

If the extension $K/\mathbb{Q}$ is not normal, let $L/\mathbb{Q}$ denote its normal closure. Then a prime p splits completely in $K/\mathbb{Q}$ if and only if it splits completely in $L/\mathbb{Q}$. Thus Kronecker's density theorem implies

Corollary 8.3. *Let $K/\mathbb{Q}$ be an extension with normal closure $L/\mathbb{Q}$. Then the set* $\mathrm{Spl}(K/\mathbb{Q})$ *has Dirichlet density* $\frac{1}{(L:\mathbb{Q})}$.

Kronecker's result has another nice corollary saying that the set $\mathrm{Spl}(K/\mathbb{Q})$ of primes splitting in a normal extension $K/\mathbb{Q}$ characterizes K in the following way:

Corollary 8.4. *Let $K/\mathbb{Q}$ and $L/\mathbb{Q}$ be normal extensions; then*

$$\mathrm{Spl}(K/\mathbb{Q}) \subseteq \mathrm{Spl}(L/\mathbb{Q}) \quad \textit{if and only if} \quad L \subseteq K.$$

Thus the set of splitting primes characterizes normal extensions of $\mathbb{Q}$. As the proof will show, the assumption $\mathrm{Spl}(K/\mathbb{Q}) \subseteq \mathrm{Spl}(L/\mathbb{Q})$ is needed only up to a set of exceptional primes of density 0.

Proof. Primes splitting completely in K and L also split completely in the compositum KL, hence $\mathrm{Spl}(K/\mathbb{Q}) \subseteq \mathrm{Spl}(KL/\mathbb{Q})$; on the other hand, any prime splitting in $KL/\mathbb{Q}$ must also split in each of its subfield, hence we have $\mathrm{Spl}(KL/\mathbb{Q}) \subseteq \mathrm{Spl}(K/\mathbb{Q})$, and thus $\mathrm{Spl}(K/\mathbb{Q}) = \mathrm{Spl}(KL/\mathbb{Q})$. By Kronecker's density theorem, this implies $(K:\mathbb{Q}) = (KL:\mathbb{Q})$, hence $(KL:K) = 1$, and so $L \subseteq K$. □

This result due to Bauer [Ba1903] has led to substantial research, first by Gaßmann [Ga1926] (who showed that the result does not hold for nonnormal extensions, not even up to conjugacy), and more recently, by Klingen, Perlis, de Smit, and others.

Next we will generalize Kronecker's density theorem to relative extensions L/K. To this end we say that a set S of prime ideals of $\mathfrak{O}_K$ has Dirichlet density δ if

$$\sum_{\mathfrak{p}\in S} N\mathfrak{p}^{-s} = -\delta \log(s-1) + O(1)$$

as $s \to 1+0$.

Lemma 8.5. *The set $\mathbb{P}_K$ of all prime ideals in $\mathfrak{O}_K$ has Dirichlet density $\delta(\mathbb{P}_K) = 1$.*

Note that the set of prime ideals of degree ≥ 2 has Dirichlet density 0. In particular, the lemma implies that the primes of degree 1 in a number field K have density 1.

Proof. We know $\lim(s-1)\zeta_K(s) = \kappa \ne 0$; replacing $\zeta_K(s)$ by its Euler factorization, taking the log and observing that the contribution from prime ideals of degree ≥ 2 is bounded as $s \to 1$ shows that

$$-\log(s-1) = \sum_{\mathfrak{p}} N\mathfrak{p}^{-s} + O(1).$$

By the definition of Dirichlet density, this implies $\delta(\mathbb{P}_K) = 1$. □

Now we can state and prove

Theorem 8.6 (Kronecker's Density Theorem)**.** *The set $S = \mathrm{Spl}(L/K)$ of prime ideals $\mathfrak{p}$ that split completely in a normal extension L/K has Dirichlet density $\frac{1}{(L:K)}$.*

Proof. Let S' denote the set of prime ideals in L above the $\mathfrak{p} \in \mathrm{Spl}(L/K)$. Since each $\mathfrak{p} \in \mathrm{Spl}(L/K)$ splits into $(L:K)$ distinct prime ideals in L, and since $\mathfrak{p}$ and $\mathfrak{P}$ have the same absolute norm because $f(\mathfrak{P}|\mathfrak{p}) = 1$, we find

$$\sum_{\mathfrak{P}\in S'} N\mathfrak{P}^{-s} = \sum_{\mathfrak{p}\in S}\sum_{\mathfrak{P}|\mathfrak{p}} N\mathfrak{P}^{-s} = (L:K)\sum_{\mathfrak{p}\in S} N\mathfrak{p}^{-s}.$$

But S' contains all prime ideals in L of degree 1; thus $\delta(S') = 1$, and now the claim follows. □

What can we say about prime ideals that do not split completely? If L/K is cyclic of prime degree p, then unramified prime ideals either split completely or are inert. Thus the set $\mathbb{P}_K$ of prime ideals in $\mathfrak{O}_K$ is the disjoint union of the finite set of ramified prime ideals, $\mathrm{Spl}(L/K)$, and the inert prime ideals; this implies that the set of inert prime ideals has Dirichlet density $1 - \frac{1}{p} = \frac{p-1}{p}$:

Corollary 8.7. *Let L/K be a cyclic extension of prime degree p. Then the set of prime ideals $\mathfrak{p}$ in $\mathfrak{O}_K$ that are inert in L/K has Dirichlet density $\frac{p-1}{p}$.*

8.2 Frobenius Density Theorem for Abelian Extensions

Kronecker's Density Theorem can be improved easily in the case of abelian extensions. Using results about Frobenius symbols and a little bit of group theory, we will later show how to generalize these results to arbitrary normal extensions.

To get started, let L/K be a cyclic extension of degree p^2, and let F/K denote the subextension of degree p. Then there are three kinds of unramified prime ideals: $\mathrm{Spl}(L/K)$, the primes in $\mathrm{Spl}(F/K)$ that remain inert in L, and the primes remaining inert in L/K (primes remaining inert in F/K cannot split in L/F, since the decomposition field must be one of K, F, or L). If we denote these sets of primes by S_0, S_1 and S_2, respectively, then

1. $\delta(S_1 \cup S_2 \cup S_3) = 1$;
2. $\delta(S_1) = \frac{1}{p^2}$ by Kronecker's density theorem applied to L/K.
3. $\delta(S_1 \cup S_2) = \frac{1}{p}$ by Kronecker's density theorem applied to F/K, and using the fact that $S_1 \cup S_2 = \mathrm{Spl}(F/K)$.
4. $\delta(S_2) = \frac{1}{p} - \frac{1}{p^2}$ is a consequence of 2. and 3.
5. $\delta(S_3) = 1 - \frac{1}{p}$ is a consequence of 1. and 3.

Thus we arrive at the following result:

Corollary 8.8. *Let L/K be a cyclic extension of degree p^2, where p is prime. Let H be the subgroup of order p. Then for every subextension F/K, the set S_F of prime ideals in K that split in F/K and are inert in L/F has Dirichlet density*

$$\delta(S_F) = \frac{\phi(L:F)}{(L:K)}.$$

The obvious generalization of this result is

Theorem 8.9 (Frobenius Density Theorem for Cyclic Extensions)**.** *Let L/K be a cyclic extension, and let F be an intermediate field. The set S_F of prime ideals $\mathfrak{p}$ with decomposition field F has Dirichlet density*

$$\delta(S_F) = \frac{\phi(L:F)}{(L:K)}.$$

Note that the statement $\delta(S_L) = \frac{1}{(L:K)}$ is just Kronecker's density theorem.

Proof. We proceed by induction on the number of prime factors of the degree $(L:K)$. We have already seen that the proposition holds if $(L:K)$ is prime.

Now let $(L:K) = n$ and assume the result holds for all cyclic extensions of degree d, where d is a proper divisor of n. Then the set of prime ideals of K is a disjoint union of the sets S_F, where F runs through the intermediate fields of L/K; since all S_F with $F \neq K$ have a Dirichlet density by induction assumption, so does S_K, and we find

$$1 = \sum_F \delta(S_F) = \delta(S_K) + \sum_{F \neq K} \delta(S_F) = \delta(S_K) + \sum_{F \neq K} \frac{\phi(L:F)}{n}.$$

Since in cyclic extensions L/K there is a bijection between the intermediate fields F and the divisors of n, we get

$$\delta(S_K) = 1 - \frac{1}{n} \sum_{d|n, d<n} \phi(d).$$

But $\sum_{d|n} \phi(d) = n$ from elementary number theory, hence

$$\delta(S_K) = 1 - \frac{1}{n}(n - \phi(n)) = \frac{\phi(n)}{n}$$

as claimed. □

The generalization to abelian extensions is now very easy:

Corollary 8.10. *Let L/K be an abelian extension, and F an intermediate field such that L/F is cyclic. Then the set S_F of prime ideals with decomposition field F has Dirichlet density*

$$\delta(S_F) = \frac{\phi(L:F)}{(L:K)}.$$

We will later see (in connection with studying the inertia subgroup of a Galois group) that we cannot drop the assumption that L/F be cyclic, since there are no inert prime ideals in noncyclic extensions. We have already seen this in the special case $K = \mathbb{Q}(\sqrt{a}, \sqrt{b}\,)$.

Proof. Set $\delta = \delta(S_F)$, and let Σ_F denote the set of prime ideals $\mathfrak{q}$ in F that remain inert in L/F. Then

$$(F:K) \sum_{\mathfrak{p} \in S_F} N\mathfrak{p}^{-s} = \sum_{\mathfrak{q} \in \Sigma} N\mathfrak{q}^{-s} + O(1),$$

since prime ideals $\mathfrak{q}$ of relative degree > 1 only contribute to $O(1)$, and every prime ideal $\mathfrak{q}$ of relative degree 1 lies over $(F:K)$ prime ideals $\mathfrak{p}$ in F, with at most finitely many exceptions due to ramified primes. Thus

$$\delta(S_F) = \frac{1}{(F:K)}\delta(\Sigma) = \frac{1}{(F:K)} \frac{\phi(L:F)}{(L:F)} = \frac{\phi(L:F)}{(L:K)},$$

where we have used Thm. 8.9 for the second equality. □

8.3 Kummer Extensions

Kummer extensions occupy a central place in class field theory. They were first studied by Kummer in connection with reciprocity laws and Fermat's Last Theorem, and became an indispensable tool for proving the existence theorem of class field theory.

Hilbert's Theorem 90

We start with two simple but important results that are called Hilbert's Theorem 90 for numbers and ideals, respectively:

Proposition 8.11 (Hilbert's Theorem 90)**.** *Let L/K be a cyclic extension of fields, and let σ be a generator of $G = \mathrm{Gal}\,(L/K)$. Then $N\alpha = 1$ for some $\alpha \in L^\times$ if and only if $\alpha = \beta^{1-\sigma}$ for some $\beta \in L^\times$. In other words: there is an exact sequence*

$$L^\times \xrightarrow{1-\sigma} L^\times \xrightarrow{N} K^\times.$$

This result was used by Kummer for cyclic extensions of cyclotomic number fields, and was called a theorem (the 90th in his famous Zahlbericht) by Hilbert. It is the grandfather of Galois cohomology.

Before we give the general proof, let us first discuss the case of quadratic extensions. If K has characteristic $\ne 2$, we can write $L = K(\sqrt{\mu}\,)$. Assume that $N\alpha = 1$; we have to find a β (which will depend on α) with $\alpha\beta^\sigma = \beta$. Trying our luck with $\beta = a + b\alpha$ for $a, b \in K$ we get $\alpha\beta^\sigma = \alpha(a+b\alpha^\sigma) = a\alpha + b$ since $\alpha^{1+\sigma} = N\alpha = 1$. This will be equal to β if $a = b$; thus we are led to put $\beta = 1 + \alpha$, and now we find $\alpha\beta^\sigma = \alpha(1 + \alpha^\sigma) = \alpha + N\alpha = \alpha + 1 = \beta$, hence $\alpha = \beta^{1-\sigma}$ unless $\beta = 0$. But $\beta = 0$ if and only if $\alpha = -1$, and in that case you can take $\beta = \sqrt{\mu}$.

If L/K is cyclic of degree 3, then it is easy to see that $\beta = 1 + \alpha + \alpha^{1+\sigma}$ has the property $\alpha\beta^\sigma = \beta$. This time, however, there seems to be no easy way out of the dilemma that we might have $\beta = 0$ for certain values of α. In order to get more general expressions, we can try $\beta = a + b\alpha + c\alpha^{1+\sigma}$. Since we want β to behave nicely under σ, we put $b = a^\sigma$ and $c = a^{\sigma^2}$, i.e., $\beta = a + a^\sigma\alpha + a^{\sigma^2}\alpha^{1+\sigma}$. Then it is easily checked that $\alpha\beta^\sigma = \beta$. It remains to show that we can choose $a \in L^\times$ in such a way that $\beta \ne 0$; this will be done in the proof below:

Proof. Although Hilbert's Theorem 90 holds for arbitrary cyclic extensions, we will prove it here only for number fields. Assume that $N\alpha = 1$, and write $L = K(\gamma)$. Set $n = \#G = (L : K)$, $a_0 = 1$, and $a_i = \alpha^{1+\sigma+\ldots+\sigma^{i-1}}$, as well as

$$\beta = \gamma + a_1\gamma^\sigma + a_2\gamma^{\sigma^2} + \ldots + a_{n-2}\gamma^{\sigma^{n-2}}.$$

It is then easily checked that $\alpha\beta^\sigma = \beta$, and this implies the claim if we can show that $\beta \ne 0$ for some choice of γ. We claim that replacing γ by γ^j for some $j = 0, 1, \ldots, n-1$ will work. For if not, then

$$\gamma^j + a_1\gamma^{j\sigma} + a_2\gamma^{j\sigma^2} + \ldots + a_{n-2}\gamma^{j\sigma^{n-2}} = 0$$

for $j = 0, 1, 2, \ldots, n-1$. Then the system of linear equations

$$\gamma^j x_0 + \gamma^{j\sigma}x_1 + \gamma^{j\sigma^2}x_2 + \ldots + \gamma^{j\sigma^{n-1}}x_{n-1} = 0$$

has the nontrivial solution $x_i = a_i$, hence the determinant of this system must vanish. But the square of this determinant is $\operatorname{disc}(1, \gamma, \ldots, \gamma^{n-1})$, and since the powers of γ form a K-basis of L, their discriminant is nonzero. □

The corresponding result for ideals states that, assuming that L/K is a cyclic extension of number fields, ideals $\mathfrak{a}$ with trivial norm have the form $\mathfrak{a} = \mathfrak{b}^{1-\sigma}$. One difference to Hilbert 90 for elements is that although there might exist algebraic *integers* $\alpha \in \mathfrak{O}_L$ with $N\alpha = 1$ (namely certain units), the only integral ideal $\mathfrak{a}$ with $N\mathfrak{a} = (1)$ is the unit ideal.

Proposition 8.12 (Hilbert's Theorem 90 for Ideals)**.** *Let L/K be a cyclic extension of number fields, and let σ be a generator of $G = \operatorname{Gal}(L/K)$. Then $N\mathfrak{a} = (1)$ for some nonzero fractional ideal $\mathfrak{a} \in D_L$ if and only if $\mathfrak{a} = \mathfrak{b}^{1-\sigma}$ for some ideal $\mathfrak{b} \in D_L$. In other words: there is an exact sequence*

$$D_L \xrightarrow{1-\sigma} D_L \xrightarrow{N} D_K.$$

Assume for the moment that L/K is a quadratic extension, and that $N\mathfrak{a} = (1)$. Then we can set $\mathfrak{b} = (1) + \mathfrak{a}$, where the sum of ideals represents forming the gcd. Obeserve that $\gcd(\prod \mathfrak{p}^{a_\mathfrak{p}}, \prod \mathfrak{p}^{b_\mathfrak{p}}) = \prod \mathfrak{p}^{c_\mathfrak{p}}$, where $c_\mathfrak{p} = \min(a_\mathfrak{p}, b_\mathfrak{p})$. If $\mathfrak{a} = \mathfrak{p}\mathfrak{q}^{-1}$, for example, then $\gcd((1), \mathfrak{a}) = \mathfrak{p}$. Thus $\mathfrak{b} = (1) + \mathfrak{a}$ is a nonzero ideal with $\mathfrak{a}\mathfrak{b}^\sigma = \mathfrak{a} + \mathfrak{a}^{1+\sigma} = \mathfrak{a} + (1) = \mathfrak{b}$. The same idea works in general:

Proof of Thm. 8.12. Formally, the proof is almost the same: we put

$$\mathfrak{b} = (1) + \mathfrak{a} + \mathfrak{a}^{1+\sigma} + \ldots + \mathfrak{a}^{1+\sigma+\ldots+\sigma^{n-1}},$$

where + denotes forming the sum (gcd) of fractional ideals. As above, we find $\mathfrak{a}\mathfrak{b}^\sigma = \mathfrak{b}$, and since $\mathfrak{b} \neq (0)$, we are done. □

Kummer Theory

8.4 Decomposition Laws in Kummer Extensions

8.5 Density Theorems of Kummer and Hilbert

Assume that $\alpha_1, \ldots, \alpha_t$ are nonzero elements of some number field K. If $\alpha_1^{e_1} \cdots \alpha_t^{e_t} = \gamma^2$ in $K^\times$ for exponents $e_j \in \{0,1\}$ implies that $e_1 = \ldots = e_t = 0$, then they are called independent modulo squares.

Hilbert's Satz 18 from his memoir on relative quadratic extensions reads

Theorem 8.13. *Let K be an algebraic number field, and assume that the elements $\alpha_1, \ldots, \alpha_t \in K^\times$ are independent modulo squares. Then for any choice of signs $c_1, \ldots, c_t = \pm 1$ the set S of prime ideals $\mathfrak{p}$ in K such that*

$$\Big(\frac{\alpha_1}{\mathfrak{p}}\Big) = c_1, \quad \ldots, \quad \Big(\frac{\alpha_t}{\mathfrak{p}}\Big) = c_t$$

has Dirichlet density $\delta(S) = 2^{-t}$.

Basically we only have to follow the proof that there exist infinitely many primes p with $(\frac{d}{p}) = c$ for a given nonsquare integer d and some $c = \pm 1$.

Lemma 8.14. *Let α be a nonsquare in K and χ a character on the group of fractional ideals defined by $\chi(\mathfrak{p}) = (\frac{\alpha}{\mathfrak{p}})$. Then $f(s) = \sum \chi(\mathfrak{p}) N\mathfrak{p}^{-s}$ is bounded as $s \to 1+0$.*

Proof. Let $L = K(\sqrt{\alpha}\,)$. Then the decomposition law in relative quadratic extensions implies $\zeta_K(s) = \zeta_k(s) L(s,\psi)$, where the character ψ is defined by

$$\psi(\mathfrak{p}) = \begin{cases} +1 & \text{if } \mathfrak{p} \text{ splits in } L/K, \\ 0 & \text{if } \mathfrak{p} \text{ ramifies in } L/K, \\ -1 & \text{if } \mathfrak{p} \text{ is inert in } L/K. \end{cases}$$

Except possibly for the finitely many prime ideals $\mathfrak{p} \mid (2\alpha)$, we have $\chi(\mathfrak{p}) = \psi(\mathfrak{p})$.

Since both $\zeta_K(s)$ and $\zeta_k(s)$ can be extended to the halfplane $\operatorname{Re} s > 1 - \frac{1}{2n}$ and have a pole of order 1 at $s = 1$, we deduce that $L(s,\chi)$ is also analytic there, and has a nonzero limit as $s \to 1$. But $\log L(s,\chi) = f(s) + O(1)$, and now the claim follows. □

Proof of Thm. 8.13. We have to show that

$$\sum_{\mathfrak{p} \in S} N\mathfrak{p}^{-s} = 2^{-t} \log \frac{1}{s-1} + O(1)$$

as $s \to 1$. To this end we identify ± 1 with $\mathbb{Z}/2Z$ and consider the character group X of $(\mathbb{Z}/2\mathbb{Z})^t$.

□

Kummer had already considered similar problems in cyclotomic number fields. For a number field K containing a primtive ℓ-th root of unity ζ we define the ℓ-th power residue character of some $\alpha \in \mathbb{Z}[\zeta]$ for all prime ideals $\mathfrak{p}$ coprime to α by $(\frac{\alpha}{\mathfrak{p}}) = \zeta^j$ if $\alpha^{(N\mathfrak{p}-1)/\ell} \equiv \zeta^j \bmod \mathfrak{p}$.

Proposition 8.15 (Decomposition in Kummer Extensions). *Let K be a number field K containing a primtive ℓ-th root of unity ζ, and assume that $L = K(\sqrt[\ell]{\mu})$ is an extension of relative degree ℓ. Then a prime ideal $\mathfrak{p}$ in K with $\mathfrak{p} \nmid \ell\alpha$ splits completely in the cyclic extension L/K if and only if $(\frac{\mu}{\mathfrak{p}}) = 1$.*

It is clear how to define algebraic integers that are independent modulo ℓ-th powers, where ℓ is a prime. The following result due to Kummer occurs as Satz 152 in Hilbert's Zahlbericht.

Theorem 8.16 (Kummer's Density Theorem). *Let K be a number field containing the ℓth roots of unity.*

Exercises

8.1 Assume that $K/\mathbb{Q}$ is an extension with $D_1 = \ldots = D_{n-1} = 0$. Show that $K/\mathbb{Q}$ is normal.

8.2 Show that the set of prime ideals of degree ≥ 2 in a number field K has Dirichlet density 0.

Part II

Hilbert Class Fields

9. The Hilbert Class Field

The theory of Hilbert class fields, conjectured by Hilbert and worked out by Furtwängler, is an extremely beautiful part of Takagi's class field theory, and is indispensible for any deeper study of class groups of number fields. We will see that the Hilbert class field of a number field K is its maximal unramified abelian extension,

9.1 Weber's Motivation

For proving that $\lim(s-1)\zeta_K(s) \neq 0$ we introduced a "partial zeta function" $\zeta_c(s)$ attached to an ideal class $c \in \mathrm{Cl}(K)$, defined as $\sum_{\mathfrak{a}\in c} N\mathfrak{a}^{-s}$, and showed that it represents an analytic function in the half plane $\operatorname{Re} s > 1$. Then we counted the number of ideals of norm $\leq t$ in each ideal class, showed that their number grows linearly with t, and that the constant of proportionality κ is independent of the ideal class c.

It therefore seems natural to ask how the *prime* ideals are distributed among the ideal classes c, and it is equally natural to conjecture

Theorem 9.1. *The set of prime ideals in a given ideal class $c \in \mathrm{Cl}(K)$ has Dirichlet density $\frac{1}{h}$, where $h = \#Cl(K)$ is the class number.*

Although this result seems "natural" at first, a closer look at the problem at hand might raise a few doubts. First of all, the prime ideals of degree > 1 need not be equidistributed among the ideal classes: in quadratic number fields, all prime ideals of degree 2 are principal and therefore contained in the principal class (this does not affect the conjecture above since prime ideals of degree > 1 have Dirichlet density 0).

Next there are Dedekind domains in which even the prime ideals of degree 1 are not equidistributed among the ideal classes: take a number field K with class number $h_K > 1$, and let S denote the set of prime ideals in the principal class. Then the localization $\mathfrak{O}_S$ (the subring of K consisting of all elements $\frac{\alpha}{\beta}$ such that β is a product of prime ideals from S) is a Dedekind ring with class number h_K whose principal class does not contain a single prime ideal.

Our only chance of proving a result such as Thm. 9.1 is by characterizing the set of primes in an ideal class c as a set $\mathrm{Spl}(L/K)$ for a suitable extension L/K:

> *An extension L of K is called a Hilbert class field of K if exactly the prime ideals in the principal class of* $\mathrm{Cl}(K)$ *split completely in L/K.*

Guided by wishful thinking, we therefore make the following bold conjecture:

Theorem 9.2 (Existence Theorem)**.** *Every number field K has a Hilbert class field $L = K^1$.*

Given the existence of Hilbert class fields, the set of prime ideals in the principal class coincides with $\mathrm{Spl}(L/K)$ and has Dirichlet density $\frac{1}{(L:K)}$. Since we expect the density to be $\frac{1}{h}$, we are led to

Theorem 9.3. *The Hilbert class field L of K has degree $(L : K) = h$.*

The truth of this conjecture automatically implies that Hilbert class fields are unique: for if L and L' are Hilbert class fields, then the prime ideals in the principal class of K split completely in both L/K and L'/K, hence in the compositum LL'/K. Since $(LL' : K) = h$, this implies that $L = L'$:

Theorem 9.4 (Uniqueness Theorem)**.** *Hilbert class fields are unique.*

The whole situation is reminiscent of our proof of Dirichlet's theorem on primes in arithmetic progression: the primes $p \equiv 1 \bmod m$ are exactly those in $\mathrm{Spl}(K/\mathbb{Q})$ for $K = \mathbb{Q}(\zeta_m)$. The question of how primes are distributed among the $\phi(m)$ residue classes in $(\mathbb{Z}/m\mathbb{Z})^\times$ is therefore connected to the splitting of primes in an extension of degree $\phi(m) = \#(\mathbb{Z}/m\mathbb{Z})^\times$. The residue class group $(\mathbb{Z}/m\mathbb{Z})^\times$ plays the role of the class group, and $\mathbb{Q}(\zeta_m)$ that of the Hilbert class field. In this situation, we even know that there is a strong connection between the "class group" $(\mathbb{Z}/m\mathbb{Z})^\times$ and the "class field" $\mathbb{Q}(\zeta_m)$: we have $\mathrm{Gal}\,(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^\times$. If we are bold enough to transfer this property to the situation above, we end up with the next conjecture:

Theorem 9.5 (Reciprocity Law)**.** *The Hilbert class field L/K is an abelian extension, and its Galois group is isomorphic to the ideal class group of K:*

$$\mathrm{Gal}\,(L/K) \simeq \mathrm{Cl}(K).$$

At this point, the name "reciprocity law" for this isomorphism is completely mysterious; we will justify this name later.

The existence of Hilbert class fields implies that the prime ideals in the principal class have Dirichlet density $\frac{1}{h}$. In order to prove that the same holds for the other ideal classes, we introduce characters $\chi : \mathrm{Cl}(K) \longrightarrow \mathbb{C}^\times$ on the ideal class group, and attach L-series $L(s,\chi)$ to them by setting $L(s,\chi) = \sum \chi(\mathfrak{a}) N\mathfrak{a}^{-s}$. Of course we expect

Theorem 9.6. *The L-series $L(s,\chi)$ for characters χ of the ideal class group represent analytic functions in the half plane* $\mathrm{Re}\, s > 1 - \frac{1}{(K:\mathbb{Q})}$, *and satisfy $L(1,\chi) \neq 0$ whenever $\chi \neq \mathbb{1}$.*

It is then an easy matter to derive the following result as a corollary:

Theorem 9.7 (Weber's Density Theorem). *Let K be a number field with class number h. Then the set of prime ideals in an ideal class $c \in \mathrm{Cl}(K)$ has Dirichlet density $\frac{1}{h}$.*

In the cyclotomic case, primes whose residue classes mod m do not lie in $(\mathbb{Z}/m\mathbb{Z})^\times$ ramify in $\mathbb{Q}(\zeta_m)/\mathbb{Q})$; since there are no prime ideals $\mathfrak{p}$ in K whose ideal classes do not lie in $\mathrm{Cl}(K)$, this suggests

Theorem 9.8 (Ramification Theorem). *The Hilbert class field of K is unramified over K.*

The most obvious analog of the decomposition law in cyclotomic extensions is

Theorem 9.9 (Decomposition Law). *Let $\mathfrak{p}$ be a prime ideal in K. If f denotes the smallest positive integer such that $\mathfrak{p}^f$ is principal, then $\mathfrak{p}$ splits into prime ideals of degree f in its Hilbert class field.*

Finally, there is an analog of the theorem of Kronecker-Weber:

Theorem 9.10 (Maximality of the Hilbert Class Field). *The Hilbert class field K of F contains every unramified abelian extension of: it is the maximal abelian unramified extension of F.*

These theorems constitute the main part of the theory of Hilbert class fields, with one famous exception: the Principal Ideal Theorem. This result, which is difficult to motivate in Weber's approach, was actually the starting place for Hilbert's research in class field theory. More exactly, Hilbert proved

Theorem 9.11 (Hilbert's Satz 94). *If L/K is a cyclic unramified extension of prime degree, then there is an ideal $c \in \mathrm{Cl}(K)$ with order p that becomes trivial in L; this means that if $c = [\mathfrak{a}]$, then $\mathfrak{a}\mathfrak{O}_L = (A)$ becomes a principal ideal in L.*

The general result that Hilbert conjectured reads

Theorem 9.12 (Principal Ideal Theorem). *Every ideal in F becomes principal in its class field K.*

Note that this does not imply that K has class number 1; in general, only ideals coming from F are principal, but there might be others. The principal ideal theorem, by the way, turned out to be the most difficult part of class field theory. Artin succeeded in reducing it to a purely group theoretical statement, which Furtwängler could finally prove at the end of the 1920s.

9.2 The Field $\mathbb{Q}(\sqrt{-5}\,)$

The Class Group

It is easily checked that $F = \mathbb{Q}(\sqrt{-5}\,)$ has discriminant $\Delta = -20$ and class number 2. In fact, the nontrivial ideal class is generated by the prime ideal $\mathfrak{z} = (2, 1+\sqrt{-5}\,)$. We know that 2 and 5 are ramified, and that the unramified primes split completely if and only if $(\frac{-20}{p}) = +1$. A quick calculation shows that

p is ramified	if $p = 2, 5$
p splits	if $p \equiv 1, 3, 7, 9 \bmod 20$,
p is inert	if $p \equiv 11, 13, 17, 19 \bmod 20$

We now will study how these primes are distributed in the ideal classes of F. It is clear that inert primes are principal; among the ramified primes $\mathfrak{z}$ is not principal, but $(5, \sqrt{-5}\,) = (\sqrt{-5}\,)$ is. This leaves us with the split primes.

Assume therefore that $p = \mathfrak{p}\mathfrak{p}'$; if $\mathfrak{p} = (a + b\sqrt{-5}\,)$ is principal, then $p = N\mathfrak{p} = a^2 + 5b^2 \equiv a^2 + b^2 \equiv 1 \bmod 4$. If, on the other hand, $\mathfrak{p}$ is not principal, then $\mathfrak{z}\mathfrak{p}$ is, and we have $\mathfrak{z}\mathfrak{p} = (a+b\sqrt{-5}\,)$ for odd integers a, b. This implies $2p = N\mathfrak{z}\mathfrak{p} = a^2 + 5b^2 \equiv 6 \bmod 8$, hence $p \equiv 3 \bmod 4$.

Proposition 9.13. *Among the split primes in F, exactly the prime ideals above primes with $p \equiv 1 \bmod 4$ are principal.*

The prime ideals that are inert in F are of course trivially principal.

The Class Field

Now consider the quadratic extension $K = F(\sqrt{-1}\,)$. We claim that K/F is unramified. Since F is totally complex, no infinite primes can ramify. Let $F_1 = \mathbb{Q}(\sqrt{-1}\,)$ and $F_2 = \mathbb{Q}(\sqrt{5}\,)$ denote the two other quadratic subfields of $K/\mathbb{Q}$. We know from the theory of the different that $\operatorname{diff}(K/F) \mid \operatorname{diff}(F_1/\mathbb{Q}) = (2)$ and $\operatorname{diff}(K/F) \mid \operatorname{diff}(F_1/\mathbb{Q}) = (\sqrt{5}\,)$; since these ideals are coprime, we conclude that $\operatorname{diff}(K/F) = (1)$, hence $\operatorname{disc}(K/F) = (1)$ as well. This implies the claim.

The prime decomposition in K/F is governed by a surprising result:

Theorem 9.14. *Let $\mathfrak{p}$ be a prime ideal in F, and let $f \geq 1$ denote the smallest integer for which $\mathfrak{p}^f$ is principal. Then the primes $\mathfrak{P}$ in K above $\mathfrak{p}$ have relative inertia degree f.*

Since K/F is unramified, we have $e = 1$ for each prime; once we know f, we can compute g from $efg = fg = (K : F) = 2$.

Proof. Assume first that $\mathfrak{p}$ is ramified in $F/\mathbb{Q}$. If $\mathfrak{p} = (\sqrt{-5}\,)$, then $f = 1$, hence we have to show that $\mathfrak{p}$ splits. In fact, 5 splits in $\mathbb{Q}(i)/\mathbb{Q}$, hence the prime $\mathfrak{p}$ above 5 in F must split in K/F. If $\mathfrak{p} = \mathfrak{2}$, then $f = 2$; in fact, 2 is ramified in $\mathbb{Q}(i)/\mathbb{Q}$ and $F/\mathbb{Q}$, and it is inert in $\mathbb{Q}(\sqrt{5}\,)/\mathbb{Q})$, hence it must have inertia degree 2 in K.

If $\mathfrak{p} = (p)$ is an inert prime, then $(\frac{-4}{p})(\frac{5}{p}) = (\frac{-20}{p}) = -1$, hence $(\frac{-4}{p}) = 1$ or $(\frac{5}{p}) = 1$; thus p splits in exactly one quadratic subfield and is inert in F and the third one, and this implies that p must split in K/F.

Finally, assume that $p = \mathfrak{p}\mathfrak{p}'$ splits in F. If $\mathfrak{p}$ is principal, then $p \equiv 1 \bmod 4$ and $p \equiv \pm 1 \bmod 5$, so p splits in all three quadratic subfields, and this implies that $\mathfrak{p}$ splits in K/F. If $\mathfrak{p}$ is not principal, then $(\frac{-20}{p}) = 1$ but $(\frac{-1}{p}) = (\frac{5}{p}) = -1$, hence p is inert in $\mathbb{Q}(i)/\mathbb{Q}$. Thus p has inertia degree ≥ 2 in $K/\mathbb{Q}$, and since it splits in $F/\mathbb{Q}$, it must be inert in K/F. □

Since the prime decomposition of a prime ideal $\mathfrak{p}$ in F is determined completely by the ideal class $[\mathfrak{p}]$ it represents, K was called a class field of F (in fact, it is the Hilbert class field of F).

9.3 The Field $\mathbb{Q}(\sqrt{3}\,)$

The Class Group of *F*

The quadratic number field $F = \mathbb{Q}(\sqrt{3}\,)$ has class number 1. Since the fundamental unit $2 + \sqrt{3}$ of F is totally positive, we have $h^+(F) = 2$, and the ideal class group in the strict sense is generated by the class $[(\sqrt{3}\,)]$.

Next we study which prime ideals are principal in the strict sense and which are not. If p is inert in F, then clearly p or $-p$ is totally positive, hence inert primes generate principal ideals in the strict sense.

There are two ramified ideals, namely those above 2 and 3, neither of which is principal since the elements $1 + \sqrt{3}$ and $\sqrt{3}$ generating these ideals both have mixed signature.

Now assume that $(p) = \mathfrak{p}\mathfrak{p}'$ splits in F, where $p > 0$. This happens if and only if $(\frac{12}{p}) = +1$, i.e., if and only if $p \equiv \pm 1 \bmod 12$. When is $\mathfrak{p}$ principal in the strict sense? If it is, then $\mathfrak{p} = (a + b\sqrt{3}\,)$ with $0 < p = N\mathfrak{p} = a^2 - 3b^2 \equiv a^2 + b^2 \equiv 1 \bmod 4$. On the other hand, $\mathfrak{p}$ is not principal in the strict sense if and only if $a + b\sqrt{3}$ has mixed signature, i.e. if and only if $-p = a^2 - 3b^2 \equiv 1 \bmod 4$, that is, iff $p \equiv 3 \bmod 4$ (equivalently, $[\mathfrak{p}]_+$ is nontrivial if and only if $\sqrt{3}\mathfrak{p} \overset{+}{\sim} (1)$, and this leads to the same result).

Proposition 9.15. *Among the split primes in F, exactly the prime ideals above primes with $p \equiv 1 \bmod 4$ are principal in the strict sense.*

Note that $p \equiv 1 \bmod 4$ actually means $p \equiv 1 \bmod 4\infty$ since we assumed that $p > 0$.

The Class Field

Now consider $K = F(\sqrt{-1}\,) = F(\sqrt{-3}\,)$. The same argument as for $\mathbb{Q}(\sqrt{-5}\,)$ shows that K/F is unramified at all finite primes. Note, however, that the two infinite primes in F both ramify in K. We say that K/F is unramified outside ∞.

The prime decomposition in K/F is now similar to the one we've seen before:

Theorem 9.16. *Let $\mathfrak{p}$ be a prime ideal in F, and let $f \ge 1$ denote the smallest integer for which $\mathfrak{p}^f$ is principal in the strict sense. Then the primes $\mathfrak{P}$ in K above $\mathfrak{p}$ have relative inertia degree f.*

For this reason we call K the Hilbert class field of F in the strict sense. Observe that $\operatorname{Gal}(K/F) \simeq \operatorname{Cl}^+(F)$, and that every ideal in F becomes principal in K (since K is totally complex we have $\operatorname{Cl}^+(K) = \operatorname{Cl}(K)$) because K has class number 1.

9.4 Hilbert Class Field Theory II

Every result about Hilbert class fields has its analog for class groups in the strict sense; we start with the definition:

> Let K/k be a normal extension of number fields. Then K is called a class field of F if exactly the prime ideals of degree 1 in the principal ideal class of k in the strict sense split into prime ideals of degree 1 in K.

Using this definition it is easily checked that e.g. $K = \mathbb{Q}(i, \sqrt{-3}\,)$ is indeed the Hilbert class field of $F = \mathbb{Q}(\sqrt{3}\,)$ in the strict sense.

Theorem 9.17 (Existence Theorem)**.** *Every number field F has a unique Hilbert class field K in the strict sense.*

This allows us to talk about "the" (Hilbert) class field of a number field. In the following, let $F^1\{\infty\}$ denote the Hilbert class field of F in the strict sense

Theorem 9.18. *The extension $F^1\{\infty\}/F$ is unramified at all finite primes: we have* $\operatorname{disc}(F^1\{\infty\}/F) = (1)$.

In particular, abelian extensions of fields with class number 1 in the strict sense must be ramified at some finite prime.

Theorem 9.19. *The Hilbert class field $F^1\{\infty\}$ is abelian over F, and* $\operatorname{Gal}(F^1\{\infty\}/F) \simeq \operatorname{Cl}^+(F)$. *In particular, $(F^1\{\infty\} : F) = h_F^+$.*

Theorem 9.20 (Decomposition Law)**.** *The decomposition law for $F^1\{\infty\}/F$ is the following: if $\mathfrak{p}^f$ is the smallest positive power of $\mathfrak{p}$ that is principal in the strict sense, then $\mathfrak{p}$ splits into primes of relative inertia degree f in K.*

Since $F^1\{\infty\}/F$ is unramified at finite primes, every prime ideal $\mathfrak{p}$ in F decomposes as $\mathfrak{p} = \mathfrak{P}_1 \cdots \mathfrak{P}_g$ with $fg = (K:F) = h_F^+$. Thus the decomposition of $\mathfrak{p}$ is completely determined by the inertia degree f.

Theorem 9.21. *$F^1\{\infty\}$ is the maximal abelian extension of F unramified outside ∞.*

We also have

Theorem 9.22 (Principal Ideal Theorem)**.** *Every ideal in F becomes principal in the strict sense in $F^1\{\infty\}/F$.*

Note that this "principalization" might happen for trivial reasons: the ideals in $\mathbb{Q}(\sqrt{3}\,)$ that are nor principal in the strict sense become so in $\mathbb{Q}(i, \sqrt{-3}\,)$ since every element in this field is totally positive for lack of real infinite primes.

Exercises

9.1 Show directly from the definition that the different of the quadratic extension $\mathbb{Q}(\sqrt{m}\,)/\mathbb{Q}$ is $(2\sqrt{m})$ if $m \equiv 2, 3 \bmod 4$, and $(\sqrt{m}\,)$ if $m \equiv 1 \bmod 4$.

9.2 Let L/K be an extension of number fields. Show that $(\operatorname{disc} K)^{(L:K)} \mid \operatorname{disc} L$.

9.3 Let K/k and L/k be Galois extensions of number fields with $K \cap L = k$. Show that $\operatorname{diff}(M|L) \mid \operatorname{diff}(K|k)$ and $\operatorname{diff}(M|K) \mid \operatorname{diff}(L|k)$.

9.4 Consider the biquadratic extension $M = \mathbb{Q}(i, \sqrt{5}\,)$. Use the preceding exercise to show that M is unramified over $\mathbb{Q}(\sqrt{-5}\,)$.

9.5 More generally, let K and L be quadratic extensions with coprime discriminants. Show that the compositum KL is unramified over the quadratic subfield of KL different from K and L.

9.6 Let K/k be an extension of number fields. Show that the norm map $N_{K/k}$ on ideals induces a homomorphism $N_{K/k} : \mathrm{Cl}(K) \longrightarrow \mathrm{Cl}(k)$.

9.7 Let K/k be an extension of number fields. The map sending an ideal $\mathfrak{a}$ in $\mathfrak{o}$ to the ideal $\mathfrak{a}\mathfrak{O}$ is called the conorm, and is often denoted by $j_{k\to K}$. Show that the conorm induces a group homomorphism $j_{k\to K}\,\mathrm{Cl}(k) \longrightarrow \mathrm{Cl}(K)$, and that $N_{K/k} \circ j_{k\to K}$ raises each ideal class to its n-th power, where $n = (K:k)$. The kernel of this map is called the capitulation kernel.

9.8 Let K/k be an extension of number fields. Show that if $\mathfrak{a}$ is an ideal in $\mathfrak{o}$ such that $\mathfrak{a}\mathfrak{O} = (\alpha)$ is principal, then the order of the ideal class $c = [\mathfrak{a}]$ in $\mathrm{Cl}(k)$ divides $n = (K:k)$.

9.9 Let K/k be an extension of number fields. Show that if $\gcd(h_k, n) = 1$ for the class number $h_k = \#\,\mathrm{Cl}(k)$ and the degree $n = (K:k)$, then the norm map $N_{K/k} : \mathrm{Cl}(K) \longrightarrow \mathrm{Cl}(k)$ is surjective, and the conorm $j_{k\to K}\,\mathrm{Cl}(k) \longrightarrow \mathrm{Cl}(K)$ is injective. Deduce that $h_k \mid h_K$ in this case.

9.10 Show that $F = \mathbb{Q}(\sqrt{6}\,)$ has $\mathrm{Cl}^+(F) \simeq \mathbb{Z}/2\mathbb{Z}$, and find a generator.

9.11 Show that $F = \mathbb{Q}(\sqrt{34}\,)$ has $\mathrm{Cl}^+(F) \simeq \mathbb{Z}/4\mathbb{Z}$, and find a generator.

9.12 Show that $\mathbb{Q}(\sqrt[4]{2}\,)$ has two real infinite primes, and that their restriction to $\mathbb{Q}(\sqrt{2}\,)$ is the infinite prime corresponding to the real embedding sending $\sqrt{2}$ to the positive real root of $x^2 - 2$.

9.13 Show that $\mathbb{Q}(\sqrt{-6}\,)$ has Hilbert class field $\mathbb{Q}(\sqrt{2}, \sqrt{-3}\,)$.

9.14 Show that $\mathbb{Q}(\sqrt{6}\,)$ has Hilbert class field $\mathbb{Q}(\sqrt{-2}, \sqrt{-3}\,)$ in the strict sense.

9.15 Let $d = \operatorname{disc} F$ be the discriminant of a quadratic number field F. Show that $d = d_1 \cdots d_t$ can be written uniquely as a product of prime discriminants $d_i \in \{-4, \pm 8, p, -q\}$, where p and q denote primes $\equiv 1 \bmod 4$ and $\equiv 3 \bmod 4$, respectively.

9.16 (continued) Show that the extensions $F(\sqrt{d_i}\,)/F$ are unramified.

9.17 For a number field F, let $\mathrm{Cl}^*(F)$ denote the group of ideal classes of odd order. Let $K/\mathbb{Q}$ be the compositum of two quadratic extensions, and let k_1, k_2, k_3 denote its three quadratic subfields. Show that

$$\mathrm{Cl}^*(K) \simeq \mathrm{Cl}^*(k_1) \times \mathrm{Cl}^*(k_2) \times \mathrm{Cl}^*(k_3).$$

Hint: Let σ, τ and $\sigma\tau$ denote the nontrivial automorphisms of $K/\mathbb{Q}$ fixing the elements of k_1, k_2 and k_3, respectively; the identity

$$2 = 1 + \sigma + \tau + \sigma\tau - (1 + \sigma\tau)\sigma$$

in $\mathbb{Z}[\mathrm{Gal}\,(K/\mathbb{Q})]$ shows $\mathfrak{P}^2 = N^1\mathfrak{P} \cdot N^2\mathfrak{P} \cdot (N^3\mathfrak{P})^{-\sigma}$ for prime ideals $\mathfrak{P}$ in K, where the N^j denote the relative norms to the quadratic subfields.

9.18 (continued) Construct a quadratic number field F with class number 2 that possesses an unramified quadratic extension K/F such that $\mathrm{Cl}(K)$ has nontrivial class number.

9.19 Let L be a cubic field with squarefree discriminant d. Show that $L/\mathbb{Q}$ is not normal. Since $d \equiv 1 \bmod 4$, d is also the discriminant of a quadratic number field F. Show that $K = LF$ is an unramified extension of F, and that K/F is a normal extension with Galois group $\simeq \mathbb{Z}/3\mathbb{Z}$ (Hint: a cubic extension of number fields K/F defined by a root of a polynomial $f \in F[X]$ is normal if and only if the discriminant of f is a square F).

9.20 Let L be the cubic field generated by a root of $f(x) = x^3 - x + 1$, and let $K = LF$ denote its normal closure, where $F = \mathbb{Q}(\sqrt{-23}\,)$. Check by numerical examples that for primes $p = \mathfrak{p}\mathfrak{p}'$ splitting in F, the following are equivalent:

1. $\mathfrak{p}$ is principal in F;
2. $4p = a^2 + 23b^2$ is solvable in integers;
3. $f(x) \equiv 0 \bmod p$ has three solutions;
4. p splits completely in $L/\mathbb{Q}$.

Here (1) $\iff$ (2) and (3) $\iff$ (4) are clear, but the equivalence (1) $\iff$ (4) is essentially the decomposition law in class fields.

9.21 Let m be a positive integer divisible by some (positive) prime $p \equiv 1 \bmod 3$. Let $F = \mathbb{Q}(\sqrt[3]{m}\,)$ and let L be the cubic subfield of $\mathbb{Q}(\zeta_p)$. Show that $K = LF$ is unramified over F.

9.22 Assume that F/k is a normal extension, and let K be the Hilbert class field of F. Show that K/k is normal.
Hint: Any conjugate K' of K is also abelian and unramified over F. Now use the maximality property of the Hilbert class field.

9.23 Let L/K be an extension of number fields, and assume that L/K does not contain an unramified subextension. Show that the class number h_K of K divides h_L.
Hint: Let F be the Hilbert class field of K. Show that LF/L is abelian, unramified, and that $(LF : L) = h_K$.

9.24 Let $K = F(\sqrt{\mu}\,)$ be a quadratic extension, where $\mu \in F^\times$ is not a square. Show that K/F is unramified at all primes above 2 if $\mu \equiv \xi^2 \bmod 4$.
Hint: Show that $\frac{\xi+\sqrt{\mu}}{2}$ is an algebraic integer.

9.25 Let F be the cubic field generated by the positive root α of $f(x) = x^3+4ax-1$, where $a \ge 1$ is an integer. Show that $K = F(\sqrt{\alpha}\,)$ is unramified over F.
Hint: $F(\sqrt{\alpha}\,) = F(\sqrt{\alpha^3}\,)$. Observe that K/F could be trivial; in fact it is not too hard to show that α is a square in $\mathbb{Q}(\alpha)$ if and only if $a = t^4 - t$. Here's how to do it: the square roots of α are roots of $x^6 + 4ax^2 - 1$; if one square root is a root of $x^3 + rx^2 + sx + 1$, then the other is a root of $x^3 - rx^2 + sx - 1$. Thus $\sqrt{\alpha} \in \mathbb{Q}(\alpha)$ if and only if there exist integers r, s with

$$x^6 + 4ax^2 - 1 = (x^3 + rx^2 + sx + 1)(x^3 - rx^2 + sx - 1).$$

Now compare coefficients.

9.26 Let $K = F(\sqrt{m}\,)$ be a quadratic extension, where $m \in F^\times$ is not a square. Let $\mu = a + b\sqrt{m}$ be a nonsquare in K, put $L = K(\sqrt{\mu}\,)$, and let σ denote the nontrivial automorphism of K/F.

1. L/F is normal if and only if $\mu^\sigma = \alpha^2\mu$ for some $\alpha \in F^\times$.
2. Show that $\alpha^{1+\sigma} = \pm 1$.
3. Show that L/F is cyclic if $\alpha^{1+\sigma} = -1$. (Hint: show that the map $\tau : \sqrt{\mu} \longmapsto \alpha\sqrt{\mu}$ is an automorphism of L/F with $\tau^2|_K = \sigma$).
4. Show that L/F is biquadratic (i.e., $\mathrm{Gal}\,(L/F)$ is isomorphic to Klein's four group) if $\alpha^{1+\sigma} = +1$.

9.27 Construct the Hilbert class field in the strict sense of $F = \mathbb{Q}(\sqrt{34}\,)$.
Hints: The Hilbert class field is a quadratic extension of $K = \mathbb{Q}(\sqrt{2}, \sqrt{17}\,)$. Solve $x^2 - 2y^2 = 17$ and put $\mu = x + y\sqrt{2}$; show that the sign of x can be chosen in such a way that μ becomes a square modulo 4; now use the preceding exercise.

9.28 Let $p \equiv 1 \bmod 8$ be a prime and put $F = \mathbb{Q}(\sqrt{2p}\,)$. Construct a cyclic quartic extension L/F that is unramified outside infinity. By class field theory, this implies that $\mathrm{Cl}^+(F)$ has a class of order 4 – can you prove this directly?

9.29 Let F be a quadratic number field and K/F a quadratic extension unramified outside ∞. Show that $\mathrm{Gal}\,(K/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^2$. Now show that $K = F(\sqrt{d_i}\,)$ for some prime discriminant $d_i \mid \operatorname{disc} F$. Deduce that the maximal elementary abelian 2-extension of F unramified outside ∞ is finite.
Hint: First show that it is normal, and then that it cannot be cyclic (look at ramification!).

9.30 Let K/F be a finite extension of number fields. Let $j_{F\to K} : \mathrm{Cl}(F) \longrightarrow \mathrm{Cl}(K)$ be the "conorm" defined by sending $[\mathfrak{a}] \in \mathrm{Cl}(F)$ to $[\mathfrak{a}\mathfrak{O}_K] \in \mathrm{Cl}(K)$. Show that $N_{K/F} \circ j_{F\to K}$ is exponentiating with $(K : F)$. Deduce that if an ideal class $c \in \mathrm{Cl}(F)$ becomes trivial in K, then the order of c divides $(K : F)$.

9.31 Let K be a number field with r real embeddings $\sigma_1, \ldots, \sigma_r$. The signature map $\operatorname{sgn} : K^\times \longrightarrow \mu_2^t$, where $\mu_2 \simeq \mathbb{Z}/2\mathbb{Z}$ is the group $\{\pm 1\}$, is defined by

$$\operatorname{sgn}(\alpha) = (\operatorname{sign}(\sigma_1(\alpha)), \ldots \operatorname{sign}(\sigma_r(\alpha))).$$

Show that there is an exact sequence

$$\begin{tikzcd} K_+^\times \arrow[r] & K^\times \arrow[r, "\operatorname{sgn}"] & \mu_2^r \arrow[r] & 1 \end{tikzcd}$$

9.32 Show that the following diagram is commutative and exact:

$$\begin{tikzcd} 1 \arrow[r] & H_K^+ \arrow[r] \arrow[d] & D_K \arrow[r] \arrow[d] & \mathrm{Cl}^+(K) \arrow[r] \arrow[d] & 1 \\ 1 \arrow[r] & H_K \arrow[r] & D_K \arrow[r] & \mathrm{Cl}(K) \arrow[r] & 1 \end{tikzcd}$$

Apply the snake lemma and conclude that $\ker(\mathrm{Cl}^+(K) \longrightarrow \mathrm{Cl}(K)) \simeq H_K/H_K^+$.

9.33 Show that the following diagram is commutative and exact:

$$\begin{tikzcd} 1 \arrow[r] & E^+ \arrow[r] \arrow[d] & K_+^\times \arrow[r] \arrow[d] & H_K^+ \arrow[r] \arrow[d] & 1 \\ 1 \arrow[r] & E \arrow[r] & K^\times \arrow[r] & H_K \arrow[r] & 1 \end{tikzcd}$$

Apply the snake lemma and conclude that $(H_K : H_K^+) = \frac{(E:E^2)}{(E:E^+)} = (E^+ : E^2)$.

9.34 Show that the kernel of the natural projection $\mathrm{Cl}^+(K) \longrightarrow \mathrm{Cl}(K)$ is an elementary abelian group of order $(E^+ : E^2)$, where $E = \mathfrak{O}_K^\times$ is the unit group and E^+ its subgroup of totally positive units. Conclude that $\mathrm{Cl}^+(K) \simeq \mathrm{Cl}(K)$ if and only if every totally positive unit is a square.

9.35 For real quadratic number fields K, show that $\mathrm{Cl}^+(K) \simeq \mathrm{Cl}(K)$ if and only if $N\varepsilon = -1$ for the fundamental unit ε.

9.36 Let K/k be a normal extension and suppose that $\mathrm{Gal}(K/k)$ is an ℓ-group. If $\ell \mid h(K)$, show that there exists a cyclic unramified extension L/K of degree ℓ such that L/k is normal.

9.37 Let K be a totally real number field with nontrivial 2-class group, and assume that $E_K^+ = E_K^2$. Let $c_1, \ldots, c_r$ be a basis for $\mathrm{Cl}(K)[2]$, the group of ideal classes of order dividing 2, and let $\omega_1, \ldots, \omega_r$ denote the corresponding singular numbers, i.e. Kummer generators of the unramified quadratic extensions of K. Show that there exist prime ideals $\mathfrak{p}_i$ of odd norm in c_i such that every unit in E_K is a quadratic residue modulo $\mathfrak{p}$. Then pick another prime ideal $\mathfrak{p}_0$ of odd norm such that $\mathfrak{p}_0\mathfrak{p}_1 \cdots \mathfrak{p}_r = (\alpha)$ is principal with $\alpha \equiv \xi^2 \bmod 4$ primary. Show that

1. $\kappa_{L/K} = 1$;
2. $E_L^+ = E_L^2$;
3. the transfer $j_{K \to L}$ maps $\mathrm{Cl}(K)[2]$ into $\mathrm{Cl}(L)^2$;
4. $\operatorname{rank} \mathrm{Cl}_2(L) = \operatorname{rank} \mathrm{Cl}_2(K)$.

9.38 Recall that an exact sequence

$$E: 1 \longrightarrow A \longrightarrow \Gamma \longrightarrow G \longrightarrow 1$$

of finite groups is called an *extension* of G by A. The extension E is called *central* if $A \subseteq Z(\Gamma)$ is contained in the center of Γ (where we have identified A and its image in Γ). A normal tower $L/K/k$ of fields is called central if the exact sequence

$$1 \longrightarrow \operatorname{Gal}(L/K) \longrightarrow \operatorname{Gal}(L/k) \longrightarrow \operatorname{Gal}(K/k) \longrightarrow 1$$

corresponding to the tower is central.
Now prove Hasse's normality criterion: Let K/k be a normal extension with $G = \operatorname{Gal}(K/k)$, and let L be an unramified abelian extension of K. Put $C = N_{L/K}\operatorname{Cl}(L)$; then L is

a) normal over k if and only if $C = C^\tau$ for every $\tau \in G$;

b) central over K/k if and only if $c^{\tau-1} \in C$ for all $c \in \operatorname{Cl}(K)$ and all $\tau \in G$.

Observe that central extensions of cyclic groups are abelian and give a criterion for L/k to be abelian if K/k is cyclic.

9.39 (Artin) Let K/k be an extension such that $K \cap k^1 = k$, where k^1 is the Hilbert class field of k. Show that $h(k) \mid h(K)$.

10. The First Inequality

In this chapter we will study unramified cyclic extensions L/K. To each such extension we associate its Takagi group

$$T_{L/K} = ND_L \cdot H_K,$$

the subgroup of nonzero fractional ideals in D_K that can be written as a product of a norm of an ideal from L and a principal ideal. Since $D_K \subseteq T_{L/K} \subseteq H_K$, the index

$$h_{L/K} = (D_K : T_{L/K})$$

is finite (it divides the class number $h = h_K$). Our goal is to prove that $h_{L/K} = (L : K)$; this will be accomplished in two steps:

- The First Inequality: $h_{L/K} \leq (L : K)$ holds for arbitrary extensions L/K of number fields.
- The Second Inequality: $(L : K) \leq h_{L/K}$ holds for cyclic unramified extensions L/K.

We call L a class field of K (in the sense of Hilbert) if $h_{L/K} = (L : K)$; the inequalities above then show that cyclic unramified extensions are class fields. We will later see that the maximal unramified abelian extension of K is the Hilbert class field of K in the sense of the preceding chapter.

10.1 Weber's Inequality

Fix an extension L/K of number fields. In the following, we put $h = h_{L/K}$; the class number of K will be denoted by h_K.

The First Inequality is a consequence of Kronecker's density theorem and the following

Theorem 10.1 (Weber's Inequality)**.** *Let S be a set of prime ideals with $S \subset T_{L/K}$. If S has a Dirichlet density, then $\delta(S) \leq \frac{1}{h}$.*

Let χ be a character on the finite abelian group D/H, where $D = D_K$ denotes the group of fractional ideals in K and where $H = T_{L/K}$ is the Takagi group. We can interpret χ as a character $\chi : D \longrightarrow \mathbb{C}^1$ via $\chi(\mathfrak{a}) = \chi(\mathfrak{a}H)$.

For L-functions attached to Dirichlet characters χ we have already seen that $L(s,\chi)$ converges for $s=1$ and $\chi \neq 1\!\!1$; the reason was that the partial sums $\sum_{0<a\le m}\chi(a)$ of the coefficients of $L(s,\chi)$ were bounded for nontrivial characters. Here the situation is not that easy: the partial sums of the coefficients $L(s,\chi)=\sum \chi(\mathfrak{a})N\mathfrak{a}^{-1}$ have the form $\sum_{N\mathfrak{a}\le m}\chi(\mathfrak{a})$. Before we can talk about $L(1,\chi)$ for characters $\chi \neq 1\!\!1$ on D/H we therefore have to prove

Lemma 10.2. *For every character $\chi \neq 1\!\!1$ on D/H, the function $L(s,\chi)$ is bounded as $s \to 1$.*

Proof. We use the orthogonality relations:

$$L(s,\chi)=\sum_{\mathfrak{a}}\chi(\mathfrak{a})N\mathfrak{a}^{-s}=\sum_{c\in \mathrm{Cl}(K)}\sum_{\mathfrak{a}\in c}\chi(\mathfrak{a})N\mathfrak{a}^{-s}=\sum_{c\in \mathrm{Cl}(K)}\chi(c)\zeta_c(s),$$

where we have used that $\chi(\mathfrak{a})$ only depends on the the coset $\mathfrak{a}H$, and where $\zeta_c(s)$ is the partial zeta function associated to $c \in D/H$. The cosets of D/H are unions of ideal classes in $\mathrm{Cl}(K)$ (each coset in D/H consists of $h_0=(H:H_K)$ ordinary ideal classes), hence their partial zeta functions $\zeta_c(s)$ have a pole of order 1 at $s=1$ with residue $h_0\kappa$, and can be extended meromorphically to the half plane $\mathrm{Re}\, s>1-\frac{1}{n}$. In fact, we have $\lim_{s\to 1}(s-1)L(s,\chi)=h_0\kappa\sum_c \chi(c)$; but the orthogonality relations say that this sum is 0 except for $\chi=1\!\!1$, when it equals $h=(D:H)$. Thus $\lim_{s\to 1}(s-1)L(s,\chi)=0$ if $\chi\neq 1\!\!1$, and this implies that $L(s,\chi)$ does not have a pole at $s=1$, i.e., that it is bounded as $s\to 1$. □

Actually, we have proved the following stronger result:

Lemma 10.3. *For any character $\chi\neq 1\!\!1$ on D/H, we have $\sum_{N\mathfrak{a}\le m}\chi(\mathfrak{a})=O(n^{1-\frac{1}{n}})$, where $n=(K:\mathbb{Q})$. In particular, $L(s,\chi)$ is analytic for all $s\in\mathbb{C}$ with* $\mathrm{Re}\, s>1-\frac{1}{n}$.

Proof of Thm. 10.1. Since χ is multiplicative, the Dirichlet series $L(s,\chi)=\sum\chi(\mathfrak{a})N\mathfrak{a}^{-s}$ has an Euler factorization, and taking logs we find in the usual way

$$\log L(s,\chi)\sim\sum\chi(\mathfrak{p})N\mathfrak{p}^{-s},$$

where $f\sim g$ means $f(s)=g(s)+O(1)$ as $s\to 1$.

The orthogonality relations for characters show that

$$\sum_{\chi\in X(D/H)}\chi(\mathfrak{p})=\begin{cases} h & \text{if } \mathfrak{p}\in H,\\ 0 & \text{if } \mathfrak{p}\notin H.\end{cases}$$

For $s>1$ we get

$$\sum_{\chi}\sum_{\mathfrak{p}}\chi(\mathfrak{p})N\mathfrak{p}^{-s}=h\sum_{\mathfrak{p}\in H}N\mathfrak{p}^{-s},$$

and the finiteness of the class number allows us to conclude that

$$\sum_{\chi} \log L(s,\chi) \sim h \sum_{\mathfrak{p}\in H} N\mathfrak{p}^{-s}.$$

We know that L-series attached to the principal character $\mathbb{1}$ behave differently at $s = 1$, so we split the sum on the left:

$$\begin{aligned} h \sum_{\mathfrak{p}\in H} N\mathfrak{p}^{-s} &= \sum_{\chi\neq 1} \log L(s,\chi) + \log L(s,\, \mathbb{1}) \\ &= \sum_{\chi\neq 1} \log L(s,\chi) + \log(s-1)L(s,\, \mathbb{1}) - \log(s-1). \end{aligned}$$

On the other hand the assumption that S has a Dirichlet density implies

$$\sum_{\mathfrak{p}\in S} N\mathfrak{p}^{-s} \sim -\delta(S)\log(s-1).$$

Moreover, since $S \subset H$, the function

$$f(s) = \sum_{\mathfrak{p}\in H} N\mathfrak{p}^{-s} - \sum_{\mathfrak{p}\in S} N\mathfrak{p}^{-s}$$

satisfies $f(s) \geq 0$ for all $s > 1$. We find

$$\begin{aligned} f(s) &\sim \frac{1}{h}\Big(\sum_{\chi\neq 1} \log L(s,\chi) + \log(s-1)L(s,\, \mathbb{1}) - \log(s-1)\Big) - \delta(S)\log(s-1) \\ &\sim -\Big(\frac{1}{h} - \delta(S)\Big)\log(s-1) + \frac{1}{h}\sum_{\chi\neq 1} \log L(s,\chi) + \frac{1}{h}\log(s-1)L(s,\, \mathbb{1}). \end{aligned}$$

Since $L(s,\, \mathbb{1}) = \zeta_K(s)$, the term $\log(s-1)L(s,\, \mathbb{1})$ is bounded as $s \to 1$, hence

$$f(s) \sim -\Big(\frac{1}{h} - \delta(S)\Big)\log(s-1) + \frac{1}{h}\sum_{\chi\neq 1} \log L(s,\chi).$$

Now assume for the moment that $L(1,\chi) \neq 0$ for all $\chi \neq 1$ (which is true, but out of reach for us at the moment): then $\log L(s,\chi)$ is bounded as $s \to 1$, and from

$$h \sum_{\mathfrak{p}\in H} N\mathfrak{p}^{-s} = \sum_{\chi\neq 1} \log L(s,\chi) + \log(s-1)L(s,\, \mathbb{1}) - \log(s-1)$$

we can deduce that the set of primes in H has density $\frac{1}{h}$, which immediately implies that $\delta(S) \leq \frac{1}{h}$ for any set of primes contained in H that has a Dirichlet density.

What if $L(1,\chi) = 0$ for some $\chi \neq \mathbb{1}$? In such a case, the term $\log L(s,\chi) \to -\infty$ as $s \to 1$. Since $f(s) \geq 0$ for $s > 1$, such terms must be cancelled by the first term; since $-\log(s-1) \to \infty$, this implies that we must have $\frac{1}{h} - \delta(S) > 0$ in such a case. □

Our proof implies the following

Corollary 10.4. *If $\delta(S) = \frac{1}{h}$ for $S = \mathrm{Spl}(L/K)$, then $L(1,\chi) \neq 0$ for all characters $\chi \neq 1$ of the class group $\mathrm{Cl}(K)$.*

10.2 Proof of the First Inequality

We now prove the First Inequality for normal unramified extensions:

Theorem 10.5 (First Inequality)**.** *Let L/K be a normal unramified extension with associated Takagi group $T_{L/K} = ND_L \cdot H_K$. Then*

$$h = (D_K : T_{L/K}) \leq (L : K) = n.$$

Proof. The set $S = \mathrm{Spl}(L/K)$ is contained in $N_{L/K}D_L$ since primes that split completely in L/K are norms of (prime) ideals from L. Since $\delta(S) = \frac{1}{(L:K)}$ by Kronecker's density theorem, Weber's inequality tells us that $\frac{1}{(L:K)} \leq \frac{1}{h}$, where $h = (D_K : H) = \#\,\mathrm{Cl}(K)$ is the class number of K. Clearing fractions then gives $h \leq (L : K)$. □

Scholz's Version

Scholz discovered that one may drop the assumption that L/K be normal:

Theorem 10.6. *Let L/K be a nonnormal extension with associated Takagi group $T_{L/K} = ND_L \cdot H_K$. Then*

$$h = (D_K : T_{L/K}) < (L : K) = n.$$

Proof. Let $n = (L : K)$, and denote by n^* the degree of the normal closure of L/K. We know

$$\sum N\mathfrak{P}^{-s} = \log \frac{1}{s-1} + O(1),$$

where the sum is over all prime ideals of degree 1 in L. For prime ideals $\mathfrak{p}$ of degree 1 in K, let $n(\mathfrak{p})$ denote the number of prime ideals $\mathfrak{P}$ in L of degree 1 over K; then

$$\sum_{\mathfrak{P}} N\mathfrak{P}^{-s} = \sum_{\mathfrak{p}} \frac{n(\mathfrak{p})}{N\mathfrak{p}^s} + O(1),$$

where the $\mathfrak{p}$ run through the unramified prime ideals of degree 1 in K. Now denote by $\mathfrak{p}^*$ those $\mathfrak{p}$ with $n(\mathfrak{p}) = n$, and by $\mathfrak{p}'$ those $\mathfrak{p}$ with $n(\mathfrak{p}) \leq n-1$ (actually this implies $n(\mathfrak{p}) \leq n-2$ since if there are $n-1$ prime ideals of degree 1 above $\mathfrak{p}$, then there are n of them). Then

$$\begin{aligned}\sum_{\mathfrak{P}} N\mathfrak{P}^{-s} &\le n\sum_{\mathfrak{p}^*}(N\mathfrak{p}^*)^{-s} + (n-1)\sum_{\mathfrak{p}'}(N\mathfrak{p}')^{-s} + O(1)\\ &= \sum_{\mathfrak{p}^*}(N\mathfrak{p}^*)^{-s} + (n-1)\sum_{\mathfrak{p}} N\mathfrak{p}^{-s} + O(1).\end{aligned}$$

Thus we find

$$\sum_{\mathfrak{p}} N\mathfrak{p}^{-s} \ge \frac{1}{n-1}\log\frac{1}{s-1} - \frac{1}{n-1}\sum_{\mathfrak{p}^*}(N\mathfrak{p}^*)^{-s} + O(1).$$

Since prime ideals $\mathfrak{p}$ split completely in L/K if and only if they split completely in the normal closure N/K, the set of prime ideals $\mathfrak{p}^*$ has Dirichlet density $\frac{1}{n^*}$, and we find

$$\sum_{\mathfrak{p}} N\mathfrak{p}^{-s} \ge \frac{n^*-1}{n^*}\frac{1}{n-1}\log\frac{1}{s-1} + O(1).$$

Since L/K is not normal, we have $n^* > n$, hence $\frac{n^*-1}{n^*} = 1-\frac{1}{n^*} > 1-\frac{1}{n} = \frac{n-1}{n}$ and thus $\frac{n^*-1}{n^*}\frac{1}{n-1} > \frac{1}{n}$.

The same argument as in the normal case now shows that $h < n$. □

Thus if L/K is not normal, then L is not a class field:

Corollary 10.7. *Class Fields are normal extensions.*

Artin's Version

Let L/K be an extension of degree n. Let $H \subseteq D_K$ be a group of ideals containing H_K and the norms ND_L from L. Let χ run through the characters of the class group D_K/H; Artin compares the zeta function $\zeta_L(s)$ with the product of the L-series $L(s,\chi)$. Taking logarithms he finds

$$\log\zeta_L(s) = \sum_{\mathfrak{P}} N\mathfrak{P}^{-s} + O(1),$$

where $\mathfrak{P}$ runs through the prime ideals of degree 1 in L. Let $\mathfrak{p} = \mathfrak{P}\cap K$ denote the prime ideal below $\mathfrak{P}$, and let $n(\mathfrak{p})$ denote the number of prime ideals of degree 1 in L above $\mathfrak{p}$. Then

$$\log\zeta_L(s) = \sum_{\mathfrak{p}} n(\mathfrak{p})N\mathfrak{p}^{-s} + O(1).$$

Since prime ideals $\mathfrak{p}$ with $n(\mathfrak{p}) > 0$ are exactly the prime ideals that can be written as norms from L, and since $D_L \subset H$, we find

$$\log\zeta_L(s) = \sum_{\mathfrak{p}\in H} n(\mathfrak{p})N\mathfrak{p}^{-s} + O(1).$$

On the other hand we know

$$\sum_\chi L(s,\chi) = h \sum_{\mathfrak{p}\in H} N\mathfrak{p}^{-s} + O(1).$$

Since $n(\mathfrak{p}) \le n$, we find

$$\log \zeta_L(s) \lesssim n \sum_{\mathfrak{p}\in H} N\mathfrak{p}^{-s} \sim \frac{n}{h} \sum_\chi \log L(s,\chi),$$

where $f \lesssim g$ means that $f(s) - g(s) \le c$ for some constant c as $s \to 1$.

In the product $\prod_\chi L(s,\chi)$, the factor $L(s, \mathbb{1})$ has a pole of order 1 at $s = 1$. If $L(1,\chi) = 0$ for at least one of the $\chi \ne 1$, this zero will cancel against the pole, and the product would be bounded at $s = 1$. This would imply that $\sum_\chi \log L(s,\chi)$ is bounded from above (it could go to $-\infty$ if the product would vanish). But since we know that $\log \zeta(s) \longrightarrow \infty$ as $s \to 1$, this is impossible, and we deduce that $L(1,\chi) \ne 0$ for $\chi \ne 1$. Dirichlet's proof then immediately implies

Theorem 10.8. *Let L/K be an extension of number fields and H an ideal group containing $T_{L/K} = ND_L \cdot H_K$. Then $L(1,\chi) \ne 0$ for all characters $\chi \ne 1$ of D_K/H, and the set S of prime ideals in an ideal class $c \in D_K/H$ has Dirichlet density $\delta(S) = \frac{1}{h}$, where $h = (D_K : H)$.*

In order to show that there are infinitely many prime ideals in the principal class of $\mathrm{Cl}(K)$, we still have to find a number field L such that $ND_L \subseteq H_K$, that is, a field in which only the principal prime ideals split.

Back to Artin's proof of the first inequality: from

$$\log \zeta_L(s) \lesssim \frac{n}{h} \sum_\chi \log L(s,\chi) \sim \frac{n}{h} \log \zeta_K(s)$$

and the fact that $\log \zeta_F(s) \sim \frac{1}{s-1}$ for any number field n we deduce that $1 \le \frac{n}{h}$, i.e., $h \le n$.

10.3 Consequences of the First Inequality

Let us now call an extension L/K a class field for the ideal group H if

- H contains $T_{L/K}$;
- $(D_K : H) = n$.

The following proposition will allow us to go back and forth between the two definitions of a class field given by Takagi and Weber.

Proposition 10.9. *Let L/K be a normal unramified extension and let H be an ideal group containing the Takagi group $T_{L/K} = ND_L \cdot H_K$ attached to L/K. Then the following conditions are equivalent:*

1. *Except possibly for a set of density* 0*, exactly the prime ideals in* H *split completely in* L/K*.*
2. *Except possibly for a set of density* 0*, all prime ideals in* H *split completely in* L/K*.*
3. $(D_K : H) \geq (L : K)$.
4. $(D_K : H) = (L : K)$.

Proof. Clearly (1) $\Longrightarrow$ (2). The converse follows by observing that prime ideals outside of H cannot split completely (all the norms of ideals are contained in H). Moreover, (3) and (4) are equivalent by the first inequality.

It remains to show that (2) $\Longrightarrow$ (4) and (4) $\Longrightarrow$ (2). Assume (2) holds. Then $n(\mathfrak{p}) = n$ for almost all prime ideals in H, hence $n = h$. Now assume that $n = h$; then $n(\mathfrak{p}) = n$ for almost all $\mathfrak{p} \in H$. □

Thus we find that L/K is a class field for the ideal group H if H contains $T_{L/K}$, and if almost all of the prime ideals in H split completely on L/K. We will use this alternative definition of a class field repeatedly in the proofs below.

Let us first make the following simple observation:

Lemma 10.10. *If* L/K *is a class field for the ideal group* H*, then* $H = T_{L/K}$*.*

Thus for every class field there is a unique class group H. The Uniqueness Theorem states the converse, namely that if L/K and L'/K are both class fields for H, then $L = L'$.

Proof. By definition, we have $T_{L/K} \subseteq H$. Since L/K is a class field, we know $(D : H) = (L : K)$. Now

$$(L : K) = (D : H) = \frac{(D : T_{L/K})}{(H : T_{L/K})} \leq \frac{(L : K)}{(H : T_{L/K})},$$

where we have used the first inequality. This implies $(H : T_{L/K}) = 1$, and now the claim follows. □

Scholz observed in 1927 that the following result can be proved using only the first inequality:

Theorem 10.11. *Assume that* L/K *is a class field for* $T_{L/K}$*, and let* F *be an intermediate field. Then both* L/F *and* F/K *are class fields. In particular, every intermediate field of a class field is normal; equivalently: if* L/K *is a class field, then every subgroup of* $\operatorname{Gal}(L/K)$ *is normal.*

This almost shows that class fields are abelian. A prominent example of a nonabelian group all of whose subgroups are normal is the quaternion group of order 8.

Proof. We will consider the three groups $T_{L/K}$, $T_{L/F}$, $T_{F/K}$, as well as $H = \{\mathfrak{b} \in D_F : N^F_K\mathfrak{b} \in T_{L/K}$. Clearly $N^L_K D_L \subseteq N^F_K D_F$, hence $T_{L/K} \subseteq T_{F/K}$. Moreover, $T_{L/F} \subseteq H$ since taking the norm N^F_K of $T_{L/F} = N^L_F D_L H_F$ gives an ideal in $T_{L/K}$.

Observe that the norm map N^F_K induces an epimorphism $D_F \longrightarrow T_{F/K}/T_{L/K}$: given an ideal $\mathfrak{b}(\alpha) \in T_{F/K}$, where $\mathfrak{b} \in N^F_K D_F$, we observe that it generates the same coset modulo $T_{L/K}$ as $\mathfrak{b}$ since $H_K \subseteq T_{L/K}$. The kernel of $N^F_K : D_F \longrightarrow T_{F/K}/T_{L/K}$ consists of all ideals in D_F whose norms land in $T_{L/K}$, and this is by definition H. Thus $D_F/H \simeq T_{F/K}/T_{L/K}$.

Now we have

$$(D_F : T_{L/F}) \geq (D_F : H) = (T_{F/K} : T_{L/K}) = \frac{(D_K : T_{L/K})}{(D_K : T_{F/K})},$$

hence

$$(D_K : T_{F/K})(D_F : T_{L/F}) \geq (D_K : T_{L/K}) = (L : K)$$

since L/K is a class field. By the first inequality, the two indices on the left hand side are $\leq (F : K)(L : F) = (L : K)$. This can only happen if we have equality everywhere, hence $(D_K : T_{F/K}) = (F : K)$ and $(D_F : T_{L/F}) = (L : F)$. This implies that L/F and F/K are class fields. □

The next result shows that composita of class fields are class fields:

Theorem 10.12 (Composition Theorem). *If L_1/K and L_2/K are class fields for the ideal groups H_1 and H_2, then the compositum $L = L_1L_2$ is a class field for the ideal group $H_1 \cap H_2$.*

Proof. Every norm of an ideal from L is also a norm from both L_1 and L_2, hence $T_{L/K} \subseteq H_1 \cap H_2$. On the other hand, every prime ideal in $H_1 \cap H_2$ splits completely in L_1/K and L_2/K, hence in the compositum L/K. Thus $(D_K : T_{L/K}) \leq (L : K)$ □

Next we prove the

Theorem 10.13 (Ordering Theorem). *Let L_1/K and L_2/K be class fields for the class groups H_1 and H_2, respectively. Then $L_1 \subseteq L_2$ if and only if $H_1 \supseteq H_2$.*

Proof. Assume first that $L_1 \subseteq L_2$. On the one hand, L_2 is the class field to H_2; on the other hand, $L_2 = L_1L_2$ is the class field corresponding to the intersection $H_1 \cap H_2$. Thus $H_2 = H_1 \cap H_2$, hence $H_2 \subseteq H_1$.

Now assume that $H_2 \subseteq H_1$. Then $H_2 = H_1 \cap H_2$, hence the compositum L_1L_2 is a class field with respect to H_2, and we get $(L_1L_2 : K) = (D_K : H_2) = (L_2 : K)$. But this implies $L_1 \subseteq L_2$. □

Corollary 10.14 (Uniqueness Theorem). *For every ideal group H there is at most one class field.*

Corollary 10.15. *Class fields are normal.*

Proof. The Takagi groups attached to L/K and its conjugate L'/K are the same. Thus $L = L'$. □

Scholz gave the following simple proof of the

Theorem 10.16 (Translation Theorem)**.** *Let L/K be a class field with respect to H, and let F/K be a finite extension. Then LF/F is a class field with respect to the group $\overline{H} = \{\mathfrak{A} \in D_F : N_{F/K}\mathfrak{A} \in H\}$.*

Proof. We first have to show that the group $\overline{H}$ contains the Takagi group $T_{LF/F}$. But $N_F^{LF} D_{LF} H_F \in \overline{H}$ since $N_K^F(N_F^{LF} D_{LF} H_F) = N_K^L N_F^{LF} D_L N_K^F H_F \subseteq N_K^L D_L H_K = T_{L/K}$.

The second condition we have to check is that almost all primes in $\overline{H}$ split in LF/F. Since primes of degree > 1 have density 0, we only need consider prime ideals $\mathfrak{q}$ in F of degree 1. Then $\mathfrak{p} = N_K^F \mathfrak{q} \in H$, and since L/K is a class field for H, $\mathfrak{p}$ splits completely in L/K. But $\mathfrak{p}$ also splits completely in F/K, hence in the compositum LF. But then $\mathfrak{q}$ must split completely in LF/F, and this concludes the proof. □

Corollary 10.17. *If L/K is a class field and F is an intermediate extension, then both L/F and F/K are class fields.*

What is missing from the theory are the Existence Theorem (there is a class field for every ideal group H), the Decomposition Law (we know that almost all prime ideals in H split in the corresponding class field; note that "almost all" excludes all prime ideals of degree > 2, so this is really quite a weak result. The Decomposition Law states that *all* prime ideals in H without exception split completely in the class field attached to H), and Artin's Reciprocity Law, which, in all modern accounts, is used to prove both the Existence Theorem and the Decomposition Law.

As a consequence of the Existence Theorem and our results so far we give Scholz's proof of the

Theorem 10.18 (Norm Limitation Theorem)**.** *Let F/K be an extension of number fields, and assume that L/K is the maximal abelian subextension of F/K. Then $T_{F/K} = T_{L/K}$.*

Proof. □

Exercises

10.1 Show directly from the definition that conjugate field extensions L/K and L'/K have the same Takagi groups. Use the ordering theorem to deduce that class fields are normal.

11. The Second Inequality

In this chapter we will prove the Second Inequality.

11.1 Preliminaries

The proof of the Second Inequality requires a few lemmas from Galois cohomology and group theory. While some of them are almost trivial, others – in particular the snake lemma and Herbrand's lemma – are less simple but quite powerful.

Lemma 11.1. *If $A \supseteq B \supseteq C$ are abelian groups, then*

$$(A : C) = (A : B)(B : C).$$

Proof. This is a consequence of the exact sequence

$$1 \longrightarrow B/C \longrightarrow A/C \longrightarrow A/B \longrightarrow 1,$$

where the map $A/C \longrightarrow A/B$ sends aC to aB. This map is clearly surjective with kernel B/C. □

We will only apply this result when the index on the left or the two indices on the right are finite.

Lemma 11.2. *For subgroups A, B of an abelian group we have*

$$AB/B \simeq A/A \cap B.$$

Proof. The map sending $a \in A$ to the coset $aB \in AB/B$ is an epimorphism with kernel $A \cap B$. □

The work horse in homological algebra is the elementary but important

Lemma 11.3 (Snake Lemma)**.** *Given an exact and commuting diagram*

$$\begin{tikzcd}
 & A \arrow[r, "f"] \arrow[d, "\alpha"'] & B \arrow[r, "g"] \arrow[d, "\beta"'] & C \arrow[r] \arrow[d, "\gamma"'] & 1 \\
1 \arrow[r] & A' \arrow[r, "f'"] & B' \arrow[r, "g'"] & C' &
\end{tikzcd}$$

of abelian groups, there is an exact sequence

$$\begin{tikzcd}
1 \arrow[r] & \ker f \arrow[r] & \ker\alpha \arrow[r] & \ker\beta \arrow[r] & \ker\gamma \arrow[d, "\delta"'] \\
1 & \operatorname{coker} g' \arrow[l] & \operatorname{coker}\gamma \arrow[l] & \operatorname{coker}\beta \arrow[l] & \operatorname{coker}\alpha \arrow[l]
\end{tikzcd}$$

You can find the proof in almost any text book on homological algebra, along with the comment that it is best to prove it for yourself.

Next there is the simple but effective

Lemma 11.4. *Let $f : A \longrightarrow G$ be a homomorphism between abelian groups. Let B be a subgroup of A, and let g be the restriction of f to B. Set $A_f = \ker f$, $B_f = \ker g$, $A^f = \operatorname{im} f$ and $B^f = \operatorname{im} g$. Then*

$$(A : B) = (A^f : B^f)(A_f : B_f).$$

If $A_f \subseteq B$, then $(A_f : B_f) = 1$.

Proof. Apply the snake lemma to the diagram

$$\begin{tikzcd}
0 \arrow[r] & B_f \arrow[r] \arrow[d] & B \arrow[r] \arrow[d] & B^f \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A_f \arrow[r] & A \arrow[r] & A^f \arrow[r] & 0;
\end{tikzcd}$$

since the vertical maps are injective, we get the exact sequence

$$0 \longrightarrow A_f/B_f \longrightarrow A/B \longrightarrow A^f/B^f \longrightarrow 0$$

of cokernels, from which the claim follows by forming the alternating product of the orders of these groups. □

Of course we can easily prove this result directly; it is, however, important to see the snake lemma in action.

Another useful consequence of the snake lemma is

Lemma 11.5. *Given two homomorphisms $\alpha : A \longrightarrow B$ and $\beta : B \longrightarrow C$ of abelian groups, the sequence*

$$\begin{tikzcd}
1 \arrow[r] & \ker\alpha \arrow[r] & \ker(\beta\circ\alpha) \arrow[r] & \ker\beta \arrow[d] \\
1 & \operatorname{coker}\beta \arrow[l] & \operatorname{coker}(\beta\circ\alpha) \arrow[l] & \operatorname{coker}\alpha \arrow[l]
\end{tikzcd}$$

is exact.

Proof. Apply the snake lemma to the diagram

$$\begin{tikzcd}
 & A \arrow[r, "\alpha"] \arrow[d, "\beta\circ\alpha"] & B \arrow[r] \arrow[d, "\beta"] & \operatorname{coker}\alpha \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & C \arrow[r, "\mathrm{id}"] & C \arrow[r] & 1 &
\end{tikzcd}$$

□

Finally, let us discuss Herbrand's Lemma. There are various versions of this result; we will only prove the special case we need, and indicate the connection to Galois cohomology at the end of this chapter.

Let $f, g : A \longrightarrow A$ be endomorphisms of an abelian group A with the property that $f \circ g = 0$ and $g \circ f = 0$. This implies that $\operatorname{im} f \subseteq \ker g$ and $\operatorname{im} g \subseteq \ker g$, so we can define the Herbrand quotient

$$q(A) = \frac{(\ker f : \operatorname{im} g)}{(\ker g : \operatorname{im} f)} = \frac{(A_f : A^g)}{(A_g : A^f)}.$$

This quotient depends on the order of f and g and thus should be denoted more precisely by $q_{f,g}(A)$; clearly $q_{f,g}(A) = 1/q_{g,f}(A)$.

We now observe

Lemma 11.6. *If A is a finite group, then $q(A) = 1$.*

Proof. If A is finite, then

$$q(A) = \frac{(\ker f : \operatorname{im} g)}{(\ker g : \operatorname{im} f)} = \frac{\#\ker f \cdot \#\operatorname{im} f}{\#\operatorname{im} g \cdot \#\ker g} = \frac{\#A}{\#A} = 1.$$

□

The special case of Herbrand's Lemma that we will use is

Lemma 11.7 (Herbrand's Lemma)**.** *If $f, g : A \longrightarrow A$ are as above, and if B is a subgroup of finite index in A, then $q(A) = q(B)$.*

Proof. We find

$$\begin{aligned}
(A : B) &= (A^f : B^f)(A_f : B_f) && \text{by Lemma 11.4} \\
&= (A^f : B^f)\frac{(A_f : B^g)}{(B_f : B^g)} && \text{by Lemma 11.1} \\
&= (A^f : B^f)\frac{(A_f : A^g)(A^g : B^g)}{(B_f : B^g)} && \text{by Lemma 11.1} \\
&= \frac{(A_f : A^g)}{(B_f : B^g)}(A^f : B^f)(A^g : B^g).
\end{aligned}$$

By symmetry, we also get

$$(A : B) = \frac{(A_g : A^f)}{(B_g : B^f)}(A^f : B^f)(A^g : B^g),$$

and comparing these two equations we see that

$$\frac{(A_f : A^g)}{(B_f : B^g)} = \frac{(A_g : A^f)}{(B_g : B^f)},$$

which immediately implies the claim. □

11.2 The Second Inequality for Unramified Extensions

Let L/K be a cyclic unramified extension. Our goal in this section is to investigate the index

$$h_{L/K} = (D_K : ND_L \cdot H_K).$$

Clearly

$$h_{L/K} = \frac{(D_K : H_K)}{(ND_L \cdot H_K : H_K)}.$$

The index in the numerator is the class number h of K. Applying $(AB : B) = (A : A \cap B)$ to the index in the denominator we see

$$(ND_L \cdot H_K : H_K) = (ND_L : ND_L \cap H_K).$$

Now consider the norm map from $A = D_L$ to D_K, as well as its restriction to the subgroup G_L of D_L consisting of ideals with principal norm. Lemma 11.4 shows that

$$(D_L : G_L) = (ND_L : ND_L \cap H_K).$$

We remark in passing that $(D_L : G_L) = (D_L/H_L : G_L/H_L)$; clearly $D_L/H_L = \mathrm{Cl}_L$, and $G_L/H_L = \mathrm{Cl}_L[N]$ is the group of ideal classes whose norm down to K is principal. Thus $(D_L/H_L : G_L/H_L) = (\mathrm{Cl}_L : \mathrm{Cl}_L[N]) = N\,\mathrm{Cl}_L$, hence

$$h_{L/K} = (\mathrm{Cl}_K : N\,\mathrm{Cl}_L). \tag{11.1}$$

Now let σ be a generator of the cyclic group $\mathrm{Gal}\,(L/K)$. Then G_L contains the group $D_L^{1-\sigma}H_L$, hence

$$(D_L : G_L) = \frac{(D_L : D_L^{1-\sigma}H_L)}{(G_L : D_L^{1-\sigma}H_L)}.$$

Let $\mathrm{Am}\,(L/K) = \{c \in \mathrm{Cl}(L) : c^\sigma = c\}$ denote the group of ambiguous ideal classes in L. Its definition provides us with the exact sequence

$$1 \longrightarrow \mathrm{Am}\,(L/K) \longrightarrow \mathrm{Cl}_L \longrightarrow \mathrm{Cl}_L^{1-\sigma} \longrightarrow 1,$$

which in turn gives

$$(\mathrm{Cl}_L : \mathrm{Cl}_L^{1-\sigma}) = \#\,\mathrm{Am}\,(L/K).$$

Now

$$(\mathrm{Cl}_L : \mathrm{Cl}_L^{1-\sigma}) = (D_L/H_L : D_L^{1-\sigma}H_L/H_L) = (D_L : D_L^{1-\sigma}H_L).$$

Combining everything so far we find

$$h_{L/K} = \frac{h_K(G_L : D_L^{1-\sigma}H_L)}{\#\,\mathrm{Am}\,(L/K)}. \tag{11.2}$$

Now we claim

Theorem 11.8 (Ambiguous Ideal Class Formula)**.** *Let L/K be a cyclic unramified extension. Then*

$$\#\,\mathrm{Am}\,(L/K) = \frac{h_K}{(L:K)(E_K : E_K \cap NL^\times)}.$$

Plugging this into (11.2) we find

$$h_{L/K} = (L:K)(E_K : E_K \cap NL^\times)(G_L : D_L^{1-\sigma}H_L).$$

The first inequality, on the other hand, shows that $h_{L/K} \le (L:K)$. Thus we must have equality, and we have proved that every unramified cyclic extension L/K is a class field. Since abelian groups are direct products of cyclic groups, and since we already know that composita of class fields are class fields, we find

Theorem 11.9. *Every unramified abelian extension L/K is a class field.*

Next we claim

Theorem 11.10. *Let L/K be a cyclic unramified extension. Then*

$$(\mathrm{Cl}_K : N\,\mathrm{Cl}_L) = (L:K).$$

In particular, $(L:K) \mid h_K$.

Theorem 11.11 (Furtwängler's Principal Genus Theorem)**.** *Let L/K be a cyclic unramified extension, and let σ be a generator of* $\mathrm{Gal}\,(L/K)$*. Then*

$$\mathrm{Cl}_L[N] = \mathrm{Cl}_L^{1-\sigma}.$$

Proof. The first and second inequalities imply $G_L = D_L^{1-\sigma}H_L$, that is, $\mathrm{Cl}_L[N] = G_L/H_L = D_L^{1-\sigma}H_L/H_L = \mathrm{Cl}_L^{1-\sigma}$. □

The fundamental inequalities also show that the index $(E_K : E_K \cap NL^\times)$ is trivial, so we get

Theorem 11.12. *Let L/K be a cyclic unramified extension. Then every unit $\varepsilon \in E_K$ is the norm of an element from L:*

$$E_K = E_K \cap NL^\times.$$

The ambiguous ideal class number formula then immediately implies

Corollary 11.13. *Let L/K be a cyclic unramified extension. Then*

$$\#\operatorname{Am}(L/K) = \frac{h_K}{(L:K)}.$$

11.3 The Ambiguous Class Number Formula

It remains to prove the ambiguous class number formula for cyclic unramified extensions L/K. In fact, the proof for arbitrary cyclic extensions is not really any more difficult, so we will treat the general case right away:

Theorem 11.14 (Ambiguous Class Number Formula)**.** *Let L/K be a cyclic extension. Then*

$$\operatorname{Am}(L/K) = h_K \frac{\prod e(\mathfrak{p})}{(L:K)(E_K : E_K \cap NL^\times)},$$

where the product is over all primes (finite and infinite).

As an example, consider a complex quadratic number field L whose discriminant is divisible by t distinct primes. Since the infinite prime of $K = \mathbb{Q}$ also ramifies, we have $\prod_{\mathfrak{p}} e(\mathfrak{p}) = 2^{t+1}$. Moreover, $E_K = \{\pm 1\}$ for $d < -4$, and since -1 cannot be the norm of an element, we deduce that $(E_K : E_K \cap NL^\times) = 2$. Thus $\#\operatorname{Am}(L/\mathbb{Q}) = 2^{t-1}$. Actually the ideal classes $c \in \operatorname{Am}(L/\mathbb{Q})$ have order dividing 2: from $c^{1+\sigma} = 1$ (every ideal class is killed by the norm since $\mathbb{Q}$ has class number 1) we deduce that $c^\sigma = c^{-1}$ for every ideal class, and consequently $c = c^\sigma = c^{-1}$ for any ambiguous ideal class. Thus $\operatorname{Am}(L/\mathbb{Q})$ is elementary abelian, and we have shown that $\operatorname{Am}(L/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^{t-1}$.

Proof. Since our proof will not use the language of cohomology, we are forced to introduce a wealth of groups along the way. Let us start by recalling what we already know:

$$\#\operatorname{Am}(L/K) = (D_L : D_L^{1-\sigma} H_L) = \frac{(D_L : H_L)}{(D_L^{1-\sigma} H_L : H_L)}.$$

Applying Lemma 11.4 with $f = 1 - \sigma$, $A = D_L$, and $B = H_L$ we find

$$(D_L : H_L) = (D_L^{1-\sigma} : H_L^{1-\sigma})(D_L^G : H_L^G),$$

where, for G-modules A, we have used the standard notation $A^G = \{a \in A : \sigma(a) = a \text{ for all } \sigma \in G\}$ for the fix module of A. Now

$$\begin{aligned}(D_L^{1-\sigma} : H_L^{1-\sigma}) &= (D_L^{1-\sigma} : D_L^{1-\sigma} \cap H_L)(D_L^{1-\sigma} \cap H_L : H_L^{1-\sigma}) \\ &= (D_L^{1-\sigma} H_L : H_L)(D_L^{1-\sigma} \cap H_L : H_L^{1-\sigma}),\end{aligned}$$

hence we get

$$\#\,\mathrm{Am}\,(L/K) = (D_L^{1-\sigma} \cap H_L : H_L^{1-\sigma})(D_L^G : H_L^G).$$

The group $D_L^{1-\sigma} \cap H_L$ consists of ideals $\mathfrak{A}^{1-\sigma}$ with the property $\mathfrak{A}^{1-\sigma} = (\theta)$ for some $\theta \in L^\times$. Taking norms in L/K gives us $(1) = N\mathfrak{A}^{1-\sigma} = (N\theta)$, hence $N\theta = \varepsilon \in E_K$ must be a unit. Conversely, assume that $\varepsilon \in E_K \cap NL^\times$ is a unit that is a norm from L; then $\varepsilon = N\theta$ for some $\theta \in L^\times$, hence $N(\theta) = (\varepsilon) = (1)$. Hilbert 90 for ideals tells us that $(\theta) = \mathfrak{A}^{1-\sigma}$ for some ideal $\mathfrak{A}$ in L.

Thus $D_L^{1-\sigma} \cap H_L$ consists of all principal ideals (θ) generated by elements $\theta \in L^\times$ with the property that $N\theta \in E_K$. We denote the group of these elements by Θ.

Now let f be the map sending elements $A \in L$ to the principal ideal (A), and apply Lemma 11.4 with $A = \Theta$ and $B = (L^\times)^{1-\sigma} E_L$. Since $\ker f = \ker g = E_L$, we get

$$(D_L^{1-\sigma} \cap H_L : H_L^{1-\sigma}) = (\Theta : (L^\times)^{1-\sigma} E_L).$$

Collecting everything we have obtained so far we find

$$\begin{aligned}\#\,\mathrm{Am}\,(L/K) &= (D_L^{1-\sigma} \cap H_L : H_L^{1-\sigma})(D_L^G : H_L^G) \\ &= (\Theta : (L^\times)^{1-\sigma} E_L)(D_L^G : H_L^G) \\ &= (\Theta : (L^\times)^{1-\sigma} E_L)\frac{(D_L^G : H_K)}{(H_L^G : H_K)} \\ &= (\Theta : (L^\times)^{1-\sigma} E_L)\frac{(D_L^G : D_K)(D_K : H_K)}{(H_L^G : H_K)}\end{aligned}$$

since ideals from K clearly are invariant under G. Clearly $(D_K : H_K) = h_K$; the index $(D_L^G : D_K)$ is also easily taken care of:

Lemma 11.15. *Let L/K be a cyclic extension. Then*

$$(D_L^G : D_K) = \prod_{\mathfrak{p} \nmid \infty} e(\mathfrak{p}),$$

where the product of over all finite primes $\mathfrak{p}$, and where $e(\mathfrak{p})$ is the ramification index of $\mathfrak{p}$ in L/K.

This is the only place where the assumption that L/K be unramified would have simplified the proof of the ambiguous class number formula.

Proof of Lemma 11.15. Every prime ideal $\mathfrak{p}$ in K factors as

$$\mathfrak{p}\mathfrak{O}_L = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^{e(\mathfrak{p})}$$

in L. We claim that every $\mathfrak{A} \in D_L^G$ can be written uniquely in the form

$$\mathfrak{A} = \mathfrak{a} \prod_{\mathfrak{p}} (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^{a(\mathfrak{p})} \tag{11.3}$$

for some ideal $\mathfrak{a} \in D_K$, where $0 \le a(\mathfrak{p}) < e(\mathfrak{p})$; note that $a(\mathfrak{p}) = 0$ for all unramified primes. Since the only ideal of the form $\prod_{\mathfrak{p}} (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^{a(\mathfrak{p})}$ lying in K is the unit ideal (any ideal in K divisibly by some $\mathfrak{P}_j$ must be divisible by $\mathfrak{p} = \mathfrak{P}_j \cap K$), these products represent the cosets of D_L^G/D_K, and since there are exactly $\prod_{\mathfrak{p} \nmid \infty} e(\mathfrak{p})$ of them, the claim will follow.

Clearly every ideal of the form (11.3) is invariant under $\sigma \in G$, since σ only permutes the $\mathfrak{P}_j$. Thus we only have to show that every $\mathfrak{A} \in D_L^G$ can be written in this form. To this end we observe that we can write $\mathfrak{A}$ uniquely in the form $\mathfrak{A} = \mathfrak{a}\mathfrak{B}$ for some integral ideal $\mathfrak{B} \in D_L$ which is not divisibly by any ideal $\ne (1)$ from D_K. We also observe that $\mathfrak{B}$ is invariant under G since $\mathfrak{A}$ and $\mathfrak{a}$ are. Thus it remains to show that $\mathfrak{B} = \prod_{\mathfrak{p}} (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^{a(\mathfrak{p})}$.

Let $\mathfrak{P}_j$ be a prime ideal dividing $\mathfrak{B}$. Since $\mathfrak{B}^\tau = \mathfrak{B}$ for every $\tau \in G$, we find $\mathfrak{P}_j^\tau \mid \mathfrak{B}$. Since G acts transitively on the prime ideals, this implies that $\mathfrak{P}_1 \cdots \mathfrak{P}_g \mid \mathfrak{B}$. Thus we can write $\mathfrak{B} = \mathfrak{P}_1 \cdots \mathfrak{P}_g \mathfrak{B}_1$ and perform induction on the norm of $\mathfrak{B}$.

The fact that $a(\mathfrak{p}) < e(\mathfrak{p})$ follows from the observation that the ideal $(\mathfrak{P}_1 \cdots \mathfrak{P}_g)^{e(\mathfrak{p})} = \mathfrak{p}$ is an ideal $\ne (1)$ in D_K, and we have assumed that $\mathfrak{B}$ is not divisible by such ideals. □

It remains to compute $(H_L^G : H_K)$; we will do this by reducing it to an index involving numbers instead of ideals. To this end we introduce the group

$$\Delta = \{A \in L^\times : A^{1-\sigma} \in E_L\}.$$

Clearly Δ contains the subgroup $K^\times E_L$. Let f be the map sending elements in Δ to the principal ideals they generate, and let g be its restriction to $K^\times E_L$. Then $\operatorname{im} f = H_L^G$, $\operatorname{im} g = H_K$ (viewed as a subgroup of H_L), and $\ker f = \ker g = E_L$. Thus

$$(H_L^G : H_K) = (\Delta : K^\times E_L). \tag{11.4}$$

At this point we know

$$\#\operatorname{Am}(L/K) = h_K \prod_{\mathfrak{p} \nmid \infty} e(\mathfrak{p}) \cdot \frac{(\Theta : (L^\times)^{1-\sigma} E_L)}{(\Delta : K^\times E_L)}.$$

Applying the norm map $f = N_{L/K}$ to the numerator we find

$$(\Theta : (L^\times)^{1-\sigma}E_L) = (E_K \cap NL^\times : NE_L).$$

Similarly, applying $f = 1 - \sigma$ to the denominator we get

$$(\Delta : K^\times E_L) = (E_L \cap (L^\times)^{1-\sigma} : E_L^{1-\sigma}).$$

Note that $E_L \cap (L^\times)^{1-\sigma} = E_L[N]$: a unit killed by the norm is an element of $(L^\times)^{1-\sigma}$ by Hilbert's Theorem 90, and the converse is trivial.

Combining everything we arrive at the formula

$$\mathrm{Am}\,(L/K) = h_K \prod_{\mathfrak{p}\nmid\infty} e(\mathfrak{p}) \frac{(E_K \cap NL^\times : NE_L)}{(E_L[N] : E_L^{1-\sigma})}.$$

Determining the quotient of these indices is a nontrivial task, and the result, in the classical literature, is called the

Theorem 11.16 (Unit Principal Genus Theorem)**.** *For cyclic extensions L/K we have*

$$\frac{(E_K : NE_L)}{(E_L[N] : E_L^{1-\sigma})} = \frac{\prod_{\mathfrak{p}\mid\infty} e(\mathfrak{p})}{(L : K)},$$

where the product os over all the infinite primes.

Plugging this into our expression for $\mathrm{Am}\,(L/K)$ we get the desired formula. □

The Unit Principal Genus Theorem will be proved in the next section. It contains as a special case

Theorem 11.17 (Hilbert's Satz 92)**.** *Let L/K be a cyclic unramified extension. Then there exists a unit $\eta \in E_L \cap L^{1-\sigma} \setminus E_L^{1-\sigma}$.*

We now show how Hilbert derived his Satz 94 (Thm. 9.11) from Satz 92. Assume that L/K is cyclic and unramified of prime degree ℓ, and let σ be a generator of $G = \mathrm{Gal}\,(L/K)$. Let $\varepsilon \in E_L$ be a unit as in Satz 92, and write $\varepsilon = A^{1-\sigma}$ for some $A \in L^\times$. Then $(A)^\sigma = (A)$, hence $(A) \in D_L^G$ is fixed by the Galois group. Since L/K is unramified, we have $D_L^G = D_K$, hence $(A) = \mathfrak{a}\mathfrak{O}_L$ for some ideal $\mathfrak{a} \in D_K$. We claim that $\mathfrak{a}$ is not principal in K: in fact, if we had $\mathfrak{a} = (\alpha)$, then $A = \alpha\eta$ for some unit $\eta \in E_L$, and applying $1 - \sigma$ gives $\varepsilon = A^{1-\sigma} = \varepsilon^{1-\sigma} \in E_L^{1-\sigma}$, which contradicts our choice of ε.

Thus $\mathfrak{a}$ is a nonprincipal ideal in K that becomes principal in L. Taking the relative norm of $\mathfrak{a}\mathfrak{O}_L = (A)$ we find $\mathfrak{a}^\ell = N_{L/K}\mathfrak{a} = (N_{L/K}A)$, hence $\mathfrak{a}^\ell$ is principal in K. This shows that the ideal class $[\mathfrak{a}]$ has order ℓ in $\mathrm{Cl}(K)$.

11.4 The Herbrand Quotient of the Unit Group

Nowadays the unit principal genus theorem is called computing the Herbrand quotient of the unit group. In fact, let $A = E_L$, $f = 1 - \sigma$, and $g = N_{L/K}$. Then $\ker f$ consists of all units in E_L killed by $1 - \sigma$, and this is $E_L^G = E_K$ (Galois theory shows that elements fixed by G live in the base field, and if an $\alpha \in K^\times$ is a unit in L, it is a unit in K). Clearly $A^f = E_L^{1-\sigma}$ and $A^g = NE_L$, and finally $\ker g = E_L[N]$. Thus

$$q(E_L) = \frac{(A_f : A^g)}{(A_g : A^f)} = \frac{(E_K : NE_L)}{(E_L[N] : E_L^{1-\sigma})}.$$

Minkowski's unit theorem is strong enough to allow us to compute the Herbrand quotient of the unit group E_L for normal extensions $L/\mathbb{Q}$.

Since we will prove the result later in general, let us now indicate the proof only in the case where L is totally real. Let $n = (L : \mathbb{Q})$ denote the degree and $G = \langle \sigma \rangle$ the cyclic Galois group. We choose a unit ε as in Minkowski's unit theorem, and set $\varepsilon_j = \sigma^j(\varepsilon)$ for $j = 1, 2, \ldots, n-1$. Then $U_L = \langle \varepsilon_1, \ldots, \varepsilon_{n-1} \rangle$ is a subgroup of E_L with finite index, so by Herbrand's lemma we know that $q(E_L) = q(U_L)$. Now let $A = U_L$, $f = 1 - \sigma$, and $g = N = 1 + \sigma + \ldots + \sigma^{n-1}$. Then $A_f = 1$ since the only units in U_L fixed by G are units from $\mathbb{Q}$, and $-1 \notin U_L$: in fact, any relation $\varepsilon_1^{a_1} \cdots \varepsilon_{n-1}^{a_{n-1}} = \pm 1$ with not all exponents equal to 0 would contradict the independence of these units. This already shows that $(A_f : A^g) = 1$. On the other hand, $A_g = U_L[N] = U_L$ and $A^f = U_L^{1-\sigma}$. We will now construct an exact sequence

$$1 \longrightarrow U_L^{1-\sigma} \longrightarrow U_L \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 1,$$

which then shows that $(U_L : U_L^{1-\sigma}) = n$.

First observe that $U_L \simeq R = \mathbb{Z}[X]/(\Phi)$ for $\Phi(X) = 1 + X + \ldots + X^{n-1}$. In fact, the map $\mathbb{Z}[X] \longrightarrow U_L$ sending $F \in \mathbb{Z}[X]$ to $\varepsilon^{F(\sigma)} \in U_L$ is a surjective group homomorphism, and its kernel is the ideal generated by Φ. Since application of σ corresponds to multiplication by X, we have $U_L/U_L^{1-\sigma} \simeq R/(1-X)$. Thus we have to show that $R/(1-X) \simeq \mathbb{Z}/n\mathbb{Z}$.

To this end we observe that the evaluation map sending $F + (\Phi) \in R$ to $F(1) + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ is well defined because of $\Phi(1) = n$. The kernel of this homomorphism consists of all cosets $F + (\Phi)$ with $n \mid F(1)$. Write $F(1) = kn$ for some $k \in \mathbb{Z}$; then $F_1 = F - k\Phi$ satisfies $F(1) = 0$, hence is a multiple of $1 - X$. Thus the kernel consists of the ideal $(1 - X)$, and the claim follows.

Armed with Herbrand's Unit Theorem we now can compute the Herbrand quotient of the unit group E_L:

Proof of Thm. 11.16. As before, it is sufficient to compute $q(U_L)$ for the subgroup U_L generated by the units ε_j, η_j, and their conjugates. Set $A = U_L$, $f = 1 - \sigma$, and $g = N = 1 + \sigma + \ldots + \sigma^{n-1}$ for $n = (L : K)$. Then $A_f = E_K$ since the only units in U_L fixed by G are the units from K, and there are no roots of unity contained in U_L. Moreover, $N_{L/K}U_L = \langle \varepsilon_1^n, \ldots, \varepsilon_\rho^n \rangle$, hence $(A_f : A^g) = (U_L^G : NU_L) = (E_K : E_K^n) = n^\rho$.

On the other hand, $A_g = U_L[N]$ is the group U_0 generated by the η_j and their conjugates, $A^f = U_L^{1-\sigma}$. Thus we have to compute $(U_0 : U_L^{1-\sigma})$.

Let U_j denote the G-module generated by η_j, that is, the subgroup of U_0 generated by η_j and its conjugates. Then $U_0 = \bigoplus_{j=1}^{\rho+1} U_j$ as a G-module, hence

$$U_0/U_0^{1-\sigma} = \bigoplus_{j=1}^{\rho+1} U_j/U_j^{1-\sigma}.$$

We have already seen that $U_j \simeq R_j = \mathbb{Z}[X]/(\Phi_j)$ for the polynomials $\Phi_j(X) = 1 + X + \ldots + X^{n_j-1}$, and that $U_j/U_j^{1-\sigma} \simeq R_j/(1-X) \simeq \mathbb{Z}/n_j\mathbb{Z}$. Thus

$$(U_0 : U_0^{1-\sigma}) = \prod (U_j : U_j^{1-\sigma}) = \prod n_j = \frac{n^{\rho+1}}{\prod e(\infty_j)},$$

and we find

$$q(E_L) = q(U_L) = \frac{(U_L^G : NU_L)}{(U_0 : U_0^{1-\sigma})} = \frac{n^\rho \prod e(\infty_j)}{n^{\rho+1}} = \frac{\prod e(\infty_j)}{n}$$

as claimed. □

Notes

The proofs of the first and second inequalities given in this chapter are taken (with minor simplifications) from Artin's three lectures on class field theory given in 1932 in Göttingen; an English translation of these lectures can be found in the appendix to Cohn's book [Co1978]. In his Marburg lectures from 1933, Hasse chose essentially the same proof.

Let me point out that there were essentially two results on which our proofs of the fundamental inequalities were based:

- The first inequality follows from the fact that the Dedekind zeta function $\zeta_K(s)$ has a pole of order 1 at $s = 1$.
- The second inequality is a consequence of the computation of the Herbrand quotient of the unit group E_L, hence of Herbrand's unit theorem.

Note that the Herbrand quotient of the unit group was also an ingredient for the proof of the ambiguous class number formula or the fact that units in cyclic unramified extensions are norms.

Exercises

11.1 Let $f : A \longrightarrow A$ be an endomorphism of an abelian group A, and let B be a subgroup of A. Explain why, in general, f does not induce a homomorphism

$A/B \longrightarrow A/B$ on the quotient groups. Show that if f induces an endomorphism $g : B \longrightarrow B$, then we get an induced homomorphism $\overline{f} : A/B \longrightarrow A/B$ with $\operatorname{im} \overline{f} = A^f B/B$ and $\ker \overline{f} = (A \cap f^{-1}(B))B/B$.

11.2 Let $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{3}\,)$, and $G = \mathrm{Gal}\,(L/K)$. Show that the principal ideal $(1 + \sqrt{3}\,)$ is an element of $H_L^G \setminus H_K$.

11.3 Show that the diagram

$$\begin{tikzcd}
1 \arrow[r] & K^\times E_L \arrow[r] \arrow[d] & \Delta \arrow[r] \arrow[d] & \Delta/K^\times E_L \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & H_K \arrow[r] & H_L^G \arrow[r] & H_L^G/H_K \arrow[r] & 1
\end{tikzcd}$$

is exact and commutative, where the vertical maps send elements to the principal ideal they generate. Now use the snake lemma to deduce (11.4) directly.

11.4 Let A, B, C be G-modules (abelian groups on which the group G acts), and assume that

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] & B \arrow[r] & C \arrow[r] & 0
\end{tikzcd}$$

is an exact sequence of G-modules (this means that the homomorphisms commute with the action of G, i.e., $f(a^\sigma) = f(a)^\sigma$). Show that taking fix modules is left exact: there is an exact sequence

$$\begin{tikzcd}
0 \arrow[r] & A^G \arrow[r] & B^G \arrow[r] & C^G
\end{tikzcd}$$

of abelian groups (the action of G on these fix modules is of course trivial), but the map $B^G \longrightarrow C^G$ is not surjective in general. (Hint: for cyclic groups, this follows immediately by applying the snake lemma to a suitably chosen commutative diagram. Observe that, in this case, A^G is the kernel of the map $1 - \sigma : A \longrightarrow A$.)

11.5 Let A be a finitely generated abelian group (this implies that the index $(B : nB)$ is finite for every $n \in \mathbb{N}$ and every subgroup B of A), on which a finite cyclic group $G = \langle\sigma\rangle$ of order n acts. Set $f = 1 - \sigma$ and $g = 1 + \sigma + \ldots + \sigma^{n-1}$. Show that the Herbrand quotient $qf, g(A)$ exists by verifying

- $nA_f \subseteq A^g \subseteq A_f$;
- $nA_g \subseteq A^f \subseteq A_g$.

11.6 Let G be a finite group, and let G act trivially on $\mathbb{Z}$ ($\sigma(a) = a$ for all $a \in \mathbb{Z}$). Show that $q_{f,g}(Z) = \#G$, where $f = N$ and $g = 1 - \sigma$.

11.7 Let $G = \{1, \sigma\}$ be a group of order 2, and let G act on $\mathbb{Z}$ via $\sigma(a) = -a$. Compute $q(\mathbb{Z})$.

11.8 Let $G = \{1, \sigma\}$ be a group of order 2, and let G act on $A = \mathbb{Z} \oplus \mathbb{Z}$ via $\sigma(a, b) = (b, a)$. Compute $q(A)$. What is $q(A)$ if you let G act trivially?

11.9 Compute $q(E_L)$ directly for quadratic extensions $L = \mathbb{Q}(\sqrt{m}\,)$.

1. If $m < 0$, show that $q(E_L) = 1$ by verifying the following claims: $(E_K : NE_L) = 2$, $E_L[N] = E_L$, $E_L^{1-\sigma} = E_L^2$, and $(E_L[N] : E_L^{1-\sigma}) = 2$.
2. If $m > 0$, show that $q(E_L) = \frac{1}{2}$ by verifying the following claims: let $E_L = \langle -1, \varepsilon\rangle$, where ε is the fundamental unit.
   - If $N\varepsilon = +1$, then $(E_K : NE_L) = 2$, $E_L[N] = E_L$, $E_L^{1-\sigma} = E_L^2$, and $(E_L[N] : E_L^{1-\sigma}) = 4$.

- If $N\varepsilon = -1$, then $(E_K : NE_L) = 1$, $E_L[N] = \langle -1, \varepsilon^2\rangle$, $E_L^{1-\sigma} = \langle -\varepsilon^2\rangle$, and $(E_L[N] : E_L^{1-\sigma}) = 2$.

11.10 Prove the First Inequality for class groups in the strict sense: let L/K be a normal extension, and set $T_{L/K} = ND_L \cdot H_K^+$, where H_K^+ is the group of principal ideals generated by totally positive elements. Show that $(D_K : T_{L/K}) \le (L : K)$.

11.11 Prove the Second Inequality for class groups in the strict sense: let L/K be a cyclic extension unramified outside ∞ (only infinite primes are allowed to ramify). With $T_{L/K} = ND_L \cdot H_K^+$ as in the preceding exercise, show that $(D_K : T_{L/K}) \ge (L : K)$.

11.12 Let $A \simeq B \oplus C$ be the direct sum of two G-modules, where $G = \langle\sigma\rangle$ is a finite cyclic group. Show that

$$A/A^{1-\sigma} \simeq B/B^{1-\sigma} \oplus C/C^{1-\sigma}.$$

One possible way of proving this is by applying the snake lemma to the exact diagram

$$\begin{tikzcd}
0 \arrow[r] & B \arrow[r] \arrow[d] & A \arrow[r] \arrow[d] & C \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & B \arrow[r] & A \arrow[r] & C \arrow[r] & 0
\end{tikzcd}$$

where the vertical maps are induced by $1-\sigma$. Then deduce from $A \simeq B \oplus C$ that the map $A^G \longrightarrow B^G$ is the natural projection, hence surjective, and deduce the two exact sequences

$$\begin{tikzcd}
0 \arrow[r] & B^G \arrow[r] & A^G \arrow[r] & C^G \arrow[r] & 0 \\
0 \arrow[r] & B/B^{1-\sigma} \arrow[r] & A/A^{1-\sigma} \arrow[r] & C/C^{1-\sigma} \arrow[r] & 0.
\end{tikzcd}$$

Now switch the roles of B and C to see that the last sequence splits.

11.13 Consider the field $K = \mathbb{Q}(\sqrt[3]{2}\,)$ and its normal closure $L = K(\sqrt{-3}\,)$. The unit group of K is given by $E_K = \langle -1, 1-\sqrt[3]{2}\,\rangle$, and $\varepsilon = 1-\sqrt[3]{2}$ and $\varepsilon' = 1-\rho\sqrt[3]{2}$ (where ρ is a primitive cube root of unity) generate a subgroup of finite index in E_L.
Show that the units $\varepsilon_1 = \varepsilon$ and $\eta_1 = (\varepsilon')^2/\varepsilon$ have the properties listed in Herbrand's unit theorem.

11.14 Let L/K be a cyclic unramified extension of prime power degree ℓ^m. Show that the following assertions are equivalent:
i) $\ell \nmid h_L$;
ii) $\mathrm{Cl}_\ell(K) \simeq \mathbb{Z}/\ell^m\mathbb{Z}$.
Also show that if these conditions are satisfied, then $E_K = N_{L/K}E_L$. (Hint: If $\ell \mid h_L$, then there exists a *central* unramified extension M/L of degree ℓ by the theory of p-groups; moreover, central extensions of cyclic groups are abelian. For proving the last claim, use the ambiguous class number formula.

12. Examples of Hilbert Class Fields

13. The Artin Symbol

Our goal in this chapter is to define the Artin symbol and to show how it induces an isomorphism between the class group $D_K/T_{L/K}$ attached to an unramified abelian extension L/K and the Galois group $\mathrm{Gal}\,(L/K)$.

13.1 Inertia Groups

Now fix a $\sigma \in Z(\mathfrak{P}|\mathfrak{p})$; then we can map a residue class $\alpha + \mathfrak{P}$ to $\alpha^\sigma + \mathfrak{P}$ (note that $\mathfrak{P}^\sigma = \mathfrak{P}$); this automorphism of $\kappa(\mathfrak{P})$ will fix the subfield $\kappa(\mathfrak{p})$ elementwise, hence is an element of the Galois group $\mathrm{Gal}\,(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$. This gives us a homomorphism $Z(\mathfrak{P}|\mathfrak{p}) \longrightarrow \mathrm{Gal}\,(\kappa(\mathfrak{P})/\kappa(/\mathfrak{p}))$. Its kernel is easily seen to be

$$T(\mathfrak{P}|\mathfrak{p}) = \{\sigma \in Z(\mathfrak{P}|\mathfrak{p}) : \alpha^\sigma \equiv \alpha \bmod \mathfrak{P} \text{ for all } \alpha \in \mathfrak{O}\},$$

which is called the inertia subgroup of $\mathfrak{P}|\mathfrak{p}$; its fixed field is called the inertia field of $\mathfrak{P}|\mathfrak{p}$. Since T is the kernel of a homomorphism, it is necessarily a normal subgroup of Z. Moreover, Z/T is isomorphic to a subgroup of the Galois group of $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$; since Galois groups of extensions of finite fields are cyclic, this implies that Z/T is also a cyclic group, and in fact must have order dividing f.

Proposition 13.1. *The homomorphism $Z(\mathfrak{P}|\mathfrak{p}) \longrightarrow \mathrm{Gal}\,(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$ is surjective; in particular, $Z/T \simeq \mathrm{Gal}\,(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$ is cyclic of order f.*

Since $(G : Z) = g$ and $efg = n = (G : 1) = (G : Z)(Z : T)(T : 1)$, this implies that $\#T = e$. In particular we have $T = 1$ whenever $\mathfrak{P}$ is unramified, and in this case Z is a cyclic group of order f isomorphic to the Galois group $\mathrm{Gal}\,(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$.

Also observe that we now know that $(K_T : K_Z) = f$ and $(K : K_T) = e$.

Proof of Prop. 13.1. We know $f(\mathfrak{P}_Z|\mathfrak{p}) = 1$, hence $\mathfrak{O}_Z/\mathfrak{P}_Z \simeq \mathfrak{o}/\mathfrak{p}$. For $\alpha \in \mathfrak{O}$ let $\overline{\alpha} = \alpha + \mathfrak{P}$ denote its residue class modulo $\mathfrak{P}$. Pick α in such a way that $\overline{\alpha}$ generates $\mathfrak{O}/\mathfrak{P}$ over $\mathfrak{o}/\mathfrak{p}$. The characteristic polynomial of α over K_Z is $\psi(X) = \prod_{\sigma\in Z}(X - \alpha^\sigma)$. The reduction $\overline{\psi}$ of ψ modulo $\mathfrak{P}$ has coefficients in $\mathfrak{O}_Z/\mathfrak{P}_Z \simeq \mathfrak{o}/\mathfrak{p}$. Its roots have the form $\overline{\alpha^\sigma}$. Thus every conjugate of $\overline{\alpha}$ has this form, and this implies the claim. □

We now can determine a few more relative indices and degrees:

Lemma 13.2. *We have $e(\mathfrak{P}|\mathfrak{P}_T) = e$ and $f(\mathfrak{P}|\mathfrak{P}_T) = 1$, as well as $e(\mathfrak{P}_T|\mathfrak{p}) = 1$ and $f(\mathfrak{P}_T|\mathfrak{p}) = f$.*

Proof. The inertia group $T(\mathfrak{P}|\mathfrak{p})$ is equal to the inertia group $T(\mathfrak{P}|\mathfrak{P}_T)$; applying Prop. 13.1 to the extension K/K_T shows that $\mathrm{Gal}\,(\kappa(\mathfrak{P})/\kappa(\mathfrak{P}_T)) \simeq Z/T = 1$ since $Z(\mathfrak{P}|\mathfrak{P}_T) = 1$. Thus $\kappa(\mathfrak{P}) = \kappa(\mathfrak{P}_T)$.

This implies $f(\mathfrak{P}|\mathfrak{P}_T) = 1$ and thus $f(\mathfrak{P}_T|\mathfrak{p}_Z) = f$. Finally, using $efg = n$ for the extension K/K_T shows that $e(\mathfrak{P}|\mathfrak{P}_T) = (K : K_T) = e$. □

Thus the primes below $\mathfrak{P}$ pick up their inertia degrees as we go from K_Z to K_T. This implies that $\kappa(\mathfrak{P}) \simeq \kappa(\mathfrak{P}_T)$; in other words: every prime ideal has a system of representatives in its inertia field:

Corollary 13.3. *For every element $\alpha \in \mathfrak{O}$ there is a $\beta \in \mathfrak{O}_T$ such that $\alpha \equiv \beta \bmod \mathfrak{P}$.*

13.2 The Symbols of Frobenius and Artin

Let K/k be a Galois extension of number fields, and assume that the prime ideal $\mathfrak{P}$ in $\mathfrak{O}$ above $\mathfrak{p}$ is unramified. Then $T = 1$ and the decomposition group $Z = Z(\mathfrak{P}|\mathfrak{p})$ is isomorphic to the Galois group of $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$. This Galois group is generated by a distinguished automorphism called the Frobenius $\sigma_{\mathfrak{P}}$, which sends a residue class $\alpha + \mathfrak{P}$ to $\sigma_{\mathfrak{P}}(\alpha) \equiv \alpha^{N\mathfrak{p}} \bmod \mathfrak{P}$. Under the isomorphism $Z \simeq \mathrm{Gal}\,(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$, the Frobenius automorphism corresponds to a well defined element in Z that we also denote by $\sigma_{\mathfrak{P}} = \big[\frac{K/k}{\mathfrak{P}}\big]$. The symbol on the right is called the Frobenius symbol, and we will now derive its basic properties.

Proposition 13.4. *Let K/k be a normal extension with Galois group G, and let $\mathfrak{P}$ denote a prime ideal in $\mathfrak{O}$ that is unramified over $\mathfrak{p}$.*

1. *$\big[\frac{K/k}{\mathfrak{P}}\big] \in G$ has order $f = f(\mathfrak{P}|\mathfrak{p})$.*
2. *$\big[\frac{K/k}{\mathfrak{P}^\sigma}\big] = \sigma^{-1}\big[\frac{K/k}{\mathfrak{P}}\big]\sigma$ for all $\sigma \in G$.*
3. *Let F be an intermediate field of K/k; then $\big[\frac{K/F}{\mathfrak{P}}\big] = \big[\frac{K/k}{\mathfrak{P}}\big]^{f(\mathfrak{P}_F|\mathfrak{p})}$.*
4. *Assume in addition that F/k is normal. Then $\big[\frac{F/k}{\mathfrak{P}_F}\big] = \big[\frac{K/k}{\mathfrak{P}}\big]\Big|_F$, where $\sigma|_F$ denotes the restriction of $\sigma \in G$ to F.*

Proof. The Frobenius automorphism $\phi = \big[\frac{K/k}{\mathfrak{P}}\big]$ generates Z/T, hence has order f.

Moreover, $\alpha^\phi \equiv \alpha^{N\mathfrak{p}} \bmod \mathfrak{P}$; this implies $\alpha^{\phi\sigma} = (\alpha^\sigma)^{\sigma^{-1}\phi\sigma} \equiv (\alpha^\sigma)^{N\mathfrak{p}} \bmod \mathfrak{P}^\sigma$, and this congruence shows that the Frobenius automorphism of $\mathfrak{P}^\sigma$ is $\sigma^{-1}\phi\sigma$.

Now let $\kappa(\mathfrak{p}) = \mathbb{F}_q$; then $\kappa(\mathfrak{P}) = \mathbb{F}_{q^f}$ and $\kappa(\mathfrak{P}_F) = \mathbb{F}_{q^{f'}}$, where $f' = f \cdot f(\mathfrak{P}_F|\mathfrak{p})$. Let ϕ be the Frobenius automorphism of $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$; it maps elements to their q-th power. The Frobenius automorphism ϕ of $\kappa(\mathfrak{P})/\kappa(\mathfrak{P}_F)$ is the one mapping elements to their $q^{f'}$-th power, hence is equal to $\phi^{f'}$. This proves the third claim.

The Frobenius automorphism for $\mathfrak{P}$ is characterized by the congruence $\alpha^\phi \equiv \alpha^{N\mathfrak{p}} \bmod \mathfrak{P}$ for all $\alpha \in \mathfrak{O}_K$. The same congruence therefore holds for all elements $\alpha \in \mathfrak{O}_F$, hence the Frobenius for $\mathfrak{P}_F$ is just the restriction of ϕ to F. □

The Artin Symbol

If K/k is an abelian extension and $\mathfrak{p}$ a prime ideal in k that is unramified in K, the symbols $[\frac{K/k}{\mathfrak{P}^\sigma}]$ all coincide, and we can write $(\frac{K/k}{\mathfrak{p}}) = [\frac{K/k}{\mathfrak{P}}]$, where $\mathfrak{P}$ is any prime ideal in K above $\mathfrak{p}$. This symbol $(\frac{K/k}{\mathfrak{p}})$ is called the Artin symbol. Since the difference between the Frobenius symbol and the Artin symbol is only a notational one, we immediately get the following

Proposition 13.5. *Let K/k be an abelian extension, and let $\mathfrak{p}$ be a prime ideal in $\mathfrak{o}$ that is unramified in $\mathfrak{O}$.*

1. *A prime ideal $\mathfrak{p}$ splits completely in K/k if and only if $\big(\frac{K/k}{\mathfrak{p}}\big) = 1$.*
2. *Let F be an intermediate field of K/k; then $\big(\frac{K/k}{\mathfrak{P}}\big)^{f(\mathfrak{P}_F|\mathfrak{p})} = \big(\frac{K/F}{\mathfrak{P}}\big)$.*
3. *We have $\big(\frac{F/k}{\mathfrak{P}_F}\big) = \big(\frac{K/k}{\mathfrak{P}}\big)\Big|_F$.*

The Artin Symbol for Quadratic Extensions

Let $K/\mathbb{Q}$ be a quadratic extension with discriminant d, let σ denote the nontrivial automorphism of $K/\mathbb{Q}$, and let p be a prime not dividing d. Then there are two cases:

1. $(\frac{d}{p}) = +1$; then $p\mathfrak{O} = \mathfrak{p}\mathfrak{p}'$ splits;
2. $(\frac{d}{p}) = -1$; then $p\mathfrak{O} = \mathfrak{p}$ is inert.

Since a prime splits completely if and only if its Artin symbol is trivial, we see that $\big(\frac{K/\mathbb{Q}}{p}\big) = 1 \iff (\frac{d}{p}) = 1$, and $\big(\frac{K/\mathbb{Q}}{p}\big) = \sigma \iff (\frac{d}{p}) = -1$.

Thus if we identify the Galois group $G = \{1, \sigma\}$ with the value group $\{+1, -1\}$ of the Kronecker symbol, we find that $\big(\frac{K/\mathbb{Q}}{p}\big) = (\frac{d}{p})$.

In this sense, the Artin symbol generalizes the Legendre symbol.

The Artin Symbol for Cyclotomic Extensions

Let $K = \mathbb{Q}(\zeta)$ be the field generated by a primitive m-th root of unity ζ. It has degree $\phi(m)$ and Galois group $\mathrm{Gal}\,(K/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^\times$; its automorphisms are determined by their action on ζ, and they have the form $\sigma_a : \zeta \longmapsto \zeta^a$ for $a \in (\mathbb{Z}/m\mathbb{Z})^\times$.

Assume that $p \nmid m$; then p is unramified. Let $\phi = \left(\frac{K/\mathbb{Q}}{p}\right)$ be the Frobenius of p. The definition of the Frobenius automorphism implies that $\zeta^\phi = \zeta^p$. If we write $p\mathfrak{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_g$ with $fg = \phi(m)$, then we know that ϕ has order f. But if ϕ^f is the identity map, then $\zeta^{p^f} = \phi^f(\zeta) = \zeta$, which holds if and only if $p^f \equiv 1 \bmod m$. Thus f is also the order of $p \bmod m$. We have proved:

Proposition 13.6. *In the field $\mathbb{Q}(\zeta - m)$ of m-th roots of unity, a prime $p \nmid m$ splits as $p\mathfrak{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_g$, where $fg = \phi(m)$ and f is the order of the residue class $p \bmod m$.*

The Quadratic Reciprocity Law

Let p and q be distinct odd primes. Consider the field $K = \mathbb{Q}(\zeta_q)$; its Galois group is cyclic of order $q-1$, hence K has a quadratic subfield F. Since $K/\mathbb{Q}$ only ramifies at q (we will often say that $K/\mathbb{Q}$ is unramified outside of q; note that we are neglecting the ramification at infinite primes here), so does $F/\mathbb{Q}$. But the only quadratic number field unramified outside q is $F = \mathbb{Q}(\sqrt{q^*}\,)$, where $q^* = (-1)^{(q-1)/2}q$.

We also know that $G = \mathrm{Gal}\,(K/\mathbb{Q}) \simeq (\mathbb{Z}/q\mathbb{Z})^\times =: \overline{G}$, where the isomorphism maps $\sigma_a : \zeta \longmapsto \zeta^a$ to the residue class $a \bmod q$. Since G is cyclic, it has a unique subgroup H of index 2, which corresponds to the subgroup $\overline{H} = \{a \bmod q : a \equiv x^2 \bmod q\}$ of squares. By Galois theory, the fixed field of H is F, and we have $\mathrm{Gal}\,(F/\mathbb{Q}) \simeq G/H$.

Now we get

$$\begin{aligned}
\left(\frac{q^*}{p}\right) = +1 \quad &\Longleftrightarrow \quad p \text{ splits in } F/\mathbb{Q} \quad \Longleftrightarrow \quad \left(\frac{F/\mathbb{Q}}{p}\right) = 1 \\
&\Longleftrightarrow \quad \left(\frac{K/\mathbb{Q}}{p}\right)\Big|_F = 1 \quad \Longleftrightarrow \quad \left(\frac{K/\mathbb{Q}}{p}\right) \in H \\
&\Longleftrightarrow \quad p \equiv x^2 \bmod q \quad \Longleftrightarrow \quad \left(\frac{p}{q^*}\right) = +1.
\end{aligned}$$

This is the quadratic reciprocity law, which we derived completely without calculation just by comparing the splitting of primes in quadratic and cyclotomic extensions.

Let me emphasize again how this proof flows very naturally from the application of Galois theory to algebraic number theory, in particularly from the theory of the Artin symbol, whose properties in turn follow quite easily from the fundamental ismorphism between Z/T and the Galois group of the residue class field extension.

13.3 The Artin Isomorphism

Let K/F be an unramified abelian extension. In order to make the Artin symbol $\left(\frac{K/F}{\cdot}\right)$ from a map on the set of prime ideals into a homomorphism from the group D_K of ideals in $\mathfrak{O}_K$ we set $\left(\frac{K/F}{\mathfrak{a}}\right) = \prod_{\mathfrak{p}|\mathfrak{a}} \left(\frac{K/F}{\mathfrak{p}}\right)$. (You should see this is as a definition analogous to the Jacobi symbol.) Now the Artin symbol gives us a homomorphism

$$\mathrm{rec}_{K/F} : D_K \longrightarrow \mathrm{Gal}\,(K/F)$$

(recall that K/F is unramified and abelian). Artin's reciprocity law identifies the kernel and the image of this map:

Theorem 13.7 (Artin's Reciprocity Law)**.** *Let K/F be an unramified abelian extension of number fields. Then the Artin map $\mathrm{rec}_{K/F}$ is surjective, and its kernel consists of the group of principal ideals. In particular, the Artin symbol $\left(\frac{K/F}{\mathfrak{p}}\right)$ only depends on the ideal class $[\mathfrak{p}]$ of $\mathfrak{p}$, and induces an isomorphism $\mathrm{Cl}(F) \simeq \mathrm{Gal}\,(K/F)$.*

Surjectivity of the Artin Map

Let us now give a first application of the density theorem of Frobenius to class field theory. Let L/K be an abelian extension, and S a set of prime ideals in K that contains all the ramified prime ideals. Then the Artin symbol $\left(\frac{L/K}{\cdot}\right)$ induces a homomorphism from the group I_K^S of fractional ideals in K coprime to all the prime ideals in S to the Galois group $\mathrm{Gal}\,(L/K)$. The Frobenius density theorem for abelian extensions immediately implies

Theorem 13.8. *Let L/K be an abelian extension, and let S denote a finite set of prime ideals in K containing all the ramified primes. Then the Artin map $\left(\frac{L/K}{\cdot}\right) : I_K^S \longrightarrow \mathrm{Gal}\,(L/K)$ is surjective.*

Proof. Take a $\sigma \in G = \mathrm{Gal}\,(L/K)$. By the Frobenius density theorem, there are infinitely many prime ideals $\mathfrak{p}$ for which $\left(\frac{L/K}{\mathfrak{p}}\right)$ generates $\langle\sigma\rangle$. Since there are only finitely many ramified primes, there is a prime ideal $\mathfrak{p} \in I_K^S$ such that $\left(\frac{L/K}{\mathfrak{p}}\right)$ generates $\langle\sigma\rangle$. But then σ is in the image of the Artin map. □

The main content of Artin's reciprocity law is the description of the kernel. Artin's reciprocity law, coupled with our knowledge about Artin symbols, immediately implies the decomposition law.

Exercises

13.1 Let K/k be an extension of number fields. Show that the norm map $N_{K/k}$ on ideals induces a homomorphism $N_{K/k} : \mathrm{Cl}(K) \longrightarrow \mathrm{Cl}(k)$.

13.2 Let K/k be an extension of number fields. The map sending an ideal $\mathfrak{a}$ in $\mathfrak{o}$ to the ideal $\mathfrak{a}\mathfrak{O}$ is called the conorm, and is often denoted by $j_{k\to K}$. Show that the conorm induces a group homomorphism $j_{k\to K}\,\mathrm{Cl}(k) \longrightarrow \mathrm{Cl}(K)$, and that $N_{K/k} \circ j_{k\to K}$ raises each ideal class to its n-th power, where $n = (K:k)$. The kernel of this map is called the capitulation kernel.

13.3 Let K/k be an extension of number fields. Show that if $\mathfrak{a}$ is an ideal in $\mathfrak{o}$ such that $\mathfrak{a}\mathfrak{O} = (\alpha)$ is principal, then the order of the ideal class $c = [\mathfrak{a}]$ in $\mathrm{Cl}(k)$ divides $n = (K:k)$.

13.4 Let K/k be an extension of number fields. Show that if $\gcd(h_k, n) = 1$ for the class number $h_k = \#\,\mathrm{Cl}(k)$ and the degree $n = (K:k)$, then the norm map $N_{K/k} : \mathrm{Cl}(K) \longrightarrow \mathrm{Cl}(k)$ is surjective, and the conorm $j_{k\to K}\,\mathrm{Cl}(k) \longrightarrow \mathrm{Cl}(K)$ is injective. Deduce that $h_k \mid h_K$ in this case.

13.5 Let $L/K/k$ be a tower of normal extensions of number fields. Let $\mathfrak{Q}$ be a prime ideal in $\mathfrak{O}_L$, and let $\mathfrak{P} = \mathfrak{Q} \cap K$ and $\mathfrak{p} = \mathfrak{Q} \cap k$ denote the prime ideals in $\mathfrak{O}_K$ and $\mathfrak{O}_k$ lying below $\mathfrak{Q}$. Show that

$$e(\mathfrak{Q}|\mathfrak{p}) = e(\mathfrak{Q}|\mathfrak{P}) \cdot e(\mathfrak{P}|\mathfrak{p}) \quad \text{and} \quad f(\mathfrak{Q}|\mathfrak{p}) = f(\mathfrak{Q}|\mathfrak{P}) \cdot f(\mathfrak{P}|\mathfrak{p}).$$

13.6 Show that the decomposition group is a group.

13.7 Let $\mathfrak{p}$ be a nonzero prime ideal in $\mathfrak{o}$; show that $\mathfrak{p}\mathfrak{O} \cap \mathfrak{o} = \mathfrak{p}$. (Hint: use the fact that $\mathfrak{p}$ is maximal in $\mathfrak{o}$.)

13.8 Let K/k be a Galois extension, and assume that $\mathfrak{p}$ is inert in K/k. Show that K/k is a cyclic extension. (Hint: look at Z/T.)

13.9 Abhyankar's Lemma: Let K_1/k and K_2/K be disjoint abelian extensions with Galois group $\mathrm{Gal}\,(K_i/k) \simeq \mathbb{Z}/\ell\mathbb{Z}$. Show that if a prime ideal $\mathfrak{p}$ is ramified in both extensions, then the primes above $\mathfrak{p}$ are unramified in K_1K_2/K_1 and K_1K_2/K_2. Hint: Look at the ramification groups.

13.10 Consider the pure extension $K = \mathbb{Q}(\sqrt[\ell]{m}\,)$, and assume that there is a prime $p \equiv 1 \bmod \ell$ with $p \mid m$. Let F be the subfield of $\mathbb{Q}(\zeta_p)$ with degree ℓ. Show that FK/K is an unramified abelian extension. Hint: Abhyankar's Lemma.

13.11 Show that the decomposition and inertia groups of the prime ideal $\mathfrak{P}^\sigma$ for some $\sigma \in G$ are given by $Z(\mathfrak{P}^\sigma|\mathfrak{p}) = \sigma^{-1}Z(\mathfrak{P}|\mathfrak{p})\sigma$ and $T(\mathfrak{P}^\sigma|\mathfrak{p}) = \sigma^{-1}T(\mathfrak{P}|\mathfrak{p})\sigma$. Similar results hold for the higher ramification groups. Here it is important to let G act from the right.

13.12 Let $p \equiv 2 \bmod 3$ be a prime not dividing m, and consider the normal closure $K = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{m}\,)$ of $F = \mathbb{Q}(\sqrt[3]{m}\,)$.

1. Show that the congruence $x^3 \equiv m \bmod p$ has a unique solution.
2. Deduce from Thus Thm. 5.5 that p splits as $p\mathfrak{O}_F = \mathfrak{p}_1\mathfrak{p}_2$, where $\mathfrak{p}_2$ is a prime ideal of norm p^2.
3. Show that p is inert in $k = \mathbb{Q}(\sqrt{-3}\,)$.
4. Show that $g \geq 2$ and $f \geq 2$ in $K/\mathbb{Q}$. Show that this implies $p\mathfrak{O}_K = \mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3$
5. Let $\mathfrak{p}_1 = \mathfrak{P}_1 \cap \mathfrak{O}_F$. Show that the decomposition field of $\mathfrak{P}_1$ is K.

13.13 Let H be a subgroup of G, and let K_H be the fixed field of H. Then $\mathfrak{P}_i$ and $\mathfrak{P}_j$ divide the same prime ideal in K_H if and only if $\mathfrak{P}_j = \mathfrak{P}_i^\sigma$ for some $\sigma \in H$.

13.14 Determine the ramification subgroups for the prime above p in $\mathbb{Q}(\zeta_p)$

1. directly from the definition;
2. from the theory.

13.15 Let $K = \mathbb{Q}(\zeta)$ for $\zeta = \zeta_m$; show that $F = \mathbb{Q}(\zeta + \zeta^{-1})$ is a subfield of F with $(K : F) = 2$, and that is is the fixed field of the subgroup H of $\mathrm{Gal}\,(K/\mathbb{Q})$ corresponding to the group $\overline{H} = \{\pm 1 \bmod m\}$.
Also show that a prime splits completely in $F/\mathbb{Q}$ if and only if $p \equiv \pm 1 \bmod m$.

13.16 Let K/k be a normal extension, and let ∞ be an infinite prime in k below $\overline{\infty}$. Define decomposition and inertia subgroups for these infinite primes, and show that $\overline{\infty}$ is ramified in K/k if and only if $\#T = 2$. Also show that $Z = T$, so infinite primes do not have a nontrivial inertia degree.

13.17 Show that the extension $K = \mathbb{Q}(\sqrt{2+\sqrt{2}}\,)$ is a quartic cyclic extension of $\mathbb{Q}$, and that its Galois group is generated by $\sigma : \sqrt{2+\sqrt{2}} \longmapsto \sqrt{2-\sqrt{2}}$. Show that primes $p \equiv 3, 5 \bmod 8$ are inert, and compute their Frobenius automorphism (it must be σ or σ^3, but which?).

14. Frobenius Density

The first "density theorem" in number theory was Dirichlet's theorem that primes $p \equiv a \bmod m$, where $\gcd(a, m) = 1$, have "Dirichlet density" $\frac{1}{\phi(m)}$. Dirichlet also showed that primes represented by a quadratic form $Ax^2 + Bxy + Cy^2$ with nonsquare discriminant $B^2 - 4AC$ have a positive density. Kronecker later conjectured that, in modern language, primes splitting completely in an extension $K/\mathbb{Q}$ have Dirichlet density $\frac{1}{(N:\mathbb{Q})}$, where N is the normal closure of $K/\mathbb{Q}$.

In this chapter we will explain how Chebotarev's density theorem contains Dirichlet's and Kronecker's theorems as special cases, but we will prove a weaker version only, namely the density theorem of Frobenius.

14.1 Frobenius and his Density Theorem

Kronecker's conjectures on the existence of the Dirichlet densities D_j were proved by Frobenius. Actually Frobenius proved something slightly stronger: he did not just count the number of linear factors, but studied the splitting type of a polynomial. A polynomial of degree 5 with exactly one root modulo p splits either into a linear factor and an irreducible quartic, or into a linear and two irreducible quadratic polynomials over $\mathbb{F}_p$. We denote these types of splitting by $(1, 4)$ and $(1, 2, 2)$, respectively, and will call them decomposition types

As examples, consider the polynomials $f(X) = X^4 - X^2 - 1$ with discriminant $\operatorname{disc} f = -400$, and $g(X) = X^4 - X^2 + 1$ with $\operatorname{disc} g = 144$. Factoring them over a few finite fields $\mathbb{F}_p$ produces the following results:

p	$X^4 - X^2 - 1$	$X^4 - X^2 + 1$
2	$(X^2 + X + 1)^2$	$(X^2 + X + 1)^2$
3	$X^4 - X^2 - 1$	$(X^2 + 1)^2$
5	$(X^2 + 2)^2$	$(X^2 + 2X - 1)(X^2 - 2X - 1)$
7	$X^4 - X^2 - 1$	$(X^2 + 2)(X^2 + 4)$
11	$(X + 2)(X - 2)(X^2 + 3)$	$(X^2 + 5X + 1)(X^2 - 5X + 1)$
13	$(X^2 + 2X + 8)(X^2 - 2X + 8)$	$(X + 2)(X + 6)(X + 7)(X + 11)$

The reduction modulo 7 shows that f is irreducible in $\mathbb{Z}[X]$. On the other hand, no matter how far we extend the calculations for g, we will not find any prime p for which g is irreducible modulo p. What is going on?

It is easy to see that the decomposition type $(1, 3)$ cannot occur for f or g. In fact, assume that $F(X) = r(X)s(X)$ splits into a linear factor r and a cubic factor s in $\mathbb{F}_p[X]$; writing $r(X) = X - a$ we see that $F(a) = 0$ in $\mathbb{F}_p$. But $F(X) = F(-X)$ for $F = f, g$, hence if they have a linear factor modulo p, then they actually must have two.

In order to show that the decomposition type (4) cannot occur for g we recall Dedekind's Theorem 5.5; since the splitting field of g is $\mathbb{Q}(\zeta_{12}) = \mathbb{Q}(i, \sqrt{-3}\,)$, and since there are no inert primes in biquadratic extensions, the decomposition type (4) cannot occur for g.

Our discussion so far suggests that decomposition types for a polynomial f are connected with the Galois group of f, which by definition is the Galois group of its splitting field. Numerical experiments suggest that primes with given decomposition type have a Dirichlet density, and that these densities do not depend on f but only on its Galois group.

For polynomials of degree 4, these experiments lead to the results in Table 14.1. The symbols in the left column of Table 14.1 denote the symmetric group of order 24, the alternating group of order 12, the dihedral group of order 8, Klein's four group and the cyclic group of order 4, respectively, and the other columns give the conjectured densities.

$\mathrm{Gal}\,(N/\mathbb{Q})$	(4)	$(1, 3)$	$(2, 2)$	$(1, 1, 2)$	$(1, 1, 1, 1)$
S_4	$\frac{1}{4}$	$\frac{1}{3}$	$\frac{1}{8}$	$\frac{1}{4}$	$\frac{1}{24}$
A_4	0	$\frac{2}{3}$	$\frac{1}{4}$	0	$\frac{1}{12}$
D_4	$\frac{1}{4}$	0	$\frac{3}{8}$	$\frac{1}{4}$	$\frac{1}{8}$
V_4	0	0	$\frac{3}{4}$	0	$\frac{1}{4}$
C_4	$\frac{1}{2}$	0	$\frac{1}{4}$	0	$\frac{1}{4}$

Table 14.1. Densities of Decomposition Types for Quartic Polynomials

Density of Primes

Is there a simple formula for these densities? Clearly the table suggests that the density of primes that split completely is the inverse of the order of the Galois group: $\frac{1}{\#G}$. But this is just Kronecker's density theorem, or rather its Corollary 8.3.

The entries for the abelian groups can be proved using Dirichlet's theorem, but the non-abelian cases seem quite mysterious. Since the densities seem to depend on the Galois group of f, it is quite natural to look for such a formula in invariants attached to this group.

The Classical Point of View. Let us first briefly discuss the classical approach. In Frobenius' times, Galois theory was a theory of Galois groups attached to polynomials; nowadays we think of Galois groups as being attached to field extensions. The connection is this: for a polynomial $f \in \mathbb{Q}[X]$ of degree n, let N denote its splitting field. The Galois group of f is, by definition, $G = \mathrm{Gal}\,(N/\mathbb{Q})$. This group G permutes the roots of the polynomial f, and thus can be interpreted as a subgroup of the permutation group S_n. Now permutations can be written as products of disjoint cycles: if $n = 4$, the permutation $(12)(34)$ switches the first and second, as well as the third and the fourth root, and is the product of two cycles of lenght 2; to this permutation we therefore attach the cycle pattern $(2, 2)$.

These cycle patterns attached to elements of G are, however, not the right ones: for understanding the decomposition types of polynomials mod p we have to consider the Galois group of the polynomial $\overline{f} \in \mathbb{F}_p[X]$, where $\overline{f}$ denotes the reduction of f mod p. The Frobenius automorphism permutes the roots of $\overline{f}$, and so each pair (f, p) determines a cycle pattern. Galois theory for finite fields predicts that the cycle pattern attached to (f, p) is the same as the decomposition type of f mod p.

Here comes

Theorem 14.1 (Frobenius Density Theorem I)**.** *The set of primes p for which an irreducible polynomial with Galois group G has a given decomposition type $(f_1, \ldots, f_g)$ has Dirichlet density $\frac{t}{n}$, where t is the number of elements $\sigma \in G$ with cycle pattern $(f_1, \ldots, f_g)$.*

As an example, consider the cyclic group C_4. It is generated by the permutation $\sigma = (1234)$, and we have $\sigma^2 = (13)(24)$, $\sigma^3 = (1432)$, and $\sigma^4 = (1)(2)(3)(4)$. Thus there are two elements (namely σ and σ^3) with cycle pattern (4), and one for each of the patterns $(2, 2)$ and $(1, 1, 1, 1)$.

The Modern Point of View. Now let us discuss the modern approach. Let f be an irreducible polynomial in $\mathbb{Z}[X]$, with splitting field N and Galois group $G = \mathrm{Gal}\,(N/\mathbb{Q})$. Any root α of the polynomial f determines a quartic number field $K = \mathbb{Q}(\alpha)$; let $N/\mathbb{Q}$ be the normal closure of $K/\mathbb{Q}$. Let H denote the subgroup of G whose fixed field is K.

Thus the polynomial f provides us with the fields K and N, and with the subgroup H of G. How do the primes p fit in? For every prime p that does not ramify in N, let $\mathfrak{P}$ denote a prime ideal in N above p, and let $\phi = \left[\frac{N/\mathbb{Q}}{\mathfrak{P}}\right]$ denote the associated Frobenius automorphism. The prime p determines ϕ only up to conjugates; in other words: p determines the conjugacy class $[\phi]$, which consists of all elements in G that are conjugate to ϕ, i.e., that have the form $\sigma^{-1}\phi\sigma$ for $\sigma \in G$.

We will now construct a cycle pattern attached to these purely group theoretical data. To this end we consider the coset decomposition

$$G = \sigma_1 H \cup \cdots \cup \sigma_k H$$

of G into disjoint left cosets modulo H. The Frobenius $\phi \in G$ permutes this decomposition by sending $\sigma_j H$ to $\phi\sigma_j H$. Each coset σH determines an orbit, which consists of the cosets

$$\sigma H, \phi\sigma H, \ldots, \phi^{t-1}\sigma H,$$

where t is the smallest positive integer for which $\phi^t\sigma H = \sigma H$. Clearly the cycle length t divides the order of the Frobenius.

Finally we partition G into orbits of cosets, and the lengths t_j of these orbits define a cycle pattern $(t_1, \ldots, t_g)$.

Example. Consider a normal extension $L/\mathbb{Q}$ with Galois group $G \simeq S_3 = \langle \rho, \tau : \rho^3 = \tau^2 = 1, \tau\rho\tau = \sigma^2 \rangle$. This group has order 6, and every element can be written uniquely in the form $\rho^a\tau^b$ with $a \in \{0,1,2\}$ and $b \in \{0,1\}$. The subgroup $H = \langle \tau \rangle$ fixes a nonnormal cubic subfield K of L, and the corresponding coset decomposition is $G = H \cup \rho H \cup \rho^2 H$.

If $\sigma = 1$, each cycle contains exactly one coset. If $\sigma = \rho$ of $\sigma = \rho^2$, there is one cycle consisting of all three cosets. If $\sigma = \tau$, then $\tau H = H$, $\tau\rho H = \{\tau\rho, \tau\rho\tau\} = \{\rho^2\tau, \rho^2\} = \rho^2 H$ and $\tau\rho^2 H = \rho H$. Thus the action of τ produces an orbit $\{H\}$ of cycle lenght 1, and an orbit $\{\rho H, \rho^2 H\}$ of cycle length 2.

We next address the question how the cycle pattern depends on ϕ.

Lemma 14.2. *The automorphisms ϕ and ϕ^k determine the same cycle pattern if* $\gcd(k,n) = 1$*, where n is the order of ϕ.*

Proof. If $\phi^t\sigma H = \sigma H$, then $(\phi^k)^t\sigma H = \sigma H$ (just apply ϕ^t repeatedly). Thus the cycle length of ϕ^k is $\le t$. But since ϕ is also a power of ϕ^k (this follows from $\gcd(k,n) = 1$ and Bezout), we also have the opposite inequality. □

Now we can show

Proposition 14.3. *Let n denote the order of ϕ. Then every automorphism of the form $\tau^{-1}\phi^k\tau$ with* $\gcd(k,n) = 1$ *produces the same cycle pattern.*

Proof. By Lemma 14.2, we may assume that $k = 1$, and claim that the cycle pattern produced by $\tau^{-1}\phi\tau$ is a permutation of the cycle pattern attached to ϕ. In fact, let t denote the cycle length of the cycle to which $\tau\sigma H$ belongs; then $\phi^t\tau\sigma H = \tau\sigma H$, hence $(\tau^{-1}\phi\tau)\sigma H = \tau^{-1}\phi^t\tau\sigma H = \sigma H$. □

This proposition suggests introducing the division $\mathrm{Div}(\phi)$ of an element $\phi \in G$: it is the set of all $\sigma \in G$ with the property that $\sigma = \tau^{-1}\phi^k\tau$ for some $\tau \in G$ and an exponent k coprime to the order of σ.

Example 1. If $G = \langle\phi\rangle$ has order 8, then

- $\mathrm{Div}(1) = \{1\}$;
- $\mathrm{Div}(\sigma) = \{\sigma, \sigma^3, \sigma^5, \sigma^7\}$;
- $\mathrm{Div}(\sigma^2) = \{\sigma^2, \sigma^6\}$;
- $\mathrm{Div}(\sigma^4) = \{\sigma^4\}$.

Example 2. If $G = \langle\phi\rangle$ is cyclic of p^2, then

- $\mathrm{Div}(1) = \{1\}$;
- $\mathrm{Div}(\sigma) = \{\sigma^k : \gcd(k,p) = 1\}$;
- $\mathrm{Div}\,/(\sigma^p) = \{\sigma^{kp} : \gcd(k,p) = 1\}$.

These are exactly the sets we came across in the proof of Cor. 8.8.

At this point it is not difficult to conjecture the following

Theorem 14.4 (Frobenius Density Theorem)**.** *Let L/K be a normal extension, and let D be a division in $G = \mathrm{Gal}\,(L/K)$. Let S denote the set of unramified prime ideals $\mathfrak{p}$ in K with the property that the prime ideals $\mathfrak{P}$ above $\mathfrak{p}$ in L satisfy $\left[\frac{L/K}{\mathfrak{P}}\right] \in D$. Then S has Dirichlet density*

$$\delta(S) = \frac{\#D}{\#G}.$$

The special case $D = \mathrm{Div}(1)$ gives us back Kronecker's density theorem, which will in fact be used in the proof of Theorem 14.4.

Corollary 14.5. *Let L/K be a cyclic extension of degree n. Then the set S of prime ideals $\mathfrak{p}$ in K that are inert in L/K has Dirichlet density $\delta(S) = \frac{\phi(n)}{n}$.*

Note that $\phi(n) > 1$ for $n > 2$, so for cyclic extensions of degree > 2 there are more inert primes than primes that split completely. If $n = p$ is prime, then $\phi(p) = p - 1$, and we get back Cor. 8.7.

A more general formulation is the following:

Corollary 14.6. *Let L/K be an abelian extension, and let $\sigma \in G =$ $\mathrm{Gal}\,(L/K)$ be an element with order n. Then the set*

$$S = \Big\{\mathfrak{p} \in \mathfrak{O}_K : \Big[\frac{L/K}{\mathfrak{P}}\Big] \in \mathrm{Div}(\sigma)\Big\}$$

has Dirichlet density $\delta(S) = \frac{\phi(n)}{\#G}$.

Proof. Since G is abelian, $\mathrm{Div}(\sigma)$ contains only the generators of $\langle\sigma\rangle$, and there are exactly $\phi(n)$ of them. □

Is the Frobenius Density Theorem the best we can hope for? Let L/K be a normal extension with Galois group $G = \mathrm{Gal}\,(L/K)$, and $\mathfrak{p} \nmid \mathrm{disc}\,(L/K)$ an unramified prime. For each prime ideal $\mathfrak{P}$ above $\mathfrak{p}$ we have the Frobenius automorphism $\big[\frac{L/K}{\mathfrak{P}}\big] \in G$. The question whether there exist infinitely many prime ideals $\mathfrak{p}$ with a given Frobenius does not make sense, however, because the Frobenius automorphism is determined by $\mathfrak{p}$ only up to conjugacy. We should therefore ask whether there are infinitely many prime ideals $\mathfrak{p}$ whose Frobenius automorphisms lie in some conjugacy class of G.

For $\sigma \in G$ let

$$[\sigma] = \{\tau \in G : \tau = \rho^{-1}\sigma\rho \text{ for some } \rho \in G\}$$

denote the conjugacy class of σ. The conjugacy class [1] of the unit element only consists of one element, namely the unit element 1; more generally, if G is abelian, then each conjugacy class only contains one element. If G is nonabelian, however, some conjugacy classes might be quite large.

The natural conjecture that generalizes Frobenius' theorem thus is

Theorem 14.7 (Chebotarev's Density Theorem)**.** *Let $K/\mathbb{Q}$ be a normal extension, and fix a $\sigma \in G = \mathrm{Gal}\,(K/\mathbb{Q})$. Let S denote the set of unramified primes p with the property that the prime ideals $\mathfrak{p}$ above p in K satisfy $\big[\frac{K/\mathbb{Q}}{\mathfrak{p}}\big] \in [\sigma]$. Then S has Dirichlet density*

$$\delta(S) = \frac{\#[\sigma]}{\#G}.$$

Since every division is a union of conjugacy classes, Chebotatev's result is stronger than that of Frobenius. It also contains Dirichlet's theorem as a special case: for $K = \mathbb{Q}(\zeta_m)$, it says that the primes p whose Frobenius automorphism $(\frac{K/\mathbb{Q}}{p})$ (we use the Artin symbol since the extension $K/\mathbb{Q}$ is abelian) lies in the conjugacy class of some σ_a (which consists of just σ_a), that is, the primes $p \equiv a \bmod m$, have Dirichlet density $\frac{1}{(K:\mathbb{Q})} = \frac{1}{\phi(m)}$.

Actually the Chebotarev density theorem can be seen as the common generalization of the density theorems of Frobenius and Dirichlet.

In this chapter we will prove the Frobenius density theorem; Chebotarev's result is most easily derived once we have Artin's reciprocity law at our disposal.

14.2 Group Theoretical Preliminaries

Let us start by recalling two basic definitions from group theory. The centralizer of an element $\sigma \in G$ is the subgroup $C_G(\sigma) = \{\tau \in G : \sigma\tau = \tau\sigma\}$ of all elements that commute with σ; the condition $\sigma\tau = \tau\sigma$ is equivalent to the vanishing of the commutator $[\sigma, \tau] = \sigma^{-1}\tau^{-1}\sigma\tau$. If H is a subgroup, we define $C_G(H) = \{\tau \in G : [\tau, \sigma] = 1 \text{ for all } \sigma \in H\}$.

The normalizer $N_G(H)$ of a subgroup H of G is defined as the subgroup $N_G(H) = \{\sigma \in G : \sigma H = H\sigma\}$. If $H = \langle\sigma\rangle$, then $C_G(\sigma) = N_G(H)$. In general, $C_G(H)$ is a normal subgroup of $N_G(H)$.

Lemma 14.8. *Let H be a subgroup of G; then $(G : N_G(H))$ is the number of different conjugates of H.*

Proof. Let $\Sigma = \{\tau^{-1}H\tau \mid \tau \in G\}$ denote the set of conjugates of H, and define a map $f : G \longrightarrow \Sigma$ by $f(\tau) = \tau^{-1}H\tau$. Then f is onto, and elements in the same coset modulo $N_G(H)$ have the same image:

$$\begin{aligned} \rho^{-1}H\rho = \tau^{-1}H\tau &\iff \tau\rho^{-1}H\rho\tau^{-1} \in H \\ &\iff \rho\tau^{-1} \in N_G(H) \\ &\iff \rho N_G(H) = \tau N_G(H). \end{aligned}$$

Thus f induces a bijection between the cosets of $G/N_G(H)$ and the elements of Σ. □

This result allows us to derive a formula for the number of elements in a division:

Lemma 14.9. *Let σ be an element of a group G, and let $H = \langle\sigma\rangle$. Then $\#\operatorname{Div}(\sigma) = \phi(n)(G : N_G(H))$.*

Proof. Consider the map $\psi : (\mathbb{Z}/n\mathbb{Z})^\times \times G/N_G(H) \longrightarrow \operatorname{Div}(\sigma\}$ defined by $\psi(m,\tau) = \tau^{-1}\sigma^m\tau$. Clearly ψ is surjective; it remains to show that it is injective. Assume therefore that $\psi(m,\tau) = \psi(k,\rho)$; this means $\tau^{-1}\sigma^m\tau = \rho^{-1}\sigma^k\rho$, hence $\rho\tau^{-1}\sigma^m\tau\rho^{-1} = \sigma^k$. But since both σ^m and σ^k generate H, this implies $\rho\tau^{-1}H\tau\rho^{-1} = H$, hence $\rho N_G(H) = \tau N_G(H)$. Thus we may assume that $\rho = \tau$, and then $m = k$ follows immediately. □

Unfortunately, this simple proof does not seem to work since the map ψ is not well defined.

todo: explain the proof by Janusz.

14.3 Prime Ideal Decomposition in Nonnormal Extensions

Let $K \subseteq F \subseteq L$ be a tower of number fields such that L/K is normal with Galois group G. Let $H = \operatorname{Gal}(L/F)$ be the subgroup of G associated to F, let $\mathfrak{P}$ be prime ideal in L, and set $\mathfrak{q} = \mathfrak{P} \cap F$ and $\mathfrak{p} = \mathfrak{P} \cap K$. In this section we will see how to compute the prime ideal decomposition of $\mathfrak{p}$ in F by using information about the Frobenius automorphism $\left[\frac{L/K}{\mathfrak{P}}\right]$ and the subgroup H of G.

$$\begin{tikzcd}
1 \arrow[d, dash] & L \arrow[d, dash] & \mathfrak{P} \arrow[d, dash] \\
H \arrow[d, dash] & F \arrow[d, dash] & \mathfrak{q} \arrow[d, dash] \\
G & K & \mathfrak{p}
\end{tikzcd}$$

Our next theorem will show that primes p with Frobenius $\left[\frac{L/\mathbb{Q}}{\mathfrak{P}}\right] = \tau$ (these primes have inertia degree 2 in L, hence split as $p\mathfrak{O}_L = \mathfrak{P}\mathfrak{P}'\mathfrak{P}''$) have decomposition $p\mathfrak{O}_K = \mathfrak{q}\mathfrak{q}'$, where $\mathfrak{q}$ is a prime ideal of degree 1 and $\mathfrak{q}'$ a prime ideal of degree 2.

Theorem 14.10. *Let $\mathfrak{P}$ be a prime ideal in $\mathfrak{O}_L$ above $\mathfrak{p}$ in $\mathfrak{O}_K$, and assume that $\mathfrak{P}$ is unramified over $\mathfrak{p}$. Let $\sigma = \left[\frac{L/K}{\mathfrak{P}}\right]$ be the Frobenius automorphism of $\mathfrak{P}$ over K, and assume that σ has cycles of length $t_1, \ldots, t_g$ when acting on the cosets of G/H. Then $\mathfrak{p}\mathfrak{O}_F = \mathfrak{q}_1 \cdots \mathfrak{q}_g$ for prime ideals $\mathfrak{q}_j = \sigma_j(\mathfrak{P}) \cap F$ with inertia degrees $f_j = t_j$.*

Proof. The $\mathfrak{q}_j$ clearly are prime ideals. We claim that they are distinct. Assume therefore that $\mathfrak{q}_i = \mathfrak{q}_j$; then $\sigma_i(\mathfrak{P})$ and $\sigma_j(\mathfrak{P})$ are two primes in L above $\mathfrak{q}_i$. Since H acts transitively on these primes, there is a $\tau \in H$ such that $\mathfrak{P}^{\sigma_j\tau} = \mathfrak{P}^{\sigma_i}$. But then $\sigma_j\tau\sigma_i^{-1} \in Z(\mathfrak{P}|\mathfrak{p})$. Since Z/T is cyclic and $\mathfrak{P}$ is unramified, we deduce that $Z(\mathfrak{P}|\mathfrak{p})$ is cyclic and generated by the Frobenius $\phi = \left[\frac{L/K}{\mathfrak{P}}\right]$. Thus $\sigma_j\tau\sigma_i^{-1} = \phi^k$ for some k, and this implies that $\sigma_j H = \phi^k\sigma_i H$. Thus $\sigma_j H$ and $\sigma_i H$ are in the same cycle, hence $i = j$.

Next we claim that $f_j = f(\mathfrak{q}_j|\mathfrak{p}) \geq t_j$. Assuming this for the moment, let us see why this implies equality: since t_j denotes the number of cosets of H in the j-th cycle, $t_1 + \ldots + t_g = (G : H)$; on the other hand, $f_1 + \ldots + f_g = (F : K)$, and Galois theory tells us $(G : H) = (F : K)$. But then $\sum t_j = \sum f_j$ implies that none of the inequalities $f_j \geq t_j$ can be strict.

For a proof of $f_j \geq t_j$, we fix $\mathfrak{q} = \mathfrak{P}_j$, and write $\sigma := \sigma_j$, $f = f_j$, and $t = t_j$; then we observe that $\left[\frac{L/F}{\mathfrak{P}}\right] = \phi^f$, hence $\left[\frac{L/F}{\mathfrak{P}^\sigma}\right] = \sigma^{-1}\left[\frac{L/F}{\mathfrak{P}}\right]\sigma = \sigma^{-1}\phi\sigma = \sigma^{-1}\phi^f\sigma$. But clearly $\left[\frac{L/F}{\mathfrak{P}^\sigma}\right] \in H$, and so $\sigma^{-1}\phi^f\sigma \in H$ as well. But this is equivalent to $\phi^f\sigma = \sigma H$, hence the cycle length t of σH divides f. □

This theorem immediately implies

Corollary 14.11. *The number of primes $\mathfrak{P}_F$ in F above $\mathfrak{p}$ with $f(\mathfrak{P}_F|\mathfrak{p}) = 1$ is equal to the number of cosets $H\sigma_j$ for which $\sigma_j^{-1}Z(\mathfrak{P}|\mathfrak{p})\sigma_j \in H$.*

Proof. In the proof of Thm. 14.10, $Z(\mathfrak{P}|\mathfrak{p}) = \langle\phi\rangle$, and $f(\mathfrak{q}|\mathfrak{p}) = 1$ was seen to be equivalent to $\sigma^{-1}\phi\sigma \in H$. Since ϕ generates the decomposition group, the claim follows. □

For the proof of the Frobenius density theorem we also will need the following

Lemma 14.12. *Let L/K be a Galois extension with Galois group G, and let $\mathfrak{p}$ be an unramified prime ideal in $\mathfrak{O}_K$. Then $\big[\frac{L/K}{\mathfrak{P}}\big] \in \operatorname{Div}(\sigma)$ for some $\mathfrak{P}$ above $\mathfrak{p}$ if and only if there is a prime ideal $\mathfrak{P}' \mid \mathfrak{p}$ such that $\big[\frac{L/K}{\mathfrak{P}'}\big]$ generates $\langle\sigma\rangle$.*

Proof. Assume that $\big[\frac{L/K}{\mathfrak{P}}\big] \in \operatorname{Div}(\sigma)$; then there is a $\tau \in G$ such that $\tau^{-1}\big[\frac{L/K}{\mathfrak{P}}\big]\tau = \sigma^m$ for some m coprime to the order n of σ. Now put $\mathfrak{P}' = \mathfrak{P}^\tau$ and observe that $\big[\frac{L/K}{\mathfrak{P}^\tau}\big] = \tau^{-1}\big[\frac{L/K}{\mathfrak{P}}\big]\tau$.

Conversely, assume that $\big[\frac{L/K}{\mathfrak{P}'}\big]$ generates $\langle\sigma\rangle$. Then $\big[\frac{L/K}{\mathfrak{P}'}\big] = \sigma^m$ for some m coprime to n, and this implies $\big[\frac{L/K}{\mathfrak{P}'}\big] \in \operatorname{Div}(\sigma)$. □

14.4 The Proof of Frobenius' Density Theorem

Consider the division $D = \operatorname{Div}(\sigma)$ for some $\sigma \in G$. We will prove the density theorem by induction on the order n of σ. If $n = 1$, then $\sigma = 1$, hence S is the set of primes that split completely in $K/\mathbb{Q}$. By Kronecker's density theorem, $\delta(S) = \frac{1}{\#G} = \frac{\#[1]}{\#G}$.

Now assume that σ has order $n > 1$, and that the theorem holds for all elements of order $d \mid n$. We introduce the following notation:

- $t_d = \#\operatorname{Div}(\sigma^d)$;
- S_d is the set of prime ideals $\mathfrak{p}$ unramified in L such that there is a $\mathfrak{P} \mid \mathfrak{p}$ in $\mathfrak{O}_L$ for which $\big[\frac{L/K}{\mathfrak{P}}\big]$ generates $\langle\sigma\rangle$.

By induction assumption we know $\delta(S_d) = \frac{t_d}{\#G}$ for all divisors $d \mid n$ with $d > 1$.

Now let $H = \langle\sigma\rangle$ and consider the fixed field F of H. Let S_F denote the set of primes $\mathfrak{P}_F$ with $f(\mathfrak{P}_F|\mathfrak{p}) = 1$.

Lemma 14.13. *We have $\mathfrak{p} \in S_d$ for some $d \mid n$ if and only if there is a prime $\mathfrak{P}_F \in S_F$ above $\mathfrak{p}$.*

Proof. Let $\mathfrak{P}$ be a prime above $\mathfrak{p}$ in L. By Cor 14.11, $\mathfrak{P}_F = \mathfrak{P} \cap F$ has inertia degree 1 over $\mathfrak{p}$ if and only if there is a $\tau \in H$ such that $\tau^{-1}Z(\mathfrak{P}|\mathfrak{p})\tau \subseteq H$. Now $\tau^{-1}Z(\mathfrak{P}|\mathfrak{p})\tau = Z(\mathfrak{P}^\tau|\mathfrak{p})$, so this condition is equivalent to the existence of a prime $\mathfrak{P}'$ above $\mathfrak{p}$ with $Z(\mathfrak{P}'|\mathfrak{p}) \subseteq H$. Since H is cyclic and generated by σ, we have $Z(\mathfrak{P}'|\mathfrak{p}) \subseteq H$ if and only if $Z(\mathfrak{P}'|\mathfrak{p}) = \sigma^d$ for some $d \mid n$ □

For $\mathfrak{p} \in S_d$ let $n(\mathfrak{p})$ denote the number of $\mathfrak{q} \in S_F$ above $\mathfrak{p}$. If $\mathfrak{q}$ is such a prime, then $f(\mathfrak{q}|\mathfrak{p}) = 1$, hence $N_{F/K}\mathfrak{q} = \mathfrak{p}$ and $N_{F/\mathbb{Q}}\mathfrak{q} = N_{K/\mathbb{Q}}\mathfrak{p}$. Since $\sum N\mathfrak{p}^{-s} \sim -\log(s-1)$ and since $\sum N\mathfrak{q}^{-s}$ is bounded for prime ideals $\mathfrak{q}$ outside of S_F, we deduce that $\sum_{\mathfrak{q}\in S_F} N\mathfrak{q}^{-s} \sim -\log(s-1)$.

Next

$$\sum_{\mathfrak{q}\in S_F} N\mathfrak{q}^{-s} \sim \sum_{d|n}\sum_{\mathfrak{p}\in S_d}\sum_{\mathfrak{q}|\mathfrak{p},\mathfrak{q}\in S_F} N\mathfrak{q}^{-s} = \sum_{d|n}\sum_{\mathfrak{p}\in S_d} n(\mathfrak{p})N\mathfrak{p}^{-s}.$$

Here $\sim$ comes from the fact that we had to throw out the finitely many ramified prime ideals above $\mathfrak{p}$.

Lemma 14.14. *Fix a prime ideal* $\mathfrak{p} \in S_d$. *Then*

$$n(\mathfrak{p}) = (N_G(\langle\sigma^d\rangle) : \langle\sigma\rangle).$$

Proof. We know that $n(\mathfrak{p})$ is the number of cosets τH such that $\sigma^d\tau H = \tau H$. This condition is equivalent to $\tau^{-1}\sigma^d\tau \in H = \langle\sigma\rangle$, and since H is cyclic, even to $\tau^{-1}\sigma^d\tau \in \langle\sigma^d\rangle$. But this is equivalent to $\tau \in N_G(\langle\sigma^d\rangle)$. □

This allows us to write

$$-\log(s-1) \sim \sum_{d|n}\sum_{\mathfrak{p}\in S_d} n(\mathfrak{p})N\mathfrak{p}^{-s} = \sum_{d|n}(N_G(\langle\sigma^d\rangle) : \langle\sigma\rangle)\sum_{\mathfrak{p}\in S_d} N\mathfrak{p}^{-s};$$

using the induction assumption this becomes

$$\begin{aligned}\sim -\Big(\sum_{1\neq d|n}\frac{(N_G(\langle\sigma^d\rangle) : \langle\sigma\rangle)t_d}{\#G}\Big)\log(s-1)\\ + (N_G(H) : H)\sum_{\mathfrak{p}\in S_1} N\mathfrak{p}^{-s}.\end{aligned}$$

But now $t_d = \phi(n/d)(G : N_G(\langle\sigma^d\rangle))$ and $t = \phi(n)(G : N_G(H))$, hence

$$\sum_{\mathfrak{p}\in S_1} N\mathfrak{p}^{-s} \sim \Big(-1 + \frac{1}{n}\sum_{1\neq d|n}\phi(n/d)\Big)\frac{nt}{\phi(n)\#G}\log(s-1).$$

Since $\sum_{d|n}\phi(d) = n$, the claim follows.

Notes

The section on the density of primes for which a polynomial has a given splitting behaviour owes much to the article [SL1996] by Lenstra & Stevenhagen.

Exercises

14.1 Derive Corollary 14.5 from the density theorem of Frobenius.

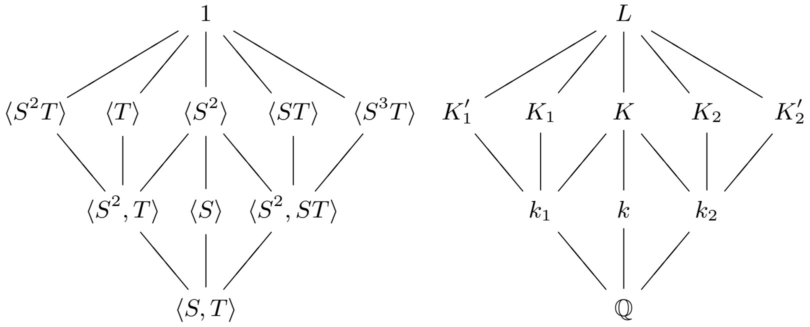
14.2 Generalize Cor. 8.8 to cyclic extensions of prime power degree p^n.

14.3 Prove directly that in a cyclic quartic extension $K/\mathbb{Q}$, inert primes have density $\frac{1}{2}$. (Hint: consider the inertia subfield).

14.4 Inside of S_4, consider the subgroup A_4 of even permutations. Show that A_4 contains $V_4 = \{(1)(2)(3)(4), (12)(34), (13)(24), (14)(23)\}$ as a (normal) subgroup, and that $A_4 \setminus V_4$ consist of the 8 elements of the form (abc). Compute the cycle patterns of these permutations, and use the classical version of the Frobenius density theorem to explain the entries for A_4 in Table 14.1.

14.5 Show that $N_G(H) = G$ if G is abelian.

14.6 Compute the divisions of $D_4 = \langle S, T \mid S^4 = T^2 = 1, TST = S^{-1} \rangle$, the dihedral group of order 8.



14.7 Let $L/\mathbb{Q}$ be a normal extension with Galois group $G \simeq D_4$. Discuss the possible factorizations of unramified primes p in L, and deduce how they split in the non-normal subfields K_1 and K_2 of degree 4.

14.8 Use Theorem 14.10 to prove that if a prime ideal $\mathfrak{p}$ splits completely in an extension L/K, then it also splits completely in the normal closure of L/K.

Part III

Takagi's Class Field Theory

15. Ideal Groups

Hilbert class field theory is a theory of abelian unramified extensions. Takagi showed that Hilbert's results can be generalized to give a similar description of *all* abelian extensions of a number field. In order to reach this goal he had to replace the ideal class groups in Hilbert's theory by bigger groups, namely Weber's generalized class groups.

We have already seen that the decomposition law in cyclotomic extensions is very similar to the one for Hilbert class fields; Takagi's class field theory is a generalization of both of these to arbitrary number fields.

15.1 Generalized Class Groups

Consider a number field K. A *modulus* is a formal product $\mathfrak{m} = \mathfrak{a}\infty_1 \ldots \infty_t$ of an integral ideal $\mathfrak{a}$ in $\mathfrak{O}_K$ and some real infinite places ∞_j corresponding to real embeddings $\sigma_j : K \longrightarrow \mathbb{R}$. We call $\mathfrak{m}_0 = \mathfrak{a}$ the finite, and $\mathfrak{m}_\infty = \infty_1 \ldots \infty_t$ the infinite part of $\mathfrak{m}$.

Next we introduce congruences modulo $\mathfrak{m}$. We write $\alpha \equiv 1 \bmod \mathfrak{a}$ if there exist $\beta, \gamma \in \mathfrak{O}_K$ with $\alpha = \beta/\gamma$ such that $(\beta, \mathfrak{a}) = (\gamma, \mathfrak{a}) = \mathcal{O}_K$ and $\beta \equiv \gamma \bmod \mathfrak{a}$. For a real infinite prime ∞_j we say that α is coprime to ∞_j if $\alpha \neq 0$, and that

$$\alpha \equiv \begin{cases} +1 \bmod \infty_j & \text{if } \sigma_j(\alpha) > 0, \\ -1 \bmod \infty_j & \text{if } \sigma_j(\alpha) < 0. \end{cases}$$

Thus the nonzero elements of $\mathfrak{O}_K$ (or of K) fall into two residue classes modulo ∞_j, and the map $\alpha \longmapsto \operatorname{sign}(\sigma_j(\alpha))$ induces an isomorphism

$$(\mathcal{O}_K/\infty_j)^\times \simeq \mathbb{Z}/2\mathbb{Z}$$

for every real infinite prime.

The classical Chinese Remainder Theorem states that if $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ are coprime ideals, then for all $\alpha_j \in \mathfrak{O}_K$ the system of linear congruences $\alpha \equiv \alpha_j \bmod \mathfrak{a}_j$ has a unique solution modulo $\mathfrak{a} = \mathfrak{a}_1 \cdots \mathfrak{a}_r$. This can be extended to include congruences modulo infinite primes:

Proposition 15.1 (Chinese Remainder Theorem)**.** *Let $\mathfrak{a}$ be an integral ideal and $\varepsilon_1, \ldots, \varepsilon_t \in \{\pm 1\}$; then for any $\beta \in \mathfrak{O}_K$ there exists an $\alpha \in \mathfrak{O}_K$ such* *that $\alpha \equiv \beta \bmod \mathfrak{a}$ and $\alpha \equiv \varepsilon_j \bmod \infty_j$ for all $j = 1, 2, \ldots, t$. In particular, for $\mathfrak{m} = \mathfrak{a}\infty_1 \cdots \infty_t$ we have*

$$(\mathcal{O}_K/\mathfrak{m})^\times = (\mathcal{O}_K/\mathfrak{a})^\times \times \prod_{j=1}^{t} (\mathcal{O}_K/\infty_j)^\times,$$

and so Euler's phi function defined by $\Phi(m) := \#(\mathfrak{O}_K/\mathfrak{m})^\times$ has the value $\Phi(\mathfrak{m}) = 2^t\Phi(\mathfrak{a})$.

Imitating the classical proofs shows that $\Phi(\mathfrak{p}^n) = (N\mathfrak{p} - 1)(N\mathfrak{p})^{n-1}$, and the classical Chinese Remainder Theorem shows that $\Phi(\mathfrak{a}\mathfrak{b}) = \Phi(\mathfrak{a})\Phi(\mathfrak{b})$ for coprime ideals $\mathfrak{a}, \mathfrak{b}$.

For the reduction to the classical Chinese Remainder Theorem we use the following

Lemma 15.2. *Let K be an algebraic number field; let $\sigma_1, \ldots, \sigma_r$ denote the r real, and $\sigma_{r+1}, \ldots, \sigma_{r+2s}$ the complex embeddings ordered in such a way that σ_{r+s+j} is the complex conjugate of σ_{r+j}.*

Given some $\varepsilon > 0$ any set of numbers $\gamma_1, \ldots, \gamma_r \in \mathbb{R}$ and $\gamma_{r+1}, \ldots, \gamma_{r+s} \in \mathbb{C}$ there exists $\alpha \in K$ such that $|\sigma_j(\alpha) - \gamma_j| < \varepsilon$ for all $1 \le j \le r + s$.

Proof. Let $\alpha_1, \ldots, \alpha_n$ be a $\mathbb{Q}$-basis of K. Then the system of linear equations

$$\gamma_j = \sum_{i=1}^{n} x_i \alpha_i^{(j)}$$

has a unique solution since its determinant is the discriminant of the α_j, which is nonzero since they form a basis of K. Taking complex conjugates shows immediately that the x_j are all real. Since linear functions are continuous, we can find rational numbers a_i sufficiently close to x_j such that

$$\Big| \sum_{i=1}^{n} a_i \alpha_i^{(j)} - \gamma_j \Big| < \varepsilon,$$

hence $\alpha = \sum_{i=1}^{n} a_i \alpha_i^{(j)}$ is an element of K with the desired properties. □

In particular we can find $\alpha \in K$ with given signature (the signature of $\alpha \in K$ is the vector $(\operatorname{sign}(\sigma_1\alpha), \ldots, \operatorname{sign}(\sigma_r\alpha))$ giving the signs of the r real conjugates of α): given $\varepsilon_1, \ldots, \varepsilon_r = \pm 1$, simply put $\gamma_j = \varepsilon_j$ for $j = 1, \ldots, r$ and choose the γ_j with $j > r$ arbitrarily (but nonzero). Since multiplication by a natrual number $n > 0$ does not change the signature, this implies

Corollary 15.3. *There exist $\alpha \in \mathfrak{O}_K$ with given signature.*

Now we can give the

Proof of Prop. 15.1. Choose $\gamma \in \mathfrak{O}_K$ such that $\gamma \equiv \varepsilon_j \bmod \infty_j$, and let $a = N\mathfrak{a}$ denote the norm of $\mathfrak{a}$. Then consider $\alpha = \beta + na\gamma$ for $n \in \mathbb{N}$. If n is large enough, α and $na\gamma$ will have the same signature, hence $\alpha \equiv \varepsilon_j \bmod \infty_j$. Moreover, we clearly have $\alpha \equiv \beta \bmod \mathfrak{a}$ since $a \equiv 0 \bmod \mathfrak{a}$. This implies the first claim.

The natural projection sending

$$\alpha \bmod \mathfrak{m} \longmapsto (\alpha \bmod \mathfrak{m}_0, \alpha \bmod \infty_1, \ldots, \alpha \bmod \infty_t)$$

is clearly a group homomorphism, and by what we have shown it is surjective. The kernel consists of all residue classes $\alpha \bmod \mathfrak{m}$ such that $\alpha \equiv 1 \bmod \mathfrak{a}$ and $\alpha \equiv 1 \bmod \infty_j$; the only such residue class is, by definition(!), the residue class $1 \bmod \mathfrak{a}\infty_1 \cdots \infty_t$. □

Using these congruences we can define the following multiplicative groups of ideals:

$$\begin{aligned} D\{\mathfrak{m}\} &= \{\mathfrak{a} \in I_K : \mathfrak{a} + \mathfrak{m}_0 = \mathcal{O}_K\}, \\ H\{\mathfrak{m}\} &= \{\mathfrak{a} \in D\{\mathfrak{m}\} : \mathfrak{a} = \alpha\mathcal{O}_K\}, \\ H^{(1)}\{\mathfrak{m}\} &= \{\mathfrak{a} \in H\{\mathfrak{m}\} : \mathfrak{a} = \alpha\mathcal{O}_K \text{ for some } \alpha \equiv 1 \bmod \mathfrak{m}\}. \end{aligned}$$

Thus $D\{\mathfrak{m}\}$ is the group of all ideals coprime to $\mathfrak{m}$, $H\{\mathfrak{m}\}$ its subgroup of principal ideals coprime to $\mathfrak{m}$, and $H^{(1)}\{\mathfrak{m}\}$ the group of principal ideals generated by elements $\equiv 1 \bmod \mathfrak{m}$.

If we need to express the reference to the base field K, we write $D_K\{\mathfrak{m}\}$ instead of $D\{\mathfrak{m}\}$ etc. The factor group $\mathrm{Cl}_K\{\mathfrak{m}\} = D\{\mathfrak{m}\}/H^{(1)}\{\mathfrak{m}\}$ is called the *ray class group* modulo $\mathfrak{m}$ of K. For any group H with $H^{(1)}\{\mathfrak{m}\} \subseteq H \subseteq D\{\mathfrak{m}\}$ we call $I = H/H^{(1)}\{\mathfrak{m}\}$ a *generalized class group.*

Some special cases of such groups are well known to us:

- $D\{(1)\}$ is the group of fractional ideals in K, $H\{(1)\}$ is the group of all fractional principal ideals, and $\mathrm{Cl}_K\{(1)\} = \mathrm{Cl}(K)$ is the class group of K in the usual (wide) sense.
- $D\{(\infty)\} = D\{(1)\}$, but $H\{(\infty)\}$ is the subgroup of principal ideals in the strict sense, and $\mathrm{Cl}_K\{\infty\} = \mathrm{Cl}^+(K)$ is the class group of K in the strict (narrow) sense.
- $\mathrm{Cl}_\mathbb{Q}\{(m)\} \simeq (\mathbb{Z}/m\mathbb{Z})^\times/\{\pm 1\}$;
- $\mathrm{Cl}_\mathbb{Q}\{m\infty\} \simeq (\mathbb{Z}/m\mathbb{Z})^\times$.

Our first aim is to show that the usual ideal class group is contained in $\mathrm{Cl}_K\{\mathfrak{m}\}$ as a factor group; to this end we need

Lemma 15.4. *Let $\mathfrak{m}$ be an integral ideal in $\mathfrak{O}_K$. Then any ideal class in* $\mathrm{Cl}(K)$ *contains an ideal coprime to $\mathfrak{m}$.*

Proof. Let $c^{-1} = [\mathfrak{a}]$, and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ be the prime ideals occurring in the factorization of $\mathfrak{a}\mathfrak{m}$, and write $\mathfrak{a} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_t^{a_t}$. Pick elements $\alpha_i \in \mathfrak{p}_i^{a_i} \setminus \mathfrak{p}_i^{a_i+1}$, and use the Chinese Remainder Theorem to find an $\alpha \in \mathfrak{O}_K$ with $\alpha \equiv \alpha_i \bmod \mathfrak{p}_i^{a_i+1}$ for $i = 1, \ldots, t$. Then $(\alpha) = \mathfrak{a}\mathfrak{c}$ for some integral ideal $\mathfrak{c}$ coprime to $\mathfrak{b}$ (in fact, the exponent of $\mathfrak{p}_i$ in (α) and $\mathfrak{a}$ is the same, hence no $\mathfrak{p}_i$ can divide $\mathfrak{c}$). Since $\mathfrak{c} \in [\mathfrak{a}]^{-1} = c$, this proves our claim. □

Now we get

Proposition 15.5. *For every modulus* $\mathfrak{m}$*, there is an exact sequence*

$$1 \longrightarrow H\{\mathfrak{m}\} \longrightarrow D\{\mathfrak{m}\} \xrightarrow{\phi} \mathrm{Cl}(K) \longrightarrow 1.$$

Proof. Let $\mathfrak{a}$ be an ideal coprime to $\mathfrak{m}$, and set $\phi(\mathfrak{a}) = [\mathfrak{a}] \in \mathrm{Cl}(K)$. This is a group homomorphism with kernel $H\{\mathfrak{m}\}$, and it is surjective by Lemma 15.4: given any ideal class $c \in \mathrm{Cl}(K)$ there is an ideal $\mathfrak{b} \in c$ coprime to $\mathfrak{m}_0$; clearly $c = \phi(\mathfrak{b})$. □

Since ϕ is trivial on $H^{(1)}\{\mathfrak{m}\}$ and $D\{\mathfrak{m}\}/H^{(1)}\{\mathfrak{m}\} = \mathrm{Cl}_K\{\mathfrak{m}\}$, the exact sequence in Proposition 15.5 can be written as

$$1 \longrightarrow H\{\mathfrak{m}\}/H^{(1)}\{\mathfrak{m}\} \longrightarrow \mathrm{Cl}_K\{\mathfrak{m}\} \longrightarrow \mathrm{Cl}(K) \longrightarrow 1.$$

In particular this shows that the class group is a factor group of the ray class group for every choice of $\mathfrak{m}$.

Now we turn to the factor group $H\{\mathfrak{m}\}/H^{(1)}\{\mathfrak{m}\}$; let E denote the unit group of $\mathcal{O}_K$, and $E_{\mathfrak{m}}^{(1)}$ its subgroup consisting of all units $\varepsilon \equiv 1 \bmod \mathfrak{m}$.

Proposition 15.6. *For every modulus* $\mathfrak{m}$*, there is an exact sequence*

$$1 \longrightarrow E/E_{\mathfrak{m}}^{(1)} \longrightarrow (\mathcal{O}_K/\mathfrak{m})^\times \xrightarrow{\psi} H\{\mathfrak{m}\}/H^{(1)}\{\mathfrak{m}\} \longrightarrow 1.$$

Proof. Define ψ by mapping $\alpha \bmod \mathfrak{m}$ to the ideal class $(\alpha)H^{(1)}\{\mathfrak{m}\}$. Then $\ker\psi$ consists of all classes $\beta \bmod \mathfrak{m}$ such that $(\beta) = (\alpha)$ for some $\alpha \equiv 1 \bmod \mathfrak{m}$, that is, of all β for which there is a unit $\varepsilon \in E_k$ such that $\beta\varepsilon^{-1} = \alpha$ and $\alpha \equiv 1 \bmod \mathfrak{m}$. In particular, $\beta \equiv \varepsilon \bmod \mathfrak{m}$, and we see that the kernel consists of residue classes generated by units, that is, of the image of the unit group E under the homomorphism $E \longrightarrow (\mathcal{O}_K/\mathfrak{m})^\times$ which maps a unit ε to its residue class modulo $\mathfrak{m}$. The other exactness assertions follow just as easily. □

Note that $\mathrm{Cl}\{\mathfrak{m}\}$ is a group extension of $\mathrm{Cl}(K)$ by $(\mathcal{O}_K/\mathfrak{m})^\times/(E/E_{\mathfrak{m}}^{(1)})$, that is, there is an exact sequence

$$1 \longrightarrow (\mathcal{O}_K/\mathfrak{m})^\times/(E/E_{\mathfrak{m}}^{(1)}) \longrightarrow \mathrm{Cl}\{\mathfrak{m}\} \longrightarrow \mathrm{Cl}(K) \longrightarrow 1$$

found by combining the preceding two exact sequences. Since both $(\mathcal{O}_K/\mathfrak{m})^\times$ and $\mathrm{Cl}(K)$ are finite, so is the ray class group $\mathrm{Cl}\{\mathfrak{m}\}$, and the ray class number $h_K\{\mathfrak{m}\} := \#\,\mathrm{Cl}_K\{\mathfrak{m}\}$ is given by the formula

$$h_K\{\mathfrak{m}\} = h(K)\frac{\Phi(\mathfrak{m})}{(E : E_{\mathfrak{m}}^{(1)})}.$$

Examples of computations of ray class numbers are given in Exercise 3.

15.2 Takagi's Class Field Theory

To any finite extension L/K of number fields and any modulus $\mathfrak{m}$ in K we can associate the ideal group

$$\begin{aligned} H_{L/K}\{\mathfrak{m}\} &= \{\mathfrak{a} \in D_K\{\mathfrak{m}\} : \mathfrak{a} = (\alpha) N_{L/K}\mathfrak{A} \\ &\qquad\qquad \text{for } \mathfrak{A} \in D_L\{\mathfrak{m}\} \text{ and } \alpha \equiv 1 \bmod \mathfrak{m}\} \\ &= N_{L/K} D_L\{\mathfrak{m}\} \cdot H^{(1)}\{\mathfrak{m}\}. \end{aligned}$$

Thus the ideal group attached to an extension L/K and some modulus $\mathfrak{m}$ consists of products of norms from ideals in L coprime to $\mathfrak{m}$ and principal ideals generated by elements $\alpha \equiv 1 \bmod \mathfrak{m}$. Clearly

$$H_K^{(1)}\{\mathfrak{m}\} \subseteq H_{L/K}\{\mathfrak{m}\} \subseteq D_K\{\mathfrak{m}\},$$

so $H_{L/K}\{\mathfrak{m}\}$ is sandwiched between the ideal groups $H_K^{(1)}\{\mathfrak{m}\}$ and $D_K\{\mathfrak{m}\}$; in particular, it has finite index $h\{\mathfrak{m}\} = (D_K\{\mathfrak{m}\} : H_{L/K}\{\mathfrak{m}\})$. The corresponding class group $I_{L/K}\{\mathfrak{m}\} = H_{L/K}\{\mathfrak{m}\}/H_K^{(1)}\{\mathfrak{m}\}$ is called the ideal class group associated to L/K and $\mathfrak{m}$.

Examples. Consider any quadratic extension $K = \mathbb{Q}(\sqrt{d}\,)$ of the base field $k = \mathbb{Q}$, and the modulus $\mathfrak{m} = (4)$. Then $D\{\mathfrak{m}\} = \{(a) : a \equiv 1 \bmod 2\} = \{(a) : a \equiv 1 \bmod 4\} = H^{(1)}\{\mathfrak{m}\}$, so $H^{(1)}\{\mathfrak{m}\} \subseteq H_{K/\mathbb{Q}}\{\mathfrak{m}\} \subseteq D\{\mathfrak{m}\}$ implies in particular that $H_{K/\mathbb{Q}}\{\mathfrak{m}\} = D\{\mathfrak{m}\}$. In particular, $h_{K/\mathbb{Q}}\{\mathfrak{m}\} = 1$ for this choice of $\mathfrak{m}$.

Proposition 15.7. *Let $K = \mathbb{Q}(\sqrt{d}\,)$ be a complex quadratic number field with discriminant d. We claim that $h_{K/\mathbb{Q}}\{\mathfrak{m}\} = 2$ for $\mathfrak{m} = d\infty$.*

Proof. □

Let us now sketch the main content of Takagi's class field theory. Using analytic methods, we will prove

Theorem 15.8 (First Inequality)**.** *For every finite extension L/K of number fields and any modulus $\mathfrak{m}$, we have the inequality*

$$h_{L/K}\{\mathfrak{m}\} = (\mathrm{Cl}_K\{\mathfrak{m}\} : I_{L/K}\{\mathfrak{m}\}) \leq (L : K). \tag{15.1}$$

Moreover, equality implies that L/K is normal.

An extension L of K is called a *class field* of K to the ideal group $H_{L/K}\{\mathfrak{m}\}$ if the first inequality is an equality; in this case, $\mathfrak{m}$ is called a *defining modulus* for L/K. If $\mathfrak{m}$ is a defining modulus for L/K, then so is any multiple of $\mathfrak{m}$. If $\mathfrak{m}_1$ and $\mathfrak{m}_2$ are defining moduli for L/K, then so is their greatest common divisor; hence there always exists a smallest defining modulus $\mathfrak{f}_{L/K}$, which we will call the *conductor* of L/K.

A few simple examples of class fields over $\mathbb{Q}$ can be given right away:

- Quadratic fields $L = \mathbb{Q}(\sqrt{d}\,)$ with discriminant d are class fields of $K = \mathbb{Q}$ with defining modulus d or $|d|\infty$ according as L is real or complex. Suppose for simplicity that $d > 0$; we have to show that $I_{L/\mathbb{Q}}\{d\}$ has index 2 in $(\mathbb{Z}/d\mathbb{Z})^\times$, and in view of the first inequality it is sufficient to prove that this index is at least 2. This will be accomplished by showing that if (a) is the norm of an ideal in $D_L\{d\}$, then $a \equiv \pm x^2 \bmod d$ for some $x \in \mathbb{Z}$. It is clearly sufficient to prove this for prime values $a = p$, and in this case it follows at once from the quadratic reciprocity law and the fact that p splits if and only if $(d/p) = +1$.
  Note that the occurrence of the quadratic reciprocity law comes as no surprise since we used the decomposition law for Kummer extensions $L/\mathbb{Q}$ in order to show that L is a class field.
- $L = \mathbb{Q}(\zeta_m)$ is a class field with defining modulus $m\infty$: in fact, this follows if we can prove that $I_{L/\mathbb{Q}}\{m\infty\} = 1$, since $\mathrm{Cl}_{\mathbb{Q}}\{m\infty\} \simeq (\mathbb{Z}/m\mathbb{Z})^\times$ by Exercise 1 and hence $(\mathrm{Cl}_{\mathbb{Q}}\{m\infty\} : I_{L/\mathbb{Q}}\{m\infty\}) = \phi(m) = (L : \mathbb{Q})$.
  But $N_{L/\mathbb{Q}}\mathfrak{a}$ is the product of ideals $N_{L/\mathbb{Q}}\,\mathfrak{p} = (p^f)$, where $p > 0$ is a prime and f is defined as the smallest positive integer such that $p^f \equiv 1 \bmod m$. In particular, the ideals $N_{L/\mathbb{Q}}\,\mathfrak{p}$ are generated by integers $\equiv 1 \bmod m\infty$, and this shows that $N_{L/\mathbb{Q}}D_L\{m\infty\} \subset H_{\mathbb{Q}}^{(1)}\{m\infty\}$. Thus $H_{L/\mathbb{Q}}\{m\infty\} = N_{L/\mathbb{Q}}D_L\{m\infty\} \cdot H_{\mathbb{Q}}^{(1)}\{m\infty\} = H_{\mathbb{Q}}^{(1)}\{m\infty\}$, and our claim is proved.
- $L = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ is a class field with defining modulus (m): a similar analysis as above immediately shows that $N_{L/\mathbb{Q}}D_L\{(m)\}$ consists only of ideals generated by positive integers $a \equiv \pm 1 \bmod m$; replacing a by $-a$ if necessary we see that $N_{L/\mathbb{Q}}D_L\{(m)\} \subseteq H_{\mathbb{Q}}^{(1)}\{m\}$, and our claim follows as above by invoking Exercise 1.
- for a quadratic number field $K = \mathbb{Q}(\sqrt{d}\,)$, its genus field $L = K_{\text{gen}}^+ = \mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_t}\,)$ is a class field for defining modulus ∞; more exactly we have $I_{L/K,\infty} = \mathrm{Cl}^+(K)^2$. Here we have to compute the norms of ideals in $\mathcal{O}_L$ to $\mathcal{O}_K$. Again it is sufficient to do this for prime ideals; thus let $\mathfrak{P}$ be a prime ideal in $\mathcal{O}_L$ above the prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$. Then we know that

$$\begin{aligned} N_{L/K}\mathfrak{P} = \mathfrak{p} \quad &\Longleftrightarrow \quad \mathfrak{p} \text{ splits completely in } L/K \\ &\Longleftrightarrow \quad [\mathfrak{p}] \text{ is in the principal genus} \\ &\Longleftrightarrow \quad [\mathfrak{p}] \in \mathrm{Cl}^+(K)^2. \end{aligned}$$

  This shows that $N_{L/K}\mathfrak{A} = \mathfrak{a}$ implies $[\mathfrak{a}] \in \mathrm{Cl}^+(K)^2$, hence we have the inclusion $I_{L/K,\infty} \subseteq \mathrm{Cl}^+(K)^2$, and we can conclude that

$$(\mathrm{Cl}_K\{\infty\} : I_{L/K}\{\infty\}) = (\mathrm{Cl}_K\{\infty\} : \mathrm{Cl}^+(K)^2)(\mathrm{Cl}^+(K)^2 : I_{L/K,\infty}).$$

  Since $\mathrm{Cl}_K\{\infty\} = \mathrm{Cl}^+(K)$, this implies

$$(\mathrm{Cl}_K\{\infty\} : I_{L/K}\{\infty\}) \geq \#\,\mathrm{Cl}_{\text{gen}}^+(K) = (L : K),$$

  and our claim follows from the First Inequality.

> Observe that the First Inequality in this example reduces to the first inequality of genus theory. The same is true for the Second Inequality of class field theory mentioned below. What this means is that the fundamental inequalities of class field theory have their roots in Gauss's Disquisitiones Arithmeticae!

Takagi's definition of a class field differs slightly from ours since he had to assume that L/K is normal; Hasse & Scholz have shown that one can do without the assumption of normality (the proof of the First Inequality that we have sketched above is theirs), and they also simplified the structure of Takagi's proof. In fact they noticed that a completely elementary index calculation sufficed to deduce the following corollary from Theorem 15.8:

Corollary 15.9. *If L is a class field of K, then, for each field F with $K \subseteq F \subseteq L$, F is a class field of K and L is a class field of F.*

Another direct consequence of the First Inequality is

Theorem 15.10 (Uniqueness Theorem)**.** *If a class field L to the ideal group $H_{L/K}\{\mathfrak{m}\}$ exists, then L is unique.*

A generalization of the Uniqueness Theorem is the following result that shows that there is a kind of Galois correspondence between ideal groups defined modulo $\mathfrak{m}$ and the corresponding class fields:

Theorem 15.11 (Correspondence Theorem)**.** *Assume that L and L' are class fields for the ideal groups H and H' defined modulo some $\mathfrak{m}$, respectively. Then $L \subseteq L'$ if and only if $H \supseteq H'$. Moreover, $\mathfrak{m}$ is a defining modulus for LL' and $L \cap L'$, and we have $I_{LL'}\{\mathfrak{m}\} = I_L\{\mathfrak{m}\} \cap I_{L'}\{\mathfrak{m}\}$ and $I_{L\cap L'}\{\mathfrak{m}\} = I_L\{\mathfrak{m}\} \cdot I_{L'}\{\mathfrak{m}\}$.*

Here we come across one of the unpleasant drawbacks of Takagi's class field theory: if L_1 is class field for an ideal group defined modulo $\mathfrak{m}_1$, and L_2 for a group defined modulo $\mathfrak{m}_2$, then we can check whether $L_1 \subseteq L_2$ only after realizing L_1 and L_2 as class groups defined modulo a common defining modulus $\mathfrak{m}$ (we can take e.g. $\mathfrak{m} = \mathfrak{m}_1\mathfrak{m}_2$; in fact, the lowest common multiple will do). Moreover, there is no bijection between abelian extensions of K and generalized class groups unless we identify class groups in the same way as we identify the subgroup $\{1 + 8\mathbb{Z}, 5 + 8\mathbb{Z}\}$ of $(\mathbb{Z}/8\mathbb{Z})^\times$ with the subgroup $\{1 + 4\mathbb{Z}\}$ of $(\mathbb{Z}/4\mathbb{Z})^\times$. The technical difficulties connected with the change of defining moduli vanished into thin air with Chevalley's introduction of idèles into class field theory.

After having proved the first inequality, the next step is to show that abelian fields are class fields. In Takagi's proof, this is first done only for cyclic extensions:

Theorem 15.12 (Second Inequality)**.** *If L/K is a cyclic extension, then there exists a modulus $\mathfrak{m}$ such that $(\mathrm{Cl}_K\{\mathfrak{m}\} : I_{L/K}\{\mathfrak{m}\}) \geq (L : K)$.*

In particular, cyclic extensions of number fields are class fields.

Theorem 15.13 (Existence Theorem). *Let $\mathfrak{m}$ be a modulus; then for every subgroup $I_{\mathfrak{m}}$ of $\mathrm{Cl}_K\{\mathfrak{m}\}$ there exists a unique abelian extension L/K such that*
i) $\mathfrak{m}$ is a defining modulus for L/K;
ii) $I_{\mathfrak{m}} = I_{L/K}\{\mathfrak{m}\}$.

The abelian extension L of K with the properties *i*) and *ii*) above is called the *class field* for the ideal class group $I_{\mathfrak{m}}$.

From Corollary 15.9 we can immediately deduce that if L is a class field of K, then every subgroup of $\mathrm{Gal}\,(L/K)$ is normal. Unfortunately, this does not suffice to prove that $\mathrm{Gal}\,(L/K)$ is abelian since e.g. the quaternion group of order 8 shares this property with abelian groups. On the other hand, Hasse & Scholz have shown that this property, together with the Correspondence Theorem, is strong enough to imply the desired property:

Theorem 15.14 (Class Fields are Abelian). *Let L be the class field for the subgroup $I_{\mathfrak{m}}$ of $\mathrm{Cl}_K\{\mathfrak{m}\}$; then L/K is abelian, and*

$$\mathrm{Gal}\,(L/K) \simeq \mathrm{Cl}_K\{\mathfrak{m}\}/I_{L/K}\{\mathfrak{m}\} = D_K\{\mathfrak{m}\}/H_{L/K}\{\mathfrak{m}\}.$$

If $I_{L/K}\{\mathfrak{m}\} = \{1\}$, then the corresponding class field is called the *ray class field* of K modulo $\mathfrak{m}$. In the examples of class fields we have given above we have seen that $\mathbb{Q}(\zeta_m)$ and $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$ are ray class fields of $\mathbb{Q}$ modulo $m\infty$ and m, respectively. The ray class fields modulo $\mathfrak{m} = (1)$ or $\mathfrak{m} = \infty$ are called the *Hilbert class field* of K in the usual (wide) and strict (narrow) sense, respectively; they will be denoted by K^1 and K^1_+. The fact that the ray class field modulo (1) is unramified follows from

Theorem 15.15 (Ramification Theorem). *A prime ideal $\mathfrak{p}$ ramifies in an abelian extension L/K if and only if $\mathfrak{p}$ divides the conductor $\mathfrak{f}_{L/K}$.*

This shows that the ray class field modulo (1) is an abelian and unramified extension; moreover, it is the maximal extension of K with these properties because of

Theorem 15.16 (Completeness Theorem). *Every finite abelian extension L/K is contained in the ray class field modulo $\mathfrak{m}$ for some suitable defining modulus $\mathfrak{m}$. The minimal defining modulus with this property is exactly the conductor of L/K.*

We also note that the Ramification Theorem implies that, for squarefree $m \in \mathbb{N}$, the ray class field $\mathbb{Q}\{m\} = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ has conductor m (since each prime dividing m is ramified) and that $\mathbb{Q}\{m\infty\} = \mathbb{Q}(\zeta_m)$ has conductor $m\infty$. Actually, this holds under the weaker assumption that $m \not\equiv 2 \bmod 4$, but one has to work harder then.

Theorem 15.17 (Abelian Fields are Class Fields). *Every abelian extension L of a number field K is a class field of K for some suitable ideal group $H_{L/K}\{\mathfrak{m}\}$.*

This is the theorem that Takagi could hardly believe even after he had proved it: he spent a long time looking for the mistake before he decided that his results are correct and published his results. The following theorem shows how unramified prime ideals split in class fields (and finally proves that Weber's and Takagi's definitions of class fields are equivalent). A slightly more complicated result holds for ramified prime ideals.

Theorem 15.18 (Decomposition Law)**.** *Let L be the class field for the ideal group $H_{L/K}\{\mathfrak{m}\}$ and let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$ not dividing $\mathfrak{m}$; if $\mathfrak{p}^f$ is the smallest power of the prime ideal $\mathfrak{p}$ that is contained in $H_{L/K}\{\mathfrak{m}\}$, then $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_g$ with $fg = (L:K)$.*

As an application, consider the field $L = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$; here $H_{L/\mathbb{Q}}\{m\} = \{a + m\mathbb{Z} : a \equiv 1 \bmod m\}$, and according to the Decomposition Law, the inertia degree f of a prime number $p \nmid m$ is the smallest integer $f \geq 1$ such that $p^f \equiv \pm 1 \bmod m$.

Our next result is the "Verschiebungssatz", sometimes also called elevator theorem:

Theorem 15.19 (Translation Theorem)**.** *Let L/K be a finite abelian extension of number fields with defining modulus $\mathfrak{m}$. Then for any finite extension F/K, the abelian extension LF/F has defining modulus $\mathfrak{m}$, and LF is the class field of F for the class group*

$$I_{LF/F}\{\mathfrak{m}\} = \{c \in \mathrm{Cl}_F\{\mathfrak{m}\} : N_{L/K}c \in I_{L/K}\{\mathfrak{m}\}\}.$$

The translation theorem has a very useful corollary:

Corollary 15.20. *For any finite extension L/K of number fields, we have*

$$(\mathrm{Cl}(K) : N_{L/K}\,\mathrm{Cl}(L)) \ = \ (L \cap K^1 : K).$$

Proof. Clearly, K^1L/L is an unramified abelian extension, and by Galois theory it has degree $(K^1L : L) = (K^1 : L \cap K^1)$. By the translation theorem, the extension is the class field to the class group

$$I_{K^1L/L}\{(1)\} \ = \ \{c \in \mathrm{Cl}(L) : N_{L/K}c = 1\} \ = \ \mathrm{Cl}(L/K),$$

where the relative class group $\mathrm{Cl}(L/K)$ is defined as the kernel of the norm map $N_{L/K} : \mathrm{Cl}(L) \longrightarrow \mathrm{Cl}(K)$. Thus $\#N_{L/K}\,\mathrm{Cl}(L) = \#\,\mathrm{Cl}(L)/\#\,\mathrm{Cl}(L/K)$, and since $I_{K^1L/L}\{(1)\}$ has index $(K^1 : L \cap K^1)$ in $\mathrm{Cl}(L)$ by the fundamental inequalities, we find $\#N_{L/K}\,\mathrm{Cl}(L) = (\mathrm{Cl}(L) : I_{K^1L/L}\{(1)\}) = (K^1 : L \cap K^1)$, hence $(\mathrm{Cl}(K) : N_{L/K}\,\mathrm{Cl}(L)) = (K^1 : K)/(K^1 : L \cap K^1) = (L \cap K^1 : K)$ as claimed. □

The results reviewed so far are the main theorems of Takagi's class field theory.

15.3 The Fundamental Inequalities

Exercises

15.1 Show that $\mathrm{Cl}_{\mathbb{Q}}\{m\} \simeq (\mathbb{Z}/m\mathbb{Z})^\times/\{\pm 1\}$ and $\mathrm{Cl}_{\mathbb{Q}}\{m\infty\} \simeq (\mathbb{Z}/m\mathbb{Z})^\times$.

15.2 Let K be a number field, and let $\mathfrak{m}$ and $\mathfrak{n}$ be moduli such that $\mathfrak{n} \mid \mathfrak{m}$. Show that there exists a natural projection $\mathrm{Cl}\{\mathfrak{m}\} \longrightarrow \mathrm{Cl}\{\mathfrak{n}\}$. (Hint: Apply the snake lemma to the diagram

$$\begin{tikzcd}
1 \arrow[r] & H\{\mathfrak{m}\}/H^{(1)}\{\mathfrak{m}\} \arrow[r] \arrow[d] & \mathrm{Cl}_K\{\mathfrak{m}\} \arrow[r] \arrow[d] & \mathrm{Cl}(K) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & H\{\mathfrak{n}\}/H^{(1)}\{\mathfrak{n}\} \arrow[r] & \mathrm{Cl}_K\{\mathfrak{n}\} \arrow[r] & \mathrm{Cl}(K) \arrow[r] & 1
\end{tikzcd}$$

and observe that the maps in the first and the last column are surjective.) Can you deduce that, for extensions L/K of number fields, $(\mathrm{Cl}_K\{\mathfrak{n}\} : I_{L/K}\{\mathfrak{n}\}) = (L:K)$ implies $(\mathrm{Cl}_K\{\mathfrak{m}\} : I_{L/K}\{\mathfrak{m}\}) = (L:K)$?

15.3 Verify the following table of ray class numbers for the fields $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{5}\,)$:

$\mathfrak{m}$	$\Phi(\mathfrak{m})$	$h_k\{\mathfrak{m}\}$
(1)	1	1
(2)	2	1
(2+2i)	4	1
(3)	8	2
(4)	8	2
(3+2i)	12	3
(4+4i)	16	4
(5)	16	4

$\mathfrak{m}$	$\Phi(\mathfrak{m})$	$h_k\{\mathfrak{m}\}$
$\infty_1\infty_2$	4	1
$(2)\infty_1\infty_2$	12	1
$(\sqrt{5}\,)\infty_1\infty_2$	16	2
(3)	8	1
$(3)\infty_1$	16	1
$(3)\infty_1\infty_2$	32	2
$(\sqrt{5}\,)^2$	20	1
$(\sqrt{5}\,)^3$	100	5

Identify the ray class groups in these tables: for $K = \mathbb{Q}(i)$, check that $K\{3\} = K(\sqrt{-3}\,)$, $K\{4\} = K(\sqrt{i}\,)$, $K\{3+2i\}$ is the field defined by the polynomial $x^3 + (-11+10i)x^2 + (7-4i)x + (3+2i)$, $K\{4+4i\} = K(\sqrt{i}, \sqrt{1+i}\,)$, and $K\{5\} = K(\zeta_5)$.

For $K = \mathbb{Q}(\sqrt{5}\,)$, show similarly that the nontrivial ray class fields are given by $K\{(\sqrt{5}\,)\infty_1\infty_2\} = K(\zeta_5)$, $K\{(3)\infty_1\infty_2\} = K(\zeta_3)$, and $K\{(5\sqrt{5}\,)\} = KL$, where L is the quintic subfield of $\mathbb{Q}(\zeta_{25})$.

15.4 Let $p \equiv 1 \bmod 4$ be a prime, and define primary $\pi, \overline{\pi} \in \mathbb{Z}[i]$ by $p = \pi\overline{\pi}$. Put $k = \mathbb{Q}(i)$, $L = k\{(1+i)^3\pi\}$ and $L' = k\{(1+i)^3\overline{\pi}\}$. Show that $LL' \subseteq k\{(1+i)^3 p\}$ and prove equality by computing $h_k\{(1+i)^3 p\}$. Deduce that $F = \mathbb{Q}(\zeta_{4p})$ is a subfield of LL'. Look at how $\overline{\pi}$ splits in L and show that LL'/F contains a cyclic unramified subextension M/F of degree $\frac{p-1}{4}$. Generalize this to prime powers π^n.

15.5 Let $K/\mathbb{Q}$ be a quadratic extension and fix an integer $f \geq 1$. Define the order

$$\mathcal{O}_f := \{\alpha \in \mathcal{O}_K : \alpha \equiv z \bmod f \text{ for some } z \in \mathbb{Z}, (z,f) = 1\}.$$

Consider the following ideal groups defined modulo f:

- $H_f^1 := H^{(1)}\{(f)\} = \{(\alpha) : \alpha \equiv 1 \bmod f\}$;
- $H_f = \{(\alpha) : \alpha \in \mathcal{O}_f\}$;
- $H = \{(\alpha) : (\alpha, f) = 1\}$; and $D_K\{(f)\} = \{\mathfrak{a} : (\mathfrak{a}, f) = (1)\}$.

Now let $E_f = \mathcal{O}_f \cap E_K$ denote the unit group of $\mathcal{O}_f$, and put $E_f^1 = \{\varepsilon \in E_f : \varepsilon \equiv 1 \bmod f\}$. Show that

$$(H_f : H_f^1) = \frac{\Phi(f)}{\phi(f) \cdot (E : E_f)}.$$

The groups H_f/H_f^1 are called ring class groups, and the corresponding class fields are the ring class fields modulo f.

(Hints: Consider the homomorphism $\psi : E_f \longrightarrow (\mathbb{Z}/f\mathbb{Z})^\times$ that maps a unit $\varepsilon \equiv z \bmod f$ to the residue class $z \cdot f\mathbb{Z}$. Conclude that $\#\mathrm{im}\,\psi = (E_f : E_f^1)$. Next show the homomorphism $\pi : H/H_f \longrightarrow (\mathbb{Z}/f\mathbb{Z})^\times/\mathrm{im}\,\pi$ defined by mapping an ideal (α) with $\alpha \equiv z \bmod f$ to the class generated by $z \cdot f\mathbb{Z}$ in the quotient group is a well defined isomorphism. Then use the knowledge about the order of the ray class group $D_K\{(f)\}/H_f^1$ to prove the claim).

16. Artin's Reciprocity Law

17. The Existence Theorem

18. Norm Residues and Higher Ramification

18.1 Higher Ramification Groups

One could spend a whole semester studying the constraints the Galois group puts on the decomposition of primes. The next step now is the introduction of the higher ramification groups:

$$V_i(\mathfrak{P}|\mathfrak{p}) = \{\sigma \in G : \alpha^\sigma \equiv \alpha \bmod \mathfrak{P}^{i+1} \ \text{ for all } \alpha \in \mathfrak{O}\}.$$

Note that $V_0 = T$; clearly we have the chain of subgroups $G \supseteq Z \supseteq T \supseteq V_1 \supseteq V_2 \supseteq \ldots$; it is easy to see that this sequence terminates, i.e., that there is an index m depending only on K/k such that $V_i = 1$ for all $i \geq m$. Each V_i is a normal subgroup of Z.

In order to work with these groups, one first shows that if we fix some $\pi \in \mathfrak{P} \setminus \mathfrak{P}^2$, we have $\sigma \in V_m$ if and only if $\pi^\sigma \equiv \pi \bmod \mathfrak{p}^{i+1}$; thus we only have to check this condition for one element instead of infinitely many.

Proposition 18.1. *The factor group T/V_1 is isomorphic to a subgroup of $\kappa(\mathfrak{P})^\times$.*

Since $\kappa(\mathfrak{P})$ is a finite field, this implies that T/V_1 is cyclic and coprime to $N\mathfrak{p}$.

Proposition 18.2. *Each factor group V_i/V_{i+1} is isomorphic to some subgroup of $\kappa(\mathfrak{P})$.*

This implies that each quotient V_i/V_{i+1} is abelian of p-power order. Thus if we write $e = e_0 p^v$ for some e_0 coprime to p, then $(T : V_1) = e_0$ (this is the tame part of the ramification) and $\#V_1 = p^v$ (the wild part).

In particular, the group Z is solvable, so the part of G that is understood the least is the piece between Z and G.

The higher ramification groups also determine the exact power of $\mathfrak{P}$ dividing the different. If we put $\#V_i = p^{r_i}$ for all $i \geq 0$, then the exponent of $\mathfrak{P}$ in the prime ideal factorization of $\operatorname{diff}(K/k)$ is given by

$$\sum_{i\geq 0}(\#V_i - 1) = \sum_{i \geq 0} i(\#V_i - \#V_{i+1}).$$

Figure 18.1 from Hasse's lectures displays this information; the exact exponent to which $\mathfrak{P}$ divides the different of $\mathfrak{P}$ is the sum of the numbers in the last column.

Let me also add the following table giving the ramification groups for quadratic extensions of $\mathbb{Q}$:

decomposition	$\mathbb{Q}$	K_Z	K_T	K_{V_1}	K_{V_2}	K_{V_3}
$(d/p) = +1$	$\mathbb{Q}$	K	K	K	K	K
$(d/p) = -1$	$\mathbb{Q}$	$\mathbb{Q}$	K	K	K	K
p odd, $p \mid d$	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	K	K	K
$p = 2, d \equiv 4 \bmod 8$	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	K	K
$p = 2, d \equiv 0 \bmod 8$	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	$\mathbb{Q}$	K

In the case where $p = 2$ and $8 \mid d$, we have, in Hasse's notation, $r_1 = r_2 = 1$ and $r_3 = 0$, so the contribution of the prime ideal $\mathfrak{P}$ above 2 to the different is $\mathfrak{P}^3$ (here $3 = 3(2^{r_2} - 2^{r_3})$).

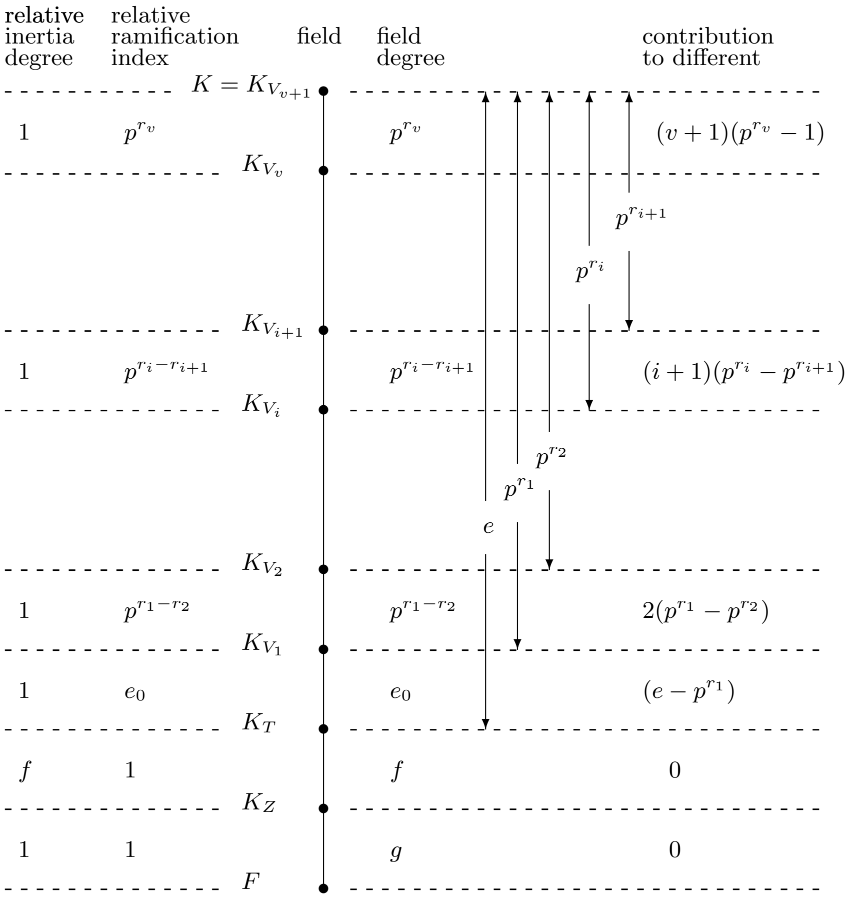


Fig. 18.1. The Prime Ideals below $\mathfrak{P}$

Part IV

Appendix

A. Gamma, Theta, and Zeta

B. A Beginner's Guide to Galois Cohomology

C. Solutions of Selected Problems

1. *Determine (r, s) for pure quartic fields $K = \mathbb{Q}(\sqrt[4]{m}\,)$.*

   Assume that m is not a square (if it is, then $(K : \mathbb{Q}) \mid 2$, and we know how to determine (r, s) for these fields). Then the minimal polynomial of $\sqrt[4]{m}$ is

   $$X^4 - m = (X - \sqrt[4]{m}\,)(X + \sqrt[4]{m}\,)(X - \sqrt[4]{m}\,)(X + \sqrt[4]{m}\,).$$

   If $m > 0$, the first two roots are real, the last two are not, hence $(r, s) = (2, 1)$. If $m < 0$, none of the roots are real, and then $(r, s) = (0, 2)$.
   We can also determine the splitting of the infinite primes. In fact, let $m < 0$, let α be a root of $X^4 - m$, and consider the two real embeddings $\sigma_1 : \alpha \longmapsto +\sqrt[4]{m}$ and $\sigma_2 : \alpha \longmapsto -\sqrt[4]{m}$. Then $\beta = \alpha^2$ is a square root of m, and $\sigma_1(\beta) = \sigma_1(\alpha)^2 = \sqrt{m}\,)$, as well as $\sigma_2(\beta) = \sqrt{m}$. Thus σ_1 and σ_2 restrict to the real embedding of $k = \mathbb{Q}(\sqrt{m}\,)$ that send β to $+\sqrt{m}$; the infinite prime ∞_1 of k thus splits into two real infinite primes in K.
   The complex embeddings of K, on the other hand, restrict to the real embedding $\beta \longmapsto -\sqrt{m}$ of k; the corresponding real infinite prime in k thus ramifies in K.

2. *Show that r and s do not depend on the choice of α or f: if $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$, show that the minimal polynomials of α and β have the same number of real roots.*

   Assume that $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$; then any embedding of K into $\mathbb{C}$ is determined by its value on α or β since every element of K is a polynomial in α or β with rational coefficients.
   Now if σ is an embedding with $\sigma(\alpha) \in \mathbb{R}$, then $\beta = a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$ has image $\sigma(\beta) = a_0 + a_1\sigma(\alpha) + \ldots + a_{n-1}\sigma(\alpha^{n-1})$, which is also real. Thus the every real root of the minimal polynomial of α corresponds to a real root of the minimal polynomial of β, and vice versa. This implies that both polynomials have the same number of real roots, and since they have the same degree, they must have the same signature.

3. *Let* $\omega = \sqrt[3]{m}$*; compute* $\operatorname{Tr}(a + b\omega + c\omega^2)$ *and* $N(a + b\omega)$*. Find a unit* $\neq \pm 1$ *in* $\mathbb{Q}(\sqrt[3]{2}\,)$*.*

   Let us first compute trace and norm using the embeddings of K. There are three of them, namely $\sigma_1(\omega) = \sqrt[3]{m}$, $\sigma_2(\omega) = \rho\sqrt[3]{m}$, and $\sigma_3(\omega) = \rho^2\sqrt[3]{m}$, where ρ is a primitive cube root of unity, i.e., a root of $x^2 + x + 1 = 0$. Then $\operatorname{Tr}\omega = \sum \sigma_j(\omega) = (1+\rho+\rho^2)\omega = 0$, and similarly $\operatorname{Tr}(\omega^2) = 0$. This implies $\operatorname{Tr}(a + b\omega + c\omega^2) = a\operatorname{Tr}(1) + b\operatorname{Tr}(\omega) + c\operatorname{Tr}(\omega^2) = 3a$. Similarly, $N(a + b\omega) = (a + b\sqrt[3]{2})(a + b\rho\sqrt[3]{2})(a + b\rho^2 sqrt[3]2) = a^3 + 2b^3$ since the mixed terms cancel.

   Next let us see how to do it using linear algebra. Choose the $\mathbb{Q}$-basis $1, \omega, \omega^2$. Multiplication by $\alpha = a + b\omega + c\omega^2$ is a $\mathbb{Q}$-linear map described by a 3×3-matrix whose columns represent the coordinates of the images of the basis elements; thus $\alpha \cdot 1 = a + b\omega + c\omega^2$ shows that the first column has the entries a, b, c. Similarly $\alpha\omega = 2c + a\omega + b\omega^2$ etc. show that the matrix attached describing multiplication by α is given by

$$M_\alpha = \begin{pmatrix} a & 2c & 2b \\ b & a & 2c \\ c & b & a \end{pmatrix}.$$

   Thus $\operatorname{Tr}\alpha = \operatorname{Tr} M_\alpha = 3a$ and $N\alpha = \det M_\alpha = a^3 + 2b^3 + 4c^3 - 6abc$. From $N(a + b\omega) = a^3 + 2b^3$ we easily see that $1 - \omega$ is a unit.

4. *Deduce from Theorem 5.5 how primes p split in quadratic extensions.*

   Consider $\alpha = \sqrt{m}$; the index $j = (\mathfrak{O}_K : \mathbb{Z}[\alpha])$ is 1 if $m \equiv 2, 3 \bmod 4$, and $j = 2$ if $m \equiv 1 \bmod 4$. Thus for odd primes p, we can simply work with the polynomial $f(x) = x^2 - m$.

   Assume that p is odd. If $p \mid m$, then $f(x) \equiv x^2 \bmod p$, and $p\mathfrak{O}_K = \mathfrak{p}^2$ for $\mathfrak{p} = (p, \sqrt{m}\,)$. If $p \nmid m$ and f splits as $f(x) \equiv (x - a)(x + a) \bmod p$, then $a^2 \equiv m \bmod p$; conversely, if $a^2 \equiv m \bmod p$, then f splits. Thus $p\mathfrak{O}_K = \mathfrak{p}\mathfrak{p}'$ for $\mathfrak{p} = (p, a - \sqrt{m}\,)$ and $\mathfrak{p}' = (p, a + \sqrt{m}\,)$ if $(\frac{m}{p}) = +1$, and p is inert if $(\frac{m}{p}) = -1$.

   Now let $p = 2$. If $m \equiv 2 \bmod 4$, we find $x^2 - m \equiv x^2 \bmod 2$, hence $2\mathfrak{O}_K = \mathfrak{p}^2$ for $\mathfrak{p} = (2, \sqrt{m}\,)$. If $m \equiv 3 \bmod 4$, we find $x^2 - m \equiv (x + 1)^2 \bmod 2$, hence $2\mathfrak{O}_K = \mathfrak{p}^2$ for $\mathfrak{p} = (2, 1 + \sqrt{m}\,)$. Finally, if $m = 4n + 1$, we have to use the minimal polynomial of $\omega = \frac{1+\sqrt{m}}{2}$, which is $f(x) = x^2 + x + n$. If $n \equiv 1 \bmod 2$ (equivalently, if $m \equiv 5 \bmod 8$), this polynomial is irreducible over $\mathbb{F}_2$, and hence 2 remains inert in K. If $n \equiv 0 \bmod 2$ (i.e., $m \equiv 1 \bmod 8$), however, $f(x) \equiv x(x + 1) \bmod 2$, and we find $2\mathfrak{O}_K = \mathfrak{p}\mathfrak{p}'$ for $\mathfrak{p} = (2, \omega)$ and $\mathfrak{p}' = (2, 1 + \omega)$.

5. *Compute the differents of quadratic extensions* $K = \mathbb{Q}(\sqrt{m}\,)$ *directly from the definition.*

   Assume first that $m \equiv 2, 3 \bmod 4$; we claim that $\operatorname{diff}(K) = (2\sqrt{m}\,)$.

Let us first show that $(2\sqrt{m}\,) \subseteq \operatorname{diff}(K)$. This means that $\operatorname{Tr}\frac{\alpha}{2\sqrt{m}} \in \mathbb{Z}$ for all $\alpha \in \mathfrak{O}_K = \mathbb{Z}[\sqrt{m}\,]$. Since the trace is $\mathbb{Q}$-linear, it is sufficient to prove this for an integral basis of $\mathfrak{O}_K$, that is, for $\alpha = 1$ and $\alpha = \sqrt{m}$. But $\operatorname{Tr}\frac{1}{2\sqrt{m}} = \operatorname{Tr}(\frac{1}{2m}\sqrt{m}\,) = 0$ and $\operatorname{Tr}\frac{\sqrt{m}}{2\sqrt{m}} = \operatorname{Tr}\frac{1}{2} = 1$.
Now for the converse $(2\sqrt{m}\,) \supseteq \operatorname{diff}(K)$. We have to show that if $\operatorname{Tr}\alpha\omega \in \mathbb{Z}$ for all $\omega \in \mathfrak{O}_K$, then $2\sqrt{m}\alpha \in \mathfrak{O}_K$. We will show that this follows already by looking only at $\omega = 1$ and $\omega = \sqrt{m}$. Write $\alpha = a + b\sqrt{m}$ for $a, b \in \mathbb{Q}$; then $\operatorname{Tr}\alpha = 2a \in \mathbb{Z}$ and $\operatorname{Tr}\alpha\sqrt{m} = \operatorname{Tr}(bm + a\sqrt{m}\,) = 2bm \in \mathbb{Z}$. But since $2\sqrt{m}\alpha = 2bm + 2a\sqrt{m}$, this implies the desired $2\sqrt{m}\alpha \in \mathbb{Z}[\sqrt{m}\,]$.
The case $m \equiv 1 \bmod 4$ is taken care of similarly; here we find that $\operatorname{diff}(K) = (\sqrt{m}\,)$.

6. *Let $L/K/k$ be a tower of normal extensions of number fields. Let $\mathfrak{Q}$ be a prime ideal in $\mathfrak{O}_L$, and let $\mathfrak{P} = \mathfrak{Q} \cap K$ and $\mathfrak{p} = \mathfrak{Q} \cap k$ denote the prime ideals in $\mathfrak{O}_K$ and $\mathfrak{O}_k$ lying below $\mathfrak{Q}$. Show that*

$$e(\mathfrak{Q}|\mathfrak{p}) = e(\mathfrak{Q}|\mathfrak{P}) \cdot e(\mathfrak{P}|\mathfrak{p}) \quad \text{and} \quad f(\mathfrak{Q}|\mathfrak{p}) = f(\mathfrak{Q}|\mathfrak{P}) \cdot f(\mathfrak{P}|\mathfrak{p}).$$

From the definition of the ramification indices we have $\mathfrak{P}^{e(\mathfrak{P}|\mathfrak{p})} \parallel \mathfrak{p}\mathfrak{O}_K$ and $\mathfrak{Q}^{e(\mathfrak{Q}|\mathfrak{p})} \parallel \mathfrak{p}\mathfrak{O}_L$, as well as $\mathfrak{Q}^{e(\mathfrak{Q}|\mathfrak{P})} \parallel \mathfrak{P}\mathfrak{O}_L$. Thus $\mathfrak{Q}^{e(\mathfrak{Q}|\mathfrak{P})e(\mathfrak{P}|\mathfrak{p})}$ is the exact power of $\mathfrak{Q}$ dividing $\mathfrak{p}\mathfrak{O}_L$, and this implies the first claim.
As for the second, we simply observe

$$(\kappa(\mathfrak{Q}) : \kappa(\mathfrak{p}) = (\kappa(\mathfrak{Q}) : \kappa(\mathfrak{P}))(\kappa(\mathfrak{P}) : \kappa(\mathfrak{p}).$$

7. *Let K/k be a Galois extension, and assume that $\mathfrak{p}$ is inert in K/k. Show that K/k is a cyclic extension.*

If $\mathfrak{p}$ is inert in K/k, then its decomposition group $Z = G$, and $T = 1$. Since Z/T is cyclic, this implies the claim.

8. *Abhyankar's Lemma: Let K_1/k and K_2/K be disjoint abelian extensions with Galois group* $\operatorname{Gal}(K_i/k) \simeq \mathbb{Z}/\ell\mathbb{Z}$, *where ℓ is a prime $\neq p$. Show that if a prime ideal $\mathfrak{p}$ above p is ramified in both extensions, then the primes above $\mathfrak{p}$ are unramified in K_1K_2/K_1 and K_1K_2/K_2.*

If $\mathfrak{p}$ is ramified in K_1/k, then it must be completely ramified since ℓ is prime and the ramification index divides the degree. Also, the ramification index e of $\mathfrak{P}$ in K_1K_2 divides ℓ^2. If $e = \ell^2$, then $\mathfrak{P}$ is completely ramified, and $T = G = \operatorname{Gal}(K_1K_2/K)$. But since $p \nmid \ell$, we must have $V_1 = 1$, hence $T/V_1 \simeq G$. But T/V_1 is always cyclic, and G is not. Thus $e = \ell$, and this means that the primes above $\mathfrak{p}$ in K_1 and K_2 cannot ramifiy in K_1K_2/K_1 and K_1K_2/K_2, resprectively.

9. *Let ℓ be an odd prime, and consider the pure extension $K = \mathbb{Q}(\sqrt[\ell]{m}\,)$; assume that there is a prime $p \equiv 1 \bmod \ell$ with $p \mid m$. Let F be the subfield of $\mathbb{Q}(\zeta_p)$ with degree ℓ. Show that FK/K is an unramified abelian extension.*

   The extension $K/\mathbb{Q}$ is not normal, so we cannot apply Abhyankar's lemma directly. The normal closure of $K/\mathbb{Q}$ is the field $K' = K\mathbb{Q}'$ for $\mathbb{Q}' = \mathbb{Q}(\zeta_\ell)$. Now K' and $F' = F\mathbb{Q}'$ are cyclic extensions of degree ℓ, and p is completely ramified in $K'/\mathbb{Q}'$ and $F'/\mathbb{Q}'$. Abhyankar's Lemma then implies that $K'F/K'$ is unramified and cyclic.
   Now

$$\operatorname{diff}(K'F/K) = \operatorname{diff}(K'F/K')\operatorname{diff}(K'/K) = \operatorname{diff}(K'/K)$$

   and

$$\operatorname{diff}(K'F/K) = \operatorname{diff}(K'F/KF)\operatorname{diff}(KF/K).$$

   Since $\operatorname{diff}(K'/K) \mid \operatorname{diff}(\mathbb{Q}'/\mathbb{Q})$ and the latter is coprime to p, we deduce that $\operatorname{diff}(KF/K)$ also must be coprime to p. But this implies the claim.

10. *Show that the decomposition and inertia groups of the prime ideal $\mathfrak{P}^\sigma$ for some $\sigma \in G$ are given by $Z(\mathfrak{P}^\sigma|\mathfrak{p}) = \sigma^{-1}Z(\mathfrak{P}|\mathfrak{p})\sigma$ and $T(\mathfrak{P}^\sigma|\mathfrak{p}) = \sigma^{-1}T(\mathfrak{P}|\mathfrak{p})\sigma$. Similar results hold for the higher ramification groups. Here it is important to let G act from the right.*

    If $\tau \in Z(\mathfrak{P}|\mathfrak{p})$, then $\mathfrak{P} = \mathfrak{P}\tau = (\mathfrak{P}^\sigma)^{\sigma^{-1}\tau}$, hence $\mathfrak{P}^\sigma = (\mathfrak{P}^\sigma)^{\sigma^{-1}\tau\sigma}$, and this shows that $\sigma^{-1}\tau\sigma \in Z(\mathfrak{P}^\sigma|\mathfrak{p})$. Thus $\sigma^{-1}Z(\mathfrak{P}|\mathfrak{p})\sigma \subseteq Z(\mathfrak{P}^\sigma|\mathfrak{p})$, and by going backwards we see that the inverse inclusion also holds.
    Similarly, $\tau \in T(\mathfrak{P}|\mathfrak{p})$ means $\alpha^\tau \equiv \alpha \bmod \mathfrak{P}$ for all $\alpha \in \mathfrak{O}_K$, hence $(\alpha^{\sigma^{-1}})^\tau \equiv \alpha^{\sigma^{-1}} \bmod \mathfrak{P}$. Applying σ now shows that $\sigma^{-1}\tau\sigma \in T(\mathfrak{P}^\sigma|\mathfrak{p})$.

11. Let A and B be abelian groups. Show that $X(A \oplus B) \simeq X(A) \oplus X(B)$.

    Let $\chi \in X(A \oplus B)$ be a character defined on $A \oplus B$; then we can define characters $\chi|_A$ and χ_B by $\chi|_A(a) = \chi(a,0)$ and $\chi_B(b) = \chi(0,b)$, and the map $\chi \longmapsto (\chi_A, \chi_B)$ is a group homomorphism $\rho : X(A \oplus B) \longrightarrow X(A) \oplus X(B)$.
    Conversely, if $\psi \in X(A)$ and $\omega \in X(B)$, then $\chi(a,b) = \psi(a)\omega(b)$ defines a character on $A \oplus B$, and the map $\lambda : (\psi, \omega) \longmapsto \chi$ is a homomorphism $\lambda : X(A) \oplus X(B) \longrightarrow X(A \oplus B)$.
    Now $\lambda \circ \rho(\chi) = \lambda(\chi|_A, \chi|B) = \chi'$, where $\chi'(a,b) = \chi|_A(a)\chi|_B(b) = \chi(a,0)\chi(0,b) = \chi(a,b)$. This $\lambda \circ \rho = \mathrm{id}$.
    Similarly, $(\psi', \omega') = \rho \circ \lambda(\psi, \omega)$ is $\rho(\chi)$ for the character χ defined by $\chi(a,b) = \psi(a)\omega(b)$. Thus $\psi'(a) = \chi(a,0) = \psi(a)\omega(0) = \psi(a)$ and $\omega'(a) = \chi(0,b) = \psi(0)\omega(b) = \omega(b)$, and this shows that $\rho \circ \lambda$ is the identity map on $X(A) \oplus X(B)$.

12. Let
$$1 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 1$$
be an exact sequence of finite abelian groups. Show that there is an exact sequence
$$1 \longrightarrow \widehat{C} \longrightarrow \widehat{B} \longrightarrow \widehat{A} \longrightarrow 1.$$

Our first task is to define the maps in the dual sequence. Assume that $f : A \longrightarrow B$ is a homomorphism between abelian groups; we need to define a map $\widehat{f} : \widehat{B} \longrightarrow \widehat{A}$. An element in $\widehat{B}$ is a character $\chi : B \longrightarrow \mathbb{C}^\times$, and we need to define a map $\widehat{f}(\chi) =: \chi' : A \longrightarrow \mathbb{C}^\times$ using $f : A \longrightarrow B$. It is clear that we must put $\chi'(a) = \chi(f(a))$. This is clearly a character since $\chi(f(ab)) = \chi(f(a)f(b)) = \chi(f(a))\chi(f(b))$.
Thus an exact sequence
$$1 \longrightarrow A \xrightarrow{\ f\ } B \xrightarrow{\ g\ } C \longrightarrow 1$$
induces a sequence
$$1 \longrightarrow \widehat{C} \xrightarrow{\ \widehat{g}\ } \widehat{B} \xrightarrow{\ \widehat{f}\ } \widehat{A} \longrightarrow 1,$$
and it remains to show that this sequence is exact.
Let $\chi \in \ker \widehat{g}$. Then $\widehat{g}(\chi) = 1\!\!1$, that is, $\chi(g(b)) = 1$ for all $b \in B$. Since $g : B \longrightarrow C$ is surjective, we have $\chi(c) = 1$ for all $c \in C$, hence $\chi = 1\!\!1$, and thus $\ker \widehat{g} = 1$.
Next we claim that $\widehat{g} \circ \widehat{f} = 0$. In fact, let $\chi \in \widehat{C}$; then $\widehat{g} \circ \widehat{f}(\chi)(a) = \chi(g \circ f(a)) = \chi(0) = 1$. Thus $\operatorname{im} \widehat{g} \subseteq \ker \widehat{f}$.
Assume conversely that $\chi \in \ker \widehat{f}$. We need to find a character $\psi \in \widehat{C}$ such that $\chi(b) = \psi(g(b))$. Since g is surjective, for every $c \in C$ there is a $b \in B$ with $c = g(b)$, and we can define $\psi(c) = \chi(b)$. This is well defined: if $g(b) = g(b')$, then $g(b/b') = 1$, hence $b/b' = f(a)$ for some $a \in A$, and $\chi(b/b') = \chi(f(a)) = 1$ since $\chi \in \ker \widehat{f}$; thus $\chi(b) = \chi(b')$. But now $\widehat{g}(\psi)(b) = \psi(g(b))) = \chi(b)$, that is, $\widehat{g}(\psi) = \chi$.
Surjectivity of $\widehat{g}$ follows by counting elements.

13. Let χ and ψ be Dirichlet characters defined modulo m, and with conductors f_χ and f_ψ. Show that if $\gcd(f_\chi, f_\psi) = 1$, then the character $\chi\psi$ has conductor $f_\chi f_\psi$.

Clearly $\chi\psi$ is defined mod $f_\chi f_\psi$: $\chi\psi(a + f_\chi f_\psi) = \chi(a + f_\chi f_\psi)\psi(a + f_\chi f_\psi) = \chi(a)\psi(a) = \chi\psi(a)$.
Let f denote the conductor of $\chi\psi$; we have just shown that $f \mid f_\chi f_\psi$. It remains to show that $f_\chi \mid f$ and $f_\psi \mid f$; the coprimality of f_χ and f_ψ will then imply the claim.
Assume therefore that $\chi\psi(a) = \chi\psi(a + f)$ for all a and some $f \in \mathbb{N}$; we need to show that $f_\chi \mid m$. To this end put $n = f_\psi f$, and use the Chinese

Remainder Theorem to find $b \equiv a \bmod f_\chi$ and $b \equiv 1 \bmod f_\psi$. Then $\chi\psi(b) = \chi(b)\psi(b) = \chi(a)\psi(1) = \chi(a)$ and $\chi\psi(b+n) = \chi(b+n)\psi(b+n) = \chi(a+n)\psi(b) = \chi(a+n)$, Thus $\chi(a) = \chi(a+n)$ for all a, hence $f_\chi \mid n$. Since $\gcd(f_\chi, f_\psi) = 1$, this implies $f_\chi \mid f$.

14. List all Dirichlet characters modulo 24, determine their conductors, and identify them with Kronecker symbols.

    Since $(\mathbb{Z}/24\mathbb{Z})^\times \simeq (\mathbb{Z}/2\mathbb{Z})^3$, there are eight characters, and all of them are quadratic. On the other hand, the characters $\chi = (\frac{m}{\cdot})$ for $m = \pm 1, \pm 2, \pm 3, \pm 6$ are all defined mod 24, and therefore form the full character group. The conductors can be read off the character table, or from quadratic reciprocity. In general, the character $(\frac{m}{\cdot})$ has conductor $|m|$ or $4|m|$ according as $m \equiv 1 \bmod 4$ or not.

References

[Ar1932] E. Artin, *Über Einheiten relativ galoisscher Zahlkörper*, J. Reine Angew. Math. **167** (1932), 153–156 80, 85

[Ay1974] R. Ayoub, *Euler and the zeta function*, Amer. Math. Monthly **81** (1974), 1067–1086

[Ba1903] M. Bauer, *Über einen Satz von Kronecker*, Arch. Math. Phys. (3) **6** (1903), 218–219 99

[Ca1986] J.W.S. Cassels, *Local Fields*, London Math. Soc. student texts 3, 1986 18

[Ch1925] N. Chebotarev, *Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören*, Math. Ann. **95** (1925), 191–228

[Co1978] H. Cohn, *A classical invitation to algebraic numbers and class fields*, Springer-Verlag 1978 143

[Da1980] H. Davenport, *Multiplicative Number Theory*, 2nd ed. Springer-Verlag 1980 18

[Eu1734] L. Euler, *De summis sserierum reciprocarum*, 1734

[Eu1737] L. Euler, *Variae observationes circa series infinitas*, 1737

[Eu1748] L. Euler, *Introductio in analysin infinitorum*, Lausanne 1748; Opera I-8, 351; English translation: *Introduction to analysis of the infinite*, Springer-Verlag 1988

[Eu1749] L. Euler, *Remarques sur un beau rapport entre les séries des puissances tant directes que réciproques*, 1749

[Fr1896] G. Frobenius, *Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe*, Sitzungsber. Berlin 1896, 689–703

[Ga1926] F. Gaßmann, *Bemerkungen zur vorstehenden Arbeit von Hurwitz*, Math. Z. **25** (1926), 665–675 99

[Ga1889] C.-F. Gauss, *Untersuchungen über höhere Arithmetik*, German Transl. of the Disquisitiones Arithmeticae by H. Maser, Springer-Verlag 1889; reprint Chelsea 1965 17

[GL1965] A.O. Gelfond, Yu.V. Linnik, *Elementary Methods in Analytic Number Theory*, Rand McNally & Co. 1965 27

[Go1971] L.J. Goldstein, *Analytic Number Theory*, Prentice-Hall 1971

[He1930] J. Herbrand, *Nouvelle démonstration et généralisation d'un théorème de Minkowski*, C. R. Acad. Sci. Paris **191** (1930), 1282–1285 85

[He1931] J. Herbrand, *Sur les unités d'un corps algébrique*, C. R. Acad. Sci. Paris **192** (1931), 24–27; Corr.: ibid. p. 188 85

[Hu1926] A. Hurwitz (F. Gaßmann, ed.), *Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe*, Math. Z. **25** (1926), 661–665

[Ja1996] G.J. Janusz, *Algebraic Number Fields*, 2nd ed. AMS 1996

[Kl1998] N. Klingen, *Arithmetical similarities. Prime decomposition and finite group theory.* Oxford University Press, New York, 1998

[Kr1880] L. Kronecker, *Über die Irreductibilität von Gleichungen*, Monatsber. Berlin 1880, 155–162; Werke II, 83–93;

[Ma1977] D. Marcus, *Number Fields*, Springer-Verlag 1977 18

[Mi1900] H.Minkowski, *Zur Theorie der Einheiten in den algebraischen Zahlkörpern*, Gött. Nachr. 1900, 90–93 85

[Mo1993] P. Monsky, *Simplifying the proof of Dirichlet's theorem*, Amer. Math. Monthly **100** (1993), no. 9, 861–862 27

[Od1994] Y. Odai, *Herbrand's unit theorem and relative units*, Comment. Math. Univ. St. Paul. **43** (1994), no. 2, 135–138 85

[Se1980] J.-P. Serre, *Local Fields*, 2nd ed. Springer-Verlag 1980 18

[St1993] H. M. Stark, *Dirichlet's class-number formula revisited*, A tribute to Emil Grosswald: number theory and related analysis, 571–577, Contemp. Math., 143, AMS 1993 37

[SL1996] P. Stevenhagen, H.W. Lenstra, *Chebotarvv and his density theorem*, Math. Intelligencer **18** (1996), no. 2, 26–37 166

[ST1987] I.N. Stewart, D.O. Tall, *Algebraic Number Theory*, Chapman & Hall, 2nd ed. 1987

[Sw2001] P. Swinnerton-Dyer, *A brief guide to algebraic number theory*, London Math. Soc. student texts 50, 2001 18

[Ta1915a] T. Takagi, *Zur Theorie der relativ-Abelschen Zahlkörper. I*, Tokyo Math. Ges. (2) **8** (1915/16), 154–162

[Ta1915b] T. Takagi, *Zur Theorie der relativ Abelschen Zahlkörper. II*, Tokyo Math. Ges. (2) **8** (1915/16), 243–254

[Ta1920] T. Takagi, *Über eine Theorie des relativ Abelschen Zahlkörpers*, Journ. Coll. of Science Tokyo **41** (1920), 133 pp.