Algebraic Number Theory

Yongquan HU

Contents

Chapter 1

W1 (03-05): Integral basis

1.1 Integral extensions

All the rings are assumed to be commutative and unital.

Definition 1.1.1. *Let $A \subset B$ be an extension of rings. We say an element $x \in B$ is integral over A if there exists a monic polynomial $f(X) = X^n + a_1 X^{n-1} + \cdots + a_n \in A[X]$ such that $f(x) = 0$. (Such an equation will be called an* integral equation.*) We say B is integral over A if every $x \in B$ is integral over A.*

Note that, integral over a field is the same as algebraic over the field.

Example 1.1.2. *(1) $\sqrt[5]{3} \in \mathbb{R}$ is integral over $\mathbb{Z}$.*
(2) If ζ_N denotes a primitive N-th roots of unity, then ζ_N is integral over $\mathbb{Z}$.

Proposition 1.1.3. *Let $A \subset B$ be an extension of rings and $x \in B$. Then the following statements are equivalent:*

1. *x is integral over A*
2. *the subring $A[x] \subset B$ is a finitely generated A-module*
3. *there exists a subring $B' \subset B$ which contains x and which is a finitely generated A-module.*

Proof. (1)⇒(2): because $\{1, x, ..., x^{n-1}\}$ generate $A[x]$.
(2)⇒(3): clear.
(3)⇒(1): let $m_1, ..., m_r \in B'$ be a set of generators as an A-module. Since $xB' \subset B'$, we may write $xm_i = \sum_{j=1}^{r} a_{ij} m_j$ with $a_{ij} \in A$. Let T be the matrix (a_{ij}). By definition, the matrix $xI_r - T$ annihilates $(m_1, ..., m_r)$. The Cramer's rule then implies a matrix T' such that $T'(xI_r - T) = \det(xI_r - T) := \det$, so that $\det \cdot m_i = 0$ for all i, and $\det \cdot B' = 0$. Since $1 \in B'$, we get $\det = 0$. Explicitly developing det, we get a *monic* polynomial which annihilates x. □

Corollary 1.1.4. *Let $A \subset B$ be an extension of rings. Then the elements of B which are integral over A form a subring of B.*

Proof. Given $x, y \in B$ integral over A, we need to show that $x + y$, xy are also integral over A. But it is easy to see that $A[x, y]$ is a finite A-module, and concludes using (3) of Proposition 1.1.3. □

Corollary 1.1.5. *Let $A \subset B \subset C$ be extension of rings. Then C is integral over A if and only if C is integral over B and B is integral over A.*

Proof. $\Rightarrow$ is clear. Prove $\Leftarrow$. Let $c \in C$ and $f(T) \in B[T]$ be an integral equation. Write $f = X^n + b_{n-1}X^n + \cdots + b_0$. Since each b_i is integral over A, $A' := A[b_0, ..., b_{n-1}]$ is a finitely generated A-module. Since c is integral over A', $A'[c]$ is a finitely generated A'-module, hence finitely generated as A-module. □

Lemma 1.1.6. *Let $A \subset B$ with B integral over A. If $\mathfrak{b}$ is an ideal of B, then $B/\mathfrak{b}$ is integral over $A/\mathfrak{a}$, where $\mathfrak{a} = \mathfrak{b} \cap A$.*

Proof. Clear. □

Example 1.1.7. *Since $\sqrt{2}, \sqrt[5]{3} \in \mathbb{R}$ are integral over $\mathbb{Z}$, we see that $\sqrt{2}+\sqrt[5]{3}$ is also integral over $\mathbb{Z}$. Try to find an integral equation for it.*

This can be done using "resultant" (an important notion in effective elimination theory). Precisely, given $f, g \in \mathbb{Q}[X]$, can define $\mathrm{Res}(f, g) \in \mathbb{Q}[X]$, *- equals to the determinant of a certain matrix constructed from the coefficients of f, g. If f, g are monic, we have in $\overline{\mathbb{Q}}$:*

$$\mathrm{Res}(f, g) = \prod_{(x,y):f(x)=g(y)=0} (x - y).$$

In this way, letting t be a variable, $\mathrm{Res}(f(X), g(t - X))$, *which is of degree mn, gives an integral equation.*

Definition 1.1.8. *(1) Let $A \subset B$ be an extension of rings. Define the* integral closure *of A in B to be the subring of B consisting of all integral elements over A.*

(2) If the integral closure of A in B is A itself, we say that A is integrally closed *in B.*

(3) Assume A is an integral domain. We say A is integrally closed *if A is integrally closed in its field of fractions.*

Example 1.1.9. *(1) $\mathbb{Z}$ is integrally closed. Indeed, let $x = \frac{a}{b} \in \mathbb{Q}$ with $(a, b) = 1$ and $b > 0$. If x is integral over $\mathbb{Z}$, then there exists an integral equation*

$$x^n + c_{n-1}x^{n-1} + \cdots + c_0 = 0$$

hence

$$a^n + c_{n-1}a^{n-1}b + \cdots c_0b^n = 0.$$

If $b \neq 1$, let p be a prime dividing b. Then we deduce $p|a^n$, hence $p|a$, a contradiction to the fact $(a, b) = 1$.

(2) More generally, every UFD is integrally closed. For example, $\mathbb{Z}[i]$ is also integrally closed. This is less trivial, using the fact that $\mathbb{Z}[i]$ is a PID.

(3) Let F be a field, and $A = F[t^2, t^3]$ be the subring of $K = F(t)$. Then A is an integral domain, with field of fractions K. But A not integrally closed: its integral closure is $F[t]$.

Definition 1.1.10. *(1) An element $x \in \mathbb{C}$ is an* algebraic number *(resp.* algebraic integer*) if it is integral over $\mathbb{Q}$ (resp. $\mathbb{Z}$).*

(2) A number field is a finite extension of $\mathbb{Q}$. For K a number field, define $\mathcal{O}_K$ to be the integral closure of $\mathbb{Z}$ in K, and call it the ring of integers of K.

Lemma 1.1.11. *The field of fractions of $\mathcal{O}_K$ is K.*

Proof. Indeed, if $x \in K$, then there exists $b \in \mathbb{Z}$ such that $bx \in \mathcal{O}_K$. $\square$

By definition, $\mathcal{O}_K$ is integrally closed.

Proposition 1.1.12. *Let $x \in \mathbb{C}$ be an algebraic number, and $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Q}[X]$ be its minimal polynomial. Then x is an algebraic integer if and only if $f(X) \in \mathbb{Z}[X]$.*

Proof. Assume x is an algebraic integer. Let $\{x = x_1, ..., x_n\}$ be the set of complex roots of $f(X)$. Then each x_i corresponds to an embedding of fields $\iota_i : \mathbb{Q}(x) \hookrightarrow \mathbb{C}$, sending x to x_i. Hence if $g(X) \in \mathbb{Z}[X]$ is monic such that $g(x) = 0$, then $g(x_i) = \iota_i(g(x)) = 0$, hence x_i is also an algebraic integer. This implies a_i are all algebraic integers, since they are symmetric functions of x_j's. Since $a_i \in \mathbb{Q}$, we obtain $a_i \in \mathbb{Z}$. $\square$

1.2 Trace and discriminant

We first recall some basic facts about traces and norms.

Recall that if L/K is a finite extension of fields, then we can define the norm and trace of an element $x \in L$:

$$\mathrm{N}_{L/K}(x) := \det(\phi_x), \quad \mathrm{Tr}_{L/K}(x) := \mathrm{Tr}(\phi_x)$$

where ϕ_x denotes the K-linear endomorphism of L, $x : L \to L$. If $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ is the minimal polynomial of x over K, then

$$\mathrm{Tr}_{K(x)/K}(x) = -a_{n-1}, \quad \mathrm{N}_{K(x)/K}(x) = (-1)^n a_0.$$

Theorem 1.2.1. *If L/K is separable, then the bilinear form $\mathrm{Tr} : L \times L \to K$, sending (x, y) to $\mathrm{Tr}_{L/K}(xy)$ is non-degenerate, that is, if $x \in L$ is such that $\mathrm{Tr}(xy) = 0$ for any $y \in L$, then $x = 0$.*

Proof. We first recall Dedekind's theorem on the independence of characters. Let G be a group and Ω be a field, and let $\sigma_1, ..., \sigma_n$ be distinct group homomorphisms $G \to \Omega^\times$. Then they are linearly independent over Ω, that is, if $c_i \in \Omega$ is such that $\sum_{i=1}^n c_i\sigma_i = 0$ identically on G, then $c_i = 0$ for all i.

Now recall that if L/K is separable, then there exists n distinct K-embeddings $L \hookrightarrow \overline{K}$, where $\overline{K}$ denotes a fixed algebraically closure of K, say $\sigma_1, ..., \sigma_n$. Moreover, we have

$$\mathrm{Tr}_{L/K}(x) = \sum_{i=1}^n \sigma_i(x).$$

Hence if $\mathrm{Tr}_{L/K}(xy) = 0$, then

$$\sum_{i=1}^n \sigma_i(xy) = \sum_{i=1}^n \sigma_i(x)\sigma_i(y) = 0, \quad \forall y \in L.$$

Apply Dedekind's theorem to $G = L^\times$, we obtain $\sigma_i(x) = 0$ for all i. Hence $x = 0$. $\square$

Corollary 1.2.2. *Assume L/K is separable. Let $\alpha_1, ..., \alpha_n \in L$, where $n = [L : K]$. Then $\alpha_1, ..., \alpha_n$ is a basis of L/K if and only if $\det(\mathrm{Tr}_{L/K}(\alpha_i\alpha_j)) \neq 0$.*

Proof. Let $\sigma_1, ..., \sigma_n$ be the n embeddings of L into $\overline{K}$. We compute

$$\det(\mathrm{Tr}(\alpha_i\alpha_j)) = \det\left(\sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j)\right) = \det(\sigma_k(\alpha_i)) \cdot \det(\sigma_k(\alpha_j)) = (\det(\sigma_k(\alpha_i)))^2.$$

This computation holds for any set of α_i.

Now we assume $\{\alpha_i\}$ is a basis of L/K. We need to show $\det(\sigma_k(\alpha_i)) \neq 0$. If not, the vectors $\sigma_k(\alpha_i)$ are linearly dependent over $\overline{K}$, i.e. there exist $c_1, ..., c_n \in \overline{K}$ such that

$$\sum_k c_k\sigma_k(\alpha_i) = 0, \quad \forall i.$$

Since $\{\alpha_i\}$ is a basis of L/K, this implies that $\sum_k c_k\sigma_k(x) = 0$ for any $x \in L$, hence $c_k = 0$ by Dedekind's theorem.

Conversely if $\{\alpha_i\}$ is not a basis, hence are linearly dependent over K, then $\sigma_k(\alpha_i)$ is also linearly dependent (note that σ_k fixes K). $\square$

Definition 1.2.3. *For $\alpha_1, ..., \alpha_n \in L$, we put*

$$\mathrm{Disc}(\alpha_1..., \alpha_n) = \det(\mathrm{Tr}_{L/K}(\alpha_i\alpha_j)),$$

and call it the discriminant *of $\alpha_1, ..., \alpha_n$.*

The elements $\alpha_1, ..., \alpha_n$ form a basis of L over K if and only if $\mathrm{Disc}(\alpha_1, ..., \alpha_n) \neq 0$.

Lemma 1.2.4. *If $C \in M_n(K)$ and $(\beta_1, ..., \beta_n) = (\alpha_1, ..., \alpha_n)C$, then*

$$\mathrm{Disc}(\beta_1, ..., \beta_n) = \mathrm{Disc}(\alpha_1, ..., \alpha_n)\det(C)^2.$$

Proof. View the matrix $(\alpha_i\alpha_j)_{1\leq i,j\leq n}$ as $\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \begin{pmatrix} \alpha_1 & \cdots & \alpha_n \end{pmatrix}$, then

$$\mathrm{Tr}(\beta_i\beta_j) = C^T \cdot \mathrm{Tr}(\alpha_i\alpha_j) \cdot C,$$

hence the result. $\square$

1.2.1 Dual basis

Given a basis $\{\alpha_i, 1 \leq i \leq n\}$ of L/K, let $C = (c_{ij})$ be the inverse matrix of $\mathrm{Tr}_{L/K}(\alpha_i\alpha_j)$. Put

$$(\alpha_1^\vee, ..., \alpha_n^\vee) := (\alpha_1, ..., \alpha_n)C.$$

Then we obtain

$$\mathrm{Tr}_{L/K}(\alpha_i\alpha_j^\vee) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise.} \end{cases}$$

That is, $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j^\vee)_{i,j} = I_{n\times n}$, the identity matrix. Indeed, by definition, one has

$$(\alpha_i\alpha_j^\vee)_{i,j} = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \begin{pmatrix} \alpha_1 & \cdots & \alpha_n \end{pmatrix} \cdot C;$$

since C has coefficients in K, and Tr is K-linear, we obtain the claim. We call $\{\alpha_i^\vee\}$ the *dual basis* of $\{\alpha_i\}$ with respect to $\mathrm{Tr}_{L/K}$. It is usually used in the following way: for any $x \in L$, if we write $x = \sum_{i=1}^n x_i\alpha_i$ with $x_i \in K$, then $x_i = \mathrm{Tr}_{L/K}(x\alpha_i^\vee)$.

Proposition 1.2.5. *Let A be a noetherian, integrally closed integral domain with field of fractions K. Let L be a finite separable extension of K. Then the integral closure B of A in L is finitely generated over A. If A is PID, then B is a free A-module of rank $[L:K]$.*

Proof. Let $\{\alpha_1, ..., \alpha_n\}$ be a basis of L/K. We may assume $\alpha_i \in B$. Let $\{\alpha_i^\vee\}$ be the dual basis of $\{\alpha_i\}$, that is,

$$\mathrm{Tr}_{L/K}(\alpha_i \alpha_j^\vee) = \delta_{ij}.$$

We claim that

$$\sum_{i=1}^n A\alpha_i \subset B \subset \sum_{i=1}^n A\alpha_i^\vee.$$

Indeed, the first inclusion is clear by choice of α_i. For the second, let $b \in B$ and write $b = \sum_j b_j \alpha_j^\vee$ with $b_j \in K$ (because $\{\alpha_i^\vee\}$ is also a basis of L/K). We shall prove that $b_j \in A$ for all j. On the one hand, we have

$$\mathrm{Tr}(b \cdot \alpha_i) = \sum_{j=1}^n b_j \mathrm{Tr}_{L/K}(\alpha_j^\vee \alpha_i) = b_i;$$

on the other hand, since $b \in B$ and $\alpha_i \in B$, we get $\mathrm{Tr}(b\alpha_i)$ is integral over A, hence lies in A because A is integrally closed. Therefore $b_i \in A$ and proves the claim.

Since A is noetherian, and B is contained in a finitely generated A-module, it is itself finitely generated. If moreover A is a PID, then $B = A^r \oplus$ (torsion). Since $B \subset L$, it is torsion free, hence $B = A^r$ is free. Finally it is to see that $r = n$, the degree of L over K. □

1.3 Integral basis

From now on, we consider the case when K is a number field.

Definition 1.3.1. *A basis $(\alpha_1, ..., \alpha_n)$ of K over $\mathbb{Q}$ is called an integral basis if it is a basis of $\mathcal{O}_K$ over $\mathbb{Z}$.*

Integral basis always exist by Proposition 1.2.5. We will discuss in next subsection how to find integral bases.

Remark 1.3.2. *The hypothesis that A be a PID is necessary to conclude that B is a free A-module. There do exist examples of number fields L/K such that $\mathcal{O}_L$ is not a free $\mathcal{O}_K$-module*[1]*.*

Corollary 1.3.3. *The ring of integers in a number field K is the largest subring that is finitely generated as a $\mathbb{Z}$-module.*

Proof. This is clear: $\mathcal{O}_K$ is finitely generated $\mathbb{Z}$-modue; if B is another subring which is finitely generated as $\mathbb{Z}$-module, then it consists of integral elements, hence is contained in $\mathcal{O}_L$. □

Proposition 1.3.4. *Let $\alpha_1, ..., \alpha_n$ be an integral basis of K and $(\beta_1, ..., \beta_n)$ be an arbitrary n-tuple of elements in $\mathcal{O}_K$ which form a basis of $K/\mathbb{Q}$. Then $\mathrm{Disc}(\beta_1, ..., \beta_n)$ equals to $\mathrm{Disc}(\alpha_1, ..., \alpha_n)$ times a square integer. In particular, $(\beta_1, ..., \beta_n)$ is an integral basis if and only if*

$$\mathrm{Disc}(\beta_1, ..., \beta_n) = \mathrm{Disc}(\alpha_1, ..., \alpha_n).$$

[1] when it is free, we have the notion of a *relative* integral basis

Proof. Write β_i as a $\mathbb{Z}$-linear combination of the α_j, we obtain a matrix $C \in M_n(\mathbb{Z})$ such that $\det(C) \neq 0$ and $(\beta_1, ..., \beta_n) = (\alpha_1, ..., \alpha_n)C$. Since $\det(C) \in \mathbb{Z}$, we obtain the result. $\square$

Definition 1.3.5. *The discriminant of K, denoted by $\Delta_K \in \mathbb{Z}$, is the discriminant of an integral basis of K.*

Remark 1.3.6. *The discriminant Δ_K need not be square-free in general.*

Chapter 2

Week 2

2.1 Quadratic fields

Theorem 2.1.1. *Let $K = \mathbb{Q}(\sqrt{d})$ with and integer $d \neq 1$ squarefree. Then we have $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\omega_d$, where*

$$\omega_d = \begin{cases} \sqrt{d} & \text{if } d \equiv 2, 3 \mod 4 \\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \mod 4 \end{cases}$$

Proof. It is easy to check that ω_d is an integer. Left to show that if $x = a + b\sqrt{d}$ with $a, b \in \mathbb{Q}$ non-zero, is an integer, tehn $x \in \mathbb{Z} + \mathbb{Z}\omega_d$. Indeed, the minimal polynomial of x over $\mathbb{Q}$ is

$$X^2 - 2aX + (a^2 - b^2 d) = 0.$$

Therefore, x is an integer if and only if $2a, a^2 - b^2 d \in \mathbb{Z}$. If $a \in \mathbb{Z}$, then $b \in \mathbb{Z}$ as d is squarefree. Otherwise, if a is a half-integer, then b has to be a half-integer too. Write $a = \frac{a'}{2}$ (resp. $b = \frac{b'}{2}$), then $a', b' \in \mathbb{Z}$ are odd, hence $a'^2, b'^2 \equiv 1 \mod 4$. So the condition $a'^2 - b'^2 d \in 4\mathbb{Z}$ holds if and only if $d \equiv 1 \mod 4$. $\square$

Fact: we also have

$$\mathrm{Disc}(1, \omega_d) = \begin{cases} 4d & \text{if } d \equiv 2, 3 \mod 4 \\ d & \text{if } d \equiv 1 \mod 4 \end{cases}$$

2.2 Computing discriminant

Proposition 2.2.1. *Let α be an arbitrary element of K, and $f(X) \in \mathbb{Q}[X]$ be its minimal polynomial. Then*

$$\mathrm{Disc}(1, \alpha, ..., \alpha^{n-1}) = \begin{cases} 0 & \text{if } \deg f < n \\ (-1)^{\frac{n(n-1)}{2}} \mathrm{N}_{K/\mathbb{Q}}(f'(\alpha)) & \text{if } \deg f = n \end{cases}$$

Proof. We already know that Disc $\neq 0$ if and only if $\{1, ..., \alpha^{n-1}\}$ form a basis, if and only if $n = \deg f$. So we assume $n = \deg f$ in the rest.

Denote by $\sigma_1, ..., \sigma_n$ the complex embeddings of K. Then

$$\mathrm{Disc}(1, \alpha, ..., \alpha^{n-1}) = [\det(\sigma_i(\alpha^{j-1}))_{1 \leq i,j \leq n}]^2 = \prod_{1 \leq i < j \leq n} (\sigma_i(\alpha) - \sigma_j(\alpha))^2,$$

where we have used Vandermonde's determinant formula. The proposition then follows frm

$$N_{K/\mathbb{Q}}(f'(\alpha)) = \prod_{i=1}^{n} \sigma(f'(\alpha)) = \prod_{i=1}^{n} \prod_{j \neq i} (\sigma_i(\alpha) - \sigma_j(\alpha)).$$

□

Example 2.2.2. *With the notation above, we denote by* Disc(f)*, called the* discriminant *of* f*:*

$$\mathrm{Disc}(f) := \prod_{1 \leq i < j \leq n} (\sigma_i(\alpha) - \sigma_j(\alpha))^2.$$

1. *if* $f(X) = X^n + a$*, with* $a \in \mathbb{Q}$ *and* $\sqrt[n]{-a} \notin \mathbb{Q}$*, then*

$$d(f) = (-1)^{n(n-1)/2} n^n a^{n-1}.$$

2. *If* $f(X) = X^n + aX + b \in \mathbb{Q}[X]$ *irreducible, then*

$$\mathrm{Disc}(f) = (-1)^{n(n-1)/2}[(-1)^{n-1}(n-1)^{n-1}a^n + n^n b^{n-1}].$$

   For example, if $n = 2, 3$*, we obtain* $a^2 - 4b$ *and* $-(4a^3 + 27b^2)$ *respectively.*

3. *If* $f(X) = X^3 + bX^2 + cX + d$*, then*

$$\mathrm{Disc} = b^2c^2 - 4c^3 - 4b^3d - 27d^2 + 18bcd.$$

2.3 Finding integral basis

Lemma 2.3.1. *Let* $\alpha_1, ..., \alpha_n$ *be* n *elements of* $\mathcal{O}_K$ *which form a basis of* K *over* $\mathbb{Q}$*. Then it is* not *an integral basis if and only if there exists a rational prime with* $p^2 | \mathrm{Disc}(\alpha_1, ..., \alpha_n)$ *and some* $x_i \in \{0, 1, ..., p-1\}$ *for* $1 \leq i \leq n$ *such that not all of* x_i *are zero and* $\sum_{i=1}^n x_i\alpha_i \in p\mathcal{O}_K$*.*

Proof. Choose an integral basis $(\beta_1, ..., \beta_n)$ and write $(\alpha_1, ..., \alpha_n) = (\beta_1, ..., \beta_n)C$ for some matrix $C \in M_n(\mathbb{Z})$. Then $(\alpha_1, ..., \alpha_n)$ is an integral basis if and only if $\det(C) = \pm 1$. Assume it is not an integral basis. Let p be a prime dividing $\det(C)$. Then $p^2 | \mathrm{Disc}(\alpha_1, ..., \alpha_n) = \det(C)^2 \Delta_K$. Denote by $\overline{C}$ the reduction of C mod p, so that $\overline{C} \in M_n(\mathbb{F}_p)$ and $\det(\overline{C}) = 0$. Let $v := (\overline{x}_1, ..., \overline{x}_n)^T \in \mathbb{F}_p^n$ be a non-zero column vector such that $\overline{C} \cdot v = 0$. If x_i denotes the unique lift of $\overline{x}_i$ in $\{0, ..., p-1\}$, then we see that $\sum_i x_i\alpha_i \in p\mathcal{O}_K$.[1] Conversely, if such a non-zero $\sum_i x_i\alpha_i \in p\mathcal{O}_K$ exists, then $0 \neq (\overline{x}_1, ..., \overline{x}_n) \in \ker(\overline{C})$. Hence $\det C$ is divisible by p, and $(\alpha_1, ..., \alpha_n)$ is not an integral basis. □

In particular, if $\mathrm{Disc}(\alpha_1, ..., \alpha_n) \in \mathbb{Z}$ is square-free, then it is an integral basis.

Example 2.3.2. *The polynomial* $f(X) = X^5 - X + 1 \in \mathbb{Q}[X]$ *is irreducible (check this!). Let* α *be a root of* f *in* $\mathbb{C}$*, then* $K := \mathbb{Q}(\alpha)$ *is a field of degree* 5*. We compute*

$$\mathrm{Disc}(\alpha) = \mathrm{N}_{K/\mathbb{Q}}(f'(\alpha)) = (4^4(-1)^5 + 5^5) = 2869 = 19 \cdot 151.$$

Since it is square-free, $\{1, \alpha, ..., \alpha^4\}$ *is an integral basis of* $\mathcal{O}_K$*. (This is called* power integral basis.*)*

[1] as $(\alpha_1 \cdots \alpha_n)(\overline{x}_1 \cdots \overline{x}_n)^T = (\beta_1 \cdots \beta_n)C(\overline{x}_1 \cdots \overline{x}_n)^T$

Example 2.3.3. *(Dedekind) Let $f(X) = X^3+X^2-2X+8 \in \mathbb{Q}[X]$. First it is irreducible*[2]. *Let α be a root in $\mathbb{C}$.*

(i) We have $\mathrm{Disc}(f) = 4+32-32-27\cdot 64+18\cdot(-2)\cdot 8 = -4.\cdot 503$.

(ii) However, $\beta := 4/\alpha \in \mathcal{O}_K$. (It is easy to get an integral equation starting from f). Moreover, $\mathrm{Disc}(1,\alpha,\beta) = 503$. *Indeed, $f(\alpha) = 4$ implies $\alpha^2 = 2-\alpha-2\beta$, so*

$$(1,\alpha,\alpha^2) = (1,\alpha,\beta)\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & -1 \\ 0 & 0 & -2 \end{pmatrix}$$

hence the result.

(iii) For any element $x \in \mathcal{O}_K$, $\{1,x,x^2\}$ can't be an integral basis, because we always have $2|\mathrm{Disc}(1,x,x^2)$. *(Exercise)*

If we write $x = a+b\alpha+c\beta$, with $a,b,c \in \mathbb{Z}$, then using $\beta^2 = -2-2\alpha+\beta$ we obtain

$$x^2 = a^2+b^2\alpha^2+c^2\beta^2+2ab\alpha+2ac\beta+8bc = const.+(-b^2-2c^2+2ab)\alpha+(-2b^2+c^2+2ac)\beta.$$

Therefore the determinant of C is

$$b(-2b^2+c^2+2ac)-c(-b^2-2c^2+2ab) = -2b^3+bc^2+b^2c+2c^3.$$

In sum, $\mathcal{O}_K$ is not of the form $\mathbb{Z}[x]$ for any $x \in \mathcal{O}_K$.

Proposition 2.3.4. *Let $\alpha \in \mathcal{O}_K$ be such that $K = \mathbb{Q}(\alpha)$ and $f(X) \in \mathbb{Z}[X]$ be its minimal polynomial. Assume that for each prime p with $p^2|\mathrm{Disc}(1,\alpha,...,\alpha^{n-1})$, there exists an integer i (which may depend on p) such that $f(T+i)$ is an Eisenstein polynomial for p. Then $\mathcal{O}_K = \mathbb{Z}[\alpha]$.*

Recall that a polynomial $f(X) = X^n + a_{n-1}X^{n-1}+\cdots+a_0$ is called an Eisenstein polynomial for p, if $p|a_i$ for all i and $p^2 \nmid a_0$.

Proof. Note that $\mathbb{Z}[\alpha] = \mathbb{Z}[\alpha+i]$ for any $i \in \mathbb{Z}$. We need to show that if $f(X) = X^n + a_{n-1}X^{n-1}+\cdots+a_0$ is Eisenstein for some prime p, then any x of the form $\frac{1}{p}\sum_{i=0}^{n-1} x_i\alpha^i$ does not belong to $\mathcal{O}_K$, where $x_i \in \{0,...,p-1\}$ not all zero. Put $j = \min\{i|x_i \neq 0\}$. Then

$$\mathrm{N}_{K/\mathbb{Q}}(x) = \frac{\mathrm{N}_{K/\mathbb{Q}}(\alpha)^j}{p^n}\mathrm{N}_{K/\mathbb{Q}}(\sum_{i=j}^{n-1} x_i\alpha^{i-j}).$$

We claim that $\mathrm{N}_{K/\mathbb{Q}}(\sum_{i=j}^{n-1} x_i\alpha^{i-j}) \equiv x_j^n \mod p$, in particular $\neq 0 \mod p$. Since the denominator of $\frac{a_0^j}{p^n}$ is divisible by p (as $p||\mathrm{N}_{K/\mathbb{Q}}(\alpha) = (-1)^n a_0$), it follows that $\mathrm{N}_{K/\mathbb{Q}}(x) \notin \mathbb{Z}$, hence $x \notin \mathcal{O}_K$. To prove the claim, let $\sigma_1,...,\sigma_n$ be the complex embeddings of K. Then

$$\mathrm{N}_{K/\mathbb{Q}}(\sum_{i=j}^{n-1} x_i\alpha^{i-j}) = \prod_{k=1}^{n}(x_j + x_{j+1}\sigma_k(\alpha)^{i-j}+\cdots+x_{n-1}\sigma_k(\alpha)^{n-1}).$$

Expanding the product, we see that all terms, except for x_j^n, are divisible by p, since they can be expressed as linear combinations of a_k for $k \geq 1$, which is elementary symmetric functions of α_i. □

Exercise: (1) Prove that $\mathbb{Z}[i]$ is a PID. (2) determine the prime elements in $\mathbb{Z}[i]$.

[2] Otherwise, there would exist a root $x \in \{\pm1,\pm2,\pm4,\pm8\}$; this is not the case by a direct check

2.4 Cyclotomic fields

Let $M \geq 3$ be an integer and $\zeta_N \in \mathbb{C}$ be a primitive N-th root of unity. Consider the number field $\mathbb{Q}(\zeta_N)$. Then we know that $\mathbb{Q}(\zeta_N)$ is a Galois extension of $\mathbb{Q}$ with Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times$. We shall determine ring of integer $\mathcal{O}_{\mathbb{Q}(\zeta_N)}$ and an integral basis of $\mathbb{Q}(\zeta_N)$.

First, recall the cyclotomic polynomial

$$\Phi_N(X) := \prod_{a \in (\mathbb{Z}/N\mathbb{Z})^\times} (X - \zeta_N^a) \in \mathbb{Z}[X].$$

We know that $\Phi_N(X)$ is just the minimal polynomial of ζ_N, with degree being $\phi(N)$, Euler's function.

Proposition 2.4.1. *If $N = p^n$ for a prime p so that $\phi(p^n) = p^{n-1}(p-1)$, then*

$$\mathrm{Disc}(1, \zeta_{p^n}, ..., \zeta_{p^n}^{\phi(p^n)-1}) = \pm p^{p^{n-1}(pn-n-1)}.$$

Moreover, we have $-$ if $p \equiv 3 \mod 4$ or $p^n = 4$, and we have $+$ otherwise.

Proof. Write $K = \mathbb{Q}_p(\zeta_{p^n})$ and $m = \phi(p^n) = p^{n-1}(p-1)$. By Proposition 2.2.1, we need to compute $|\mathrm{N}_{\mathbb{Q}(\zeta_{p^n}/\mathbb{Q})}(\Phi'_{p^n}(\zeta_{p^n}))|$, with sign $(-1)^{\frac{m(m-1)}{2}}$. Since $N = p^n$, we get

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

In other words,

$$(X^{p^{n-1}} - 1)\Phi_{p^n}(X) = X^{p^n} - 1.$$

Taking derivation, and substituting X by ζ_{p^n}, we obtain

$$(\zeta_{p^n}^{p^{n-1}} - 1)\Phi'_{p^n}(\zeta_{p^n}) = p^n \zeta_{p^n}^{p^n - 1}.$$

Hence, $\Phi'_{p^n}(\zeta_{p^n}) = p^n/\zeta_{p^n}(\zeta_{p^n}^{p^{n-1}} - 1)$ (using $\zeta_{p^n}^{p^n} = 1$), and it suffices to compute respectively $\mathrm{N}_{K/\mathbb{Q}_p}(p^n)$, $\mathrm{N}_{K/\mathbb{Q}_p}(\zeta_{p^n})$ and $\mathrm{N}_{K/\mathbb{Q}_p}(\zeta_{p^n}^{p^{n-1}} - 1)$.

(a) $\mathrm{N}_{K/\mathbb{Q}_p}(p^n) = (p^n)^m = p^{nm}$;

(b) it is clear that $\mathrm{N}_{K/\mathbb{Q}_p}(\zeta_{p^n}) = (-1)^m$;

(c) Let $\omega = \zeta_{p^n}^{p^{n-1}}$, then ω is a primitive p-th root of unity, i.e. $\sim \zeta_p$. The minimal polynomial of ω over $\mathbb{Q}$ is Φ_p, so the one of $\omega - 1$ is

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

Therefore, $\mathrm{N}_{\mathbb{Q}(\omega)/\mathbb{Q}}(\omega - 1) = (-1)^{p-1}p$, and

$$\mathrm{N}_{K/\mathbb{Q}}(\omega - 1) = \mathrm{N}_{K/\mathbb{Q}(\omega)}(\mathrm{N}_{\mathbb{Q}(\omega)/\mathbb{Q}}(\omega - 1)) = ((-1)^{p-1}p)^{p^{n-1}} = (-1)^m p^{p^{n-1}}.$$

Here we have used the fact that $[K : \mathbb{Q}(\omega)] = p^{n-1}$.

Finally we deduce that

$$\mathrm{Disc}(1, \zeta_{p^n}, ..., \zeta_{p^n}^{m-1}) = (-1)^{m(m-1)/2} p^{p^{n-1}(np-n-1)}.$$

To check the last assertion, $m(m-1)/2$ is odd if and only if $m \equiv 2, 3 \mod 4$, i.e.

$$p^{n-1}(p-1) \equiv 2, 3 \mod 4.$$

If $p = 2$, this holds only when $n = 2$, i.e. $p^2 = 4$. If $p \geq 3$, this holds if and only if $p \equiv 3 \mod 4$ (since $p \geq 3$ is prime, it is $\equiv 1, 3 \mod 4$). □

Corollary 2.4.2. *If p is a prime, then the ring of integers of $\mathbb{Q}(\zeta_{p^n})$ is $\mathbb{Z}[\zeta_{p^n}]$.*

Proof. Because $\Phi_{p^n}(X+1)$ is an Eisenstein polynomial for p, we may apply Proposition 2.3.4. □

Lemma 2.4.3. *If $M, N \geq 2$ are integers with $\gcd(M, N) = 1$, then we have $\mathbb{Q}(\zeta_M) \cap \mathbb{Q}(\zeta_N) = \mathbb{Q}$.*

Proof. Note that $\mathbb{Q}(\zeta_{MN}) = \mathbb{Q}(\zeta_M)\mathbb{Q}(\zeta_N)$. By field theory,

$$[\mathbb{Q}(\zeta_{MN}) : \mathbb{Q}(\zeta_N)] = [\mathbb{Q}(\zeta_M) : \mathbb{Q}(\zeta_M) \cap \mathbb{Q}(\zeta_N)].$$

Hence, it suffices to prove that $[\mathbb{Q}(\zeta_{MN}) : \mathbb{Q}(\zeta_N)] = \phi(M)$. However, their degrees over $\mathbb{Q}$ are respectively $\phi(MN)$ and $\phi(N)$, so it suffices to check $\phi(MN) = \phi(M)\phi(N)$ when $(M, N) = 1$. This is well-known. □

If K and L are two number fields, let KL be the composite field inside $\mathbb{C}$. Consider the subring

$$\mathcal{O}_K\mathcal{O}_L = \{x_1y_1 + \cdots + x_ry_r | x_i \in \mathcal{O}_K, y_j \in \mathcal{O}_L\}.$$

We always have $\mathcal{O}_K\mathcal{O}_L \subset \mathcal{O}_{KL}$, but they are not equal in general.

Proposition 2.4.4. *Assume that $K \cap L = \mathbb{Q}$, and let $d = \gcd(\Delta_K, \Delta_L)$. Then we have*

$$\mathcal{O}_{KL} \subset \frac{1}{d}\mathcal{O}_K\mathcal{O}_L.$$

Proof. Let $(\alpha_1, ..., \alpha_n)$ and $(\beta_1, ..., \beta_m)$ be integral bases of K and L respectively. Any $x \in \mathcal{O}_{KL}$ can be written as

$$x = \sum_{i,j} \frac{x_{ij}}{r}\alpha_i\beta_j, \quad \text{with } x_{ij}, r \in \mathbb{Z},\ \gcd(x_{11}, ..., x_{nm}, r) = 1.$$

We have to show that $r|d$, i.e. $r|\Delta_K$ and $r|\Delta_L$. By symmetry, it suffices to prove that $r|\Delta_L$. Let $(\alpha_i^\vee)_{1\leq i\leq n} \in K$ be the dual basis of $(\alpha_i)_{1\leq i\leq n}$ with respect to $\mathrm{Tr}_{K/\mathbb{Q}}$. Then we have

$$\mathrm{Tr}_{KL/L}(x\alpha_i^\vee) = \sum_{k,l} \frac{x_{k,l}}{r}\mathrm{Tr}_{KL/L}(\alpha_k\beta_l\alpha_i^\vee) = \sum_l \frac{x_{i,l}}{r}\beta_l.$$

Here we used that, for $x \in K$, $\mathrm{Tr}_{KL/L} = \mathrm{Tr}_{K/\mathbb{Q}} = \sum_{\sigma:K\hookrightarrow\overline{\mathbb{Q}}} \sigma(x)$.[3] On the other hand, we have $\alpha_i^\vee \in \frac{1}{\Delta_K}\mathcal{O}_K$ by definition of $\alpha_i^\vee$ and Cramer's rule. So $x\alpha_i^\vee \in \frac{1}{\Delta_K}\mathcal{O}_{KL}$, and $\mathrm{Tr}_{KL/L}(x\alpha_i^\vee) \in \frac{1}{\Delta_K}\mathrm{Tr}_{KL/L}(\mathcal{O}_{KL}) \subset \frac{1}{\Delta_K}\mathcal{O}_L$, i.e.

$$\Delta_K\mathrm{Tr}_{KL/L}(x\alpha_i^\vee) \in \mathcal{O}_L.$$

But $(\beta_j)_{1\leq j\leq m}$ is a basis of $\mathcal{O}_L$ over $\mathbb{Z}$, thus $\Delta_K\frac{x_{ij}}{r} \in \mathbb{Z}$ for all i, j (because any element in $\mathcal{O}_L$ has a *unique* expression as combination of β_j with coefficients in $\mathbb{Z}$), and so $r|\Delta_K$. □

[3] We may extend $\sigma : K \hookrightarrow \overline{\mathbb{Q}}$ to L-embeddings $KL \hookrightarrow \overline{\mathbb{Q}}$

Corollary 2.4.5. *Assume that* $K \cap L = \mathbb{Q}$ *and* $\gcd(\Delta_K, \Delta_L) = 1$. *Then*

1. $\mathcal{O}_{KL} = \mathcal{O}_K \mathcal{O}_L$.
2. *If* $\{\alpha_1, ..., \alpha_n\}$ *and* $\{\beta_1, ..., \beta_m\}$ *are integral bases of* K, L *respectively, then* $\{\alpha_i \beta_j\}$ *is an integral basis of* KL *over* $\mathbb{Q}$.
3. $\Delta_{KL} = \Delta_K^m \Delta_L^n$.

Proof. (1), (2) are clear. We left the proof of (3) as an exercise. ☐

Theorem 2.4.6. *The ring of integers of* $\mathbb{Q}(\zeta_N)$ *is* $\mathbb{Z}[\zeta_N]$.

Proof. Proof goes by induction on the number of prime factors of N based on 2.4.2 and 2.4.5. ☐

Week 2 Exercise

1. Complete the example of Dedekind (iii).
2. Let α be a root of $X^3 - X - 4 = 0$. Prove that $\{1, \alpha, \frac{1}{2}(\alpha + \alpha^2)\}$ is an integral basis of $\mathbb{Q}(\alpha)$.
3. For any number field d, prove that $\Delta_K \equiv 0, 1 \mod 4$.

Chapter 3

W3 (03-19): Dedekind domains

3.1 Dedekind domains

Definition 3.1.1. *An integral domain A is called a* Dedekind domain *if it is Noetherian and integrally closed, and one-dimensional, i.e. every non-zero prime ideal is maximal.*

Example 3.1.2. *Every principal ideal domain is a Dedekind domain, e.g. $\mathbb{Z}$ and $F[X]$ where F is a field.*

The following result provides us with many interesting Dedekind domains.

Proposition 3.1.3. *Let K be a number field. Then $\mathcal{O}_K$ is a Dedekind domain.*

Proof. It is clearly Noetherian, and integrally closed by definition. Left to show that $\mathcal{O}_K$ is one-dimensional. We shall use the following proof. Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_K$; then $\mathfrak{p} \cap \mathbb{Z} \neq 0$. Indeed, take any $0 \neq \alpha \in \mathfrak{p}$ and let $X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$ be an integral equation with $a_0 \neq 0$, then $a_0 = -(\cdots) \in \alpha\mathcal{O}_K \cap \mathbb{Z}$, hence $a_0 \in \mathfrak{p} \cap \mathbb{Z}$. Hence $\mathfrak{p} \cap \mathbb{Z} \neq 0$ and is of the form (p) for some prime number p.

Since $\mathcal{O}_K/\mathfrak{p}$ is integral over $\mathbb{Z}/(p) \cong \mathbb{F}_p$, we conclude by the next lemma. $\square$

Lemma 3.1.4. *If A is a domain and contains a subfield k. If A is algebraic (or integral) over k, then A is a field.*

Proof. For any $0 \neq u \in A$, $k[u]$ is a domain and finite over k, hence is a field, meaning that u is invertible. So A is a field itself. $\square$

Definition 3.1.5. *Let A be domain with fraction field K. Then a fractional ideal I of A is a sub-A-module of K such that there exists $d \in A$ with $dI \subset A$.*

Every finitely generated R-submodule of K is a fractional ideal; if R is noetherian, these are all the fractional ideals of R. If I and J are fractional ideals of A, then

$$I + J, I \cdot J$$

are both fractional ideals. More importantly, if R is noetherian, I is a fractional ideal, and define

$$I^{-1} := \{x \in K |\ xI \subset A\},$$

then I^{-1} is also a fractional ideal.

The main result of this subsection is the following important theorem.

Theorem 3.1.6. *Let A be a Dedekind domain. Every ideal I of A has a factorization*

$$I = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$$

where $\mathfrak{p}_i$ are distinct prime ideals and $a_i \in \mathbb{Z}_{\geq 1}$. Moreover the factorization is unique up to order, i.e. if I has two factorizations $\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r} = \mathfrak{q}_1^{b_1} \cdots \mathfrak{q}_s^{b_s}$, then $r = s$ and for each $1 \leq i \leq r$, there exists a unique j such that $\mathfrak{p}_i = \mathfrak{q}_j$ and $a_i = b_j$.

We first establish some lemmas.

Lemma 3.1.7. *Let A be a Noetherian ring. Then every ideal $I \neq 0$ of A contains a product of prime ideals.*

Proof. Let $\mathcal{S}$ be the set of ideals that do not contain any product of prime ideals. Suppose that $\mathcal{S}$ is non-empty. Since A is Noetherian, $\mathcal{S}$ contains a maximal element, say I. Then I can not be a prime ideal, so there exist $a, b \in A$ such that $a, b \notin I$ but $ab \in I$. Let $I_1 = I + (a)$ and $I_2 = I + (b)$. The maximality of I implies that $I_1, I_2 \notin \mathcal{S}$, hence both contain a product of prime ideals. But we have $I_1 I_2 \subset I$, so I also contains a product of prime ideals, a contradiction. □

Lemma 3.1.8. *Let A be a Dedekind domain and $\mathfrak{p}$ be a non-zero prime ideal of A. Then for any non-zero ideal $\mathfrak{a}$ of A, we have $\mathfrak{a}\mathfrak{p}^{-1} \neq \mathfrak{a}$. Consequently, $\mathfrak{p}\mathfrak{p}^{-1} = A$.*

Proof. Let $a \in \mathfrak{p}$, $a \neq 0$ and $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subset (a) \subset \mathfrak{p}$, with r as small as possible. Then one of the $\mathfrak{p}_i$, say $\mathfrak{p}_1$, is contained in $\mathfrak{p}$ (otherwise take $x_i \in \mathfrak{p}_i \backslash \mathfrak{p}$), and so $\mathfrak{p}_1 = \mathfrak{p}$ because $\mathfrak{p}_1$ is maximal. Since $\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\subseteq (a)$ (by the minimality of r), there exists $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r$ such that $b \notin (a)$, i.e. $a^{-1}b \notin A$. On the other hand, we have $b\mathfrak{p} \subseteq (a)$, i.e. $a^{-1}b\mathfrak{p} \subseteq A$, thus $a^{-1}b \in \mathfrak{p}^{-1}$. It follows that $\mathfrak{p}^{-1} \neq A$.

Now let $\mathfrak{a} \neq 0$ be an ideal of A and $\alpha_1, ..., \alpha_n$ a set of generators (because A is noetherian). Let us assume that $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$. Then for every $x \in \mathfrak{p}^{-1}$,

$$x\alpha_i = \sum_j a_{ij}\alpha_j, \quad a_{ij} \in A.$$

Writing T for the matrix a_{ij}, then as seen before, $\det(xI_n - T) = 0$. It follows that x is integral over A. But A is integrally closed, so $x \in A$. This implies $\mathfrak{p}^{-1} = A$, a contradiction.

For the second assertion, note that $\mathfrak{p} \subset \mathfrak{p}\mathfrak{p}^{-1} \subset A$ by definition. Since $\mathfrak{p}$ is maximal, we have either $\mathfrak{p} = \mathfrak{p}\mathfrak{p}^{-1}$ or $\mathfrak{p}\mathfrak{p}^{-1} = A$. We conclude by the first assertion. □

Proof of Theorem 3.1.6. **Existence:** Let $\mathcal{S}$ be the set of ideals of A distinct from (0) and A which do not admit a prime ideal decomposition. Suppose that $\mathcal{S}$ is non-empty and let I be a maximal element in $\mathcal{S}$. Then I can not be prime. Thus there exists a prime (maximal) ideal $I \subsetneq \mathfrak{p}$. By Lemma, we have

$$I \subsetneq I\mathfrak{p}^{-1} \subsetneq \mathfrak{p}\mathfrak{p}^{-1} = A.$$

By the maximality of I, we see that $I\mathfrak{p}^{-1}$ is a product of primes, that is $I\mathfrak{p}^{-1} = \prod_{i=2}^r \mathfrak{p}_i$. Since $\mathfrak{p}\mathfrak{p}^{-1} = A$, we obtain $I = \mathfrak{p}\mathfrak{p}_2 \cdots \mathfrak{p}_r$.

Uniqueness: Suppose that $\prod_{i=1}^r \mathfrak{p}_i = \prod_j \mathfrak{q}_j$. If $r \geq 1$, then $\mathfrak{p}_1 \supset \prod_{j=1}^s \mathfrak{q}_j$. It follows that $\mathfrak{p}_1 \supset \mathfrak{q}_j$ for some j.[1] Since every non-zero prime ideal of A is maximal, we see that $\mathfrak{p}_1 = \mathfrak{q}_j$. We may assume that $j = 1$ up to renumerate the $\mathfrak{q}_j$. By Lemma 3.1.8, we get a cancellation: $\prod_{i=2}^r \mathfrak{p}_i = \prod_{j=2}^s \mathfrak{q}_j$. By induction, we obtain the result. □

[1] Otherwise, assume $\mathfrak{q}_j \not\subseteq \mathfrak{p}_1$ for any j; let $x_j \in \mathfrak{q}_j \backslash \mathfrak{p}_1$, then $\prod_j x_j \notin \mathfrak{p}_1$, a contradiction to $\prod_j \mathfrak{q}_j \subset \mathfrak{p}_1$.

Corollary 3.1.9. *A Dedekind domain is a unique factorization domain UFD if and only if it is a PID.*

Proof. Let A be a Dedekind domain. $\Leftarrow$ is clear (every PID is a UFD). Prove $\Rightarrow$. By Theorem 3.1.6, it suffices to prove that every prime ideal $\mathfrak{p}$ of A is principal. Choose $0 \neq x \in \mathfrak{p}$ and let $x = p_1 \cdots p_r$ be a prime factorization of x (by UFD property). Then $p_i \in \mathfrak{p}$ for some i. But (p_i) is a non-zero prime ideal, hence maximal, so we get $\mathfrak{p} = (p_i)$. □

Corollary 3.1.10. *Let I be a fractional ideal of a Dedekind domain. Then I admits a unique factorization $I = \prod_{i=1}^{r} \mathfrak{p}_i^{a_i}$, where $\mathfrak{p}_i$ are prime ideals distinct with each other and $a_i \in \mathbb{Z}$ non-zero (for uniqueness). Moreover, I is an ideal if and only if $a_i > 0$ for all i.*

Proof. Clear. One need to show, if I is an ideal with some $a_i < 0$, then I is not an ideal of A, i.e. $I \not\subseteq A$. □

Definition 3.1.11. *A fractional ideal I is called* invertible *if there exists another ideal J such that $IJ = R$.*

Corollary 3.1.12. *In a Dedekind domain, every non-zero fractional ideal is invertible.*

This follows from Theorem 3.1.6. In fact, this can be used as a definition of Dedekind domains.

Example 3.1.13. *Let $K = \mathbb{Q}(\sqrt{-5})$. Then its ring of integers is just $\mathbb{Z}[\sqrt{-5}] = \mathbb{Z} \oplus \mathbb{Z}\sqrt{-5}$. In this ring, 21 can be decomposed in two ways*

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5}) \cdot (1 - 2\sqrt{-5}).$$

All factors here are irreducible in $\mathcal{O}_K$. For example, if $3 = \alpha\beta$ with α, β non-units, then $9 = \mathrm{N}(\alpha)\mathrm{N}(\beta)$, so $\mathrm{N}(\alpha) = \pm 3$. But the equation

$$\mathrm{N}(x + y\sqrt{-5}) = x^2 + 5y^2 = \pm 3$$

has no solutions in $\mathbb{Z}$. This leads Kummer to introduce ideal numbers*. We would have*

$$3 = \mathfrak{p}_1\mathfrak{p}_2, \quad 7 = \mathfrak{p}_3\mathfrak{p}_4, \quad 1 + 2\sqrt{-5} = \mathfrak{p}_1\mathfrak{p}_3, \quad 1 - 2\sqrt{-5} = \mathfrak{p}_2\mathfrak{p}_4$$

so that $21 = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$. Here we have explicitly by a direct check ($\mathcal{O}_K$ is not a PID!)

$$\mathfrak{p}_1 = (3, 1 - \sqrt{-5}), \quad \mathfrak{p}_2 = (3, 1 + \sqrt{-5}), \quad \mathfrak{p}_3 = (7, 1 + 2\sqrt{-5}), \quad \mathfrak{p}_4 = (7, 1 - 2\sqrt{-5}).$$

For two fractional ideals I, J, we say that I divides J and write $I|J$ if $J \subseteq I$. For a fractional ideal I and a prime ideal $\mathfrak{p}$, let $v_\mathfrak{p}(I)$ denote the index of $\mathfrak{p}$ in the prime decomposition of I. For $x \in K$, we put $v_\mathfrak{p}(x) = v_\mathfrak{p}((x))$ if $x \neq 0$ and $v_\mathfrak{p}(0) := \infty$ for any $\mathfrak{p}$.

Proposition 3.1.14. *Let I, J be fractional ideals of a Dedekind domain A. Then $I|J$ if and only if $v_\mathfrak{p}(I) \leq v_\mathfrak{p}(J)$ for all primes $\mathfrak{p}$.*

Proof. Clear. □

Corollary 3.1.15. *Let I, J be fractional ideals of a Dedekind domain A. Then*

1. $I = \{x \in K | v_\mathfrak{p}(x) \geq v_\mathfrak{p}(I), \ \forall \mathfrak{p}\}$

2. $v_{\mathfrak{p}}(I+J) = \min(v_{\mathfrak{p}}(I), v_{\mathfrak{p}}(J))$ *for all primes* $\mathfrak{p}$*;*

3. $v_{\mathfrak{p}}(x+y) \geq \min(v_{\mathfrak{p}}(x), v_{\mathfrak{p}}(y))$ *for all primes* $\mathfrak{p}$*;*

4. $v_{\mathfrak{p}}(I \cap J) = \max(v_{\mathfrak{p}}(I), v_{\mathfrak{p}}(J))$ *for all primes* $\mathfrak{p}$*.*

Proof. Clear. □

Lemma 3.1.16. *(Chinese Remainder Theorem) In a Dedekind domain A, given $\mathfrak{p}_1, ..., \mathfrak{p}_r$ distinct non-zero prime ideals and given $a_1, ..., a_r \geq 0$, there exists $x \in A$ such that $v_{\mathfrak{p}_i}(x) = a_i$, for any $1 \leq i \leq r$.*

Proof. Indeed, we have isomorphisms $A/(\mathfrak{p}_1^{a_1+1} \cdots \mathfrak{p}_r^{a_r+1}) = A/\mathfrak{p}_1^{a_1+1} \oplus \cdots A/\mathfrak{p}_r^{a_r+1}$. Choose for any i, $x_i \in \mathfrak{p}_i^{a_i} - \mathfrak{p}_i^{a_i+1}$, and take $x \in A$ corresponding to (x_i). □

Note that we have no control of the behavior of x at other primes.

Corollary 3.1.17. *Let A be a Dedekind domain and I be a non-zero ideal. For any $0 \neq \alpha \in I$, there exists $\beta \in I$ such that $I = (\alpha, \beta)$. In other words, I can be generated by (at most) two elements and one of them can be chosen arbitrarily.*

Proof. Since $\alpha \in I$, $I|\alpha\mathcal{O}_K$, so we may write

$$I = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}, \quad \alpha\mathcal{O}_K = \mathfrak{p}_1^{b_1} \cdots \mathfrak{p}_r^{b_r} \mathfrak{p}_{r+1}^{b_{r+1}} \cdots \mathfrak{p}_s^{b_s}$$

with $a_i \leq b_i$ for $1 \leq i \leq r$. Using the above (2) for $(\alpha) + (\beta)$, we need to find $\beta \in \mathcal{O}_K$, such that

- $v_{\mathfrak{p}_i}(\beta) = a_i$, for $1 \leq i \leq r$;
- $v_{\mathfrak{p}_i}(\beta) = 0$ for $r+1 \leq i \leq s$.

This is possible by Chines Remainder Theorem. □

Corollary 3.1.18. *A Dedekind domain with a finite number of prime ideals is a PID.*

Proof. Let $\{\mathfrak{p}_1, ..., \mathfrak{p}_r\}$ be a complete list of all non-zero prime ideals of A. For any I, write $I = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$, with $a_i \geq 0$. For each i, choose an element $x_i \in \mathfrak{p}_i^{a_i} - \mathfrak{p}_i^{a_i+1}$, then lift them to $x \in \mathcal{O}_K$. Easy to check that $I = (x)$. □

3.2 Ideal class groups

Definition 3.2.1. *Let A be a Dedekind domain with fraction field K.*

(1) The set of fractional ideals of A form an abelian group (with respect to multiplication of ideals), which we denote by $\mathcal{I}$.

(2) A fractional ideal is called principal *if it is of the form xA with $x \in K^\times$. Principal fractional ideals form a subgroup of $\mathcal{I}$, denoted by $\mathcal{P}$.*

(3) We define Cl_K to be the quotient group $\mathcal{I}/\mathcal{P}$, called the ideal class group *of K. This is an abelian group.*

In general, Cl_K could be of infinite rank. In the case of number fields, we have the following fundamental result (see Chap. 6).

Theorem 3.2.2. *Let K be number field. Then Cl_K is a finite abelian group.*

3.3 Localization

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

Definition 3.3.1. *A subset S of A is said to be* multiplicative *if $0 \notin S$, $1 \in S$, and S is closed under multiplication, i.e. if $r, s \in S$ then $rs \in S$. If S is a multiplicative subset, then we define*

$$S^{-1}A = \{a/b \in K : b \in S\},$$

which is obviously a subring of K.

Example 3.3.2. *(1) Let $t \in A$ be non-zero. Then $\{1, t, t^2, ...\}$ is a multiplicative subset of A.*

(2) If $\mathfrak{p}$ is a prime ideal, then $S = A \backslash \mathfrak{p}$ is a multiplicative set, and we write commonly $A_{\mathfrak{p}}$ for $S^{-1}A$. Then $A_{\mathfrak{p}}$ is a local ring with maximal ideal $\mathfrak{p}A_{\mathfrak{p}}$. For example,

$$\mathbb{Z}_{(p)} = \{m/n \in \mathbb{Q} \mid n \text{ is not divisible by } p\}.$$

Proposition 3.3.3. *The map $\mathfrak{p} \mapsto \mathfrak{p}^e := \mathfrak{p}S^{-1}A$ is a bijection betwen*

$$\{\text{prime ideals of } A\} \to \{\text{prime ideals of } S^{-1}A,\ \mathfrak{p} \cap S = \emptyset\}.$$

The inverse map is $\mathfrak{q} \mapsto \mathfrak{q} \cap A$.

Note that, if $\mathfrak{p}$ is a prime ideal of A such that $\mathfrak{p} \cap S \neq \emptyset$, then any non-zero $a \in \mathfrak{p} \cap S$ becomes invertible in $S^{-1}A$, hence $\mathfrak{p}(S^{-1}A) = S^{-1}A$.

Proof. See [Milne], Prop.1.11, Prop. 1.12. □

3.3.1

Proposition 3.3.4. *Let A be a Dedekind domain, and S is some multiplicative subset.*

1. *If A is noetherian, so is $S^{-1}A$.*
2. *If B is the integral closure of A in a finite extension L/K, then $S^{-1}B$ is the integral closure of $S^{-1}A$ in L.*
3. *If A is integrally closed, so is $S^{-1}A$.*
4. *If A is Dedekind, so is $S^{-1}A$.*
5. *If $S = A \backslash \mathfrak{p}$, then $S^{-1}A$ is a PID.*

Proof. (1) is Easy. For (2), let $x = b/s \in S^{-1}B$. If b is integral over A, then clearly x is integral over $S^{-1}A$. Conversely, if $x \in L$ is integral over $S^{-1}A$, and

$$g(T) = X^n + c_{n-1}X^{n-1} + \cdots + c_0, \quad c_i \in S^{-1}A$$

is an integral equation of x, then there exists $s \in S$ such that $sc_i \in A$ for all i. Then sx is a root of $f(X) = X^n + sc_{n-1}X^{n-1} + \cdots s^n c_0 \in A[X]$, therefore sx is integral over A and $sx \in B$.

(3), (4) are easy, following from (2). For (5), uses Corollary 3.1.18. □

Proposition 3.3.5. *Let A be a Dedekind domain, and $A' = S^{-1}A$ for some multiplicative subset S.*

1. *Let $\mathfrak{p} \subset A$ be a non-zero prime, and $\mathfrak{p}' = \mathfrak{p}A'$. then $\mathfrak{p}' = A'$ if and only if $S \cap \mathfrak{p} \neq \emptyset$. If $\mathfrak{p} \cap S = \emptyset$, $\mathfrak{p}' \subset A'$ is a maximal ideal of A' with*

$$A/\mathfrak{p} \cong A'/\mathfrak{p}'.$$

2. *If I is a fractional ideal of A with prime decomposition $I = \prod_{i=1}^r \mathfrak{p}_i^{a_i}$, then $I' = IA'$ is a fractional ideal of A' with prime decomposition $I' = \prod_{i=1}^r \mathfrak{p}_i'^{a_i}$, where $\mathfrak{p}_i' = \mathfrak{p}_i A'$.*

Proof. (1) (1) is very special to Dedekind domains. In general, when $S = A - \mathfrak{p}$, then $A' = A_\mathfrak{p}$ is a local ring and $A'/\mathfrak{p}'$ is a field, the field of fractions of $A/\mathfrak{p}$. Since $A/\mathfrak{p}$ is already a field, we get the desired isomorphism.

Alternative argument: There is a natural morphism $A/\mathfrak{p} \to A'/\mathfrak{p}'$ which is injective because $\mathfrak{p}' \cap A = \mathfrak{p}$. To show the surjectivity, let $a/s \in A'$. Since $\mathfrak{p}$ is maximal and $s \notin \mathfrak{p}$, $\mathfrak{p} + (s) = A$. So let $x \in \mathfrak{p}, t \in A$ be such that $x + st = A$, then

$$\frac{a}{s} = \frac{x}{s} + t$$

so $A' = A + \mathfrak{p}'$.

(2) follows from Proposition. ☐

3.4 Norm of ideals

Let K be a number field, and $\mathcal{O}_K$ be its ring of integers.

Definition 3.4.1. *Let $0 \neq I \subset \mathcal{O}_K$ be an ideal. Define the norm of I to be*

$$N(I) := |\mathcal{O}_K/I| = [\mathcal{O}_K : I].$$

Proposition 3.4.2. 1. *If $I = (x)$ for some $x \in \mathcal{O}_K$, then $\mathrm{N}(I) = |\mathrm{N}_{K/\mathbb{Q}}(x)|$.*

2. *We have $\mathrm{N}(IJ) = \mathrm{N}(I)\mathrm{N}(J)$ for any ideals $I, J \subseteq \mathcal{O}_K$.*

3. *For $n \geq 0$, there exist only finitely many ideals $I \subset \mathcal{O}_K$ such that $N(I) = n$.*

Proof. Let $\{\alpha_1, ..., \alpha_n\}$ be a $\mathbb{Z}$-basis of $\mathcal{O}_K$. Then there exists a matrix $C \in M_n(\mathbb{Z})$ such that

$$(x\alpha_1, ..., x\alpha_n) = (\alpha_1, ..., \alpha_n)C.$$

It follows that

$$\mathrm{N}(I) = [\mathcal{O}_K : I] = [\sum_i \mathbb{Z} \cdot \alpha_i : \sum_i \mathbb{Z} : x\alpha_i] = |\det(C)|.$$

By definition, $\mathrm{N}_{K/\mathbb{Q}}(x) = \det(C)$.

(2) First the Chinese Remainder theorem implies

$$\mathcal{O}_K/(\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}) \cong \mathcal{O}_K/\mathfrak{p}_1^{a_1} \oplus \cdots \oplus \mathcal{O}_K/\mathfrak{p}_r^{a_r},$$

so we may assume I is of the form $\mathfrak{p}^a$ and show

$$N(I) = N(\mathfrak{p})^a.$$

For this we consider the natural morphism, where $\alpha \in \mathfrak{p}^a \backslash \mathfrak{p}^{a+1}$:

$$\varphi : \mathcal{O}_K \to \mathfrak{p}^a/\mathfrak{p}^{a+1}, \quad x \mapsto \alpha x + \mathfrak{p}^{a+1}.$$

This is a morphism of additive groups. Moreover, it is surjective, because $v_{\mathfrak{p}}(\alpha) = a$, so $\alpha\mathcal{O}_K + \mathfrak{p}^{a+1} = \mathfrak{p}^a$. On the other hand, the kernel of φ is $\mathfrak{p}$. Hence, φ induces an isomorphism

$$\mathcal{O}_K/\mathfrak{p} \cong \mathfrak{p}^a/\mathfrak{p}^{a+1}$$

and an induction gives the result.

(3) If $I \subset \mathcal{O}_K$ is an ideal of norm n, then $(n) \subset I \subset \mathcal{O}_K$. Note that $\mathcal{O}_K/(n)$ is finite of cardinality $n^{[K:\mathbb{Q}]}$. Therefore, there are only finitely many possibilities for I. □

If $I = \mathfrak{a}\mathfrak{b}^{-1}$ is a non-zero fractional ideal with $\mathfrak{a}, \mathfrak{b} \subset A$ ideals, then we define the norm of I as

$$N(I) := \frac{N(\mathfrak{a})}{N(\mathfrak{b})} \in \mathbb{Q}^{\times}.$$

We see that this is independent of the expression $I = \mathfrak{a}\mathfrak{b}^{-1}$.

3.5 Prime decomposition

Let L/K be a finite extension of number fields, and $\mathfrak{p} \neq 0$ be a prime of $\mathcal{O}_K$. We have

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}.$$

Lemma 3.5.1. *Let L/K be an extension of number fields and $\mathfrak{P}$ (resp. $\mathfrak{p}$) be a non-zero prime of $\mathcal{O}_L$ (resp. $\mathcal{O}_K$). Then*

1. *$\mathfrak{P} \cap \mathcal{O}_K$ is a prime of $\mathcal{O}_K$, and $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$ if and only if $\mathfrak{P}|\mathfrak{p}$.*
2. *if $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$, then $\mathcal{O}_K/\mathfrak{p}$ and $\mathcal{O}_L/\mathfrak{P}$ are both finite fields, and the latter field is a finite extension of the former one.*

Proof. (1) It is a direct check that $\mathfrak{P} \cap \mathcal{O}_K$ is still a prime ideal.

Assume $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$, then $\mathfrak{p}\mathcal{O}_L \subset \mathfrak{P}$, hence $\mathfrak{P}|\mathfrak{p}\mathcal{O}_L$, i.e. $\mathfrak{P}|\mathfrak{p}$. Conversely, if $\mathfrak{P}|\mathfrak{p}$, i.e. $\mathfrak{P}$ appears in the prime decomposition of $\mathfrak{p}\mathcal{O}_L$, so $\mathfrak{p}\mathcal{O}_L \subset \mathfrak{P}$, hence $\mathfrak{p} \subset \mathfrak{p}' := \mathfrak{P} \cap \mathcal{O}_K$. Now $\mathfrak{p}$ is non-zero prime ideal, hence is maximal, from which we deduce the equality $\mathfrak{p} = \mathfrak{p}'$.

(2) Since both $\mathfrak{p}$ and $\mathfrak{P}$ are maximal ideals, the quotients are (finite) fields of cardinality N($\mathfrak{p}$). □

Definition 3.5.2. *(1) We put*

$$e(\mathfrak{P}|\mathfrak{p}) = e_i = v_{\mathfrak{P}_i}(\mathfrak{p}\mathcal{O}_L)$$

and call it the ramification index of $\mathfrak{P}_i$ above $\mathfrak{p}$.

(2) Note that $k(\mathfrak{P}_i) := \mathcal{O}_L/\mathfrak{P}_i$ is a finite extension of $k(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}$. We put

$$f(\mathfrak{P}_i|\mathfrak{p}) = [k(\mathfrak{P}_i) : k(\mathfrak{p})],$$

and call it the residue degree of $\mathfrak{P}_i$ above $\mathfrak{p}$.

(3) We say that $\mathfrak{p}$ is

- unramified *in* L/K*, if* $e(\mathfrak{P}_i|\mathfrak{p}) = 1$ *for all* i*,*
- split *in* L/K*, if* $e(\mathfrak{P}_i|\mathfrak{p}) = f(\mathfrak{P}_i|\mathfrak{p}) = 1$ *for all* i*;*
- inert *in* L/K*, if* $g = 1$ *and* $e(\mathfrak{P}_1|\mathfrak{p}) = 1$*;*
- ramified *in* L/K*, if not unramified, i.e. there exists* i *such that* $e(\mathfrak{P}_i|\mathfrak{p}) > 1$*;*
- totally ramified *in* L/K*, if* $g = 1$ *and* $f(\mathfrak{P}_1|\mathfrak{p}) = 1$*.*

Proposition 3.5.3. *Under the above notation, we have* $\sum_{i=1}^{g} e(\mathfrak{P}_i|\mathfrak{p}) f(\mathfrak{P}_i|\mathfrak{p}) = [L : K]$*.*

This important equality is called **fundamental equality**.

Proof. (1) Note that $\mathfrak{P} \cap \mathcal{O}_K$ is always a non-zero prime of $\mathcal{O}_K$. Take $x \in$.

(2) Let q denote the cardinality of $k(\mathfrak{p})$. Then

$$[\mathcal{O}_K : \mathfrak{p}\mathcal{O}_L] = \mathrm{N}(\mathfrak{p}\mathcal{O}_L) = \prod_{i=1}^{g} \mathrm{N}(\mathfrak{P}_i)^{e_i} = \prod_{i=1}^{g} q^{e_i f_i} = q^{\sum_i e_i f_i}.$$

Note that $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ is a finite dimensional vector space over $k(\mathfrak{p})$. Thus the above computation shows that

$$\dim_{k(\mathfrak{p})} \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = \sum_{i=1}^{g} e_i f_i.$$

To conclude the proof, we have to show that $\dim_{k(\mathfrak{p})} \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = [L : K]$.

- Consider first the special case that $\mathcal{O}_L$ is a free module over $\mathcal{O}_K$ (e.g. $K = \mathbb{Q}$). Then the rank of $\mathcal{O}_L$ over $\mathcal{O}_K$ is $[L : K]$ and $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ is of dimension n over $k(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$.
- In the general case, we consider the localization of $\mathcal{O}_K$ and $\mathcal{O}_L$ at the multiplicative subset $S = \mathcal{O}_K \backslash \mathfrak{p}$, giving $\mathcal{O}_{K,\mathfrak{p}}$ and $\mathcal{O}_{L,\mathfrak{p}}$. Both of them are Dedekind domains. Moreover, $\mathcal{O}_{K,\mathfrak{p}}$ is a PID, hence $\mathcal{O}_{L,\mathfrak{p}}$ is a finite free $\mathcal{O}_{K,\mathfrak{p}}$-module of rank $n = [L : K]$ (because L, K are respectively the fields of fractions of $\mathcal{O}_{L,\mathfrak{p}}$, $\mathcal{O}_{K,\mathfrak{p}}$). Modulo the ideal $\mathfrak{p}$, we obtain $\mathcal{O}_{L,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{L,\mathfrak{p}}$ is of dimension $[L : K]$ over $k(\mathfrak{p})$. To conclude, we note the isomorphism $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong \mathcal{O}_{L,\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{L,\mathfrak{p}}$.

□

We have the following transitivity of ramification and residue indices.

Proposition 3.5.4. *Let* L/K *be as above, and* M/L *be another field extension. Let* $\mathfrak{P}_M$ *be a prime ideal of* M*,* $\mathfrak{P}_L = \mathfrak{P}_M \cap \mathcal{O}_L$ *and* $\mathfrak{p} = \mathfrak{P}_M \cap \mathcal{O}_K$*. Then we have*

$$f(\mathfrak{P}_M|\mathfrak{p}) = f(\mathfrak{P}_M|\mathfrak{P}_L) f(\mathfrak{P}_L|\mathfrak{p}), \quad e(\mathfrak{P}_M|\mathfrak{p}) = e(\mathfrak{P}_M|\mathfrak{P}_L) e(\mathfrak{P}_L|\mathfrak{p}).$$

Proof. Easy, left as an exercise. □

Exercise, Week 3

1. Let I be an integral ideal of $\mathcal{O}_K$. Consider the units in the finite ring $\mathcal{O}_K/I$; let $\varphi(I)$ be the order $|(\mathcal{O}_K/I)^\times|$. Prove that
$$\varphi(\mathfrak{p}^a) = N(\mathfrak{p})^{a-1}(N(\mathfrak{p}) - 1);$$
$$\varphi(I) = N(I) \cdot \prod_{\mathfrak{p}|I} (1 - \frac{1}{N(\mathfrak{p})}).$$
2. Determine all the integral ideals in $\mathbb{Q}(\sqrt{-5})$ with norm ≤ 15.

Chapter 4

W4: Decomposition of primes in number fields

Let L/K be an extension of number fields, $\mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal.

Theorem 4.0.1. *Let $\alpha \in \mathcal{O}_L$ be such that $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = (\mathcal{O}_K/\mathfrak{p})[\overline{\alpha}]$, where $\overline{\alpha}$ denotes the image of α. Let $f(X) \in \mathcal{O}_K[X]$ be the minimal polynomial of α. Assume that*

$$f(X) \equiv \prod_{i=1}^{g} g_i(X)^{e_i} \mod \mathfrak{p}\mathcal{O}_K[X]$$

where $e_i \geq 1$, and $g_i(X)$ is a monic polynomial whose image in $k(\mathfrak{p})[X]$ is irreducible and distinct with each other. Then $\mathfrak{P}_i = (\mathfrak{p}, g_i(\alpha)) = \mathfrak{p}\mathcal{O}_L + g_i(\alpha)\mathcal{O}_L$ is a maximal ideal of $\mathcal{O}_L$ for each i and we have the prime decomposition

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$$

with residue dgrees $f(\mathfrak{P}_i|\mathfrak{p}) = \deg(g_i)$.

Proof. (i) Put $k(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}$. We have

$$\mathcal{O}_L/\mathfrak{P}_i = (\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L)/(\overline{g}_i(\overline{\alpha})) = (\mathcal{O}_K/\mathfrak{p})[\overline{\alpha}]/(\overline{g}_i(\overline{\alpha})) = k(\mathfrak{p})[X]/(\overline{g}_i(X)).$$

Since $\overline{g}_i(X)$ is irreducible in $k(\mathfrak{p})[X]$, the quotient $k(\mathfrak{p})[X]/(\overline{g}_i(X))$ is a field. This shows that $\mathfrak{P}_i$ is a maximal ideal of $\mathcal{O}_L$. Moreover, we have

$$f(\mathfrak{P}_i|\mathfrak{p}) = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}] = \deg(\overline{g}_i) = \deg(g_i).$$

(2) To prove the decomposition, we note the assumption $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = k(\mathfrak{p})[\overline{\alpha}]$ so that

$$\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L \cong k(\mathfrak{p})[X]/(\overline{f}(X)) \cong \prod_{i=1}^{g} k(\mathfrak{p})[X]/(\overline{g}_i^{e_i}(X)).$$

Here, the last isomorphism used Chinese remainder theorem. On the other hand, note that

$$k(\mathfrak{p})[X]/(\overline{g}_i^{e_i}(X)) \cong \mathcal{O}_L/(\mathfrak{p}\mathcal{O}_L + g_i^{e_i}(\alpha)).$$

Hence, to finish the proof, it suffices to show that $\mathfrak{P}_i^{e_i} = (\mathfrak{p}, g_i^{e_i}(\alpha))$. We have

$$\mathfrak{P}_i^{e_i} = (\mathfrak{p}, g_i(\alpha))^{e_i} \subset (\mathfrak{p}, g_i^{e_i}(\alpha)).$$

We deduce $\mathfrak{P}_i^{e_i} = (\mathfrak{p}, g_i^{e_i}(\alpha))$ from the equality

$$\begin{aligned}\dim_{k(\mathfrak{p})} \mathcal{O}_L/(\mathfrak{p}, g_i^{e_i}(\alpha)) = \dim_{k(\mathfrak{p})} k(\mathfrak{p})[X]/(\overline{g}_i^{e_i}(X)) &= e_i \dim_{k(\mathfrak{p})} k(\mathfrak{p})[X]/(\overline{g}_i(X)) \\ &= e_i \dim_{k(\mathfrak{p})} \mathcal{O}_L/\mathfrak{P}_i = \dim_{k(\mathfrak{p})} \mathcal{O}_L/\mathfrak{P}_i^{e_i}.\end{aligned}$$

□

Remark 4.0.2. *There are two important special cases where the assumption $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = k(\mathfrak{p})[\overline{\alpha}]$ is satisfied:*

1. *$\mathcal{O}_L = \mathcal{O}_K[\alpha]$; then Thm. applies to any prime $\mathfrak{p}$. For example, when $K = \mathbb{Q}$ and $\{1, \alpha, ..., \alpha^{n-1}\}$ is an integral basis of $\mathcal{O}_L$.*
2. *If $\alpha \in \mathcal{O}_L$ with $\mathfrak{p} \nmid N_{L/K}(f'(\alpha))$, then $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L = k(\mathfrak{p})[\overline{\alpha}]$.*

Example 4.0.3. *Consier $f(X) = X^3 + X + 1 \in \mathbb{Q}[X]$ which is irreducible. Let α be a root of f and let $K = \mathbb{Q}(\alpha)$ which is a degree 3 extension of $\mathbb{Q}$. It is easy to see that*

$$\mathrm{Disc}(1, \alpha, \alpha^2) = -31$$

is square-free, so $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Therefore the above applies.

1. *If $p = 2$, one checks that $f(X) = 0$ has no root in $\mathbb{F}_2[X]$, hence is irreducible. So $2\mathcal{O}_K$ remains a prime ideal in $\mathcal{O}_K$, i.e. 2 is inert in $\mathcal{O}_K$.*
2. *If $p = 3$, then $f(X) = (X - 1)(X^2 + X - 1)$ in $\mathbb{F}_3[X]$ and $X^2 + X - 1$ is irreducible. Therefore $3\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$, with two prime ideals*

   $$\mathfrak{p}_1 = (3, \alpha - 1), \quad \mathfrak{p}_2 = (3, \alpha^2 + \alpha - 1).$$

   *Moreover, $f_1 = 1$ and $f_2 = 2$, and 3 is unramified in K. (*Will see that $K/\mathbb{Q}$ is not Galois.*)*
3. *If $p = 31$, then*

   $$X^3 + X + 1 \equiv (X - 3)(X - 14)^2 \mod 31.$$

   So $31\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2^3$ with $\mathfrak{p}_1 = (31, \alpha - 3)$, $\mathfrak{p}_2 = (31, \alpha - 14)$. $\mathfrak{p}_3$ is ramified so 31 is ramified in K.

4.1 Quadratic fields

Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field. Recall that $\mathcal{O}_K = \mathbb{Z}[\omega]$ with

$$\omega = \begin{cases} \sqrt{d} & d \equiv 2, 3 \mod 4 \\ \frac{1}{2}(1 + \sqrt{d}) & d \equiv 1 \mod 4 \end{cases}$$

The discriminant is respectively $4d$ and d. Also recall the Legendre symbol, $\left(\frac{d}{p}\right)$, defined by: let p be a prime, $p \nmid d$, let $\left(\frac{d}{p}\right)$ be 1 is d is a square mod p, be -1 otherwise.

Theorem 4.1.1. *Let $K = \mathbb{Q}(\sqrt{d})$ with d a square free interger. Let p be a prime. Then*

1. *p is ramified in K (i.e. $p\mathcal{O}_K = \mathfrak{p}^2$) if and only if $p|\Delta_K$; in particular, 2 is ramified in K if and only if $d \equiv 2, 3 \mod 4$;*

2. *if p is odd and unramified in K, then p splits in K if and only if* $(\frac{d}{p}) = 1$*; and p is inert if and only if* $(\frac{d}{p}) = -1$*;*

3. *when* $d \equiv 1 \mod 4$*, then* 2 *splits in K if and only if* $d \equiv 1 \mod 8$*; and p is inert in K if and only if* $d \equiv 5 \mod 8$*.*

Proof. Let α be as above. Then the minimal polynomial of α is

$$f(x) = \begin{cases} x^2 + x + \frac{1-d}{4} & \text{if } d \equiv 1 \mod 4 \\ x^2 - d & \text{if } d \equiv 2, 3 \mod 4 \end{cases}$$

and Δ_K is equal to $\mathrm{Disc}(f)$ (i.e. $b^2 - 4ac$).

(1) By Theorem 4.0.1, p is ramified in K if and only if $\overline{f}(X) = (X-a)^2$ for some $a \in \mathbb{F}_p$, where $\overline{f} \in \mathbb{F}_p[X]$ denotes the image of $f(x)$. The latter condition is equivalent to saying that $p | \Delta_K$.

(2) Assume p is odd and unramified in K. We have $p \not| \Delta_K$ by (1). By Theorem 4.0.1, we have the following

$$p \text{ splits in } K \Longleftrightarrow \overline{f}(X) \text{ has distinct roots in } \mathbb{F}_p.$$

So if $\overline{f}(X) = (X-a)(X-b)$ with $a, b \in \mathbb{F}_p$ and $a \neq b$, then $\Delta_K = (a-b)^2 \mod p$, i.e. it is a square in $\mathbb{F}_p$, hence equivlently $(\frac{d}{p}) = 1$. Conversely, if $(\frac{d}{p}) = 1$, assume that $d = c^2 \mod p$ with $p \not| c$. Then $\frac{1 \pm c}{2}$ (resp. $\pm c$) are two distinct roots of $\overline{f}(x)$ in $\mathbb{F}_p$ if $d \equiv 1 \mod 4$ (resp. if $d \equiv 2, 3 \mod 4$).

(3) If $d \equiv 1 \mod 8$, then $\overline{f}(X) = X^2 + X$ has two distinct roots in $\mathbb{F}_2$. If $d \equiv 5 \mod 8$, then $\overline{f}(X) = X^2 + X + 1$ is the unique irreducible polynomial of degree 2 in $\mathbb{F}_2[X]$. □

4.1.1 Fermat's theorem on sums of two squares

Question: for which positive integers n, it can be written as the sum of two squares?

By the prime decomposition, it is equivalent to ask for which primes p, it can be written as the sum of two squares?

The answer is that $p \equiv 1 \mod 4$ if $p \geq 3$. This was first claimed by Fermat. But as his many other claims, he did not write down a proof. Euler first gave such a proof based on infinite descent. Here is the proof of Dedekind[1] using the arithmetic of the imaginary quadratic number field $\mathbb{Q}(i)$, also called *Gaussian rational numbers.* It is well-known that $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$ and it is a PID. So every ideal $\mathfrak{a}$ of $\mathbb{Z}[i]$ has the form $(a + bi)$. Since

$$N(\mathfrak{a}) = (a + ib)(a - ib) = a^2 + b^2$$

is the sum of two squares, we get the following facts

(a) $n \in \mathbb{Z}_{\geq 0}$ is the sum of two squares $\Leftrightarrow n = N(\mathfrak{a})$ for some ideal $\mathfrak{a}$ of $\mathbb{Z}[i]$;

(b) If n, m are both sums of two squares, then so is nm.

Theorem 4.1.2. *(Gauss) Let* $n \in \mathbb{Z}_{\geq 0}$*,* $n = m^2 n_0$*, with* $m \in \mathbb{Z}$ *and* n_0 *squarefree. Then n is the sum of two squares if and only if* n_0 *does not admit prime factor p which* $\equiv 3 \mod 4$*.*

[1]Not Gauss himself ! His proof is more involved.

Proof. $\Leftrightarrow$: if $n_0 = 1$, it is clear. So assume $n_0 \geq 2$ and write $n_0 = p_1 \cdots p_r$, with p_i distinct primes and $p_i = 2$ or $p_i \equiv 1 \mod 4$. By (b) above, we may assume $n_0 = p$ is a prime, i.e. $r = 1$. If $p = 2$, then $p = 1^2 + 1^2$, we are done. If $p \equiv 1 \mod 4$, then $(\frac{-1}{p}) = 1$, so by Theorem ? p splits in $\mathbb{Z}[i]$, i.e. $p\mathbb{Z}[i] = \mathfrak{p}_1\mathfrak{p}_2$. Therefore $N(\mathfrak{p}_1) = p$. Hence by property (a), we know that p is a sum of two squares.

$\Rightarrow$: We may assume $m = 1$. Assume $n_0 = N(\mathfrak{a})$ for some ideal $\mathfrak{a}$ of $\mathbb{Z}[i]$. If $p|n_0$ for some $p \equiv 3 \mod 4$, then $(\frac{-1}{p}) = 1$, so $p\mathbb{Z}[i] = \mathfrak{p}$ remains a prime ideal in $\mathbb{Z}[i]$ and $N(\mathfrak{p}) = p^2$. Moreover, $\mathfrak{p}$ is the unique prime ideal such that $p|N(\mathfrak{p})$. Therefore, by writing down the prime decomposition of $\mathfrak{a}$, we obtain that $p^2|N(\mathfrak{a}) = n_0$. This contradicts the assumption that n_0 is square-free. $\square$

We could also determine the number of solutions of the equation $a^2 + b^2 = n$. Let $N(n)$ denote the cardinality of the solutions. Let

$$n = 2^l p_1^{e_1} \cdots p_r^{e_r} q_1^{f_1} \cdots q_s^{f_s},$$

where $l, r, s \geq 0$, $e_i, f_i \geq 1$, and $p_i \equiv 1 \mod 4$, $q_j \equiv 3 \mod 4$. We know that $N(n) \geq 1$ if and only if $2|f_j$ for all $1 \leq j \leq s$.

Now assume this condition holds. Then (a, b) is a solution if and only if $N(a + bi) = n$, henc $N(n)$ equals to the number of elements in $\mathbb{Z}[i]$ with norm being n. Let $\alpha \in \mathbb{Z}[i]$, if $N(\alpha) = n$, then $N(\alpha\mathcal{O}_K) = n$. Each ideal in $\mathbb{Z}[i]$ is principal, since $\mathbb{Z}[i]$ is a PID, and each ideal has 4 possibilities of generators (the units in $\mathbb{Z}[i]$ is $\{\pm 1, \pm i\}$), so we are left to determine the number of ideals with norm n.

We know the following decomposition in $\mathbb{Z}[i]$:

$$(2) = \mathfrak{p}^2, \quad N(\mathfrak{p}) = 2$$

$$(p_i) = \mathfrak{p}_i\mathfrak{p}_i', \quad N(\mathfrak{p}_i) = N(\mathfrak{p}_i') = p, \quad \mathfrak{p}_i \neq \mathfrak{p}_i'$$

$$(q_j) = \mathfrak{q}, \quad N(\mathfrak{q}_j) = q_j^2.$$

We deduce that

$$n\mathcal{O}_K = \mathfrak{p}^{2l} \prod_{i=1}^{r} (\mathfrak{p}_i\mathfrak{p}_i')^{e_i} \prod_{j=1}^{s} \mathfrak{q}_j^{f_j}.$$

If $\mathfrak{a} \subset \mathbb{Z}[i]$ is an ideal with norm n, then $n \in \mathfrak{a}$, i.e. $\mathfrak{a}|(n)$. So the prime decomposition of $\mathfrak{a}$ has the form:

$$\mathfrak{a} = \mathfrak{p}^L \prod_{i=1}^{r} \mathfrak{p}_i^{E_i} \prod_{i=1}^{r} \mathfrak{p}_i'^{E_i'} \prod_{j=1}^{s} \mathfrak{q}_j^{F_j}.$$

And the condition $N(\mathfrak{a}) = n$ reads as

$$n = 2^L \prod_{i=1}^{r} p_i^{E_i + E_i'} \prod_{j=1}^{s} q_j^{2F_j}.$$

Hence we obtain

$$l = L, \quad E_i + E_i' = e_i, \quad F_j = f_j/2.$$

In particular, L and F_j are uniquely determined by n, while (E_i, E_i') are not unique, with $e_i + 1$ possibilities. Hence the number of *ideals* $\mathfrak{a}$ with $N(\mathfrak{a}) = n$ is $\prod_{i=1}^{s}(e_i + 1)$, and

$$N(n) = 4 \prod_{i=1}^{r} (e_i + 1).$$

4.2 Dedekind's criterion

Theorem 4.2.1. *Let K be a number field, p be a prime. The following statements are equivalent:*

1. *p is unramified in K*
2. *$\mathcal{O}_K/p\mathcal{O}_K$ is reduced (i.e. $\mathrm{Nil}(\cdot) = 0$);*
3. *The $\mathbb{F}_p$-bilinear form $\overline{\mathrm{Tr}}_{K/\mathbb{Q}} : \mathcal{O}_K/(p) \times \mathcal{O}_K/(p) \to \mathbb{F}_p$ sending (x, y) to $\mathrm{Tr}(xy) \mod p$ is non-degenerate.*
4. *$p \not| \Delta_K$, where Δ_K denotes the discriminant of K.*

Proof. (1)⇔(2): By Chinese remainder theorem, we have

$$\mathcal{O}_K/p\mathcal{O}_K \cong \prod_{\mathfrak{p}|p} \mathcal{O}_K/\mathfrak{p}^{e(\mathfrak{p}|p)}.$$

Note that each $\mathcal{O}_K/\mathfrak{p}^e$ is reduced if and only if $e(\mathfrak{p}|p) = 1$.

(2)⇔(3): Note that if $x \in \mathcal{O}_K/p\mathcal{O}_K$ is nilpotent, then xy is also nilpotent for any $y \in \mathcal{O}_K/p\mathcal{O}_K$, say $(xy)^n = 0 \mod p$. Since $\mathrm{Tr}_{K/\mathbb{Q}}(xy) = \sum_\sigma \sigma(xy)$, it is also nilpotent mod p. But an integer is nilpotent mod p means it is already zero mod p; hence $\overline{\mathrm{Tr}}_{K/\mathbb{Q}}(xy) = 0$. Hence, if $\overline{\mathrm{Tr}}_{K/\mathbb{Q}}(xy)$ is non-degenerate, then $\mathcal{O}_K/p\mathcal{O}_K$ is reduced. Conversely, if $\mathcal{O}_K/p\mathcal{O}_K$ is reduced, then we have necessarily $\mathcal{O}/p\mathcal{O}_K = \oplus_{\mathfrak{p}|p} k(\mathfrak{p})$ by Chinese Remainder theorem, where $k(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}$ is a finite extension of $\mathbb{F}_p$. Since $\mathbb{F}_p$ is a perfect field, $\mathrm{Tr}_{k(\mathfrak{p})/\mathbb{F}_p}$ is non-degenerate. It follows that $\overline{\mathrm{Tr}}_{K/\mathbb{Q}_p} = \oplus_{\mathfrak{p}|p} \mathrm{Tr}_{k(\mathfrak{p})/\mathbb{F}_p}$ is non-degenerate.

(3)⇔(4): Let $\{\alpha_i, 1 \le i \le n\}$ be a basis of $\mathcal{O}_K$ over $\mathbb{Z}$, and $\overline{\alpha}_i \in \mathcal{O}_K/(p)$ be the image of α_i. The pairing $\overline{\mathrm{Tr}}_{K/\mathbb{Q}}$ on $\mathcal{O}_K/(p)$ induces an $\mathbb{F}_p$-linear map:

$$\phi : \mathcal{O}_K/(p) \to (\mathcal{O}_K/(p))^\vee$$

where $(\mathcal{O}_K/(p))^\vee$ denotes the $\mathbb{F}_p$-dual of $\mathcal{O}_K/(p)$. If $\{\overline{\alpha}_i^\vee\}$ denotes the basis of $(\mathcal{O}_K/(p))^\vee$ dual to $\{\overline{\alpha}_i\}$, then the matrix of ϕ with respect these bases is $\overline{\mathrm{Tr}}_{K/\mathbb{Q}_p}(\overline{\alpha}_i\overline{\alpha}_j)$. Hence the paring is non-degenerate if and only if $\det(\overline{\mathrm{Tr}}_{K/\mathbb{Q}}(\overline{\alpha}_i\overline{\alpha}_j)) \neq 0$ in $\mathbb{F}_p$, i.e. $p \nmid \Delta_K$. This finishes the proof. □

Corollary 4.2.2. *For any number field K, there are only finitely many primes which are ramified in K.*

Remark 4.2.3. *In general, if we consider a finite extension L/K and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$, then a similar result holds for Dedekind's theorem, provide that we give a correct definition of $\mathrm{Disc}_{L/K}$: it is an ideal, not an element. See Milne's notes.*

Remark 4.2.4. *No good criterion for inertness. It could happen that there are infinitely many inert primes. However, if L/K is a finite, Galois extension of number fields such that $\mathrm{Gal}(L/K)$ is not cyclic, then no prime of K remains inert in L.*

Remark 4.2.5. *We will see later that for any $K \neq \mathbb{Q}$, $|\Delta_K| \geq 2$, hence at least one prime is ramified in K. But for $K \neq \mathbb{Q}$, there exists a maximal abelian unramfied extension such that any prime $\mathfrak{p}$ of K remains unramified in L; this field is called* Hilbert class field.*, whose degree equals to $cl(K)$. Caution: even of class number 1, K could admit a non-abelian unramified extension.*

Example 4.2.6. *In the example $K = \mathbb{Q}(\alpha)$ with α being a root of $X^3 + X + 1 = 0$. We get that 31 is the only prime which is ramified in K.*

4.3 Eisenstein extensions

A monic polynomial in $\mathbb{Z}[X]$,

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 T + a_0$$

is *Eisenstein* at a prime p, if $v_p(a_i) \geq 1$ and $v_p(a_0) = 1$.

Remark 4.3.1. *Let α be a root of an Eisenstein polynomial $f(X)$, and let $K = \mathbb{Q}(\alpha)$. Then $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$. Compare with one proposition proved before. In some case, we may deduce that $\mathcal{O}_K = \mathbb{Z}[\alpha]$, e.g. cyclotomic extensions.*

Proposition 4.3.2. *Let $K = \mathbb{Q}(\alpha)$ be as above. Then p is totally ramified in K, i.e. $p\mathcal{O}_K = \mathfrak{p}^n$. Moreover, $\mathfrak{p} = (p, \alpha)$.*

Proof. Since in general $\mathcal{O}_K \neq \mathbb{Z}[\alpha]$, we can't apply Theorem 4.0.1 directly. Let $\mathfrak{p}$ be a prime ideal above p, and write $(p) = \mathfrak{p}^e\mathfrak{a}$, with $\mathfrak{p} \nmid \mathfrak{a}$. We claim that $n = e$. By this claim, taking norm gives $N((p)) = p^n = N(\mathfrak{p})^n N(\mathfrak{a})$, we obtain $N(\mathfrak{a}) = \pm 1$, so $\mathfrak{a} = (1)$.

Now prove the claim. Mod $\mathfrak{p}$, $0 = f(\alpha) \equiv \alpha^n$, we get $\alpha^n \in \mathfrak{p}$, hence $\alpha \in \mathfrak{p}$ as $\mathfrak{p}$ is prime. On the other hand, $v_\mathfrak{p}(p) = e \leq n$, hence

$$v_\mathfrak{p}(c_i) \geq e, \quad v_\mathfrak{p}(c_0) = e.$$

Since $v_\mathfrak{p}(\alpha) \geq 1$ (as $\alpha \in \mathfrak{p}$), we obtain $v_\mathfrak{p}(\alpha^n + c_0) \geq e + 1$, hence $v_\mathfrak{p}(\alpha^n) = e$. This implies $e \geq n$, hence the equality. □

Corollary 4.3.3. *We have $v_\mathfrak{p}(\alpha) = 1$.*

Example 4.3.4. *Since $\sqrt[3]{10}$ is a root of $X^3 - 10$, which is Eisenstein at 2 and 5, the primes 2 and 5 are totally ramified in K, $(2) = \mathfrak{p}^3$ and $(5) = \mathfrak{q}^3$. However, the ring of integers in* not $\mathbb{Z}[\sqrt[3]{10}]$*; an integral basis is given by*

$$\{1, \alpha, (1 + \alpha + \alpha^2)/3\}$$

The discriminant of $\mathrm{Disc}(1, \alpha, \alpha^2)$ *is*

$$\pm N_{K/\mathbb{Q}}(3\alpha^2) = 27 \times 10^2,$$

so still there is a problem at 3. Indeed, 3 is ramified in K.

Example 4.3.5. *Let $K = \mathbb{Q}(\zeta)$, with $\zeta = \zeta_{p^n}$. We saw that Δ_K is a power of p, hence only p ramifies in K. Let $\mathfrak{p}_k = (1 - \zeta^k)\mathcal{O}_K$ where $0 \leq k \leq p^n - 1$ and $p \nmid k$. We know that $\prod_{p\nmid k}(1 - \zeta^k) = p$, so that $p\mathcal{O}_K = \prod_{p\nmid k} \mathfrak{p}_k$.*

Claim: for any k, $\mathfrak{p}_1 = \mathfrak{p}_k$.

***Proof**: Since $p \nmid k$, let $k'k \equiv$* mod p^n *for some k'. Then $1 - \zeta = 1 - \zeta^{kk'}$ so that $(1 - \zeta^k)|(1 - \zeta)$. The other division is clear. Hence $(1 - \zeta)\mathcal{O}_K = (1 - \zeta^k)\mathcal{O}_K$.*

We deduce that $p\mathcal{O}_K = \mathfrak{p}_1^{\varphi(p^n)}$, with $[K : \mathbb{Q}] = \varphi(p^n)$; that is p is totally ramified in K.

4.4 Decomposition of primes in Galois extensions

Let L/K be a finite Galois extension of number fields with $G = \mathrm{Gal}(L/K)$. Two fractional ideals I_1, I_2 are called *conjugate under* G, if there exists $\sigma \in G$ such that $\sigma(I_1) = I_2$.

Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ with prime decomposition in $\mathcal{O}_L$:

$$\mathfrak{p}\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{P}_i^{e_i}.$$

Since $\mathfrak{p}\mathcal{O}_L$ is invariant under G, the group G acts on the set $\{\mathfrak{P}_1, ..., \mathfrak{P}_g\}$.

Proposition 4.4.1. *Any two primes $\mathfrak{P}_i$ and $\mathfrak{P}_j$ are conjugate under G and we have $e := e_1 = \cdots = e_g$, $f := f_1 = \cdots = f_g$, and $[L : K] = efg$.*

Proof. Note that for any $\sigma \in G$, we have $\mathfrak{p}\mathcal{O}_L = \sigma(\mathfrak{p})\mathcal{O}_L$, which implies that

$$\prod_{i=1}^{g} \mathfrak{P}_i^{e_i} = \prod_{i=1}^{g} \sigma(\mathfrak{P}_i)^{e_i}.$$

Hence $e_i = e_{\sigma^{-1}(i)}$ by the uniqueness of the decomposition. Moreover, if $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$, then σ induces an isomorphism

$$\sigma : \mathcal{O}_L/\mathfrak{P}_i \xrightarrow{\sim} \mathcal{O}_L/\mathfrak{P}_j$$

and hence $f(\mathfrak{P}_i|\mathfrak{p}) = f(\mathfrak{P}_j|\mathfrak{p})$. So in all we are left to prove that for any $\mathfrak{P}_i$, there exists $\sigma \in G$ such that $\sigma(\mathfrak{P}_i) = \mathfrak{P}_i$. If not, then for some $\mathfrak{P}' = \mathfrak{P}_i$, $\sigma(\mathfrak{P}_1) \neq \mathfrak{P}'$ for any σ. By Lemma below, there exists $x \in \mathfrak{P}'$ such that $x \notin \sigma(\mathfrak{P}_1)$ for any $\sigma \in G$, or equivalently $\sigma(x) \notin \mathfrak{P}_i$ for any $\sigma \in G$. But then $\mathrm{N}_{L/K}(x) = \prod_{\sigma \in G} \sigma(x) \notin \mathfrak{P}_1$ since $\mathfrak{P}_1$ is a prime ideal, i.e. $\mathrm{N}_{L/K}(x) \notin \mathfrak{P}_1 \cap \mathcal{O}_K = \mathfrak{p}$. This gives a contradiction, as $\mathrm{N}_{L/K}(\mathfrak{P}') \subset \mathfrak{p}$. $\square$

Lemma 4.4.2. *Let R be a commutative ring, $\mathfrak{p}_1, ..., \mathfrak{p}_r$ be prime ideals of R. Assume $\mathfrak{a} \subset R$ is an ideal such that $\mathfrak{a} \not\subseteq \mathfrak{p}_i$ for any $1 \leq i \leq n$. Then there exists $x \in \mathfrak{a}$ such that $x \notin \mathfrak{p}_i$ for any i.*

Proof. Easy. $\square$

Week 4 Exercise

1. Determine the prime decomposition of $p = 3, 7, 11, 13$ in $K = \mathbb{Q}(\sqrt{-5})$ and in $K = \mathbb{Q}(\sqrt{7})$.

2. For which integers n can be represented as $n = a^2 + 2b^2$, $a, b \in \mathbb{Z}$. (Use the fact that $\mathbb{Z}[\sqrt{-2}]$ is a PID.) (when p is a prime, then iff $p \equiv 1, 3 \mod 8$.)

3. Let a be a square-free integer. Let $\alpha = \sqrt[3]{a}$ and $K = \mathbb{Q}(\alpha)$. Then an integral basis is

$$\{1, \alpha, \alpha^2\}, \quad \text{if } a^2 \neq 1 \mod 9;$$

$$\{1, \alpha, (1 \pm \alpha + \alpha^2)/3\}, \quad \text{if } a \equiv \pm 1 \mod 9.$$

Chapter 5

W5: Prime decomposition-continued

5.1 Decomposition and Inertia subgroups

Definition 5.1.1. *For a prime ideal $\mathfrak{P}$ of $\mathcal{O}_L$ with $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$, we put*

$$D(\mathfrak{P}|\mathfrak{p}) = \{\sigma \in G | \sigma(\mathfrak{P}) = \mathfrak{P}\},$$

and call it the decomposition group of $\mathfrak{P}$ relative to $\mathfrak{p}$. Any $\sigma \in D(\mathfrak{P}|\mathfrak{p})$ induces an automorphism

$$\sigma : \mathcal{O}_L/\mathfrak{P} = k(\mathfrak{P}) \to k(\mathfrak{P})$$

which fixes the subfield $k(\mathfrak{p})$. We get thus a homomorphism

$$\varphi_{\mathfrak{P}} : D(\mathfrak{P}|\mathfrak{p}) \to \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p})).$$

Define

$$I(\mathfrak{P}|\mathfrak{p}) := \mathrm{Ker}(\varphi_{\mathfrak{P}}) = \{\sigma \in D(\mathfrak{P}|\mathfrak{p}) | \sigma(x) \equiv x \mod \mathfrak{P}, \forall x \in \mathcal{O}_L\},$$

and call it the inertia subgroup *of $\mathfrak{P}$ relative to $\mathfrak{p}$.*

Proposition 5.1.2. *(1) The map $\varphi_{\mathfrak{P}}$ is surjective, i.e.*

$$1 \to I(\mathfrak{P}|\mathfrak{p}) \to D(\mathfrak{P}|\mathfrak{p}) \to \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p})) \to 1.$$

Moreover, one has $e(\mathfrak{P}|\mathfrak{p}) = |I(\mathfrak{P}|\mathfrak{p})|$ and $e(\mathfrak{P}|\mathfrak{p})f(\mathfrak{P}|\mathfrak{p}) = |D(\mathfrak{P}|\mathfrak{p})|$.

(2) For any $\tau \in G$, we have $D(\tau(\mathfrak{P})|\mathfrak{p}) = \tau D(\mathfrak{P}|\mathfrak{p})\tau^{-1}$ and $I(\tau(\mathfrak{P})|\mathfrak{p}) = \tau I(\mathfrak{P}|\mathfrak{p})\tau^{-1}$.

Proof. We denote $D_{\mathfrak{P}} = D(\mathfrak{P}|\mathfrak{p})$ and $I_{\mathfrak{P}} = I(\mathfrak{P}|\mathfrak{p})$. Statement (2) is immediate by definition of $D_{\mathfrak{P}}$ and $I_{\mathfrak{P}}$. It remains to prove (1). By Proposition, G acts transitively on the set $\{\mathfrak{P} = \mathfrak{P}_1, \cdots, \mathfrak{P}_g\}$ of primes above $\mathfrak{p}$, and $D_{\mathfrak{P}}$ is the stabilizer. Hence we see that $g = [G : D_{\mathfrak{P}}]$. Since $|G| = efg$, we get $|D_{\mathfrak{P}}| = ef$.

Let $K_D = L^{D_{\mathfrak{P}}}$, and $\mathfrak{P}_D = \mathfrak{P} \cap \mathcal{O}_D$. Then $\mathfrak{P}$ is the unique prime above $\mathfrak{P}_D$ (since $D(\mathfrak{P}|\mathfrak{p})$ acts transitively on the orbit), i.e. $\mathfrak{P}_D\mathcal{O}_L = \mathfrak{P}^{e'}$. Let $f' = f(\mathfrak{P}|\mathfrak{P}_D)$. Since $e'f' = |D_{\mathfrak{P}}| = ef$ and $e' \leq e$, $f' \leq f$, we in fact equalities. So replacing K by K_D, we may assume $\mathrm{Gal}(L/K) = D(\mathfrak{P}|\mathfrak{p})$.

We need to show the natural morphism $\mathrm{Gal}(L/K) \to \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$ is surjective. Let $\overline{\alpha}$ be a generator such that $k(\mathfrak{P}) = k(\mathfrak{p})(\overline{\alpha})$ and let $\alpha \in \mathcal{O}_L$ be a lifting. Let $f \in \mathcal{O}_K[X]$ be the minimal polynomial of α. Then the minimal polynomial of $\overline{\alpha}$, $\overline{g} \in k[X]$, divides $\overline{f}$. So for any element $\overline{\sigma} \in \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$, sending $\overline{\alpha}$ to $\overline{\beta}$, $\overline{\beta}$ must be a root of $\overline{g}$, so there exists a root β of f such that $\beta \mapsto \overline{\beta}$. In this way we obtain a lifting of $\overline{\sigma}$. □

Theorem 5.1.3. *Let L/K be a finite Galois extension of number fields, $n := [L : K]$. Let $\mathfrak{p}$ be a prime in K and*

$$\mathfrak{p}\mathcal{O}_L = (\mathfrak{P}_1 \cdots \mathfrak{P}_g)^e, \quad n = efg.$$

Let $D_{\mathfrak{P}}, I_{\mathfrak{P}}$ be the decomposition and inertia subgroups, K_D, K_I be the corresponding fields. Then letting $\mathfrak{P}_D = \mathfrak{P} \cap K_D$, $\mathfrak{P}_I = \mathfrak{P} \cap K_I$:

1. *$\mathfrak{P}_D$ inert in K_I, i.e. $\mathfrak{P}_D\mathcal{O}_I = \mathfrak{P}_I$;*

2. *$\mathfrak{P}_I$ totally ramified in L, $\mathfrak{P}_I = \mathfrak{P}^e$.*

*If, moreover, $D_{\mathfrak{P}}$ is normal subgroup of G (e.g. L/K is abelian), then $\mathfrak{p}$ splits completely in K_D (*Not true in general*).*

Proof. Clear. □

Corollary 5.1.4. *If L/K is finite Galois, and* $\mathrm{Gal}(L/K)$ *is non-cyclic. Then no prime $\mathfrak{p}$ of K is inert in L.*

Proof. Since being inert implies $e = g = 1$, we have $\mathrm{Gal}(L/K) \cong D_{\mathfrak{P}} \cong \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$ which is a cyclic group. □

5.2 Frobenius

Assume $\mathfrak{p}$ is unramified in L, so $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_g$, and set $\mathfrak{P} = \mathfrak{P}_1$. Then $I_{\mathfrak{P}} = \{1\}$ and $D_{\mathfrak{P}}$ is a cyclic group of order f isomorphic to $\mathrm{Gal}(l/k)$. Since $\mathrm{Gal}(l/k)$[1] is generated by $\sigma : x \mapsto x^{\sharp k}$, where $\sharp k = N(\mathfrak{p})$, so it corresponds to an element in $D_{\mathfrak{P}}$, usually denoted by $\left(\frac{L/K}{\mathfrak{P}}\right)$, and called the *Frobenius element* of $\mathfrak{P}$ over $\mathfrak{p}$.

Remark 5.2.1. *In some references, even when $\mathfrak{p}$ is ramified, we call any lifting of σ a Frobenius element (not uniquely determined).*

Lemma 5.2.2. *Let L/K be a Galois extension of number fields, $\mathfrak{P}|\mathfrak{p}$ with $e(\mathfrak{P}|\mathfrak{p}) = 1$. Then*

1. *for any $\tau \in \mathrm{Gal}(L/K)$, $\left(\frac{L/K}{\tau(\mathfrak{P})}\right) = \tau\left(\frac{L/K}{\mathfrak{P}}\right)\tau^{-1}$;*

2. *If M/K is an intermediate subfield, $\mathfrak{P}_M := \mathfrak{P} \cap \mathcal{O}_M$, then $e(\mathfrak{P}|\mathfrak{P}_M) = 1$ and $\left(\frac{L/M}{\mathfrak{P}}\right) = \left(\frac{L/K}{\mathfrak{P}}\right)^{f(\mathfrak{P}_M|\mathfrak{p})}$;*

3. *If M/K is also Galois, then $\left(\frac{M/K}{\mathfrak{P}_E}\right) = \left(\frac{L/K}{\mathfrak{P}}\right)|_E$.*

Proof. Clear. □

Proposition 5.2.3. *Let L_1, L_2 be two finite extensions of K, and let $L = L_1L_2$. Then a prime $\mathfrak{p}$ of K is unramified in L if and only if it is unramified in both L_1 and L_2. Similarly $\mathfrak{p}$ splits completely in L if and only if it is in both L_1 and L_2.*

[1] write $l = k(\mathfrak{P})$ and $k = k(\mathfrak{p})$ for simplicity

Proof. Let M be a finite Galois extension containing L. Let H_1, H_2 be the subgroups of $\mathrm{Gal}(M/K)$ corresponding to L_1, L_2, so that L corresponds to $H_1 \cap H_2$. Then $\mathfrak{p}$ is unramified in L if and only if $L \subset M^{I(\mathfrak{P}|\mathfrak{p})}$ for any $\mathfrak{P}|\mathfrak{p}$, if and only if $H_1 \cap H_2 \supseteq I(\mathfrak{P}|\mathfrak{p})$ for any $\mathfrak{P}|\mathfrak{p}$, if and only if $H_i \supseteq I(\mathfrak{P}|\mathfrak{p})$ for $i = 1, 2$, if and only if $L_i \subset M^{I(\mathfrak{P}|\mathfrak{p})}$, i.e. $\mathfrak{p}$ is unramified in both L_1 and L_2.

Next, $\mathfrak{p}$ splits completely means that $e = f = 1$, if and only if $L \subset M^{D(\mathfrak{P}|\mathfrak{p})}$, and we conclude similarly. □

5.3 Example

Example 5.3.1. *We put $L = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$. Then $G = \mathrm{Gal}(L/\mathbb{Q}) \cong \langle \sigma, \tau \rangle / (\sigma^3 = \tau^2 = 1, \sigma\tau = \tau\sigma^2)$, $|G| = 6$, with (where $\omega = e^{2\pi i/3} = \frac{-1+\sqrt{-3}}{2}$):*

$$\sigma(\sqrt[3]{2}) = \omega\sqrt[3]{2}, \quad \sigma(\sqrt{-3}) = \sqrt{-3},$$
$$\tau(\sqrt[3]{2}) = \sqrt[3]{2}, \quad \tau(\sqrt{-3}) = -\sqrt{-3}.$$

A rational prime p ramifies in L if and only if $p = 2, 3$.

(1) The prime 2 is inert in $\mathbb{Q}(\sqrt{-3})$ and totally ramifies in $\mathbb{Q}(\sqrt[3]{2})$ (as $X^3 - 2$ is Eisenstein at 3). So there exists a unique prime $\mathfrak{p}_2$ in $\mathcal{O}_L$ of degree above 2 such that $2\mathcal{O}_L = \mathfrak{p}_2^3$. We have $g = 1$, $D(\mathfrak{p}_2|2) = G$ and $I(\mathfrak{p}_2|2) = \mathrm{Gal}(L/\mathbb{Q}(\sqrt{-3})) = \langle \sigma \rangle$, of order 3 since $e = 3$.

(2) The prime 3 is ramified in both $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt[3]{2})$, so its ramification degree in $L/\mathbb{Q}$ is divisible by 6. Thus we see that $3\mathcal{O}_L = \mathfrak{p}_3^6$ for some prime $\mathfrak{p}_3$ of residue degree 1 above 3. We have $D(\mathfrak{p}_3|3) = I(\mathfrak{p}_3|3) = G$.

(3) It is easy to see that $p = 5$ is inert in $K = \mathbb{Q}(\sqrt{-3})$ so that $\mathcal{O}_K/(5) \cong \mathbb{F}_{25}$. Note that $X^3 - 2$ has 3 distinct solutions in $\mathbb{F}_{25}$, and exactly one of them is in $\mathbb{F}_5$, namely $x = 3 \in \mathbb{F}_5$. Therefore, there are 3 distinct primes of $\mathcal{O}_L$ above 5:

$$\mathfrak{p}_5^{(1)} = (5, \sqrt[3]{2} - 3), \quad \mathfrak{p}_5^{(2)} = (5, \sqrt[3]{2} - 3\omega), \quad \mathfrak{p}_5^{(3)} = (5, \sqrt[3]{2} - 3\omega^2)$$

and each of them has residue degree 2 over 5. The decomposition group of $\mathfrak{p}_5^{(1)}$, $\mathfrak{p}_5^{(2)}$ and $\mathfrak{p}_5^{(3)}$ are respectively

$$\mathrm{Gal}(L/\mathbb{Q}(\sqrt[3]{2})) = \langle \tau \rangle, \quad \mathrm{Gal}(L/\mathbb{Q}(\sqrt[3]{2}\omega^2)) = \langle \sigma\tau \rangle, \quad \mathrm{Gal}(L/\mathbb{Q}(\sqrt[3]{2}\omega)) = \langle \sigma^2\tau \rangle.$$

The Frobenius elements of $\mathfrak{p}_5^{(1)}$, $\mathfrak{p}_5^{(2)}$ and $\mathfrak{p}_5^{(3)}$ are respectively $\tau, \sigma\tau, \sigma^2\tau$. Note that in $K' := \mathbb{Q}(\sqrt[3]{2}) = L^{\langle \tau \rangle}$, $5\mathcal{O}_{K'} = \mathfrak{q}_5\mathfrak{q}_5'$ with $f(\mathfrak{q}_5|5) = 1$ and $f(\mathfrak{q}_5'|5) = 2$. In fact, in $\mathbb{F}_5$,

$$X^3 - 2 \equiv (X - 3)(X^2 + 3X - 1) \mod 5.$$

Moreover, $\mathfrak{p}_5^{(1)}$ is above $\mathfrak{q}_5$, and $\mathfrak{p}_5^{(2)}, \mathfrak{p}_5^{(3)}$ are above $\mathfrak{q}_5'$. In particular, 5 does not split completely in K'.

(4) Consider the case $p = 7$. Then 7 is split in $\mathbb{Q}(\sqrt{-3})$ and inert in $\mathbb{Q}(\sqrt[3]{2})$[2]. Hence $g \geq 2$ and $f \geq 3$. Therefore

$$e = 1, \quad f = 3, \quad g = 2.$$

Thus 7 splits in $\mathcal{O}_K$ into two primes of degree 3, namely

$$\mathfrak{p}_7^{(1)} = (7, \frac{1 + \sqrt{3}}{2} + 4), \quad \mathfrak{p}_7^{(2)} = (7, \frac{1 + \sqrt{-3}}{2} + 2).$$

[2]since $X^3 - 2$ is irreducible in $\mathbb{F}_7$

The decomposition groups of both $\mathfrak{p}_7^{(1)}$, $\mathfrak{p}_7^{(2)}$ *are* $\mathrm{Gal}(K/\mathbb{Q}(\sqrt{-3})) = \langle\sigma\rangle$. *The Frobenius element is the unique element of* $\mathrm{Gal}(K/\mathbb{Q}(\sqrt{-3}))$ *such that*

$$\sigma_{\mathfrak{p}_7^{(i)}}(x) = x^7 \mod \mathfrak{p}_7^{(i)}, \quad \forall x \in \mathcal{O}_L.$$

Since, $\omega = \frac{-1+\sqrt{-3}}{2}$, *we check* $\omega = 2 \mod \mathfrak{p}_7^{(1)}$ *and* $\omega \equiv 4 \mod \mathfrak{p}_7^{(2)}$, *we have*

$$(\sqrt[3]{2})^7 \equiv \sqrt[3]{2}\omega^2 \mod \mathfrak{p}_7^{(1)}, \quad (\sqrt[3]{2})^7 \equiv \sqrt[3]{2}\omega \mod \mathfrak{p}_7^{(2)}.$$

Thus it follows that $\sigma_{\mathfrak{p}_7^{(1)}} = \sigma^2$ *and* $\sigma_{\mathfrak{p}_7^{(2)}} = \sigma$.

Example 5.3.2. *Let* $K = \mathbb{Q}(\sqrt{5}, \sqrt{-1})$. *Then* $[K : \mathbb{Q}] = 4$ *with Galois groups isomorphic to* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. *It is easy to see that*

(1) only 2 *and* 5 *ramify in* K, *with* $e = 2$.

(2) Let $M = \mathbb{Q}(\sqrt{-5}) \subset K$. *Then also* 2, 5 *ramify in* M *with* $e = 2$, *hence no prime ideal in* M *is ramified in* K. *Since* $Cl_M = 2$ *(it is not a PID) which we will prove later,* K *is in fact the Hilbert class field of* M.

5.4 Cyclotomic fields

Let $N \geq 2$ and $K = \mathbb{Q}(\zeta_N)$.

Theorem 5.4.1. *(1)* p *is unramified in* K *if and only if* $p \nmid N$. *In this case,* $(p) = \mathfrak{p}_1 \cdots \mathfrak{p}_g$, *with* $g = \frac{\varphi(N)}{f}$, $f =$*order of* p *in* $(\mathbb{Z}/N\mathbb{Z})^\times$. *Moreover the Frobenius element* Frob_p [3] *is just the element sending* $\zeta_N \to \zeta_N^p$.

(2) If $p|N$, *let* $N = p^r N'$ *with* $p \nmid N'$. *Then*

$$(p) = (p_1 \cdots \mathfrak{p}_g)^e$$

with $e = \varphi(p^r)$, $g = \frac{\varphi(N)}{f}$, $f =$*order of* p *in* $(\mathbb{Z}/N'\mathbb{Z})^\times$.

Proof. (1) The first statement follows from Dedekind's theorem and the computation of Δ_K. For the second, we only need compute $f(\mathfrak{p}|p)$. But, since p is unramified, $e(\mathfrak{p}|p) = 1$, so $f(\mathfrak{p}|p)$ is the order of Frobenius $(\frac{K/\mathbb{Q}}{p})$. We have

$$(\frac{K/\mathbb{Q}}{p})\zeta_N \equiv \zeta_N^p \mod \mathfrak{p}.$$

We need to show that, in the residue field $\mathcal{O}_K/\mathfrak{p}$, the order of ζ_N is N (as in K itself). Indeed, consider the polynomial $P := X^N - 1 \in k(\mathfrak{p})[X]$: its solutions are $\{\zeta_N^i : 0 \leq i \leq N-1\}$, also it has no multiple root in $\mathcal{O}_K/\mathfrak{p}$, since $(P, P') = 1$. So ζ_N has order N. This implies the assertion.

On the other hand, since p is unramified, Frob_p is unique. Since any element of $\mathrm{Gal}(K/\mathbb{Q})$ sends ζ_N to a power of ζ_N, and $\zeta_N \to \zeta_N^p$ has image $\overline{\sigma}$, we obtain the result.

(2) Let $K_0 = \mathbb{Q}(\zeta_{p^r})$ and $K' = \mathbb{Q}(\zeta_{N'})$ so that $K = K_0K'$ and $K_0 \cap K' = \mathbb{Q}$. Assume

$$p\mathcal{O}_K = (\mathfrak{p}_1 \cdots \mathfrak{p}_g)^{e(\mathfrak{p}|p)}.$$

On the other hand,

[3] well-defined since in an abelian extension

(a) Inside K_0, we have p is totally ramified and $p\mathcal{O}_{K_0} = \mathfrak{p}_0^{\varphi(p^r)}$. Hence $e \geq \varphi(p^r)$.

(b) Since $p\mathcal{O}_{K'} = \mathfrak{p}'_1 \cdots \mathfrak{p}'_{g'}$ (unramified), with $g'f' = \varphi(N')$ where f' =order of p in $(\mathbb{Z}/\mathbb{N}'\mathbb{Z})^\times$.

Therefore

$$\varphi(N) = [K : \mathbb{Q}] = e(\mathfrak{p}|p)f(\mathfrak{p}|p)g \geq \varphi(p^r)f'g' = \varphi(p^r)\varphi(N') = \varphi(N)$$

hence we get equalities $e(\mathfrak{p}|p) = \varphi(p^r)$, $f(\mathfrak{p}|p) = f'$ =order of p in $(\mathbb{Z}/N'\mathbb{Z})^\times$, and $g = g'$. $\square$

In particular, a prime $p \nmid N$ splits completely in $\mathbb{Q}(\zeta_N)$, if and only if $p \equiv 1 \mod N$.

Example 5.4.2. *Consider the number field $L = \mathbb{Q}(\zeta_{31})$ and $p = 2$. Since 2 has order 5 in $(\mathbb{Z}/31\mathbb{Z})^\times$, it splits into 6 primes in $\mathcal{O}_K$ and each of them has residue degree 5. Let $H = \langle 2\rangle \subset (\mathbb{Z}/31\mathbb{Z})^\times$, and $K = \mathbb{Q}(\zeta_{31})^H$. Then K is the decomposition field of each prime above 2. Thus 2 splits into 6 primes, each of them has degree 1. We claim that there is noo $\alpha \in \mathcal{O}_K$ such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Otherwise, let $f(X) \in \mathbb{Z}[X]$ be the minimal polynomial of α. Then by Kummer's theorem, $\overline{f}$ has 6 distinct roots in $\mathbb{F}_2$. But this is impossible since $\sharp\mathbb{F}_2 = 2$.*

Next we derive the quadratic reciprocity law using the above results.

Lemma 5.4.3. *Let p be an odd prime. Then $\mathbb{Q}(\zeta_p)$ contains a unique quadratic field K, which is*

$$K = \begin{cases} \mathbb{Q}(\sqrt{p}) & \text{if } p \equiv 1 \mod 4 \\ \mathbb{Q}(\sqrt{-p}) & \text{if } p \equiv 3 \mod 4. \end{cases}$$

Proof. The Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic of order $p-1$. It contains a unique subgroup H of index 2, so $\mathbb{Q}(\zeta_p)$ contains a unique quadratic field K. Explicitly if $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ denotes a generator, then $H = \langle a^2\rangle$, that is H consists of the quadratic residues in $\mathbb{F}_p^\times$. Since p is the only prime ramified in $\mathbb{Q}(\zeta_p)$, so every prime different from p is unramified in K. Therefore by Theorem, we see that $K = \mathbb{Q}(\sqrt{p})$ if $p \equiv 1 \mod 4$ and $\mathbb{Q}(\sqrt{-p})$ if $p \equiv 3 \mod 4$ (use the decomposition of 2 in K: unramified). $\square$

Theorem 5.4.4. *(Quadratic Reciprocity Law) Let $p \neq q$ be odd primes. Then we have*

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

Proof. Using $\left(\frac{-1}{q}\right) = (-1)^{(q-1)/2}$, the statement is equivalent to saying that $\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$, where $p^* = p$ if $p \equiv 1 \mod 4$, and $p^* = -p$ if $p \equiv 3 \mod 4$. Hence we deduce the result from

$$\begin{aligned} \left(\tfrac{p^*}{q}\right) = 1 \quad &\Leftrightarrow \quad x^2 - p^* \equiv 0 \mod q \text{ has solutions} \\ &\Leftrightarrow \quad q \text{ splits in } \mathbb{Q}(\sqrt{p^*}) \quad \text{as known unramified} \\ &\Leftrightarrow \quad \left(\tfrac{\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}}{q}\right) = \left(\tfrac{\mathbb{Q}(\zeta_p)/\mathbb{Q}}{q}\right)|_{\mathbb{Q}(\sqrt{p^*})} = 1 \\ &\Leftrightarrow \quad \sigma_q = \left(\tfrac{\mathbb{Q}(\zeta_p)/\mathbb{Q}}{q}\right) \in H, \quad \zeta_p \mapsto \zeta_p^q \\ &\Leftrightarrow \quad q \text{ is a quadratic residue in } \mathbb{F}_p. \end{aligned}$$

$\square$

Chapter 6

W6: Finiteness of class numbers

6.1 Minkowski's theory

Definition 6.1.1. *An additive subgroup Λ of $\mathbb{R}^n$ is called a lattice in $\mathbb{R}^n$, if there exists a basis $\{\alpha_1, ..., \alpha_n\}$ such that*

$$\Lambda = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n.$$

Define

$$P(\alpha_1, ..., \alpha_n) = \{\sum_{i=1}^{n} a_i\alpha_i | 0 \leq a_i < 1\}$$

which is parallelogram in $\mathbb{R}^n$. Call

$$\mathrm{Vol}(\mathbb{R}^n/\Lambda) := \mu(P(\alpha_1, ..., \alpha_n))$$

the volume of Λ.

If $e_1, ..., e_n$ denotes the canonical basis of $\mathbb{R}^n$, and if writing $(\alpha_1, ..., \alpha_n) = A(e_1, ..., e_n)$, then we know that

$$\mathrm{Vol}(\mathbb{R}^n/\Lambda) = |\det A|.$$

Definition 6.1.2. *We say an additive subgroup $\Lambda \subset \mathbb{R}^n$ is* discrete *if for every bounded subset $B \subset \mathbb{R}^n$, $B \cap \Lambda$ is finite.*

Lemma 6.1.3. *(1) Every lattice in $\mathbb{R}^n$ is discrete.*

(2) Every discrete subgroup of $\mathbb{R}^n$ is a lattice in some sub-space of $\mathbb{R}^n$.

Proof. Left as an exercise. □

Definition 6.1.4. *A subset $S \subset \mathbb{R}^n$ is called convex, if*

$$x, y \in S \Rightarrow \frac{1}{2}(x + y) \in S.$$

It is called centrally symmetric *if $x \in S \Rightarrow -x \in S$.*

Theorem 6.1.5. *(Minkowski) Let Λ be a lattice in $\mathbb{R}^n$, S be a mesurable subset.*

(1) if $\mu(S) > \mathrm{Vol}(\mathbb{R}^n/\Lambda)$, then there exist $s, s' \in S$, $s \neq s'$ such that $s - s' \in \Lambda$;

(2) If S is convex and centrally symmetric, and $\mu(S) > 2^n\mathrm{Vol}(\mathbb{R}^n/\Lambda)$, then $S \cap \Lambda \neq 0$.

(3) If S is convex and centrally symmetric, and compact, and $\mu(S) \geq 2^n\mathrm{Vol}(\mathbb{R}^n/\Lambda)$, then $S \cap \Lambda \neq 0$.

Proof. (1) Take $\{\alpha_1, ..., \alpha_n\}$ be a basis of Λ, and $P = P(\alpha_1, ..., \alpha_n)$ be the parallelogram spanned by α_i. Then

$$\begin{aligned} & \mathbb{R}^n = \sqcup_{h\in\Lambda}(h+P) \text{ disjoint} \\ \Rightarrow \quad & S = \sqcup_{h\in\Lambda} S \cap (h+P) \\ \Rightarrow \quad & \mu(S) = \textstyle\sum_{h\in\Lambda} \mu(S\cap(h+P)) = \sum_{h\in\Lambda}\mu((-h+S)\cap P). \end{aligned}$$

If $(-h+S)\cap P$ and $(-h'+S)\cap P$ are all disjoint for distinct $h \neq h'$, then we would obtain $\mu(S) \leq \mu(P) = \mathrm{Vol}(\mathbb{R}^n/\Lambda)$, which contradicts the assumption. Hence, for some $h \neq h'$,

$$\big((-h+S)\cap P\big) \cap \big((-h'+S)\cap P\big) \neq \emptyset,$$

which implies the assertion.

(2) Let $S' = \frac{1}{2}S$, then $\mu(S') = \frac{1}{2^n}\mu(S) > \mathrm{Vol}(\mathbb{R}^n/\Lambda)$. By (1), there exist $x, y \in S'$ such that $x \neq y$, $x - y \in \Lambda$. But then $2x, -2y \in S$ (centrally symmetric), and (convexity)

$$x - y = \frac{1}{2}(2x + (-2y)) \in S$$

so $x - y \in S \cap \Lambda$.

(3) Let $S_m = (1 + \frac{1}{m})S$. Then S_m is also convex, centrally symmetric, as S is, and

$$\mu(S_m) = (1 + \frac{1}{m})^n \mu(S) > 2^n \mathrm{Vol}(\mathbb{R}^n/\Lambda).$$

By (2), there exists $0 \neq h_m \in S_m \cap \Lambda$. Since $\{h_m : m \geq 1\}$ is a sequence contained in a compact set $S_1 = 2S$, we can find a sub-sequence which converges to h, say. The limit h must be contained in the closure of S, i.e. S itself, since S is compact. On the other hand, Λ is discrete, so the limit h is also in Λ and non-zero, hence $0 \neq h \in S \cap \Lambda$. □

6.2 Embeddings

Let K be a number field of degree n. Then there exist n $\mathbb{Q}$-embeddings $\sigma_i : K \hookrightarrow \mathbb{C}$. Let r_1 denote the number of real embeddings and $2r_2$ be the number of non-real ones (they appear naturally in pair), so that

$$n = r_1 + 2r_2.$$

Precisely, let $\alpha \in K$ be such that $K = \mathbb{Q}(\alpha)$ (primitive element). Then look at the conjugates, α_i. Then r_1 is just the number of α_i which are real.

Remark 6.2.1. *Note that for a Galois extension $K/\mathbb{Q}$, either $r_1 = 0$, or $r_2 = 0$: all are real or non-real. This is because all embeddings have the same image.*

Example of non-Galois extension: $\mathbb{Q}(\sqrt[3]{2})$, in which case $r_1 = 1$, $r_2 = 1$.

We assume that $\sigma_1, ..., \sigma_{r_1}$ are real embeddings and $\sigma_{r_1+2i} = \overline{\sigma}_{r_1+2i-1}$. Consider the embedding

$$\begin{array}{rccccc} \lambda : & K & \to & \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} & \overset{\iota}{\cong} & \mathbb{R}^n \\ & x & \mapsto & (\sigma_1(x), ..., \sigma_{r_1}(x), ..., \sigma_{r_1+2j}(x)...) & & \end{array}$$

where ι sends $(y_1, ..., y_{r_1}, z_1, ..., z_{r_2})$ to $(y_1, ..., y_{r_1}, \mathfrak{R}(z_j), \mathfrak{I}(z_j))$.

Let I be a fractional ideal of $\mathcal{O}_K$. Then I is a free abelian group of rank n.

Lemma 6.2.2. *For any fractional ideal I, $\lambda(I)$ is a lattice of $\mathbb{R}^n$ with*

$$\mathrm{Vol}(\mathbb{R}^n/\lambda(I)) = \frac{1}{2^{r_2}}\sqrt{|\Delta_K|}N(I).$$

Proof. It is clear that $\lambda(I)$ is a $\mathbb{Z}$-lattice of rank n. To compute $\mathrm{Vol}(\mathbb{R}^n/\lambda(I))$, we choose a basis $(\alpha_1, ..., \alpha_n)$ of I over $\mathbb{Z}$. Denote by $\lambda(\alpha_i) \in \mathbb{R}^n$ the image (as column vectors). Then

$$\mathrm{Vol}(\mathbb{R}^n/\lambda(I)) = |\det(\lambda(\alpha_1), ..., \lambda(\alpha_n))|.$$

On the other hand, we have[1]

$$(\sigma_i(\alpha_j))_{1\le i,j\le n} = \begin{pmatrix} I_{r_1} & 0 & \cdots & 0 \\ 0 & \left(\begin{smallmatrix} 1 & i \\ 1 & -i \end{smallmatrix}\right) & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ 0 & 0 & & \left(\begin{smallmatrix} 1 & i \\ 1 & -i \end{smallmatrix}\right) \end{pmatrix} (\lambda(\alpha_1), ..., \lambda(\alpha_n)).$$

It follows that

$$\det(\sigma_i(\alpha_j)) = (2i)^{r_2}\det(\lambda(\alpha_1), \cdots, \lambda(\alpha_n)).$$

But

$$|\det(\sigma_i(\alpha_j))| = |\mathrm{Disc}(\alpha_1, ..., \alpha_n)|^{1/2} = N(I)|\Delta_K|^{1/2},$$

giving the result. □

6.3 Finiteness of class numbers

Lemma 6.3.1. *For $t \in \mathbb{R}_{\ge 0}$, let B_t denote the subset of all $(y_1, ..., y_n) \in \mathbb{R}^n$ such that*

$$\sum_{i=1}^{r_1}|y_i| + 2\sum_{j=1}^{r_2}|y_{r_1+2j-1} + iy_{r_1+2j}| \le t.$$

Then the Lebesgue measure of B_t is

$$\mu(B_t) = 2^{r_1}(\frac{\pi}{2})^{r_2}\frac{t^n}{n!}.$$

Proof. See Tian's note. For example, when $n = r_1 = 1$, then $B_t = [-t, t]$, so the measure is $2t$. When $n = 2$ and $r_2 = 1$, then B_t is a circle with radius $t/2$, so the measure is $\pi(t/2)^2$. Note that B_t is centrally symmetric, convex and compact. □

Theorem 6.3.2. *Let K be a number field of degree n.*

1. *Let I be a fractional ideal of $\mathcal{O}_K$. There exists $0 \ne x \in I$ such that*

$$|N_{K/\mathbb{Q}}(x)| \le (\frac{4}{\pi})^{r_2}\frac{n!}{n^n}|\Delta_K|^{1/2}N(I).$$

2. *Every ideal class C contains an integral ideal $\mathfrak{a}$ such that*

$$N(\mathfrak{a}) \le (\frac{4}{\pi})^{r_2}\frac{n!}{n^n}|\Delta_K|^{1/2}.$$

[1] because $\begin{pmatrix} a+bi \\ a-bi \end{pmatrix} = \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix}$

Proof. (1) We consider the region B_t, for some $t \in \mathbb{R}_{\geq 0}$, defined in the lemma. Let t be chosen so that

$$\mu(B_t) = 2^n \mathrm{Vol}(\mathbb{R}^n/\lambda(I)).$$

Explicitly, we need[2]

$$t^n = (\frac{4}{\pi})^{r_2} |\Delta_K|^{1/2} n! N(I).$$

By Minkowski's theorem 6.1.5 (3), $B_t \cap \lambda(I)$ contains a non-zero element $\lambda(x)$ with $x \in I$. For this x, we have (as $x \in B_t$)

$$|N_{K/\mathbb{Q}}(x)| = \prod_{i=1}^{n} |\sigma_i(x)| \leq \big(\frac{1}{n}\sum_{i=1}^{n} |\sigma_i(x)|\big)^n \leq \frac{1}{n^n} t^n,$$

giving the result (where the middle inequality: if $x_i \geq 0$, then $\frac{x_1+\cdots+x_n}{n} \geq \sqrt[n]{x_1 \cdots x_n}$).

(2) Let J be any fractional ideal in the ideal class C and $I = J^{-1}$. By (1), we can find $x \in I$ such that $|N_{K/\mathbb{Q}}(x)| \leq (*)$. By definition, xJ is an integral ideal in the class C, and

$$N(xJ) = |N_{K/\mathbb{Q}}(x)| N(J) \leq (*) \cdot \frac{1}{N(I)} = (\frac{4}{\pi})^{r_2} \frac{n!}{n^n} |\Delta_K|^{1/2}.$$

□

Definition 6.3.3. *Given a number field of degree n, the quantity*

$$M_K := (\frac{4}{\pi})^{r_2} \frac{n!}{n^n} \sqrt{|\Delta_K|}$$

is called Minkowski's constant *(only depends on K).*

Theorem 6.3.4. *For every number field K, its ideal class group Cl_K is a finite abelian group.*

Proof. Clear. Since every ideal class contains an integral ideal of norm $\leq C$ (independent of the ideal class), and since such integral ideals are finite. □

Corollary 6.3.5. *For a number field K of degree n, we have*

$$|\Delta_K|^{1/2} \geq (\frac{\pi}{4})^{n/2} \frac{n^n}{n!}.$$

In particular, if $K \neq \mathbb{Q}$, then $|\Delta_K| > 1$, so that there always exist primes which ramify in K.

Proof. Since for every integral ideal $\mathfrak{a}$, $N(\mathfrak{a}) \geq 1$, we obtain by Theorem (2),

$$|\Delta_K|^{1/2} \geq (\frac{\pi}{4})^{r_2} (\frac{n^n}{n!}),$$

then use the fact that $\pi/4 < 1$ and $r_2 < n/2$. It is easy to check that for $a_n := (\frac{\pi}{4})^{r_2}(\frac{n^n}{n!})$, it is strictly increasing, because

$$\frac{a_{n+1}}{a_n} = \sqrt{\frac{\pi}{4}} (1 + \frac{1}{n})^n > \sqrt{\frac{\pi}{4}} (1 + \frac{1}{2})^2 > 1;$$

so $|\Delta_K|^{1/2} \geq a_2 = \sqrt{\pi} > 1$. □

[2] because $\mu(B_t) = 2^{r_1} (\frac{\pi}{2})^{r_2} \frac{1}{n!} \cdot (\frac{4}{\pi})^{r_2} |\Delta_K|^{1/2} n! N(I) = 2^{r_1+r_2} |\Delta_K|^{1/2} N(I) = 2^n \mathrm{Vol}(\mathbb{R}^n/\lambda(I))$

Theorem 6.3.6. *(Hermite) For a fixed integer Δ, there exists only finitely many number fields K with discriminant Δ.*

Proof. By the previous corollary, if K is a number field with discriminant Δ, then its degree $n = [K : \mathbb{Q}]$ is bounded by a constant in terms of $|\Delta|$. If suffices to prove that there are only finitely many number fields K of given discriminant Δ, and whose number of real and non-real embeddings are respectively r_1 and r_2. We want to find $\alpha \in \ cO_K$ such that $K = \mathbb{Q}(\alpha)$ and with $|\sigma_i(\alpha)|$ uniformly bounded.

First treat the case $r_1 > 0$, i.e. K admits real embeddings. Given $c_1, ..., c_{r_1+r_2} > 0$, consider the subset

$$W(c) = \{x = (y, z) \in \mathbb{R}^n \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} ||y_i| \leq c_i, 1 \leq i \leq r_1;\ |z_j|^2 \leq c_{r_1+j},\ 1 \leq j \leq r_2\}.$$

One checks that $\mu(W(c)) = 2^{r_1}\pi^{r_2}\prod_{i=1}^{r_1+r_2} c_i$.

Choose c_i for $1 \leq i \leq r_1 + r_2$ such that $c_1 > 1$, $c_i < 1$ for $i > 1$, and

$$\mu(W(c)) \geq 2^n \mathrm{Vol}(\mathbb{R}^n/\lambda(\mathcal{O}_K)) = 2^n\sqrt{|\Delta|}.$$

Then Theorem 6.1.5 implies that there exists a non-zero $\alpha \in \mathcal{O}_K$ such that

$$|\sigma_i(\alpha)| < c_i, \quad 1 \leq i \leq r_1; \quad |\sigma_{r_1+2j}(\alpha)|^2 < c_{r_1+j},\ 1 \leq j \leq r_2.$$

Since $|N_{K/\mathbb{Q}}(\alpha)| \geq 1$, we must have $|\sigma_1(\alpha)| > 1$ (since $|\sigma_i(\alpha)| < 1$ for all $i \neq 1$). It follows that $\sigma_1(\alpha) \neq \sigma_i(\alpha)$ for all $i \neq 1$, hence $\sigma_i(\alpha) \neq \sigma_j(\alpha)$ for $i \neq j$. This implies that α has degree n over $\mathbb{Q}$, i,e, $K = \mathbb{Q}(\alpha)$. If $f \in \mathbb{Q}[X]$ denotes the minimal polynomial of α, then $f \in \mathbb{Z}[X]$ and its coefficients are clearly bounded above in terms of functions of c_i. But the c_i are chosen only depending on Δ, and such polynomials are finite, implying the result.

The case $r_1 = 0$ can be treated similarly. □

6.4 Examples

Example 6.4.1. *For real quadratic field $K = \mathbb{Q}(\sqrt{d})$, $d > 0$ square-free, we have $n = 2$, $r_2 = 0$, so $M_K = \frac{1}{2}|\Delta_K|^{1/2}$.*

1. *If $K = \mathbb{Q}(\sqrt{5})$, $M_K < 2$, so every ideal class contains an integral ideal with norm 1, i.e. $\mathcal{O}_K$. So $Cl(K) = 1$.*

2. *For $K = \mathbb{Q}(\sqrt{10})$, $\Delta_K = 40$, $M_K = \frac{1}{2}\sqrt{40} < 4$. We need study the integral ideals of norm 2, 3. In particular, ideals containing respectively 2, 3. We know*

$$2\mathcal{O}_K = \mathfrak{p}^2, \quad N(\mathfrak{p}) = 2, \quad \mathfrak{p} = (2, \sqrt{10}).$$

One checks that $\mathfrak{p}$ is not a principal ideal, with $[\mathfrak{p}]^2 = 1$. On the other hand,

$$3\mathcal{O}_K = \mathfrak{q}_1\mathfrak{q}_2, \quad N(\mathfrak{q}_1) = N(\mathfrak{q}_2) = 3, \quad \mathfrak{q}_1 = (3, 1 + \sqrt{10}), \quad \mathfrak{q}_2 = (3, 1 - \sqrt{10}).$$

They are not principal ideals and $[\mathfrak{q}_1] = [\mathfrak{q}_2]^{-1}$. So $Cl(K)$ is generated by $\mathfrak{p}, \mathfrak{q}_1$. Next, since

$$\mathfrak{p}\mathfrak{q}_1 = (2, \sqrt{10})(3, 1 + \sqrt{10}) \supset (2 - \sqrt{10})$$

so for some integral ideal $\mathfrak{a}$, we have $(2 - \sqrt{10}) = \mathfrak{a}\mathfrak{p}\mathfrak{p}_1$. However, looking at the norms, $N((2 - \sqrt{10})) = 6$, so $N(\mathfrak{a}) = 1$, i.e. $\mathfrak{a} = \mathcal{O}_K$. Hence $\mathfrak{p}\mathfrak{p}_1$ is principal. This shows that $Cl(K) = \langle[\mathfrak{p}]\rangle \cong \mathbb{Z}/2\mathbb{Z}$.

Example 6.4.2. *For $K = \mathbb{Q}(\sqrt{-d})$ imaginary, we have $n = 2$, $r_2 = 1$, $M_K = \frac{2}{\pi}|\Delta_K|^{1/2}$.*

1. *for $\mathbb{Q}(\sqrt{-23})$, $M_K = \frac{2}{\pi}\sqrt{23} < 4$, so need study the decomposition of (2) and (3). Since $-23 \equiv 1 \mod 8$, 2 decomposes completely*

$$(2) = \mathfrak{p}_1\mathfrak{p}_2, \quad [\mathfrak{p}_1] = [\mathfrak{p}_2]^{-1}, \quad N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = 2.$$

Note that $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}(\frac{1+\sqrt{-23}}{2})$. If $\mathfrak{p}_1 = (\alpha)$ with $\alpha = a + b\omega$, then

$$2 = N(\mathfrak{p}_1) = (a + \frac{b}{2})^2 + \frac{23}{4}b^2$$

i.e. $(2a + b)^2 + 23b^2 = 8$. But this equation has no solution in $\mathbb{Z}^2$, hence $\mathfrak{p}_1$ is not principal. Similarly, since $\left(\frac{-23}{3}\right) = 1$, 3 decomposes completely:

$$(3) = \mathfrak{q}_1\mathfrak{q}_2, \quad N(\mathfrak{q}_i) = 3, \quad [\mathfrak{q}_1] = [\mathfrak{q}_2]^{-1}.$$

Also the equation $(2a + b)^2 + 23b^2 = 12$ has no solution in $\mathbb{Z}^2$, so $\mathfrak{q}_1$ is not principal, and $[\mathfrak{q}_1] \neq 1$. However,

$$(2a + b)^2 + 23b^2 = 24$$

has solution $(a, b) = (0, 1)$, so $N(I) = 6$ where $I = (\frac{1+\sqrt{-23}}{2})$. We obtain $I = \mathfrak{p}_i\mathfrak{q}_j$ for some pair (i, j). Hence $Cl(K)$ is a cyclic group generated by $[\mathfrak{p}_1]$. To determine its order, look at $[\mathfrak{p}]^2 = [\mathfrak{p}^2]$. Since the equation $(2a+b)^2+23b^2 = 16$ has a solution $(2, 0)$, but we saw that $(2) = \mathfrak{p}_1\mathfrak{p}_2$. On the other hand, the equation $(2a + b)^2 + 23b^2 = 32$ has solution $(1, 1)$, so we obtain a principal ideal J with norm 2^3. There are four possibilities for the prime decomposition of J:

$$\mathfrak{p}_1^3, \quad \mathfrak{p}_1^2\mathfrak{p}_2, \quad \mathfrak{p}_1\mathfrak{p}_2^2, \quad \mathfrak{p}_2^3.$$

If $J = \mathfrak{p}_1^2\mathfrak{p}_2$, then since $\mathfrak{p}_1\mathfrak{p}_2$ is principal, we obtain $\mathfrak{p}_1$ is also principal, a contradiction. Similarly, $J \neq \mathfrak{p}_1\mathfrak{p}_2^2$. Therefore, we obtain finally $[\mathfrak{p}_1]^3$ and $Cl(K) \cong \mathbb{Z}/3\mathbb{Z}$.

2. *For $\mathbb{Q}(\sqrt{-163})$, $M_K = \frac{2}{\pi}\sqrt{163} \sim 8$, so need study integral ideals with norm ≤ 8. If knowing a priori $h_K = 1$, we need to show every ideal is principal. A principal ideal (α) with $|N(\alpha)| = n$ means that*

$$(2a + b)^2 + 163b^2 = 4n.$$

If $n = 2$, it does not have solutions, so equivalently we need check that no *ideal with norm 2, i.e. 2 is inert in K, i.e. $-163 \neq 1 \mod 8$; this is ok. For $|N(\alpha)| = 3$, we need show 3 inerts in K, i.e. $\left(\frac{-163}{3}\right) = -1$; still ok.*

Example 6.4.3. *For $K = \mathbb{Q}(\sqrt[3]{2})$, we have $n = 3$, $r_2 = 1$ and $\Delta_K = -2^2 3^3$. The Minkowski bound for K is*

$$(\frac{4}{\pi})\frac{3!}{3^3}\sqrt{3^3 2^2} \sim 2.94 < 3.$$

But the only integral ideal of $\mathcal{O}_K$ with norm 2 is $\sqrt[3]{2}$. It follows that K has class number 1, hence $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$ is a PID.

Remark 6.4.4. *Gauss conjectured that for imaginary quadratic fields $K = \mathbb{Q}(\sqrt{-d})$, $h_K = 1$ only for*

$$d = 1, 2, 3, 7, 11, 19, 43, 67, 163.$$

1. *Hecke(1918)-Deuring(1933)-Heilbronn (1934), proved the following conjecture*[3]*:*

$$h_K \to \infty, \quad d \to \infty.$$

2. *Heilbronn-Linfoot (1934) if* $d > 163$*, there exists at most one* d*, such that* $h_K = 1$*. Also*

3. *Baker, Stark (1967), the possible exceptional* d *does not exist.*

4. *For real quadratic fields, it is more difficult, Gauss conjectures that there are infinitely many* d *such that* $h_K = 1$*. (Still open.)*

Week 6 Exercise:

1. Determine the class group for the follow real quadratic fields $K = \mathbb{Q}(\sqrt{d})$:

$$d = 7, 11, 15, 17, 21$$

2. Determine the class group for the follow imaginary quadratic fields $K = \mathbb{Q}(\sqrt{-d})$:

$$d = 5, 7, 11, 15, 17, 21.$$

[3]Precisely, first a theorem of Hecke says that the generalized Riemann hypothesis implies Gauss' conjecture; later a Theorem of Heilbronn proved that if GRH is false, then also implies Gauss' conjecture.

Chapter 7

W7: Dirichlet's unit theorem

7.1 Roots of unity

Let U_K denote the unit group of $\mathcal{O}_K$, which is an abelian group. We will show that it is finitely generated. Let W_K be the torsion subgroup of U_K, i.e.

$$W_K := \{x \in U_K : \exists m \geq 1, x^m = 1\}.$$

We call $x \in W_K$ a root of unity.

Lemma 7.1.1. *W_K is a finite cyclic group.*

Proof. (1) Let ζ_N be a primitive root of unity. If $\zeta_N \in W_K \subset K$, then $\mathbb{Q}(\zeta_N) \subset K$, hence $\varphi(N) \leq n := [K : \mathbb{Q}]$. It is clear that such N form a finite set.

(2) It is known that in a field, any finite multiplicative subgroup is cyclic. □

Example 7.1.2. *(i) If $K \subset \mathbb{R}$ is a real field, then $W_K = \{\pm 1\}$.*

(ii) If $K = \mathbb{Q}(\sqrt{-d})$ be imaginary quadratic. If $\zeta_N \in K$ with $p^r | N$, then

$$2 = [K : \mathbb{Q}] \geq \varphi(N) \geq \varphi(p^r) = p^{r-1}(p-1)$$

which forces that $p = 2$ and $m \in \{1, 2\}$, or $p = 3$ and $m = 1$. So if $d = 1$, $W_K = \{\pm 1, \pm i\}$. If $d = 3$, $W_K = \{\pm 1, \pm\omega, \pm\omega^2\}$ of cardinality 6. Otherwise, $W_K = \pm 1$.

(iii) If $K = \mathbb{Q}(\zeta_N)$ is a cyclotomic field, then

(a) if $N \equiv 1 \mod 2$, $W_K = \{\zeta_{2N}^k : 0 \leq k \leq 2N - 1\}$, and $|W_K| = 2N$;

(b) if $N \equiv 0 \mod 4$, $W_K = \{\zeta_N^k : 0 \leq k \leq N - 1\}$ and $|W_K| = N$.

Lemma 7.1.3. *Let $\sigma_1, ..., \sigma_n$ be the set of embeddings $K \to \mathbb{C}$. Let $u \in \mathcal{O}_K$.*

(1) $u \in U_K \Leftrightarrow N_{K/\mathbb{Q}} = \pm 1$.

(2) $u \in W_K \Leftrightarrow |\sigma_i(u)| = 1, 1 \leq i \leq n$.

Proof. (1) Recall that $|N_{K/\mathbb{Q}}(x)| = N((x))$ for $x \in \mathcal{O}_K$, so $N_{K/\mathbb{Q}}(x) = \pm 1$ if and only if $\mathcal{O}_K/(x) = 0$, i.e. x is a unit.

We can also use the condition $N_{K/\mathbb{Q}}(u) = \pm 1$ to see that the minimal polynomial of u has the shape

$$X^n + \cdots + (\pm 1) \in \mathbb{Z}[X],$$

hence u^{-1} also satisfies a monic integral equation, hence integral over $\mathbb{Z}$.

(2) If u is a root of unity, $u^m = 1$, then $\sigma_i(u)^m = 1$ for any i, so $|\sigma_i(u)| = 1$. Conversely, for any fixed j, consider the polynomial

$$f(X) = \prod_{i=1}^{n}(X - \sigma_i(u^j)) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X].$$

Since $|\sigma_i(u^j)| = 1$, we obtain $|a_i| \leq \binom{n}{i}$ for any i. But there are only finitely many such polynomials in $\mathbb{Z}[X]$, so there exist $j > k$ such that $u^j = u^k$, i.e. $u^{j-k} = 1$, as required. $\square$

7.2 Dirichlet's unit theorem

Theorem 7.2.1. *Let K be a number field of degree n, with $n = r_1 + 2r_2$. Then*

$$U_K \cong V_K \times W_K, \quad V_K \cong \mathbb{Z}^{r_1+r_2-1}.$$

Remark 7.2.2. *The free part is not canonically determined by U_K: if x is not torsion and y is torsion, then xy is not torsion. A $\mathbb{Z}$-basis of V_K is called a system of fundamental units of K. If $\eta_1, ..., \eta_r$ is such a basis, then every $u \in U_K$ can be written uniquely as*

$$u = w\eta_1^{a_1} \cdots \eta_r^{a_r}, \quad a_i \in \mathbb{Z}.$$

Proof. We consider the map $\ell : U_K \to \mathbb{R}^{r_1+r_2}$, defined to be the composite

$$U_K \subset \mathcal{O}_K \backslash \{0\} \to \mathbb{R}^{\times, r_1} \times \mathbb{C}^{\times, r_2} \overset{\text{Log}}{\to} \mathbb{R}^{r_1+r_2}$$

where Log is the logarithm map defined by:

$$(y_1, ..., y_{r_1}, z_1, ..., z_{r_2}) \mapsto (\log|y_1|, ..., \log|y_{r_1}|, 2\log|z_1|, ..., 2\log|z_{r_2}|).$$

Then ℓ is a homomorphism of abelian groups. By Lemma,

$$u \in \ker(\ell) \Leftrightarrow \log|y_i| = \log|z_j| = 0 \Leftrightarrow |y_i| = |z_j| = 1 \overset{Lem.}{\Leftrightarrow} u \in W_K.$$

Moreover, if $u \in U_K$, Lemma implies that

$$\sum_{i=1}^{r_1} \log|\sigma_i(u)| + 2\sum_{j=1}^{r_2} \log|\sigma_{r_1+2j}(u)| = \log|N_{K/\mathbb{Q}}(u)| = 0,$$

that is, $\text{Im}(\ell)$ is contained in the hyperplane $H \subset \mathbb{R}^{r_1+r_2}$ defined by $\sum_{i=1}^{r_1+r_2} x_i = 0$. This already shows that $\text{rank}(U_K) \leq r_1 + r_2 - 1$.

We will prove that $\ell(U_K)$ is a full lattice in H, hence of rank $r_1 + r_2 - 1$. $\square$

Lemma 7.2.3. *For each integer $1 \leq k \leq r_1 + r_2$, there exists $u_k \in U_K$ such that*

$$|\sigma_k(u_k)| > 1, \quad |\sigma_i(u_k)| < 1, \ \forall i \neq k.$$

Proof. Fix k as in the lemma. We will construct a sequence of elements in $\mathcal{O}_K$: $a_1, a_2, ...$ such that $N(a_m) < A$ uniformly bounded, and

$$|\sigma_i(a_{m+1})| < |\sigma_i(a_m)|, \quad \forall i \neq k.$$

Since the number of integral ideals with norm bounded by A is finite, we must have $(a_m) = (a_{m'})$ for some $m < m'$, hence there exists $u \in U_K$ such that $a_{m'} = u \cdot a_m$. Since for any $i \neq k$, $|\sigma_i(a_{m'})| < |\sigma_i(a_m)|$, we obtain $|\sigma_i(u)| < 1$ (for $i \neq k$). Also, $|\sigma_k(u)| > 1$ since product gives the norm.

Let A be a constant $> (\frac{2}{\pi})^{r_2}\sqrt{|\Delta_K|}$. Let $c_1, ..., c_{r_1+r_2} > 0$ be such that $c_i < 1$ for all $i \neq k$ and $\prod_i c_i = A$. As seen before, there exists $a_1 \in \mathcal{O}_K$ such that

$$|\sigma_i(a_1)| < c_i \; 1 \leq i \leq r_1; \quad |\sigma_i(a_1)|^2 < c_i$$

Define new c_i as follows:

$$c_i' = |\sigma_i(a_1)| \; \forall i \neq k, \quad \prod_i c_i' = A.$$

Argue as above we get a_2 with $|\sigma_i(a_2)| < |\sigma_i(a_1)|$ whenever $i \neq k$. Continuing this construction gives a sequence $(a_m)_{m \geq 1}$ as required. □

Lemma 7.2.4. *Let $A = (a_{i,j})_{1 \leq i,j \leq m}$ be a real matrix. Assume that $\sum_{i=1}^m a_{i,j} = 0$ for all j, and*[1]

$$a_{i,i} > 0, \; \forall i, \quad a_{i,j} < 0 \;\; \forall i \neq j.$$

Then the rank A is $m-1$.

Proof. The rank is $\leq m-1$ as $A \cdot (1, ..., 1)^T = 0$. Let us show that the first $m-1$ rows of A, $\mathbf{v}_1, ..., \mathbf{v}_{m-1}$ are linearly independent. Otherwise, there exist $x_1, ..., x_{m-1} \in \mathbb{R}$ such that $\sum_{i=1}^{m-1} x_i \mathbf{v}_i = 0$. Let k be such that $x_k = \max_{1 \leq i \leq m-1}\{x_i\} > 0$: it is positive because the x_i can not be all negative by looking at the last row $\sum_{i=1}^{m-1} x_i a_{m,i} = 0$ (with all $a_{m,i} < 0$). Thus, for this j_0, one has

$$0 = \sum_i x_i a_{i,j_0} = x_{j_0} \sum_{i=1}^{m-1} a_{i,j_0} + \sum_{1 \leq i \leq m-1} (x_i - x_{j_0}) a_{i,j_0} = x_{j_0} \sum_{i=1}^{m-1} a_{i,j_0} + \sum_{1 \leq i \leq m-1, i \neq j_0} (x_i - x_{j_0}) a_{i,j_0} > 0,$$

because $\sum_{i=1}^{m-1} a_{i,j_0} = -a_{m,j_0} > 0$, and because $x_i - x_{j_0} < 0$ by choice a conradiction. □

Define the *regulator* of K: Let $\{\eta_1, ..., \eta_r\}$ be a system of fundamental units, write

$$l(\eta_i) = (y_{1,i}, ..., y_{r+1,i}) = (\log|\sigma_1(\eta_i), ... \log|\sigma_{r_1}(\eta_i)|, \ldots, 2\log|\sigma_j(\eta_i)|) \in \mathbb{R}^{r+1}$$

and define

$$R(\eta_1, ..., \eta_r) := |\det(y_{ij})_{1 \leq i,j \leq r}|$$

and call it the *regulator* of K, denoted R_K.

This is well-defined. There is another description of R_K: consider the matrix

$$\begin{vmatrix} 1 & \log|\sigma_1(\eta_1)| & \cdots & \log|\sigma_1(\eta_r)| \\ \vdots & \cdots & & \vdots \\ 1 & \log|\sigma_{r+1}(\eta_1)| & \cdots & \log|\sigma_{r+1}(\eta_r)| \end{vmatrix},$$

multiply the i-th row $(1 \leq i \leq r_1)$ by 1 and the row $(r_1 + 1 \leq i \leq r_1 + r_2)$ by 2, and add the sum of the first r row to the last row. We obtain $\det = \pm N|\det(y_{ij})_{1 \leq i,j \leq r}|$. Moreover, R_K is independent of the choice of $\{\eta_1, ..., \eta_r\}$.

[1] i.e. of the shape $\begin{pmatrix} + & \cdots & - \\ - & + & - \\ - & \cdots & + \end{pmatrix}$

The regulator of an algebraic number field of degree greater than 2 is usually quite cumbersome to calculate, though there are now computer algebra packages that can do it in many cases. It is usually much easier to calculate the product $h_K R_K$ of the class number h_K and the regulator using the class number formula, and the main difficulty in calculating the class number of an algebraic number field is usually the calculation of the regulator.

7.3 Fundamental units in real quadratic fields

Let $K = \mathbb{Q}(\sqrt{d})$ with $d > 0$ square-free. Then $r_1 + r_2 - 1 = 2 - 1 = 1$, that is, a system of fundamental units of K consists of one single unit. Moreover, if ϵ is such a unit, the others are $\{\pm\epsilon, \pm\epsilon^{-1}\}$, so there is a unique one such that $\epsilon > 1$, and $U_K = \{\pm\epsilon^n : n \in \mathbb{Z}\}$.

For $d \equiv 2, 3 \mod 4$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$, so any integer is of the form $a + b\sqrt{d}$, $a, b \in \mathbb{Z}$. Since

$$a + b\sqrt{d} \in U_K \Leftrightarrow N(a + b\sqrt{d}) = a^2 - db^2 = \pm 1,$$

we need study the equation $x^2 - dy^2 = \pm 1$, which is called a Pell equation.

Lemma 7.3.1. *With the above assumption, let $\epsilon = a + b\sqrt{d}$ be the unique fundamental unit such that $\epsilon > 1$. Let $\epsilon^n = (a + b\sqrt{d})^n = a_n + b_n\sqrt{d}$.*

1. *If $N(\epsilon) = 1$, then Pell's equation $x^2 - dy^2 = -1$ has no integral solution, and $x^2 - dy^2 = 1$ has all integral solutions given by $\{(\pm a_n, \pm b_n) | n \in \mathbb{Z}\}$.*

2. *If $N(\epsilon) = -1$, then $x^2 - dy^2 = -1$ has all integral solutions given by $\{(\pm a_{2n+1}, \pm b_{2n+1}) | n \in \mathbb{Z}\}$, while $x^2 - dy^2 = 1$ has all integral solutions given by $\{(\pm a_{2n}, \pm b_{2n}) | n \in \mathbb{Z}\}$.*

Proof. This is clear. $\square$

Example 7.3.2. *(1) Let $d = 5$. A fundamental unit is $\frac{\sqrt{5}+1}{2}$, and its images under the two embeddings into $\mathbb{R}$ are $\frac{\sqrt{5}+1}{2}$ and $\frac{-\sqrt{5}+1}{2}$, so the regulator is $\log \frac{\sqrt{5}+2}{1}$.*

(2)Let $d = 14$. Pell's equation is $x^2 - 14y^2 = \pm 1$. Since 14 ± 1, $14 \times 2^2 \pm 1$, $14 \times 3^2 \pm 1$ are not squares, while $14 \times 4^2 + 1 = 15^2$, so $15 + 4\sqrt{14}$ is the fundamental unit. Since $N(\epsilon) = -1$, the integral solutions of $x^2 - 14y^2 = 1$ are

$$\{(\pm a_{2n}, \pm b_{2n}) | a_{2n} + b_{2n}\sqrt{14} = (15 + 4\sqrt{14})^{2n}, n \in \mathbb{Z}\},$$

while the integral solutions of $x^2 - 14y^2 = -1$ are

$$\{(\pm a_{2n+1}, \pm b_{2n+1}), n \in \mathbb{Z}\}.$$

Remark 7.3.3. *If $d \equiv 1 \mod 4$, $\mathcal{O}_K = \mathbb{Z} \oplus \omega$, with $\omega = \frac{1}{2}(1 + \sqrt{d})$, so $\epsilon = \frac{1}{2}(A + B\sqrt{d})$ (can always be written into this form) is a unit iff $A^2 - dB^2 = \pm 4$. We can similarly compute the fundamental unit.*

7.4 Cyclotomic fields

Let $K = \mathbb{Q}(\zeta_{p^t})$, p is odd prime and $t \geq 1$. Then W_K is a cyclic group of order $2p^t$. Since

$$n = [K : \mathbb{Q}] = \varphi(p^t) = p^{t-1}(p-1), \quad r_1 = 0, \quad r_2 = \frac{1}{2}\varphi(p^t)$$

we obtain $r := r_1 + r_2 - 1 = \frac{1}{2}\varphi(p^t) - 1$.

Note that K contains a maximal real subfield K_+:

$$K_+ := \mathbb{Q}(\zeta_{p^t} + \zeta_{p^t}^{-1}).$$

Lemma 7.4.1. *We have the following facts:*

1. $[K_+ : \mathbb{Q}] = \frac{1}{2}\varphi(p^t)$.
2. *there exists a set of real units in K: $\eta_1, ..., \eta_r$, which is a system of fundamental units for K and also for K_+.*
3. $R_K / R_{K_+} = 2^r$.

Week 7 Exercise

1. Compute the fundamental unit ≥ 1 of $\mathbb{Q}(\sqrt{d})$, with $d = 2, 3, 4, 6, 7, 10$.
2. Let $d = t^2 + 4$ be square-free, $t \in \mathbb{Z}_{>0}$. Prove that $\epsilon_0 = \frac{1}{2}(t + \sqrt{t^2 + 4})$ is a fundamental unit in $\mathbb{Q}(\sqrt{d})$.
3. Let $p \equiv 1 \mod 4$, prove that the fundamental unit of $\mathbb{Q}(\sqrt{p})$ is -1 ?

Chapter 8

W8: Riemann Zeta function

8.1 Dirichlet Series

Definition 8.1.1. *An arithmetic function is a function*

$$f : \mathbb{N} \to \mathbb{C}.$$

Its associated Dirichlet series is a formal series which depends on a parameter s: $F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$. [1]

Let F, G be Dirichelet series associated to f, g. Then

$$F(s)G(s) = \sum_n \frac{\sum_{de=n} f(d)g(e)}{n^s}.$$

So we may define *convolution* of f, g by

$$f * g : \mathbb{N} \to \mathbb{C}, \quad n \mapsto \sum_{de=n} f(d)g(e),$$

i.e. $h = f * g$ if and only if $H = FG$.

Example 8.1.2. *(1) Identity arithmetic function:* $i(n) = 1$ *if* $n = 1$*, and* $= 0$ *otherwise. The Dirichlet series* $F(s) = 1$.

(2) Unit *arithmetic function is* $u(n) = 1$ *for all* n*. We obtain the famous Riemann Zeta function*

$$\zeta(s) = \sum_n \frac{1}{n^s}.$$

(3) The inverse (reciprocal) of $\zeta(s)$ *is (formally) the one associated to*

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^k & \text{if } n = p_1 \cdots p_k \\ 0 & \text{otherwise} \end{cases}$$

Lemma 8.1.3. *(Mobius Inversion formula)*

$$g(n) = \sum_{d|n} f(d) \Leftrightarrow f(n) = \sum_{d|n} g(d)\mu(n/d).$$

[1] Sometimes uses $\sum_{n\geq 1} \frac{a_n}{n^s}$.

Definition 8.1.4. *An arithmetic function is called* multiplicative *if*

$$f(mn) = f(m)f(n), \quad (m,n) = 1.$$

It is said completely multiplicative *(or totally multiplicative) if $f(mn) = f(m)f(n)$ for any $m, n \geq 1$.*

Lemma 8.1.5. *We have the following:*

$$f \text{ multiplicative } \Leftrightarrow F(s) = \prod_p \sum_{m=0}^{\infty} \frac{f(p^m)}{p^{ms}}$$

$$f \text{ comp.multiplicative } \Leftrightarrow F(s) = \prod_p (1 - f(p)p^{-s})^{-1}.$$

Example 8.1.6. *Some multiplicative functions*

- *The Mobius function μ.*
- *$n \mapsto n^k$. (also completely multiplicative)*
- *Euler totient function ϕ.*
- *The divisor function d: $d(n) := \sum_{d|n, d\geq 1} 1$.*
- *The divisor sum function σ: $\sigma(n) = \sum_{d|n} d$. More generally, $\sigma_k(n) := \sum_{d|n} d^k$.*

Example 8.1.7. *Define an arithmetic function by*

$$\Lambda(n) = \begin{cases} \log(p) & n = p^i, i \geq 1 \\ 0 & \text{else} \end{cases}$$

Prove that the Dirichlet series for Λ is $-\zeta'/\zeta$.

8.2 Convergence (without proof)

Write $s = \sigma + it$, and we will view $F(s)$ as a complex function. Recall how to define n^s:

1. if $z \in \mathbb{C}$, $e^z := \sum_{m=0}^{\infty} \frac{z^m}{m!} = e^{\sigma}(\cos(t) + i\sin(t))$.
2. if $s \in \mathbb{C}$, $n^s := e^{s \log n}$, where log is the natural (real) logarithm with base e. One has $|n^s| = n^{\sigma}$.
3. Hence $n^s = \sum_{m=0}^{\infty} \frac{(s \log n)^m}{m!}$.

Theorem 8.2.1. *Let $F(s) = \sum_{n\geq 1} \frac{f(n)}{n^s}$ be a Dirichlet series.There exists a number $\sigma_c \in \mathbb{R} \cup \{\pm\infty\}$ with the following properties:*

(i) If $R(s) > \sigma_c$, then $F(s)$ converges (not necessarily absolutely).

(ii) If $R(s) < \sigma_c$, then $F(s)$ diverges.

Definition 8.2.2. *The quantity σ_c is called the* abscissa of convergence *of the Dirichlet series.*

Theorem 8.2.3. *$F(s)$ uniformly converges on compact subsets of the half plane $R(s) > \sigma_c$.*

As a consequence, we may differentiate and integrate Dirichlet series term-by-term. For example:

$$F'(s) = -\sum_{n\geq 1} \frac{f(n)\log n}{n^s}.$$

Hence: the function $F(s)$ defined by a Dirichlet series in its half-plane $\Re(s) > \sigma_c$ of convergence is complex analytic.

Lemma 8.2.4. *Let $A(N) = \sum_{n=1}^{N} f(n)$. If $\{A_N : N \geq 1\}$ diverges, then*

$$\sigma_c = \inf\{\alpha | A(N) = O(N^\alpha)\} = \mathrm{limsup}_{N\to\infty} \frac{\log |A(N)|}{\log N}.$$

Proof. Omit. ◻

Similarly, we have a notion *abscissa of absolute convergence* , denoted by σ_{ac}, defined to the σ_c of $\sum_{n\geq 1} \frac{|f(n)|}{n^s}$.

Lemma 8.2.5. *We always have*

$$0 \leq \sigma_{ac} - \sigma_c \leq 1.$$

Example 8.2.6. *(1) If $f(n) = 1$, then $A(N) = N \to \infty$, so for $\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s}$, $\sigma_c = \sigma_{ac} = 1$, so $\zeta(s)$ defines an analytic function on $\Re(s) > 1$. Also, we will see that $s = 1$ is a pole of $\zeta(s)$.*

(2) If $f(n) = (-1)^n$, then $A(N) \in \{0, -1\}$ and it diverges, so that $\sigma_c = 0$ (while $\sigma_{ac} = 1$). In particular $F(s)$ is analytic at $s = 1$: $F(1) = -1 + \frac{1}{2} - \frac{1}{3} + \cdots = -\log 2$. On the other hand,

$$F(s) = \sum_{n\geq 1} \frac{(-1)^n}{n^s} = -\sum_{n\geq 1} \frac{1}{n^s} + 2\sum_{n\geq 1} \frac{1}{(2n)^s} = -(1 - 2^{-(s-1)})\zeta(s), \quad \Re(s) > 1.$$

But, $(1 - 2^{-(s-1)}) = (s-1)\log 2 + (s-1)^2 a + \cdots$ has a simple zero at $s = 1$, so that $\zeta(s)$ is a simple pole at $s = 1$ with residue

$$\mathrm{Res}_{s=1}\zeta(s) = \frac{\log 2}{\log 2} = 1.$$

Recall that an ordinary power series in a complex variable must have a singularity on the boundary of its radius convergence. For Dirichlet series with non-negative real coefficients, we have the following analogous fact. Note that the condition of $f(n) \geq 0$ is critical, as the above example $\sum_{n\geq 1} \frac{(-1)^n}{n^s}$ can be analytically extended to $\mathbb{C}$ (as we will see later).

Theorem 8.2.7. *(Landau) Let $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ be a Dirichlet series with $a_n \geq 0$. Suppose $\sigma_c \in \mathbb{R}$ is the abscissa of (absolute) convergence for $F(s)$. Then F cannot be extended to a holomorphic function on a neighbourhood of $s = \sigma_c$.*

Proof. Suppose on the contrary that f extends to a holomorphic function on the disc $|s - \sigma_c| < \epsilon$. Pick a real number $\sigma' \in (\sigma_c, \sigma_c + \epsilon/2)$, and write

$$\begin{aligned} F(s) &= \textstyle\sum_{n=1}^{\infty} f(n) n^{-\sigma'} n^{\sigma'-s} \\ &= \textstyle\sum_{n=1}^{\infty} f(n) n^{-\sigma'} e^{(\sigma'-s)\log n} \\ &= \textstyle\sum_{n=1}^{\infty} \sum_{i=0}^{\infty} \frac{f(n)n^{-\sigma'}(\log n)^i}{i!} (\sigma' - s)^i \\ &= \textstyle\sum_{i=0}^{\infty} (\sum_{n=1}^{\infty} \frac{f(n)n^{-\sigma'}(\log n)^i}{i!})(\sigma' - s)^i. \end{aligned}$$

Since all coefficients in this double series are nonnegative, everything must converge absolutely in the disc $|s - \sigma'| < \epsilon/2$. In particular, when viewed as a power series in $\sigma' - s$, this must give the Taylor series for f around $s = \sigma'$. Since f is holomorphic in the disc $|s - \sigma'| < \epsilon/2$, the Taylor series converges on the whole disc. In particular, the original Dirichlet series $F(s)$ converges absolutely at some real point $< \sigma_c$. This contradicts the definition of σ. $\square$

For example, it follows from Landau's theorem that the Riemann zeta function $\zeta(s)$ must have a singularity at $s = 1$, as we just checked.

Theorem 8.2.8. *(Uniqueness Theorem) Let $f(n), g(n)$ be arithmetical functions whose Dirichlet series are both absolutely convergent in the half-plane $\Re(s) > \sigma_0$. Suppose there exists an infinite sequence s_k of complex numbers, with $\Re(s_k) > \sigma_0$ for all k and $\Re(s_k) \to \infty$ such that $F(s_k) = G(s_k)$ for all k. Then $f(n) = g(n)$ for all n.*

We could also talk about the convergence of the product decomposition.

Theorem 8.2.9. *If f is multiplicative we have an equality of functions*

$$F(s) = \prod_p (1 + \frac{f(p)}{p^s} + \cdots)$$

for all s with $\Re(s) > \sigma_{ac}$. A similar equality holds if f is completely multiplicative.

Proof. See Feng Keqin. For example, the infinite product is absolutely convergent for $\Re(s) > 1$, since the corresponding series

$$\sum_p |\frac{1}{p^s}| = \sum_p \frac{1}{p^\sigma} < \infty, \quad \sigma > 1.$$

$\square$

8.3 Riemann zeta function

Theorem 8.3.1. *(Riemann). The function ζ can be analytically extended to a meromorphic function on $\mathbb{C}$, which satisfies the functional equation*

$$\pi^{-s/2}\Gamma(s/2)\zeta(s) = \pi^{(1-s)/2}\Gamma((1-s)/2)\zeta(1-s). \tag{8.1}$$

where Γ denotes the Gamma function (see below). Moreover,

(1) ζ has a unique simple pole at $s = 1$, with residue 1;

(2) *ζ has simple zeros at the negative even integrals $-2, -4, -6, \ldots$.*

(3) *all the other zeros lie in strip $0 < \Re(s) < 1$, and are symmetric with respect to $\Re(s) = 1/2$ (called the* critical line*).*

The zeros $-2, -4, -6, \ldots$ of ζ are called the trivial zeros of the Riemann zeta function, and the famous Riemann hypothesis says that all non-trivial zeros of $\zeta(s)$ lies on $\Re(s) = 1/2$.

If we set [2]

$$\xi(s) := \pi^{-s/2}\Gamma(s/2)\zeta(s),$$

then Riemann's theorem says that $\xi(s)$ can be extended to a meromorphic function on $\mathbb{C}$ satisfying a simpler functional equation

$$\xi(s) = \xi(1-s).$$

The proof has two ingredients: properties of $\Gamma(s)$ as a meromorphic function of $s \in \mathbb{C}$, and the Poisson summation formula. We next review these two topics.

8.3.1 Gamma function

The Gamma function was first defined Euler for real $s > 0$, as the integral

$$\Gamma(s) := \int_0^\infty x^{s-1}e^{-x}dx. \tag{8.2}$$

We have $\Gamma(1) = \int_0^\infty e^{-x}dx = 1$ and, integrating by parts,

$$s\Gamma(s) = \int_0^\infty e^{-x}d(x^s) = -\int_0^\infty x^s d(e^{-x}) = \Gamma(s+1), \quad s > 0$$

so by induction $\Gamma(n) = (n-1)!$ for positive integers n. Since $|x^s| = x^\sigma$, the integral (8.2) defines an analytic function on $\Re(s) > 0$, which still satisfies the recursion $s\Gamma(s) = \Gamma(s+1)$. Using the formula

$$\Gamma(s) = \lim_{n\to\infty} \frac{n^s n!}{s(s+1)\cdots(s+n)}, \quad s \neq 0, -1, -2, \ldots$$

we extend Γ to a meromorphic function on $\mathbb{C}$, analytic except for simple poles at $0, -1, -2, -3, \ldots$ with residue $(-1)^n/n!$ at $s = -n$. It has no zeros.

We also note that Γ satisfies

$$\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin(\pi s)}.$$

In particular, $\Gamma(1/2) = \sqrt{\pi}$.

When $\Re(s) > 1$, $t > 0$, we compute

$$\begin{aligned}\pi^{-s/2}\Gamma(s/2)\zeta(s) &= \int_0^\infty \pi^{-s/2}\sum_{n\geq 1} n^{-s}t^{s/2-1}e^{-t}dt \qquad (t \mapsto \pi n^2 t) \\ &= \int_0^\infty t^{s/2-1}\big(\sum_{n\geq 1} e^{-\pi n^2 t}\big)dt.\end{aligned}$$

[2]Riemann uses $\xi(s) := \frac{1}{2}s(s-1)\pi^{-s/2}\Gamma(s/2)\zeta(s)$ and call it *completed zeta function*, which is an entire function (i.e. analytic on the whole complex plane) of s and satisfies $\xi(s) = \xi(1-s)$.

8.3.2 Theta function

Definition 8.3.2. *Let theta function be*

$$\theta(u) := \sum_{n=-\infty}^{\infty} e^{-\pi n^2 u} = 1 + 2(e^{-\pi u} + e^{-4\pi u} + \cdots);$$

it converges absolutely to an analytic function on $\Re(u) > 0$.

Lemma 8.3.3. *The function $\theta(u)$ satisfies the identity*

$$\theta(1/u) = u^{1/2}\theta(u).$$

Proof. We use the Poisson summation formula recalled below. First, the Fourier transform of $f(x) := e^{-\pi u x^2}$ is (here $x, y \in \mathbb{R}$)

$$\hat{f}(y) = \int_{-\infty}^{\infty} e^{2\pi i x y} e^{-\pi u x^2} dx = u^{-1/2} e^{-\pi u^{-1} y^2} \tag{8.3}$$

To see this, we note

$$\hat{f}(y) = e^{-\pi y^2/u} \int_{-\infty}^{\infty} e^{-\pi u (x - \frac{iy}{u})^2} dx$$

while using contour integral, [3]

$$\int_{-\infty}^{\infty} e^{-\pi u (x - \frac{iy}{u})^2} dx = \int_{-\infty}^{\infty} e^{-\pi u x^2} dx = \frac{1}{\sqrt{u}}.$$

where the last equality follows from Gauss integral by a change of variable

$$\int_{-\infty}^{\infty} e^{-x^2}\, dx = \sqrt{\pi}.$$

We thus obtain (8.3).

So the Poisson formula gives

$$\theta(u) = \sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}} \hat{f}(n) = \sum_{n\in\mathbb{Z}} u^{-1/2} e^{-\pi u^{-1} n^2} = u^{-1/2}\theta(1/u).$$

□

Theorem 8.3.4. *(Poisson summation formula) Let $f : \mathbb{R} \to \mathbb{C}$ be a $\mathcal{C}^2$ function such that $|f|, |f''| \in L^1(\mathbb{R})$, and let $\hat{f}$ be its Fourier transform*

$$\hat{f}(y) = \int_{-\infty}^{+\infty} e^{2\pi i n y} f(x) dx.$$

Then

$$\sum_{n=-\infty}^{+\infty} f(n) = \sum_{n=-\infty}^{\infty} \hat{f}(n),$$

with the sums converging absolutely.

Proof. We omit the proof. □

[3]because $e^{-\pi u z^2}$ is analytic in the rectangle region C with end-points $(-x, x)$ and $(-x - it, x - it)$, hence the integration is zero. However, since

$$|e^{-\pi u (x - it)^2}| = e^{-\pi u (x^2 - t^2)} \to 0, \quad x^2 \to +\infty$$

we get $\lim_{x\to\infty} \int_{x-it}^{x} e^{-\pi u z^2} dz = 0$, i.e. the integration along vertical lines vanish.

8.3.3 Analytic continuation

Proof of Theorem. We may rewrite the integral $2\xi(s)$ as

$$\begin{aligned} & \int_0^1(\theta(u)-1)u^{s/2}\frac{du}{u}+\int_1^\infty(\theta(u)-1)u^{s/2}\frac{du}{u} \\ = \quad & -\frac{2}{s}+\int_0^1\theta(u)u^{s/2}\frac{du}{u}+\int_1^\infty(\theta(u)-1)u^{s/2}\frac{du}{u}, \end{aligned}$$

and use the change of variables $u\mapsto 1/u$ to find (as $\frac{d(1/u)}{1/u}=-\frac{du}{u}$)

$$\begin{aligned} & \int_0^1\theta(u)u^{s/2}\frac{du}{u}=\int_1^\infty\theta(u^{-1})u^{-s/2}\frac{du}{u} \\ \overset{Lem.}{=} \quad & \int_1^\infty\theta(u)u^{(1-s)/2}\frac{du}{u}=\frac{2}{s-1}+\int_1^\infty(\theta(u)-1)u^{(1-s)/2}\frac{du}{u} \end{aligned}$$

Therefore,

$$\xi(s)+\frac{1}{s}+\frac{1}{1-s}=\frac{1}{2}\int_1^\infty(\theta(u)-1)(u^{s/2}+u^{(1-s)/2})\frac{du}{u} \tag{8.4}$$

which is symmetrical under $s\leftrightarrow 1-s$, and analytic since $\theta(u)$ decreases exponentially as $u\to\infty$. This concludes the proof of the functional equation and analytic continuation of $\zeta(s)$. □

8.3.4 Poles

As a consequence of (8.4), $\xi(s)$ has only poles at $s=0,1$, both being simple. Since $\Gamma(s)$ has no zeros, this implies that $\zeta(s)$ has at most poles at $s=0,1$. At $s=1$, we already saw that it is indeed a simple pole with residue 1. However, we will see later that $\zeta(0)=-1/2$, so $s=1$ is the only pole of $\zeta(s)$.

8.3.5 Zeros

Proof. When $\Re(s)>1$, $\zeta(s)$ has no zeros: this is because $\zeta(s)=\prod_p(1-p^{-s})^{-1}$. (A convergent infinite product of non-zero factors is non-zero.)

When $\Re(s)<0$, by the functional equation

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

Since $\Re(1-s)>1$, $\zeta(1-s)\neq 0$, we are left to study zeros and poles of Γ. Since $\Gamma(s)$ has no zeros, while has poles at $0,-1,-2,...$, so the only zeros of $\zeta(s)$ when $\Re(s)<0$ are $s=-2,-4,...$ (moreover, simple zeros). Note that

$$\zeta(0)=\lim_{s\to 0}\frac{\pi^{-1/2}\zeta(1-s)\Gamma(1/2)}{\Gamma(s/2)}=\lim_{s\to 0}\frac{\zeta(1-s)}{\Gamma(s/2)}=\lim_{s\to 0}\frac{s/2}{(1-s)-1}=-1/2\neq 0.$$

The next theorem shows that $\zeta(s)$ has no zeros on the line $\Re(s)=1$, hence also no zeros on the line $\Re(0)$ by symmetry, and completes the proof. □

Theorem 8.3.5. *For any $t\in\mathbb{R}$, $\zeta(1+it)\neq 0$.*

Proof. We only need consider the case $t\neq 0$. We first give the proof assuming Lemma 8.3.6 below. Dividing by $(\sigma-1)$, we get when $\sigma>1$,

$$((\sigma-1)\zeta(\sigma))^3\cdot|\frac{\zeta(\sigma+it)}{\sigma-1}|^4\cdot|\zeta(\sigma+2it)|\geq 1.$$

Now let $\sigma\to 1^+$.

1. the first factor approaches to 1 since $\zeta(s)$ has residue 1 at the pole $s = 1$.
2. the third factor tends to $|\zeta(1 + 2it)|$.
3. if $\zeta(1 + it) = 0$, then the second term would tend to

$$|\zeta'(1 + it)|^4, \quad \sigma \to 1^+.$$

So if for some $t \neq 0$, we had $\zeta(1 + it) = 0$, then the LHS would be a constant as $\sigma \to 1^+$, while the RHS tends to ∞, a contradiction. □

Lemma 8.3.6. *If $\sigma > 1$ we have*

$$\zeta^3(\sigma)|\zeta(\sigma + it)|^4|\zeta(\sigma + 2it)| \geq 1.$$

Proof. Let $s = \sigma + it$. If $\sigma > 1$, $\zeta(s) = \prod_p (1 - p^{-s})^{-1}$, so that

$$\log \zeta(s) = -\sum_p \log(1 - p^{-s}) = \sum_p \sum_{m=1}^{\infty} \frac{1}{mp^{ms}},$$

and

$$\zeta(s) = \exp\big(\sum_p \sum_{m=1}^{\infty} \frac{e^{-imt\log p}}{mp^{m\sigma}}\big)$$

$$|\zeta(s)| = \exp\Big\{\sum_p \sum_{m=1}^{\infty} \frac{\cos(mt\log p)}{mp^{m\sigma}}\Big\}.$$

Therefore we obtain

$$\zeta^3(\sigma)|\zeta(\sigma + it)|^4\zeta(\sigma + 2it) = \exp\Big\{\sum_p \sum_{m=1}^{\infty} \frac{A_m}{mp^{m\sigma}}\Big\},$$

where

$$A_m = 3 + 4\cos(mt\log p) + \cos(2mt\log p) = 2(\cos(mt\log p) + 1)^2 \geq 0,$$

hence the result. □

Chapter 9

W9: Dirichlet L-functions

9.1 Dirichlet character

Definition 9.1.1. *A Dirichlet character is a character χ of the group $(\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ for some integer $N \geq 1$.*

Note that for $N|M$, χ induces a character of $(\mathbb{Z}/M\mathbb{Z})^\times \to \mathbb{C}\times$ by the natural surjection $(\mathbb{Z}/M\mathbb{Z})^\times \to (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$. We say $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to C^\times$ is primitive, if it is not induced by any characters of $(\mathbb{Z}/d\mathbb{Z})^\times$ for $d|N$ and $d \neq N$; in that case, we say has conductor N, and write $\mathrm{cond}(\chi) = N$.

It is convenient to regard a Dirichlet character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ as a function $\mathbb{Z} \to \mathbb{C}$ by setting $\chi(a) = 0$ if $(a, N) \neq 1$. Note that $\chi(nm) = \chi(n)\chi(m)$ for all $n, m \in \mathbb{Z}$.

We say χ is even if $\chi(-1) = 1$ and odd if $\chi(-1) = -1$; say χ is principal, usually denoted χ_0, if $\chi(a) = 1$ (resp. $= 0$) for all $(a, N) = 1$ (resp. otherwise). It is called real if $\chi(a) \in \mathbb{R}$ for all a. Let $\overline{\chi}$ be the complex conjugate of χ.

Example 9.1.2. *(1) Let $\chi : (\mathbb{Z}/8\mathbb{Z})^\times \to \mathbb{C}^\times$ be defined by $\chi(1) = 1$, $\chi(3) = 1$, $\chi(5) = -1$ and $\chi(7) = -1$. It is clear that* $\mathrm{cond}(\chi) = 4$.

(2) Let p be an odd prime. Then Legendre symbol $a \mapsto \left(\frac{a}{p}\right)$ defines a Dirichlet character of conductor p.

Let χ be a Dirichlet character mod N. We put

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

Proposition 9.1.3. *(1) The series $L(s, \chi)$ absolutely converges in $\Re(s) > 1$.*

(2) We have the Euler product:

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

(3) When χ is non-trivial, $L(s, \chi)$ defines an analytic function on $\Re(s) > 0$.

(4) If $\mathrm{cond}(\chi) = N' \neq N$ *(hence $N'|N$) and is induced from χ', then*

$$L(s, \chi) = L(s, \chi') \cdot \prod_{p|N} (1 - \chi'(p)p^{-s}).$$

Proof. (1) Since $|\chi(n)| \le 1$, we get $\sigma_{ac} = 1$.

(2) This is because χ is completely multiplicative.

(3) When χ is non-trivial, we have $\sum_{a=0}^{N-1} \chi(a) = 0$, which implies that $\{A(M) := \sum_{n=1}^{M} \chi(n)\}$ is bounded. Hence $\sigma_c = 0$.

(4) We have $\chi(p) = \chi'(p)$ for any $p \nmid N$, hence (noting $\chi(p) = 0$ if $p|N$)

$$L(s,\chi) = \prod_{p\nmid N} \frac{1}{(1-\chi(p)p^{-s})} = \prod_{p\nmid N} \frac{1}{1-\chi'(p)p^{-s}} = L(s,\chi') \cdot \prod_{p|N}(1-\chi'(p)p^{-s}).$$

□

Theorem 9.1.4. *Let χ be a primitive character mod $N \ge 2$. Let $\delta(\chi) = \delta = \begin{cases} 0 & \chi \text{ even} \\ 1 & \chi \text{ odd} \end{cases}$. Let*

$$\xi(s,\chi) = (\frac{N}{\pi})^{s/2}\Gamma((s+\delta)/2)L(s,\chi).$$

Then $L(s,\chi)$ analytically extended to an entire function on $\mathbb{C}$ satisfying the following functional equation:

$$\xi(s,\chi) = \frac{G(1,\chi)}{i^\delta\sqrt{N}}\xi(1-s,\overline{\chi}).$$

Moreover, $L(s,\chi)$ has simple zeros (called trivial zeros) at

$$s = -\delta(\chi) - 2n, \quad n = 0,1,2,...$$

and all other zeros lie in $0 < \Re(s) < 1$.

Remark 9.1.5. *In particular, as we will see, $|G(1,\chi)| = \sqrt{N}$, we get equality $|\xi(s,\chi)| = |\xi(1-s,\overline{\chi})|$.*

Conjecture 9.1.6. *The Generalized Riemann hypothesis (GRH) says that: for every primitive χ, all non-trivial zeros of $L(s,\chi)$ lie on the critical line $\Re(s) = \frac{1}{2}$.*

9.1.1 Gauss sums

Definition 9.1.7. *For $\lambda : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}^\times$ (additive character), $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$,*

$$G(\lambda,\chi) = \sum_{a\in\mathbb{Z}/N\mathbb{Z}} \lambda(a)\chi(a)$$

is called a Gauss sum modulo N.

Every character of $\mathbb{Z}/N\mathbb{Z}$ has the form $a \mapsto \zeta^{ka}$ for some $0 \le k \le N-1$, where $\zeta := e^{2\pi i/N}$, so Gauss also takes the form

$$G(k,\chi) = \sum_{a\in\mathbb{Z}/N\mathbb{Z}} \chi(a)\zeta^{ka}.$$

In particular, $G(1,\chi) = G(\chi) = \sum_{a\in\mathbb{Z}/N\mathbb{Z}} \chi(a)\zeta^a$.

Proposition 9.1.8. *Assume χ is primitive of conductor N.*[1]

(1) If $(k,N) = 1$, then $G(k,\chi) = \overline{\chi}(k)G(1,\chi)$.

(2) If $(k,N) > 1$, then $G(k,\chi) = 0$ (hence $G(k,\chi) = \overline{\chi}(k)G(1,\chi)$ still holds true).

(3) $G(1,\chi)G(1,\overline{\chi}) = \chi(-1)N$ and $|G(1,\chi)| = \sqrt{N}$.

[1] not always necessary, for example not for (1)

Proof. (1) If $(k, N) = 1$, then

$$G(k, \chi) = \sum_{a \in \mathbb{Z}/N\mathbb{Z}} \chi(a)\zeta^{ka} = \sum_{a \in \mathbb{Z}/N\mathbb{Z}} \overline{\chi}(k)\chi(ka)\zeta^{ka} = \overline{\chi}(k)G(1, \chi).$$

Note that here we used the condition that $\chi(k) \neq 0$, ensured by $(k, N) = 1$.

(2) Fact: χ is induced from χ' for $N'|N$ if and only if $\chi(a) = 1$ for any $a \equiv 1 \mod N'$, $a \in (\mathbb{Z}/N\mathbb{Z})^{\times}$.

Letting $(k, N) = d > 1$ and write $k = k'd, N = N'd$. Hence (setting $\tilde{\zeta} = \zeta^d$ so that $\tilde{\zeta}^{N'} = 1$)

$$\begin{aligned} G(k, \chi) &= \textstyle\sum_{a \in \mathbb{Z}/N\mathbb{Z}} \chi(a)\tilde{\zeta}^{ak'} \\ &= \sum_{\lambda \in \mathbb{Z}/N'\mathbb{Z}} \Big(\sum_{a \equiv \lambda\ (N')} \chi(a)\tilde{\zeta}^{\lambda k'} \Big) \\ &= \sum_{\lambda \in \mathbb{Z}/N'\mathbb{Z}} \tilde{\zeta}^{\lambda k'} \Big(\sum_{a \equiv \lambda\ (N')} \chi(a) \Big) \end{aligned}$$

We claim that $\sum_{a \equiv \lambda\ (N')} \chi(a) = 0$. In fact, since χ is assumed primitive, there exists r such that

$$r \equiv 1 \mod N', \quad (r, N) = 1, \quad \chi(r) \neq 1.$$

Then

$$\sum_{a \equiv \lambda\ (N')} \chi(a) = \sum_{a \equiv \lambda r^{-1}\ (N')} \chi(a) = \sum_{a \equiv \lambda\ (N')} \chi(ar) = \chi(r) \cdot \sum_{a \equiv \lambda\ (N')} \chi(a),$$

giving the result.

(3) Compute:

$$\begin{aligned} G(1, \chi)G(1, \overline{\chi}) &= G(1, \chi) \sum_{a \in \mathbb{Z}/N\mathbb{Z}} \overline{\chi}(a)\zeta^a \\ &= \sum_{a \in \mathbb{Z}/N\mathbb{Z}} G(a, \chi)\zeta^a \\ &= \sum_{a' \in \mathbb{Z}/N\mathbb{Z}} \chi(a') \big(\sum_{a \in \mathbb{Z}/N\mathbb{Z}} \zeta^{aa'+a} \big) \end{aligned}$$

Since $\sum_{a \in \mathbb{Z}/N\mathbb{Z}} \zeta^{a(a'+1)} = 0$ expect when $a' + 1 \equiv 0$, in which case the sum is equal to N, we get the result $\chi(-1)N$.

We compute $|G(1, \chi)|^2$:

$$\begin{aligned} |G(1, \chi)|^2 = G(1, \chi)\overline{G(1, \chi)} &= G(1, \chi) \sum_{a \in \mathbb{Z}/N\mathbb{Z}} \overline{\chi}(a)\zeta^{-a} \\ &= \sum_{a \in \mathbb{Z}/N\mathbb{Z}} G(a, \chi)\zeta^{-a} \\ &= \sum_{a' \in \mathbb{Z}/N\mathbb{Z}} \chi(a') \big(\sum_{a \in \mathbb{Z}/N\mathbb{Z}} \zeta^{aa'-a} \big) \end{aligned}$$

Since $\sum_{a \in \mathbb{Z}/N\mathbb{Z}} \zeta^{a(a'-1)} = 0$ expect when $a' - 1 \equiv 0$, in which case the sum is equal to N, we get the result N and $|G(1, \chi)| = \sqrt{N}$. □

9.1.2 Proof

Let $\theta(u, \chi) := \sum_{n=-\infty}^{\infty} \chi(n)e^{-n^2\pi u/N}$.

Lemma 9.1.9. *We have*

$$G(1,\overline{\chi})\theta(u,\chi)=\sqrt{\frac{N}{u}}\theta(u^{-1},\overline{\chi}).$$

Proof. The tool is still the Poisson summation formula. □

Now we can prove the main theorem.

Proof of Theorem. As for Riemann zeta function, since by a change of variable $x\mapsto n^2\pi x/N$,

$$(\frac{N}{\pi})^{s/2}\Gamma(s/2)n^{-s}=\int_0^\infty(\frac{N}{\pi})^{s/2}u^{s/2}e^{-2}n^{-s}\frac{du}{u}=\int_0^\infty e^{-n^2\pi u/N}u^{s/2}\frac{du}{u},$$

we have

$$\begin{array}{rcl}\xi(s,\chi) & = & \sum_{n\geq 1}(\frac{N}{\pi})^{s/2}\Gamma(s/2)n^{-s}\\ & = & \int_0^\infty u^{s/2}\big(\sum_{n\geq 1}\chi(n)e^{-n^2\pi u/N}\big)\frac{du}{u}\\ & = & \frac{1}{2}\int_0^\infty u^{s/2}\theta(u,\chi)\frac{du}{u}\\ & = & \frac{1}{2}\int_1^\infty+\frac{1}{2}\int_0^1\end{array}$$

Here is the main difference with Riemann ζ function, because $\chi(0)=0$ when $N\geq 2$.

Lemma implies that

$$\begin{array}{rcl}\int_0^1 u^{s/2}\theta(u,\chi)\frac{du}{u} & = & \int_1^\infty u^{-s/2}\theta(1/u,\chi)\frac{du}{u}\\ & = & \int_0^1 u^{-s/2}\sqrt{u}\frac{\sqrt{N}}{G(1,\overline{\chi})}\theta(u,\overline{\chi})\frac{du}{u}\\ & = & \frac{\sqrt{N}}{G(1,\overline{\chi})}\int_0^1 u^{(1-2)/2}\theta(u,\overline{\chi})\frac{du}{u}.\end{array}$$

Since the two integrations converge for any $s\in\mathbb{C}$, and when χ is primitive, $|G(1,\overline{\chi})|=\sqrt{N}\neq 0$, we obtain a extension of $L(s,\chi)$ to the whole complex plane. Moreover, the functional equation is

$$\begin{array}{rcl}\xi(1-s,\overline{\chi}) & = & \frac{1}{2}\int_1^\infty u^{(1-s)/2}\theta(u,\overline{\chi})\frac{du}{u}+\frac{1}{2}\frac{\sqrt{N}}{G(1,\chi)}\int_1^\infty u^{s/2}\theta(u,\chi)\frac{du}{u}\\ & = & \frac{\sqrt{N}}{G(1,\chi)}\xi(s,\chi)\end{array}$$

here we used the formula (since χ is even):

$$G(1,\chi)G(1,\overline{\chi})=N\chi(-1)=N.$$

We can similarly handle the case χ is odd. □

9.1.3 Zeros

Theorem 9.1.10. *Let χ be a primitive character mod N with $N\geq 2$. Then $L(s,\chi)$ is an entire function on $\mathbb{C}$. Its zeros are*

$$s=-\delta(\chi)-2n,\quad n=0,1,2,...$$

and are all simple, called trivial zeros. All the other zeros lie in $0<\Re(s)<1$.

Conjecture 9.1.11. *The GRH says that the non-trivial zeros of $L(s,\chi)$ lie in the critical line $\Re(s)=\frac{1}{2}$.*

Proof. The same as Riemann zeta function case. □

Lemma 9.1.12. *Let χ be a primitive character mod N. For any $t\in\mathbb{R}$, $L(1+it,\chi)\neq 0$.*

Proof. The proof is similar to the case of $\zeta(s)$. □

9.2 Special values of zeta function

9.2.1 Bernoulli numbers

Definition 9.2.1. *Bernoulli numbers are defined by the Taylor expansion*

$$\frac{t}{e^t-1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} t^n.$$

Example 9.2.2. *The first values are*

$$B_0 = 1, \quad B_1 = -\frac{1}{2}, \quad B_2 = \frac{1}{6}, \quad B_3 = 0, \quad B_4 = -\frac{1}{30}.$$

Lemma 9.2.3. *For $n \geq 3$ odd, we have $B_n = 0$.*

Proof. This is because

$$2 \sum_{n \geq 0 \text{ odd}} \frac{B_n}{n!} t^n = \sum_{n \geq 0} \frac{B_n}{n!} t^n - \sum_{n \geq 0} \frac{B_n}{n!} (-t)^n = \frac{t}{e^t-1} - \frac{-1}{e^{-t}-1} = -t$$

so $B_1 = -1/2$ and $B_n = 0$ for $n \geq 3$ odd. □

9.2.2 Special values of $\zeta(s)$

Theorem 9.2.4. *We have $\zeta(0) = -1/2$, and*

$$\zeta(-n) = (-1)^n \frac{B_{n+1}}{n+1}, \quad n = 0, 1, 2, \ldots.$$

$$\zeta(2n) = \frac{(-1)^{n+1} B_{2n} (2\pi)^{2n}}{2(2n)!}.$$

Proof. (1) Consider slightly general situation: $F(s) = \sum_{n \geq 1} \frac{a_n}{n^s}$ with $\sigma_c < +\infty$. We compute

$$\begin{array}{rcl} \Gamma(s)F(s) & = & \int_0^\infty t^{s-1} e^{-t} \sum_{n\geq 1} a_n n^{-s} dt \\ & \overset{t \mapsto nt}{=} & \int_0^\infty t^{s-1} \sum_{n \geq 1} a_n e^{-nt} dt \\ & = & \int_0^\infty t^{s-1} f(t) dt \\ & = & \int_1^\infty t^{s-1} f(t) dt + \int_0^1 t^{s-1} f(t) dt \end{array}$$

where $f(t) := \sum_{n \geq 1} a_n e^{-nt}$. The term $\int_1^\infty$ converges absolutely, because e^{-nt} decreases very rapidly (in fact for any $t > 0$). However, at $t = 0$, $f(t)$ need not have good property, possibly diverges (e. g. $\sum_{n \geq 1} e^{-nt}$).

For our situation, $f(t) = \sum_{n \geq 1} e^{-nt}$ is equal to $\frac{1}{e^t-1}$, hence has a (meromorphic) Taylor development around 0 as follows:

$$f(t) := \sum_{n \geq -1} b_n t^n := \frac{1}{e^t - 1} \sim \frac{1}{t} + \sum_{n \geq 1} \frac{B_{n+1}}{(n+1)!} t^n, \quad t \to 0.$$

Integration gives for any $N \geq 1$,

$$\int_0^1 t^{s-1} f(t) dt = \frac{1}{s-1} + \sum_{0 \leq n < N} \frac{b_n}{s+n} + G(s, N)$$

with $G(s,N)$ converges on $\Re(s) > -N$. So $\Gamma(s)F(s)$ has a simple pole at $s=-n$; since so is $\Gamma(s)$ with residue

$$\lim_{s\to -n}\Gamma(s)(s+n) = (-1)^n/n!$$

we obtain

$$F(-n) = \frac{b_n}{\mathrm{res}_{s=-n}\Gamma(s)} = (-1)^n n! b_n = (-1)^n \frac{B_{n+1}}{n+1}$$

(2) For the values at positive even integers $2n$, one uses the functional equation to get

$$\zeta(2n) = \frac{\pi^{-(1-2n)/2}\Gamma((1-2n)/2)\zeta(1-2n)}{\pi^{-n}\Gamma(n)} = \pi^{2n-\frac{1}{2}}\frac{\Gamma((1-2n)/2)\zeta(1-2n)}{\Gamma(n)},$$

then conclude using

- $\zeta(1-2n) = (-1)^{2n-1}\frac{B_{2n}}{2n}$
- $\Gamma(n) = (n-1)!$ (as $\Gamma(s+1) = s\Gamma(s)$)
- use the equality $\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin(\pi s)}$ to compute

$$\Gamma((1-2n)/2) = \frac{\pi}{\sin((n+1/2)\pi)\Gamma(n+1/2)} = \frac{\pi}{(-1)^n\Gamma(n+1/2)}$$

$$\Gamma(n+1/2) = \Big((n-\frac{1}{2})\cdots\frac{1}{2}\Big)\cdot\Gamma(\frac{1}{2}) = \Big((n-\frac{1}{2})\cdots\frac{1}{2}\Big)\cdot\sqrt{\pi}.$$

□

Remark 9.2.5. *However, one sees that for positive odd integers $2n+1$, one falls into*

$$\zeta(2n+1) = \pi^{2n+1/2}\cdot\frac{\Gamma(-n)\zeta(-2n)}{\Gamma((2n+1)/2)}$$

since $\zeta(-2n) = 0$ ($B_{2n+1} = 0$) and $\Gamma(s)$ has a simple pole at $s=-n$, the above equality does not gives information about $\zeta(2n+1)$. (we used this to compute the residue of $\zeta(s)$ at $-2n$.)

For example, $\zeta(3) = 1.20205...$ is irrational (Apéry's theorem) and that infinitely many of the values $\zeta(2n+1)$ are irrational. These values are thought to be related to the algebraic K-theory of $\mathbb{Z}$.

9.2.3 Special values of Dirichlet L-functions

Theorem 9.2.6. *Let χ be a mod N Dirichlet character with $\chi \neq \chi_0$. We have*

$$L(-n,\chi) = (-1)^{n+1}\frac{B_{n+1,\chi}}{n+1}, \quad n = 0,1,2,...$$

Where the generalized Bernoulli numbers are defined by

$$\sum_{a=1}^{N}\frac{\chi(a)te^{at}}{e^{Nt}-1} = \sum_{n=0}^{\infty}B_{n,\chi}\frac{t^n}{n!}.$$

Proof. We omit the proof. □

Sometime we need the explicit formula of $B_{n,\chi}$. Define for $n \geq 0$, the Bernoulli polynomial,

$$B_n(x) = \sum_{k=0}^{n} \binom{n}{k} B_{n-k} x^k$$

For example,

$$B_0(x) = 1, \quad B_1(x) = x - 1/2, \quad B_2(x) = x^2 - x + 1/6, \quad B_3(x) = x^3 - 3/2x^2 + 1/2x.$$

Then we have

$$B_{n,\chi} = N^{n-1} \sum_{k=1}^{N} \chi(k) B_n(\frac{k}{N}).$$

In particular, when $n = 0$, we obtain

$$L(0, \chi) = -B_{1,\chi} = -\sum_{k=1}^{N} \chi(k)(\frac{k}{N} - 1/2) = -\frac{1}{N} \sum_{k=1}^{N} \chi(k)k.$$

Week 9 Exercise

1. Let χ be the unique primitive mod 4 Dirichlet character. Compute $L(1, \chi)$ and $L(0, \chi)$.
2. prove that for $n \geq 1$, $B_{4n} < 0$ and $B_{4n-2} > 0$.
3. Let G be an abelian group of order fg. Let $a \in G$ be such that $o(a) = f$. Prove that

$$\prod_{\chi \in \widehat{G}} (1 - \chi(a)x) = (1 - x^f)^g.$$

Chapter 10

W10: Dedekind zeta function

10.1 Dedekind zeta functions $\zeta_K(s)$

For any number field K, Dedekind defined his zeta function, analogous to $\zeta(s)$:

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

where $\mathfrak{a}$ runs through all non-zero integral ideals of $\mathcal{O}_K$; call it Dedekind zeta function.

Note that if $a_n := \sum_{N(\mathfrak{a})\leq n} 1$ denotes the number of integral ideals with $N(\mathfrak{a}) \leq n$, then $\zeta_K(s)$ is just the Dirichlet series associated to a_n.

Theorem 10.1.1. *(1) when $\Re(s) > 1$, the infinite product $\prod_{\mathfrak{p}}(1 - N(\mathfrak{p})^{-s})^{-1}$ converges, where $\mathfrak{p}$ runs over all prime ideals (non-zero). Moreover,*

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

(2) $\zeta_K(s)$ has abissica of absolute convergence 1.

Proof. Let $d = [K : \mathbb{Q}]$. We consider the Euler product $\prod_{\mathfrak{p}}(1-N(\mathfrak{p})^{-s})^{-1}$ and will show that it converges for $\Re(s) > 1$. It is equivalent to show the convergence of $\prod_{\mathfrak{p}}(1 - N(\mathfrak{p})^{-s})$. We know that a product $\prod_{n\geq 1}(1+x_n)$ with $|x_n| < 1$ converges absolutely if the series $\sum_{n>1} x_n$ converges. So we consider the series $\sum_{\mathfrak{p}} N(\mathfrak{p})^{-s}$. If $\mathfrak{p}$ divides p then $N(\mathfrak{p}) = p^f \geq p$ and there are at most $[K : \mathbb{Q}]$ primes $\mathfrak{p}$ dividing each p. Therefore

$$\sum_{\mathfrak{p}} \frac{1}{N(\mathfrak{p})} \leq \sum_{p} \frac{[K : \mathbb{Q}]}{p^s} < \infty$$

by convergence of the Dirichlet series for the Riemann zeta function. This proves that $\prod_{\mathfrak{p}}(1 - N(\mathfrak{p})^{-s})^{-1}$ converges and is equal to $\zeta_K(s)$. $\square$

Remark 10.1.2. *We will show later that $A(N) := \sum_{1\leq n\leq N} a_n$ grows asymptotically as*

$$A(N) = \kappa N + O(N^{1-1/[K:\mathbb{Q}]})$$

which implies $\sigma_{\mathrm{ac}} = 1$ by a general fact for Dirichlet series.

Theorem 10.1.3. *(1) $\zeta_K(s)$ can be analytically extended to a meromorphic function on $\mathbb{C}$, and satisfy the following functional equation: letting*

$$\Gamma_{\mathbb{R}}(s) = \pi^{-s/2}\Gamma(s/2), \quad \Gamma_{\mathbb{C}}(s) = (2\pi)^{-s}\Gamma(s)$$

and the completed zeta function

$$\xi_K(s) := |\Delta_K|^{s/2}\Gamma_{\mathbb{R}}(s)^{r_1}\Gamma_{\mathbb{C}}(s)^{r_2}\zeta_K(s),$$

then $\xi_K(s) = \xi_K(1-s)$. [1]

(2) $\zeta_K(s)$ has a unique simple pole at $s = 1$, with residue $\rho_K h_K$. About its zeros, let $r = r_1 + r_2 - 1$, then

- *$s = 0$ is a zero of order r;*
- *$s = -2, -4, -6, \ldots$ are zeros of order $r + 1$;*
- *$s = -1, -3, -5, \ldots$ are zeros of order r_2.*

These are all trivial zeros. The other zeros of $\zeta_K(s)$ lie in $0 < \Re(s) < 1$ and are symmetric with respect to $\Re(s) = 1/2$.

Proof. (1) Very long computation; we omit its proof.

(2) Clear because $\Gamma(s)$ has no zeros, and simple poles at $s = 0, -1, -2, \ldots$. ☐

The following is called *Extended Riemann Hypothesis.*

Conjecture 10.1.4. *(EGH) All non-trivial zeros of $\zeta_K(s)$ lie on the critical line $\Re(s) = 1/2$.*

10.2 Hasse's theorem

10.2.1 Characters

Let G be a finite abelian group. Recall that a character of G is a group homomorphism

$$\chi : G \to \mathbb{C}^\times.$$

If χ_1 and χ_2 are two characters,we define their product by the formula $\chi_1\chi_2(g) = \chi_1(g)\chi_2(g)$. The set of characters of G form an abelian group, which we denote by $\widehat{G}$.

Lemma 10.2.1. *There exists a non-canonical isomorphism $G \xrightarrow{\sim} \widehat{G}$.*

Proof. Since every finite abelian group is a direct sum of cyclic groups, we may assume that $G = \mathbb{Z}/n\mathbb{Z}$. Then a character χ of G is determined by its value at $1 \in \mathbb{Z}/n\mathbb{Z}$, which is necessarily an n-th root of unity, and vice versa. Thus $\widehat{G}$ is canonically isomorphic to the group of n-th roots of unity, which is isomorphic to $\mathbb{Z}/n\mathbb{Z}$. ☐

A group homomorphism $f : G_1 \to G_2$ induces a natural map $\widehat{f} : \widehat{G}_2 \to \widehat{G}_1$ given by $\chi \mapsto \chi \circ f$.

Lemma 10.2.2. *If $0 \to G_1 \to G \to G_2 \to 0$ is an exact sequence of finite abelian groups, then the induced sequence $0 \to \widehat{G}_2 \to \widehat{G} \to \widehat{G}_1 \to 0$ is also exact.*

Proof. The functor $\mathrm{Hom}_{\mathrm{Gr}}(-, \mathbb{C}^\times)$ is left exact, and counting order shows the exactness. ☐

In other words, $\widehat{G}_2$ is identified with the set of characters of G which are trivial on G_1.

Remark 10.2.3. *One can show that the canonical morphism $G \to \widehat{\widehat{G}}$ is an isormophism.*

[1] that is, $\Lambda_K(s) = \left(\frac{|\Delta_K|}{4^{r_2}\pi^n}\right)^{s/2}\Gamma(s/2)^{r_1}\Gamma(s)^{r_2}\zeta_K(s)$ using $n = r_1 + 2r_2$.

10.2.2 Kronecker-Weber theorem

We will need the following important theorem.

Theorem 10.2.4. *(Kronecker-Weber) Any abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension of $\mathbb{Q}$, i.e. there exists $N \geq 1$ such that $K \subset \mathbb{Q}(\zeta_N)$.*

Definition 10.2.5. *The smallest N as in the above theorem is called the conductor of K. (Well-defined because: $m = \gcd(N, N')$ implies $\mathbb{Q}(\zeta_N) \cap \mathbb{Q}(\zeta_{N'}) = \mathbb{Q}(\zeta_m)$.*

Example 10.2.6. *When $K = \mathbb{Q}(\sqrt{d})$ is quadratic, $\mathfrak{f}(K) = |\Delta_K|$.*

Proof. Recall that $\Delta_K = 4d$ if $d \equiv 2, 3 \mod 4$, and $= d$ if $d \equiv 1 \mod 4$. Since d is square-free, we do induction on the number k of prime factors of d. In the special case $d = -1$, the result if clear, since $|\Delta_K| = 4$ and $\sqrt{-1} \in \mathbb{Q}(\zeta_4)$. If $k = 1$, then $d = \pm p$ with p prime. If $d = 2$, then it is a direct check that $\sqrt{\pm 2} \in \mathbb{Q}(\zeta_8)$. If p is odd, we write[2] $d = (\pm 1)p^*$ with $p^* \equiv 1 \mod 4$, then as shown before $\mathbb{Q}(\sqrt{p^*})$ is contained in $\mathbb{Q}(\zeta_p)$.

Assume now d has $k+1$ prime factors and write $d = d'p^*$ with p odd prime and $p^* \equiv 1 \mod 4$. Therefore,

$$\mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}(\sqrt{d'}, \sqrt{p^*}) \subset \mathbb{Q}(\zeta_{|\Delta_{K'}|}, \zeta_p)$$

where $K' := \mathbb{Q}(\sqrt{d'})$. It is left to check that $|\Delta_K| = |\Delta_{K'} p|$, so that $\mathbb{Q}(\zeta_{|\Delta_{K'}|}, \zeta_p) \subset \mathbb{Q}(\zeta_{|\Delta_K|})$. But this is clear because $p^* \equiv 1(4)$ implies $d \equiv d'(4)$.

To see $|\Delta_K|$ is the smallest, we use the ramification behavior of $K/\mathbb{Q}$ and $\mathbb{Q}(\zeta_{|\Delta_K|})/\mathbb{Q}$. $\square$

10.2.3 Characters of abelian fields

Fix an abelian extension K with Galois group G, and let $N = \mathrm{cond}(K)$ be the conductor. Since $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times$, K corresponds to a subgroup $H < (\mathbb{Z}/N\mathbb{Z})^\times$ such that

$$K = \mathbb{Q}(\zeta_N)^H, \quad (\mathbb{Z}/N\mathbb{Z})^\times/H \cong G.$$

A character $\chi \in \widehat{G}$ can be identified with a mod N Dirichlet character which is trivial on H. Therefore Dirichlet L-function $L(s, \chi)$ is defined for $\chi \in \widehat{G}$.

Lemma 10.2.7. *Let K be an abelian extension of $\mathbb{Q}$.*

(1) K is real if and only if $\chi \in \widehat{K}$ is even, i.e. $\chi(-1) = 1$.

(2) K is imaginary, K_+ be its maximal real subfield, then $[K : K_+] = 2$ and $\widehat{K}_+$ is identified with the subset of even characters of $\widehat{K}$.

Proof. (1) First look at $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times$; under this isomorphism, -1 correspond to the automorphism $\zeta_N \mapsto \zeta_N^{-1} = \overline{\zeta}_N$, i.e. the complex conjugation c on $\mathbb{Q}(\zeta_N)$. Therefore, K is fixed by c if and only if the image of -1 in $G \cong (\mathbb{Z}/N\mathbb{Z})^\times/H$ is 1, if and only every character of G is even when viewed as a character of $(\mathbb{Z}/N\mathbb{Z})^\times$.

(2) Assume K is imaginary. Then there exists $\chi \in \widehat{G}$ which is odd. The set of even characters of $\widehat{G}$ form a subgroup of index 2, which corresponds to the character group of a quotient group G_+ of G, which corresponds again to a subfield K_+ of K, such that $G_+ \cong \mathrm{Gal}(K_+/\mathbb{Q})$. By construction and (1), K_+ is real. $\square$

[2] precisely $p^* = (-1)^{\frac{p-1}{2}} p$

10.2.4 L-series factorization

Lemma 10.2.8. *Let p be a prime, let $N \geq 1$, and $N = p^k N'$ with $(p, N') = 1$. Then $\mathbb{Q}(\zeta_{N'})$ is the maximal extension of $\mathbb{Q}$ in $\mathbb{Q}(\zeta_N)$ unramified at p, i.e. if $K \subset \mathbb{Q}(\zeta_N)$ is unramified at p, then $K \subset \mathbb{Q}(\zeta_{N'})$.*

Proof. We saw that p is unramified in $\mathbb{Q}(\zeta_{N'})$, so the compositum $K\mathbb{Q}(\zeta_{N'})$ is also unramified at p; hence we may assume K contains $\mathbb{Q}(\zeta_{N'})$.

Consider $T := K \cap \mathbb{Q}(\zeta_{p^k})$. We claim that $T = \mathbb{Q}$. Indeed, since $\mathbb{Q}(\zeta_{p^k})$ is ramified only at p while K is unramifed at p, T is everywhere unramified over $\mathbb{Q}$. But by Dedekind's discriminant theorem, this implies $T = \mathbb{Q}$ (as always have $|\Delta_T| > 1$).

The claim implies that $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/K) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_{p^k})/\mathbb{Q})$, hence $K = \mathbb{Q}(\zeta_{N'})$ (since $K \supset \mathbb{Q}(\zeta_{N'})$ by assumption). □

Theorem 10.2.9. *Let K be an abelian extension of $\mathbb{Q}$ with Galois group G. We have*

$$\zeta_K(s) = \prod_{\chi \in \widehat{K}} L(s, \chi^*).$$

Here χ^* denotes the primitive character inducing χ.

Remark 10.2.10. *For example, if $\chi = \chi_0$ is the principal character, $\chi_0^* = \mathbb{1}$ is the trivial one and $L(s, \mathbb{1}) = \zeta(s)$ is Riemann zeta function. In particular, $\zeta(s)$ divides $\zeta_K(s)$ as $L(s, \chi^*)$ is entire when $\chi \neq \chi_0$.*

In general, Artin conjectures that: if K is a subfield of L, then $\zeta_L(s)/\zeta_K(s)$ is entire. We know that they both have simple poles at $s = 1$. So this means that, every zero of $\zeta_K(s)$ is also zero of $\zeta_L(s)$, and the order of the former is not bigger than the order of the latter. For trivial zeros, this is easily checked.

Remark 10.2.11. *(1) In particular, the statement does not depend on the cyclotomic field we take such that $K \subset \mathbb{Q}(\zeta_N)$.*

(2) Since we view G as a quotient of $(\mathbb{Z}/N\mathbb{Z})^\times$, so $\chi(p)$ depends on N. For example, if view χ as a character mod pN, then always $\chi(p) = 0$. The advantage of taking χ^* avoids this problem.

Proof. By the Euler products of $\zeta_K(s)$ and $L(s, \chi^*)$, it suffices to prove that, for each prime number p, one has

$$\prod_{\mathfrak{p}|p} (1 - N(\mathfrak{p})^{-s}) = \prod_{\chi \in \widehat{K}} (1 - \chi^*(p) p^{-s}). \tag{10.1}$$

where $\mathfrak{p}$ runs through the primes of K above p.[3] If we decompose

$$p\mathcal{O}_K = (\mathfrak{p}_1 \cdots \mathfrak{p}_g)^e, \quad N(\mathfrak{p}_i) = p^f, \quad efg = n$$

then LHS is equal to $(1 - p^{-fs})^g$. We are left to compute the RHS.

First assume K is unramified at p, so by Lemma $\mathrm{cond}(\chi)|N'$, i.e. we may take $(p, N) = 1$. In this case, we have $I_p = 1$, $D_p = \langle \mathrm{Frob}_p \rangle \cong \mathbb{Z}/f\mathbb{Z}$ and $\widehat{D}_p$ is identified with μ_f (the set of f-th roots of unity) by sending Frob_p to a root of unity. Moreover, the image of p via

[3] If $K = \mathbb{Q}(\zeta_p)$, then $\chi(p) = 0$ for any $\chi \in \widehat{K}$; this explains why we should take χ^*.

the quotient map $(\mathbb{Z}/N\mathbb{Z})^\times \to G$ lies in D_p. Consider the exact sequence $1 \to D_p \to G \to G/D_p \to 1$ which induces

$$1 \to \widehat{(G/D_p)} \to \widehat{G} \to \widehat{D}_p \to 1.$$

So each element of $\widehat{D}_p$ has g lifts to $\widehat{G}$, hence

$$\prod_{\chi \in \widehat{G}} (1 - \chi(p)p^{-s}) = \prod_{\xi \in \mu_f} (1 - \xi p^{-s})^g = (1 - p^{-fs})^g.$$

Here we have used the equality that

$$\prod_{\xi \in \mu_f} (X - \xi a) = X^f - a^f.$$

Now treat the general case. Write $N = p^k N'$. Note that LHS of (10.1) is unchanged if we replace K by $K' := K \cap \mathbb{Q}(\zeta_{N'})$ - the maximal subfield unramified at p (because f, g do not change). On the other hand, for $\chi \in \widehat{K}$, if $p | \mathrm{cond}(\chi)$, then $\chi^*(p) = 0$, so we may forget it in RHS of (10.1). If $p \nmid \mathrm{cond}(\chi)$, then we have $\mathrm{cond}(\chi) | N'$, so we may view χ^* as a Dirichlet character mod N'. That is,

$$\prod_{\chi \in \widehat{K}} (1 - \chi^*(p)p^{-s}) = \prod_{\chi \in \widehat{K'}} (1 - \chi^*(p)p^{-s})$$

which allows to conclude by the unramified case. □

Theorem 10.2.12. *Let K and G be as above and $\chi_0 \in \widehat{G}$ be the trivial character. Then*

$$\prod_{\chi \in \widehat{G}, \chi \neq \chi_0} L(1, \chi^*) = \frac{2^{r_1}(2\pi)^{r_2} R_K h_K}{w_K |\Delta_K|^{1/2}} = \rho_K h_K.$$

In particular, $L(1, \chi^*) \neq 0$ if $\chi \neq \chi_0$.

Proof. It follows from that both $\zeta_K(s)$ and $\zeta(s)$ have a simple zero at $s = 1$, hence $L(1, \chi^*) \neq 0$ for $\chi \neq \chi_0$. □

10.3 Conductor-discriminant formula

We use the above factorization to show the famous conductor-discriminant formula of Hasse.

Theorem 10.3.1. *(Hasse) For each $\chi \in \widehat{K}$, let f_χ denote the conductor of χ. Then*

$$\prod_{\chi \in \widehat{K}} f_\chi = |\Delta_K|.$$

Proof. Recall that if

$$\xi_K(\chi) := \left(\frac{|\Delta_K|}{4^{r_2}\pi^n}\right)^{s/2} \Gamma(s/2)^{r_1} \Gamma(s)^{r_2} \zeta_K(s)$$

then $\xi_K(\chi) = \xi_K(1 - s)$. Since K is Galois, we know either $r_2 = 0$ (if K is real) or $r_1 = 0$ (if K is imaginary).

On the other hand, for each $\chi \in \widehat{K}$, let f_χ be its conductor, the functional equation says that $|\xi(s,\chi)| = |\xi(1-s,\overline{\chi})|$, where

$$\xi(s,\chi) = \big(\frac{f_\chi}{\pi}\big)^{s/2}\Gamma((s+\delta_\chi)/2)L(s,\chi),$$

where $\delta_\chi \in \{0,1\}$ depending on χ is even or odd. First assume K is real, so that $r_2 = 0$, $r_1 = n$, and all characters of $\widehat{K}$ is even, hence $\delta_\chi = 0$ for all χ. Then

$$\frac{\xi_K(\chi)}{\prod_{\chi\in\widehat{K}}\xi(s,\chi)} = \Big(\frac{|\Delta_K|}{\prod_{\chi\in\widehat{K}} f_\chi}\Big)^{s/2}.$$

On the other hand, the functional equations for $\Lambda_K(s)$ and $L(s,\chi)$ imply RHS is unchanged when s is replaced by $1-s$ (using that $f_\chi = f_{\overline{\chi}}$). This forces that $|\Delta_K| = \prod_{\chi\in\widehat{K}} f_\chi$.

Now assume K is imaginary. Then $r_1 = 0$, $r_2 = n/2$, and there are $n/2$ odd (resp. even) characters. We note the following equality

$$\frac{\Gamma(s)}{\Gamma(s/2)\Gamma((s+1)/2)} = \frac{2^{s-1}}{\sqrt{\pi}},$$

which implies that

$$\frac{\xi_K(s)}{\prod_{\chi\in\widehat{K}}\xi(s,\chi)} = \Big(\frac{|\Delta_K|}{\prod_\chi f_\chi}\Big)^{s/2}\cdot\big(\frac{1}{2\sqrt{\pi}}\big)^{n/2}.$$

Again, replacing s by $1-s$, the RHS remains unchanged, and we conclude as the real case. □

Example 10.3.2. *When K is quadratic, $G = \mathrm{Gal}(K/\mathbb{Q})$ has order 2, so there are two characters of G: one is principal, and another one, say λ. Hasse's formula then implies that, when viewed as a Dirichlet character, the conductor of λ is equal to $|\Delta_K|$.*

10.4 Example

Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field. Since $\mathrm{Gal}(K/\mathbb{Q}) = \{1,\sigma\}$ has order 2, there is a unique non-trivial character, say λ. Since $1\cdot\mathrm{cond}(\lambda) = |\Delta_K|$, we get λ is a primitive character mod $|\Delta_K|$. Below we give an explicit description of λ (as Dirichlet character).

Define a character χ_K as follows: if p is a prime number, let

$$\chi_K(p) = \begin{cases} 1 & p \text{ splits}\\ -1 & p \text{ inert}\\ 0 & p \text{ ramified}\end{cases}$$

then extends it to $\mathbb{N}$ using prime decomposition. Therefore, χ_K is a completely multiplicative function. Explicitly, we have

$$\chi_K(2) = \begin{cases} 1 & d\equiv 1 \mod 8\\ -1 & d\equiv 5 \mod 8;\\ 0 & \text{else}\end{cases} \qquad \chi_K(p) = \begin{cases} (\frac{d}{p}) & p\nmid d\\ 0 & p|d,\end{cases} \qquad p\neq 2.$$

Consider the associated Dirichlet series

$$\sum_{n\geq 1}\frac{\chi_K(n)}{n^s}.$$

It converges absolutely on $\Re(s) > 1$ and has an Euler product decomposition

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

Lemma 10.4.1. *We have $\lambda = \chi_K$.*

Proof. By the uniqueness of Dirichlet series, it suffices to prove equality

$$\sum_{n\geq 1} \frac{\lambda(n)}{n^s} = \sum_{n\geq 1} \frac{\chi_K(n)}{n^s}$$

for all s with $\Re(s) > 1$. Since $\zeta_K(s) = \zeta(s)\sum_{n\geq 1} \frac{\lambda(n)}{n^s}$, it suffices to show

$$\zeta_K(s) = \zeta(s) \sum_{n\geq 1} \frac{\chi_K(s)}{n^s}.$$

However, both the sides admit Euler product decomposition (for $\Re(s) > 1$), we are left to show

$$\prod_{\mathfrak{p}|p} (1 - N(\mathfrak{p})^{-s}) = (1 - p^{-s})(1 - \chi_K(p)^{-s}).$$

This is clear, because

$$\text{LHS} = \begin{cases} (1 - p^{-s})^2 & p \text{ splits} \\ (1 - p^{-2s}) & p \text{ inert} \\ (1 - p^{-s}) & p \text{ ramified} \end{cases}$$

which is the same as RHS. □

10.5 Residue at $s = 1$

Theorem 10.5.1. *(Analytic class number formula) Let K be a number field of degree n, then*

$$\lim_{s\to 1} (s - 1)\zeta_K(s) = \rho_K h_K = \frac{2^{r_1}(2\pi)^{r_2} h_K R_K}{w_K |\Delta_K|^{1/2}}.$$

We first note the following general lemma.

Lemma 10.5.2. *Let $\sum_{n\geq 1} \frac{a_n}{n^s}$ be a Dirichlet series. Assume*

$$\sum_{n=1}^{t} a_n = \rho t + O(t^\epsilon), \quad t \to \infty$$

for some $0 \leq \epsilon < 1$ and $\rho \in \mathbb{C}^\times$. The Dirichlet series $\sum_{n\geq 1} \frac{a_n}{n^s}$ converges on $\Re(s) > 1$ and has a meromorphic continuation to $\Re(s) > \epsilon$ that is holomorphic except for a simple pole at $s = 1$ with residue ρ.

Proof. Write $b_n = a_n - \rho$. Then $b_1 + \cdots + b_t = O(t^\epsilon)$ and

$$\sum_n \frac{a_n}{n^s} = \rho \sum_{n\geq 1} \frac{1}{n^s} + \sum_{n\geq 1} \frac{b_n}{n^s} = \rho\zeta(s) + \sum \frac{b_n}{n^s}.$$

We have shown that $\zeta(s)$ has a meromorphic continuation and has a simple pole at $s = 1$ with residue 1. On the other hand, $\sum \frac{b_n}{n^s}$ is holomorphic on $\Re(s) > \epsilon$, in particular at $s = 1$. The result follows. □

Therefore, the theorem is reduced to study the distribution of primes in $\mathcal{O}_K$.

10.6 Distribution of ideals

Theorem 10.6.1. *Let C be an ideal class of K, $n = [K : \mathbb{Q}]$. Let*

$$f(C, x) = \sum_{\mathfrak{a} \in C, N(\mathfrak{a}) \leq x} 1.$$

Then as $x \to \infty$,[4]

$$f(C, x) = \rho_K x + O(x^{1-1/n}), \qquad \rho_K = \frac{2^{r_1}(2\pi)^{r_2} R_K}{w_K \cdot \sqrt{|\Delta_K|}},$$

where

- *$n = r_1 + 2r_2$ as usual;*
- *R_K is the regulator, $w_K = \sharp W_K$ the order the subgroup of roots of unity.*

10.6.1 Lipschitz parametrizability

Definition 10.6.2. *Let X and Y be metric spaces. A function $f : X \to Y$ is* Lipschitz continuous *if there exists $c > 0$ such that for all distinct $x_1, x_2 \in X$,*

$$d(f(x_1), f(x_2)) \leq c \cdot d(x_1, x_2).$$

This is stronger than *uniform continuity.* For example, if $f : \mathbb{R} \to \mathbb{R}$ is everywhere differentiable, and f' is bounded, then f is Lipschitz continuous.

Definition 10.6.3. *A set B in a metric space X is d-*Lipschit parametrizable *if it is the union of the images of a finite number of Lipschitz continuous functions $f_i : [0,1]^d \to B$.*

Lemma 10.6.4. *Let $B \subset \mathbb{R}^n$ be a set whose boundary $\partial B = \overline{B} - B^\circ$ is $(n-1)$-Lipschitz parametrizable. Then*

$$\sharp(tB \cap \mathbb{Z}^n) = \mu(B)t^n + O(t^{n-1})$$

as $t \to \infty$, where μ is the standard Lebesgue measure on $\mathbb{R}^n$.

Proof. It suffices to prove the lemma for positive integers, since $\sharp(tB \cap \mathbb{Z}^n)$ and $\mu(B)t^n$ are both monotonically increasing functions of t and $\mu(B)(t+1)^n - \mu(B)t^n = O(t^{n-1})$. We can partition $\mathbb{R}^n$ as the disjoint union of half-open cubes of the form

$$L(a_1, ..., a_n) = \{(x_1, ..., x_n) \in \mathbb{R}^n : x_i \in [a_i, a_i + 1)\},$$

with $a_1, ..., a_n \in \mathbb{Z}$. Let $\mathcal{L}$ be the set of all such half-open cubes. For each $t > 0$ define

$$c_0(t) := \sharp\{L \in \mathcal{L} : L \subseteq tB\}, \quad c_1(t) := \sharp\{L \in \mathcal{L} : tB \cap L \neq \emptyset\}.$$

Then

$$c_0(t) \leq \sharp(tB \cap \mathbb{Z}^n) \leq c_1(t).$$

Finally show the bound $c_1(t) - c_0(t) = O(t^{n-1})$. □

[4]the asymptotic notation $f(t) = g(t) + O(h(t))$ as $t \to a$, means that $\limsup_{t \to a} |\frac{f(t)-g(t)}{h(t)}| < \infty$.

Corollary 10.6.5. *Let Λ be a lattice in an $\mathbb{R}$-vector space $V \cong \mathbb{R}^n$ and let $B \subset V$ be a set whose boundary is $(n-1)$-Lipschitz parametrizable. Then*

$$\sharp(tB \cap \Lambda) = \frac{\mu(B)}{\mathrm{Vol}(\mathbb{R}^n/\Lambda)} t^n + O(t^{n-1}).$$

Proof. Let $L : \mathbb{R}^n \to \mathbb{R}^n$ be a linear transformation such that $L(\Lambda) = \mathbb{Z}^n$. If S' denotes the image of B, then

$$\mu(B') = \mu(B)|\det(L)| = \frac{\mu(B)}{\mathrm{Vol}(\mathbb{R}^n/\Lambda)}.$$

Clearly, we have $\sharp(tB' \cap \mathbb{Z}^n) = \sharp(tB \cap \Lambda)$, so the statement follows from the above lemma. $\square$

Example 10.6.6. *Let us take $\mathbb{R}^2 \cong \mathbb{C}$, and $B = B_{\leq 1} = \{z : |z| \leq 1\}$. Then what is $\sharp(tB \cap \mathbb{Z}^2)$? That is, how many $(m, n) \in \mathbb{Z}^2$ such that $m^2 + n^2 \leq t^2$? This is called the* Gauss circle problem*, determining how many integer lattice points there are in a circle centered at the origin and with radius t. If $N(t)$ denotes the cardinality then, since the fundamental domain of the lattice $\mathbb{Z}^2$ is 1, $N(t)$ is expected to be approximately equal to πt^2, i.e.*

$$N(t) = \pi t^2 + E(t)$$

for some error term $E(t)$ of relatively small (absolute) value. Define $c_0(t)$ and $c_1(t)$ as in the proof, and let $\delta = \sqrt{2}$ be the maximal length of two elements in a fundamental domain D of $\mathbb{Z}^2$. Then

$$\pi(t-\delta)^2 = \mu(B_{\leq t-\delta}) \leq c_0(t), \quad c_1(t) \leq \mu(B_{\leq t+\delta}) = \pi(t+\delta)^2,$$

and $c_1(t) - c_0(t) = O(t)$. The error term $E(t)$ is expected to have order $O(t^{1/2} + \epsilon)$ for any $\epsilon > 0$, but still open problem.

10.6.2 Proof of Theorem

Proof of Theorem. Let $K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n$, we have the embedding

$$\sigma = (\sigma_1, ..., \sigma_{r_1}, ..., \sigma_{r_1+r_2}) : K \hookrightarrow K_{\mathbb{R}};$$

moreover if

$$N(y) := \prod_{v|\infty} |y_v|_v = \prod_{v \text{ real}} |y_v|_{\mathbb{R}} \prod_{v \text{ comp.}} |y_v|^2_{\mathbb{C}}$$

then σ preserves the norm function (on K). We have also defined

$$\mathrm{Log} : \mathbb{R}^{\times, r_1} \times \mathbb{C}^{\times, r_2} \to \mathbb{R}^{r_1+r_2}$$

given by

$$\mathrm{Log} : (y_1, ..., y_{r_1}, z_1, ..., z_{r_2}) \mapsto (\log|y_1|, ..., \log|y_{r_2}|, 2\log|z_1|, ..., 2\log|z_{r_2}|).$$

If $\ell : \mathcal{O}_K^\times \to \mathbb{R}^{r_1+r_2}$ denotes the composition, then $\mathrm{Im}(\ell)$ is contained in the hyperplane $H := \{(x_i) : \sum_i x_i = 0\}$ of $\mathbb{R}^{r_1+r_2}$ and there is an exact sequence of abelian groups

$$0 \to W_K \to \mathcal{O}_K^\times \xrightarrow{\ell} \Lambda_K \to 0$$

where Λ_K is a lattice in H.

We want to estimate the quantity

$$\sharp\{\mathfrak{a} : N(\mathfrak{a}) \leq t\}, \quad t \to \infty$$

where $\mathfrak{a}$ ranges over the non-zero ideals of $\mathcal{O}_K$. We first consider the principal ideal class; since $(\alpha) = (\alpha')$ iff $\alpha/\alpha' \in \mathcal{O}_K^\times$, we need estimate

$$\sharp\{\alpha \in \mathcal{O}_K - \{0\} : |N_{K/\mathbb{Q}}(\alpha)| \leq t\}/\mathcal{O}_K^\times.$$

or equivalently (identify $\mathcal{O}_K$ inside $K_\mathbb{R}$ via σ),

$$\sharp\Big(K_{\mathbb{R},\leq t}^\times \cap \mathcal{O}_K\Big)/\mathcal{O}_K^\times$$

where

$$K_{\mathbb{R},\leq t}^\times := \{x \in K_\mathbb{R}^\times : N(x) \leq t\}.$$

Recall that $\mathcal{O}_K^\times \cong U_K \times W_K$, where U_K is the free part, then it suffices to estimate (dividing the result by w_K)

$$\sharp\Big(K_{\mathbb{R},\leq t}^\times \cap \mathcal{O}_K\Big)/U.$$

Step 1. We construct a fundamental domain for $K_\mathbb{R}^\times/U$ as follows. Define

$$\begin{array}{ccccc} K_\mathbb{R}^\times & \overset{\nu}{\twoheadrightarrow} & K_{\mathbb{R},1}^\times & \overset{\mathrm{Log}}{\twoheadrightarrow} & H \\ y & \mapsto & y\mathrm{N}(y)^{-1/n} & & \end{array}$$

Fix a fundamental domain D for the lattice Λ_K in H and let $B = (\nu \circ \mathrm{Log})^{-1}(D)$. So B is a set of unique coset representatives for the quotient $K_\mathbb{R}/U_K$. Define

$$B_{\leq t} := \{x \in B : |N_{K/\mathbb{Q}}(y)| \leq t\} \subset S,$$

we are left to estimate

$$\sharp(B_{\leq t} \cap \mathcal{O}_K).$$

Example 10.6.7. *We look at the case when K is quadratic:*

(a) If $r_1 = 0$ and $r_2 = 1$, then $K_\mathbb{R} \cong \mathbb{C}$, and $H = 0$, so $B = \mathbb{C}$ and

$$B_{\leq t} = \{z \in \mathbb{C} : |z| \leq t\}.$$

When $t = 1$, one has $\mu(B_{\leq 1}) = \pi$.

(b) If $r_1 = 2$ and $r_2 = 0$, then $K_\mathbb{R} \cong \mathbb{R}^2$ and $H \cong \mathbb{R}$ with lattice $\Lambda_K = \mathbb{Z}\log\epsilon$, where $\epsilon > 1$ is the fundamental unit. Then $K_{\mathbb{R},\leq 1}$ is the region inside $|y_1 y_2| \leq 1$. If we take $D = [0, \log\epsilon)$ as the fundamental domain for $\Lambda_K = \mathbb{Z}\log\epsilon$ in $H \cong \mathbb{R}$, then the above defined B is just [5]

$$B = \{(y_1, y_2) \in \mathbb{R}^2 : 1 \leq |\frac{y_1}{y_2}| \leq \frac{\epsilon}{\sigma_2(\epsilon)} = \epsilon^2\}.$$

The square of $\mu(B_{\leq 1})$ is $4\log\epsilon$. Note that $R_K = \log\epsilon$ in this case.

[5] here we take $\sigma_1 = \mathrm{Id}$

Step 2. We are in the following situation: $\mathcal{O}_K$ is a lattice in $K_{\mathbb{R}}$ ($\cong \mathbb{R}^n$). Note that $tB_{\leq 1} = B_{\leq t^n}$. Show that $B_{\leq 1}$ is $(n-1)$-Lipschitz parametrizable. We illustrate this by looking at a special case $n = 2$.

Step 3. So Corollary implies that

$$\sharp(t^{1/n}B_{\leq 1} \cap \mathcal{O}_K) = \frac{\mu(B_{\leq 1})}{\mathrm{Vol}(\mathbb{R}^n/\sigma(\mathcal{O}_K))}(t^{1/n})^n + O((t^{1/n})^{n-1}) = \frac{\mu(B_{\leq 1})}{|\Delta_K|^{1/2}}t + O(t^{1-1/n}).$$

Proposition 10.6.8. *We have $\mu(B_{\leq 1}) = 2^{r_1}\pi^{r_2}R_K$.*

Proof. Omitted, see Tian's note. □

Finally recalling : for any fractional ideal $\mathfrak{a}$,

$$\mathrm{Vol}(\mathbb{R}^n/\sigma(\mathfrak{a})) = \frac{1}{2^{r_2}}\sqrt{\Delta_K}N(\mathfrak{a}),$$

we get

$$\sharp(B_{\leq t} \cap \mathcal{O}_K) = \Big(\frac{2^{r_1}(2\pi)^{r_2}R_K}{|\Delta_K|^{1/2}}\Big)t + O(t^{1-1/n})$$

and

$$\sharp\{(\alpha) \subset \mathcal{O}_K : N(\alpha) \leq t\} = \Big(\frac{2^{r_1}(2\pi)^{r_2}R_K}{w_K|\Delta_K|^{1/2}}\Big)t + O(t^{1-1/n}). \tag{10.2}$$

Step 4. Show that the estimation (10.2) holds for any ideal class C, giving the result (by multiplying h_K). Fix an ideal class $C = [\mathfrak{a}]$ with $\mathfrak{a} \subset \mathcal{O}_K$. Multiplication by $\mathfrak{a}$ gives a bijection

$$\begin{aligned}\{\text{ideals } \mathfrak{b} \in [\mathfrak{a}^{-1}] : N(\mathfrak{b}) \leq t\} &\leftrightarrow \{\text{ideals } (\alpha) \subset \mathfrak{a} : |N_{K/\mathbb{Q}}(\alpha)| \leq tN(\mathfrak{a})\} \\ &\leftrightarrow \{0 \neq \alpha \in \mathfrak{a} : |N_{K/\mathbb{Q}}(\alpha)| \leq tN(\mathfrak{a})\}/\mathcal{O}_K^\times.\end{aligned}$$

Let $B_{C,\leq t}$ denote the RHS set. Replacing $\mathcal{O}_K$ by $\mathfrak{a}$ in the above argument, we obtain

$$\sharp B_{C,\leq t} = \Big(\frac{2^{r_1}(2\pi)^{r_2}R_K}{w_K\mathrm{Vol}(\mathbb{R}^n/\mathfrak{a})}\Big)tN(\mathfrak{a}) + O(t^{1-1/n}).$$

Since $\mathrm{Vol}(\mathfrak{a}) = \mathrm{Vol}(\mathcal{O}_K)N(\mathfrak{a})$, we obtain the assertion. □

Chapter 11

W11: Analytic class number formula

11.1 Abelian fields

Recall first the theorem proved last time: let $K/\mathbb{Q}$ be an abelian extension, then

$$\zeta_K(s) = \prod_{\chi \in \widehat{K}} L(s, \chi^*).$$

On the other hand, since $\mathrm{Res}_{s=1}\zeta_K(s) = \rho_K h_K$ and $\mathrm{Res}_{s=1}\zeta(s) = 1$, we obtain

$$\rho_K h_K = \prod_{\chi \in \widehat{K}, \chi \neq \chi_0} L(1, \chi^*)$$

where[1] (since $w_K = 2$ if K is real)

$$\rho_K = \frac{2^{r_1}(2\pi)^{r_2} R_K}{w_K |\Delta_K|^{1/2}} = \begin{cases} R_K \frac{2^{n-1}}{|\Delta_K|^{1/2}} & K \text{ real} \\ R_K \frac{(2\pi)^{n/2}}{w_K |\Delta_K|^{1/2}} & K \text{ imaginary.} \end{cases}$$

Lemma 11.1.1. *Let χ be a primitive character mod $N \geq 3$. Then*

$$L(1, \chi) = \begin{cases} -\frac{2G(1,\chi)}{N} \sum_{1 \leq k < N/2} \overline{\chi}(k) \log \sin \frac{k\pi}{N}, & \text{if } \chi(-1) = 1 \\ \frac{\pi i G(1,\chi)}{N^2} \sum_{k=1}^{N-1} \overline{\chi}(k) k = \frac{\pi i G(1,\chi)}{N(\chi(2)-2)} \sum_{1 \leq k < N/2} \overline{\chi}(k), & \text{if } \chi(-1) = -1 \end{cases}$$

Proof. Write $\zeta_N = e^{2\pi i/N}$. We first remark the following identity:[2]

$$\sum_{k=0}^{N-1} (\zeta_N)^{ak} = \begin{cases} N & \text{if } N | a \\ 0 & \text{else} \end{cases}$$

[1] using that if K is Galois, then either $r_1 = 0$ or $r_2 = 0$

[2] even if $(a, N) \neq 1$ but $N \nmid a$, we still get 0

Therefore, for $\Re(s) > 1$,

$$\begin{aligned} L(s,\chi) &= \sum_{a=0}^{N-1} \chi(a) \sum_{n\geq 1, n\equiv a\ (N)} \tfrac{1}{n^s} \\ &= \sum_{a=0}^{N-1} \chi(a) \sum_{n\geq 1} \big(\tfrac{1}{N} \sum_{k=0}^{N-1} \zeta_N^{(a-n)k} \tfrac{1}{n^s}\big) \\ &= \tfrac{1}{N} \sum_{k=0}^{N-1} G(k,\chi) \big(\sum_{n\geq 1} \zeta_N^{-nk} \tfrac{1}{n^s}\big) \\ &= \tfrac{G(1,\chi)}{N} \sum_{k=0}^{N-1} \overline{\chi}(k) \sum_{n\geq 1} \zeta_N^{-nk} \tfrac{1}{n^s} \\ &\overset{k\mapsto -k}{=} \chi(-1) \tfrac{G(1,\chi)}{N} \sum_{k=0}^{N-1} \overline{\chi}(k) \big(\sum_{n\geq 1} \zeta_N^{nk} \tfrac{1}{n^s}\big). \end{aligned}$$

The Dirichlet series $\sum_{n\geq 1} \zeta_N^{nk} \frac{1}{n^s}$ converges on $\Re(s) > 0$ (i.e. $\sigma_c = 0$), and is continuous at $s = 1$. Clearly its value at $s = 1$ is $-\log(1-\zeta_N^k)$; here we take the branch of the multiple valued function $\log(z)$ on $z \in \mathbb{C}\backslash\{0\}$ which takes real values on $z \in \mathbb{R}_{>0}$. Note that[3]

$$\log(1-\zeta_N^a) = \log|1-\zeta_N^a| + (\frac{k}{N} - \frac{1}{2})\pi i.$$

So we obtain

$$L(1,\chi) = -\chi(-1)\frac{G(1,\chi)}{N} \sum_{k=0}^{N-1} \overline{\chi}(k) \big(\log|1-\zeta_N^k| + (\frac{k}{N} - \frac{1}{2})\pi i\big) \tag{11.1}$$

On the other hand, one has

$$|1-\zeta_N^k| = \sqrt{(1-\cos\frac{2\pi k}{N})^2 + (\sin\frac{2\pi k}{N})^2} = \sqrt{2-2\cos\frac{2\pi k}{N}} = 2\sin\frac{\pi k}{N}$$

for $1 \leq k \leq N-1$. We now distinguish two cases depending on the parity of χ.

- χ is even, i.e. $\chi(-1) = 1$, then next lemma shows that

  $$\sum_{k=0}^{N-1} \overline{\chi}(k) \frac{k}{N} = 0.$$

  so that

  $$L(1,\chi) = -\frac{G(1,\chi)}{N} \sum_{k=1}^{N-1} \overline{\chi}(k) \log\sin\frac{k\pi}{N} = -\frac{2G(1,\chi)}{N} \sum_{1\leq k<N/2} \overline{\chi}(k) \log\sin\frac{k\pi}{N}.$$

- χ is odd, i.e. $\chi(-1) = -1$, then next lemma shows that

  $$\sum_{k=1}^{N-1} \overline{\chi}(k) \log\sin\frac{k\pi}{N} = 0,$$

  so we obtain

  $$L(1,\chi) = \frac{G(1,\chi)}{N^2} \cdot \pi i \sum_{k=1}^{N-1} \overline{\chi}(k) k.$$

  The last equality also follows from next lemma.

[3]the function is multiple values: $\log z = \log|z| + i(\mathrm{Arg} z + 2\pi k)$ for any k, taking the principal value means $k = 0$

$\square$

Lemma 11.1.2. *Let χ be a primitive character mod $N \geq 2$.*

(1) If χ is even, then

$$\sum_{k=1}^{N-1} \chi(k)k = 0.$$

(2) If χ is odd, then

$$\sum_{k=1}^{N-1} \chi(k) \log \sin \frac{k\pi}{N} = 0$$

$$\sum_{k=1}^{N-1} \chi(k)k = \frac{N}{\overline{\chi}(2) - 2} \sum_{1 \leq k < N/2} \chi(k).$$

Proof. (1) Note that although χ is defined mod N, the term k is not. However, dividing $\{1, ..., N-1\}$ into $\{1, ..., [N/2]\}$ and $\{N-k : k = 1, ..., [N/2]\}$ (if $2|N$, then forget $N/2$ since $\chi(N/2) = 0$). Using $\chi(-1) = 1$, we obtain

$$\sum_{k=1}^{N-1} \chi(k)k = N \cdot \sum_{k=1}^{[N/2]} \chi(k) = N \cdot \frac{1}{2} \sum_{k=1}^{N-1} \chi(k) = 0.$$

(2) We similarly treat the first statement. For the second, we only explain the proof when $2 \nmid N$. As in (1), we have

$$\sum_{k=1}^{N-1} \chi(k)k = \sum_{1 \leq k < N/2} \chi(k)k + \sum_{1 \leq k < N/2} \chi(N-k)(N-k) = \sum_{1 \leq k < N/2} (2k - N)\chi(k).$$

On the other hand, we may also divide $\{1, ..., N-1\}$ as $\{\text{even}\} \cup \{\text{odd}\}$, so that

$$\sum_{k=1}^{N-1} \chi(k)k = \sum_{2|k} \chi(k) + \sum_{2|k} \chi(N-k)(N-k) = \sum_{2|k} \chi(k)(2k-N) = \chi(2) \sum_{1 \leq k < N/2} \chi(k)(4k-N).$$

Combining them we get

$$(\overline{\chi}(2) - 2) \sum_{k=1}^{N-1} \chi(k)k = N \sum_{1 \leq k < N/2} \chi(k),$$

giving the result. $\square$

Theorem 11.1.3. *(Hasse) (1) If K is real abelian field, then*

$$R_K h_K = \prod_{\chi \in \widehat{K}, \chi \neq \chi_0} \left| \sum_{1 \leq k < f_\chi/2} \chi^*(k) \log \sin \frac{k\pi}{f_\chi} \right|.$$

(2) If K is imaginary abelian field, then

$$R_{K_+} h_{K_+} = \prod_{\chi \in \widehat{K}, \chi \neq \chi_0, \chi(-1)=1} \left| \sum_{1 \leq k < f_\chi/2} \chi^*(k) \log \sin \frac{k\pi}{f_\chi} \right|,$$

$$\begin{aligned} \frac{R_K h_K}{R_{K_+} h_{K_+}} &= \frac{w_K}{2} \prod_{\chi \in \widehat{K}, \chi(-1)=-1} \frac{1}{f_\chi} \left| \sum_{1 \leq k < f_\chi - 1} \chi^*(k)k \right| \\ &= \frac{w_K}{2} \prod_{\chi \in \widehat{K}, \chi(-1)=-1} \frac{1}{|\chi^*(2) - 2|} \left| \sum_{1 \leq k < f_\chi/2} \chi^*(k) \right|. \end{aligned}$$

Proof. We take the product over all $\chi \in \widehat{G}$ of $L(1, \chi^*)$. Recall the following facts:

- Analytic class number formula:

$$\rho_K = \frac{2^{r_1}(2\pi)^{r_2} R_K}{W_K |\Delta_K|^{1/2}} = \begin{cases} R_K \frac{2^{n-1}}{|\Delta_K|^{1/2}} & K \text{ real} \\ R_K \frac{(2\pi)^{n/2}}{w_K |\Delta_K|^{1/2}} & K \text{ imaginary}. \end{cases}$$

- Hasse's conductor-discriminant formula says that

$$\prod_{\chi \in \widehat{G}} f_\chi = |\Delta_K|;$$

- $|G(1, \chi^*)| = \sqrt{f_\chi}$;

Hence if K is real,

$$\prod_{\chi \in \widehat{K}, \chi \neq \chi_0} \frac{2|G(1, \chi)|}{f_\chi} = \frac{2^{n-1}}{|\Delta_K|^{1/2}}$$

while if K is imaginary, we have $(n/2 - 1)$ even characters and $n/2$ odd characters. We omit the details. □

11.2 Quadratic fields

Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field. Since $\mathrm{Gal}(K/\mathbb{Q}) = \{1, \sigma\}$ has order 2, there is a unique non-trivial character: λ. Since $1 \cdot \mathrm{cond}(\lambda) = |\Delta_K|$, we get λ is a primitive character mod $|\Delta_K|$. Define a character χ_K as follows: if p is a prime number, let

$$\chi_K(p) = \begin{cases} 1 & p \text{ splits} \\ -1 & p \text{ inert} \\ 0 & p \text{ ramified} \end{cases}$$

then extends it to $\mathbb{N}$ using prime decomposition. We have proved that $\lambda = \chi_K$. Explicitly, we have

$$\chi_K(2) = \begin{cases} 1 & d \equiv 1 \mod 8 \\ -1 & d \equiv 5 \mod 8; \\ 0 & \text{else} \end{cases} \qquad \chi_K(p) = \begin{cases} (\frac{d}{p}) & p \nmid d \\ 0 & p | d, \end{cases} \quad p \neq 2.$$

We deduce the analytic class number formula for quadratic fields.

Theorem 11.2.1. *(1) Let $K = \mathbb{Q}(\sqrt{-d})$ imaginary quadratic with $d \neq 1, 3$. Then*

$$\begin{aligned} h_K &= \tfrac{1}{|\Delta_K|} \Big| \sum_{k=1}^{|\Delta_K|} \chi_K(k) k \Big| \\ &= -\tfrac{1}{|\Delta_K|} \sum_{k=1}^{|\Delta_K|} \chi_K(k) k \\ &= \tfrac{1}{2 - \chi_K(2)} \sum_{1 \leq k < \frac{|\Delta_K|}{2}} \chi_K(k). \end{aligned}$$

(2) If $K = \mathbb{Q}(\sqrt{d})$ be real quadratic and let $\epsilon > 1$ be the unique fundamental unit. Then

$$h_K = -\frac{1}{\log \epsilon} \cdot \sum_{1 \leq k < \frac{|\Delta_K|}{2}} \chi_K(k) \log \sin \frac{k\pi}{|\Delta_K|}.$$

Proof. (1) In imaginary case, we know $w_K = 2$ (for $d \neq 1, 3$) and $R_K = 1$. Also, $\lambda = \chi_K$ is odd of conductor $|\Delta_K|$ and $\overline{\chi}_K = \chi_K$. So we obtain

$$\frac{2\pi}{2|\Delta_K|^{1/2}} \cdot h_K = \frac{\pi i G(1,\chi)}{|\Delta_K|^2} \sum_{k=1}^{|\Delta_K|-1} \chi_K(k)k.$$

Since $|G(1,\chi_K)| = |\Delta_K|^{1/2}$ and $h_K \in \mathbb{N}$, we obtain

$$h_K = \frac{1}{|\Delta_K|} \sum_{k=1}^{|\Delta_K|-1} \chi_K(k)k.$$

In fact, we can decide explicitly $G(1,\chi_K)$, see Tian's note:

$$G(1,\chi_K) = \begin{cases} |\Delta_K|^{1/2} & \chi(-1) = 1 \\ i|\Delta_K|^{1/2} & \chi(-1) = -1 \end{cases}$$

so we in fact have

$$h_K = -\frac{1}{\Delta_K} \sum_{k=1}^{|\Delta_K|-1} \chi_K(k)k.$$

(2) We similarly handle the real case. $\square$

Corollary 11.2.2. *If $p \equiv 3 \mod 4$, and $K = \mathbb{Q}(\sqrt{-p})$, then h_K is odd.*

Proof. The assumption implies that $\Delta_K = -p$, so $\chi_K(l) = (\frac{-p}{l})$ for any prime number l. The quadratic reciprocity law implies that $(\frac{-p}{l}) = (\frac{l}{p})$, so that χ_K is given by

$$\chi_K(a) = (\frac{a}{p}), \quad (p,a) = 1$$

which is equal to 1 if a is a quadratic residue and -1 otherwise. Therefore

$$h = \frac{1}{p}(\sum_{b \text{ non residue}} b - \sum_{a \text{ residue}} a) = \frac{p-1}{2} - \frac{2}{p}\sum_{a \in R} a,$$

which is odd since $p \equiv 1 \mod 4$. Here we used that $\sum_a a + \sum_b b = (1 + \cdots + (p-1)) = \frac{p(p-1)}{2}$. $\square$

Example 11.2.3. *(1) Consider $K = \mathbb{Q}(\sqrt{5})$. Then $|\Delta_K| = 20$ and $\chi_K = \lambda$ is a primitive mod 20 character with*

$$\chi_K(2) = 0, \quad \chi_K(3) = 1, \quad \chi_K(5) = 0 \text{ (ramified)}, \quad \chi_K(7) = 1.$$

Hence, $h_K = \frac{1}{2}(1 + 1 + 0 + 1 + 1) = 2$.

(2) Consider $K = \mathbb{Q}(\sqrt{-14})$. Then $|\Delta_K| = 4 \times 14$ and χ_K is a primitive character mod 56. A computation shows that (for $p < 28$)

$$\chi_K(2) = \chi_K(7) = 0, \quad \chi_K(3) = \chi_K(5) = \chi_K(13) = \chi_K(19) = \chi_K(23) = 1$$

$$\chi_K(11) = \chi_K(17) = -1$$

so $\chi_K(\text{even}) = 0$, *and*

$$h_K = \frac{1}{2}(1+1+1+0+1+(-1)+1+1+(-1)+1+0+1+1+1) = 4.$$

(3) Consider $K = \mathbb{Q}(\sqrt{2})$, $|\Delta_K| = 8$, $\chi_K(2) = 0$, $\chi_K(3) = -1$. *The fundamental unit is* $\epsilon = 1+\sqrt{2}$, *so*

$$\begin{aligned} h_K &= \tfrac{1}{\log(1+\sqrt{2})}|\chi_K(1)\log\sin\tfrac{\pi}{8} + \chi_K(3)\log\sin\tfrac{3\pi}{8}| \\ &= \frac{\log\left(\frac{\sin(3\pi/8)}{\sin(\pi/8)}\right)}{\log(1+\sqrt{2})}, \end{aligned}$$

i.e. [4]

$$(1+\sqrt{2})^{h_K} = \frac{\sin(3\pi/8)}{\sin(\pi/8)} = 1 + 2\cos(\pi/4) = 1+\sqrt{2},$$

hence $h_K = 1$.

Form this, we see that a main obstacle to compute the class number is the determination of the fundamental unit.

Remark 11.2.4. *(1) For real quadratic field* $K = \mathbb{Q}(\sqrt{d})$, *Hua proved that*

$$h_K < \sqrt{d}.$$

(2) For imaginary $K = \mathbb{Q}(\sqrt{-d})$, *one has the following theorem of Siegel (1936): for any* $\epsilon > 0$, *there exists a constant* $d(\epsilon) > 0$ *such that*

$$h_K \gg d^{1/2-\epsilon}, \quad d > d(\epsilon).$$

11.3 Cyclotomic fields

We only state some results of Kummer about the class number of cyclotomic fields. Let p be an odd prime. Let h_p (resp. h_p^+) denote the class number of $K := \mathbb{Q}(\zeta_p)$ (resp. K_+); R_p (resp. R_p^+) denote the regulator of K (resp. K_+)

Theorem 11.3.1. *(Kummer)*

(1) $h_p^+|h_p$. *The quotient* h_p^- *is called the first factor of* h_p, *and* h_p^+ *the second factor.*

(2) If $p \nmid h_p$, *then Fermat's Last Theorem holds for exponent* p.

(3) $p|h_p$ *if and only if* $p|h_p^-$ *if and only if for some* $k \in \{2,4,...,p-3\}$, p *divides the numerator of* B_k.

The first factor h_p^- is well understood and can be computed easily in terms of Bernoulli numbers, and is usually rather large (see below). The second factor h_p^+ is not well understood and is hard to compute explicitly, and in the cases when it has been computed it is usually small.

Prime numbers with $p \nmid h_p$ are called *regular primes*, so Fermat's Last Theorem holds for regular primes. However, there are infinitely many irregular primes.

Example 11.3.2. *If* p *is irregular and* $p < 100$, *then* $p \in \{37, 59, 67\}$. *Indeed, the numerator of* B_{32} *is*

$$-7709321041217 = 37 \times -208360028141.$$

[4] use $\sin(3x) = 3\sin(x) - 4\sin^3(x)$ and $2\sin^2(x) = 1 - \cos(2x)$

Conjecture 11.3.3. *(Kummer-Vandiver)* $p \nmid h_p^+$.

Proposition 11.3.4. *One has*

$$\begin{aligned} h_p^- &= (2p^{-(p-3)/2}) \prod_{\chi(-1)=-1} |\textstyle\sum_{k=1}^{p-1} \chi(k)k \\ &= 2^{-(p-3)/2} p \prod_{\chi(-1)=-1} \left(\frac{1}{2-\chi(2)} |\textstyle\prod_{k=1}^{(p-1)/2} \chi(k)|\right). \end{aligned}$$

Proof. The analytic class number formula allows us to compute $\frac{R_p h_p}{R_p^+ h_p^+}$. It suffices to determine R_p/R_p^+; in fact we have

$$R_p = R_p^+ \cdot 2^{(p-3)/2}.$$

Since p is a prime, all non-trivial characters mod p are primitive. □

Lemma 11.3.5. *Let a be the order of 2 in $(\mathbb{Z}/p\mathbb{Z})^\times/\{\pm 1\}$. Then*

$$\prod_{\chi \text{ odd}} (2 - \chi(2)) = (2^a \pm 1)^{(p-1)/(2a)}$$

with the + sign iff $2^a \equiv -1 \mod p$.

Proof. Omit, left as an exercise. □

Example 11.3.6. *Take $p = 7$ and compute h_p^-. Then $a = 3$ and Lemma shows that*

$$\prod_{\chi \text{ odd}} (2 - \chi(2)) = (2^3 - 1)^{(7-1)/6} = 7$$

and

$$h_p^- = \frac{7}{2^2} \cdot \frac{1}{7} \cdot \prod_{\chi \text{ odd}} |\sum_{k=1}^{3} \chi(k)|.$$

Note that 3 is a generator of $(\mathbb{Z}/7\mathbb{Z})^\times$. There are 3 odd characters, which are listed below (use $2 \equiv 3^2 \mod 7$):

$$\begin{aligned} \chi_1(3) = \zeta_6, \quad \chi_2(3) = \zeta_6^3 = -1, \quad \chi_3(3) = \zeta_6^5 \\ \chi_1(2) = \zeta_6^2, \quad \chi_2(2) = \zeta_6^6 = 1, \quad \chi_3(2) = \zeta_6^4. \end{aligned}$$

So

$$\begin{aligned} |\chi_1(1) + \chi_1(2) + \chi_1(3)| = |1 + \zeta_6^2 + \zeta_6| = |1 + \sqrt{3}i| = 2 \\ |\chi_2(1) + \chi_2(2) + \chi_2(3)| = |1 + 1 + (-1)| = 1 \\ |\chi_3(1) + \chi_3(2) + \chi_3(3)| = |1 + \zeta_6^4 + \zeta_6^5| = 2 \end{aligned}$$

and

$$h_p^- = \frac{1}{2^2} \cdot (2 \cdot 2) = 1.$$

W11: Exercise

1. Use the class number formula to compute: (a) $K = \mathbb{Q}(\sqrt{-d})$ for $d = 6, 15, 23$; (b) $K = \mathbb{Q}(\sqrt{d})$ for $d = 3, 6$ (first determine the fundamental unit).

2. Prove that for $d > 3$ square-free and $K = \mathbb{Q}(\sqrt{-d})$:

$$\begin{aligned} h_K < d/4, \quad \text{if } -d \equiv 1 \mod 4 \\ h_K \leq d/2 \quad \text{if } -d \equiv 2, 3 \mod 4. \end{aligned}$$

Chapter 12

Density theorem

12.1 Primes in arithmetic progressions

It is a classical result that there are infinitely many rational prime numbers. Now we prove the following application of Dirichlet series, saying that there are infinitely many primes numbers in arithmetic progressions.

Theorem 12.1.1. *Let $N \geq 2$ and $(a, N) = 1$. There are infinitely many primes numbers in the arithmetic progression $\{kN + a : k = 0, 1, 2, ...\}$.*

Proof. Let χ be a mod N Dirichlet character. When $\Re(s) > 1$, one has

$$\begin{aligned}
\log L(s,\chi) &= -\sum_p \log(1-\chi(p)p^{-s}) \\
&= \sum_p \textstyle\sum_{m\geq 1} \frac{\chi(p)^m}{m} p^{-ms} \\
&= \sum_p \chi(p)p^{-s} + g_\chi(s)
\end{aligned}$$

where $g_\chi(s) = \sum_p \sum_{m\geq 2} \frac{\chi(p)^m}{m} p^{-ms}$. It is easy to see that $g_\chi(s)$ converges when $\Re(s) > 1/2$. In particular, $g_\chi(s)$ is holomorphic at $s = 1$.

On the other hand, using the identity

$$\frac{1}{\varphi(N)} \sum_{\chi:(\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times} \chi(p/a) = \begin{cases} 1 & \text{if } p \equiv a(N) \\ 0 & \text{otherwise} \end{cases}$$

we obtain

$$\begin{aligned}
\sum_{p\equiv a(N)} p^{-s} &= \tfrac{1}{\varphi(k)} \sum_\chi \overline{\chi}(a) \sum_p \chi(p)p^{-s} \\
&= \tfrac{1}{\varphi(k)} \sum_\chi \overline{\chi}(a) \log L(s,\chi) - \tfrac{1}{\varphi(k)} \sum_\chi \overline{\chi}(a) g_\chi(s).
\end{aligned}$$

If $\chi \neq \chi_0$, then $L(s, \chi)$ is holomorphic at $s = 1$, so $L(1, \chi) = O(1)$. For $\chi = \chi_0$ the principal character,

$$L(s,\chi_0) = \zeta(s) \cdot \prod_{p|N} (1-p^{-s}),$$

so

$$\mathrm{Res}_{s=1} L(s,\chi_0) = \prod_{p|N} (1-p^{-1}) = \frac{\varphi(N)}{N}$$

$$\log L(s,\chi_0) \sim \log\zeta(s) \sim \log\frac{1}{s-1}, \quad \text{as } s \to 1.$$

We obtain finally that

$$\sum_{p\equiv a(N)} \frac{1}{p^s} \sim \frac{1}{\varphi(N)} \log\frac{1}{s-1}, \quad s \to 1.$$

Since the RHS is unbounded, so is the LHS, and the result follows. □

12.2 Dirichlet density

First note the following fact.

Proposition 12.2.1. *Let K be a number field. Then we have*

$$\sum_{\mathfrak{p}} \frac{1}{N(\mathfrak{p})^s} \sim \log\zeta(s) \sim \log\frac{1}{s-1}, \quad s \to 1^+$$

where $\mathfrak{p}$ runs over all the prime ideals of O_K.

Proof. See Tian's note. □

Definition 12.2.2. *For a subset A of prime ideals of $\mathcal{O}_K$, we say A has a Dirichlet density, if the limit*

$$\lim_{s\to 1} \frac{\sum_{\mathfrak{p}\in A} \frac{1}{N(\mathfrak{p})^s}}{\log\frac{1}{s-1}}$$

exists; we denote the limit by $\delta(A)$.

Remark 12.2.3. *Proposition says that it is a well-defined measure.*

Example 12.2.4. *The set A of prime numbers p such that $p \equiv a \mod N$ has density $1/\varphi(N)$.*

Remark 12.2.5. *(1) This is another notion of 'density': natural density, which is based on the prime number theorem[1]: let $\pi_K(x)$ denotes the number of prime ideals of norm $\leq x$, then*

$$\pi_K(x) \sim \frac{x}{\log x}, \quad x \to +\infty.$$

Then the density is defind as

$$C(A) := \lim_{x\to\infty} \frac{\sharp\{\mathfrak{p} \in A,\ N(\mathfrak{p}) \leq x\}}{\pi_K(x)}.$$

It can be shown that if A has a natural density, then $\delta(A)$ exists and is equal to $C(A)$.

(2) Remark that the quantity $x/\log x$ contains no information of K. This is reasonable as shown by the example of $K = \mathbb{Q}(i)$. Forgetting the (finite) ramified primes, for any prime number p of the form $4n+1$, p factors as a product of two Gaussian primes of norm p.

[1]For $K = \mathbb{Q}$, the theorem is due to Hadamard and de la Vallée-Poussin (1896), using Riemann zeta function; and elementary proofs found by Selberg and Erdös (1949). For general K, it is due to Landau (1903).

Primes of the form $4n+3$ remain prime, giving a Gaussian prime of norm p^2. Therefore, we should estimate

$$2r(x)+r'(\sqrt{x}),$$

where r counts primes in the arithmetic progression $4n+1$, and r' in the arithmetic progression $4n+3$. By the quantitative form of Dirichlet's theorem on primes,

$$r(x) \sim \frac{x}{2\log x}, \quad r'(\sqrt{x}) \sim \frac{\sqrt{x}}{2\log\sqrt{x}} = \frac{\sqrt{x}}{\log x},$$

hence the asymptotic growth is $x/\log x$.

Theorem 12.2.6. *Let L/K be a Galois extension of number fields, with $n=[L:K]$. Let*

$$A = \{\mathfrak{p} \subset \mathcal{O}_K : \mathfrak{p} \text{ splits completely in } L\}$$

then $\delta(A) = 1/n$.

Proof. For $\Re(s) > 1$, we have

$$\begin{array}{rcl} \log\zeta_L(s) & = & \sum_{\mathfrak{P}} N(\mathfrak{P})^{-s} + O(1) \\ & = & \sum_{\mathfrak{p}\subset\mathcal{O}_K}\sum_{\mathfrak{P}|\mathfrak{p}} N(\mathfrak{P})^{-s} + O(1) \end{array}$$

Since there are only finitely many ramified primes, we may ignore them in the above sum. Assume $\mathfrak{p}$ is unramified, and write $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1\cdots\mathfrak{P}_g$ with $gf=n$. If $f \geq 2$, then

$$|N(\mathfrak{P})^{-s}| = |N(\mathfrak{p})^{-fs}| \leq N(\mathfrak{p})^{-2\sigma}$$

so that $\sum_{\mathfrak{p},f\geq 2} N(\mathfrak{p})^{-s}$ converges when $\Re(s) > 1$. Therefore,

$$\log\zeta_L(s) = \sum_{\mathfrak{p}\in A}\sum_{\mathfrak{P}|\mathfrak{p}} N(\mathfrak{P})^{-s} + O(1) = n\sum_{\mathfrak{p}\in A} N(\mathfrak{p})^{-s} + O(1),$$

and the result follows from Proposition. □

The case where L/K is a general extension can be deduced easily.

Corollary 12.2.7. *Let L/K be an extension of number fields and N be the Galois closure of L. Let*

$$A = \{\mathfrak{p} \subset \mathcal{O}_K : \mathfrak{p} \text{ splits completely in } L\}$$

then $\delta(A) = 1/[N:K]$.

Proof. Consider a set A' defined by

$$A' = \{\mathfrak{p} \subset \mathcal{O}_K : \mathfrak{p} \text{ splits completely in } L\},$$

and show that $A = A'$; then conclude by Theorem. □

Definition 12.2.8. *Let A, A' be two subsets of prime ideals in K. We say that $A \overset{p.p.}{=} A$ (almost equal) if $\delta(A\Delta A') = 0$ (e.g. this is satisfied if $A\Delta A'$ is finite).*

Theorem 12.2.9. *(Brauer) Let L_1, L_2 be two Galois extensions of K. Let*

$$S_i := \{\mathfrak{p}|\mathfrak{p} \text{ splits completely in } L_i\}.$$

If $S_1 \overset{p.p.}{=} S_2$, then $L_1 = L_2$.

Proof. Let $L = L_1L_2$. Then L/K is also a Galois extension, and we have shown that $\mathfrak{p}$ splits completely in L if and only if $\mathfrak{p}$ splits completely in L_i, so that

$$S = S_1 \cap S_2.$$

The above theorem implies that

$$\delta(S) = \frac{1}{[L:K]}, \quad \delta(S_i) = \frac{1}{[L_i:K]}.$$

But by assumption $\delta(S) = \delta(S_i)$, so that $[L:K] = [L_i:K]$, and $L_1 = L_2$. □

12.3 Generalization

One may ask the more general question: let L/K be a Galois extension, what is the Dirichlet density of prime ideals in $\mathcal{O}_K$ whose decomposition has the shape (f, g) (we may always ignore the ramified primes which form a finite set): i.e.

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_g, \quad n = fg.$$

The answer is as follows.

Theorem 12.3.1. *Let L/K be a Galois extension of number fields, with degree n. Let (f, g) be a pair such that $n = fg$ and*

$$A = \{\mathfrak{p} \subset \mathcal{O}_K : \mathfrak{p} \text{ has shape } (f, g)\}.$$

Then $\delta(A) = n_f/n$, where

$$n_f = \sharp\{\sigma \in \mathrm{Gal}(L/K) : o(\sigma) = f\}.$$

Example 12.3.2. *Let L/K be a Galois extension with $G \cong \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. Then G contains one element of order 1 (i.e. $f = 1$) and three elements of order 3. Since we could ignore the primes which ramify, the set of primes which completely split has Dirichlet density 1/4, and the set of primes of shape (2,2) (i.e. $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1\mathfrak{P}_2$) has density 3/4. Since there is no element of order 4 in G, the density of the set of inert primes is equal to 0. Indeed, we already noted that for a non-cyclic Galois extension, there is no inert primes!*

12.3.1 Abelian case

We first treat the abelian case. Clearly we are reduced to prove the following result for a given element $\sigma \in G$ of order f.

Theorem 12.3.3. *Let L/K be an abelian extension, For any $\sigma \in \mathrm{Gal}(L/K)$, Let*

$$A(\sigma) = \{\mathfrak{p} \subset \mathcal{O}_K : \mathfrak{p} \text{ unramified in } L, \ \big(\frac{L/K}{\mathfrak{p}}\big) = \sigma\}$$

Then $\delta(A(\sigma)) = 1/[L:K]$.

Example 12.3.4. *We will give another proof of Dirichlet's arithmetic progression theorem, using the above theorem. Take $K=\mathbb{Q}$ and $L=\mathbb{Q}(\zeta_N)$, then*

$$[L:\mathbb{Q}]=\varphi(N),\quad G\cong(\mathbb{Z}/N\mathbb{Z})^\times=\{\sigma_a:(a,N)=1\}.$$

Moreover, if p is unramified in L (i.e. $p\nmid N$), then $(\frac{L/\mathbb{Q}}{p})=\sigma_p$. Hence we obtain

$$(\frac{L/\mathbb{Q}}{p})=\sigma_a\Longleftrightarrow p\equiv a\mod N.$$

By Theorem, we deduce $\delta(A)=1/\varphi(N)$.

Example 12.3.5. *Let p be an odd prime. The set $\{q \text{ prime}|(\frac{q}{p})=1\}$ has density $1/2$.*

The proof uses Artin's L-function. Precisely, analogous to $L(s,\chi)$, for every $\chi:\mathrm{Gal}(L/K)\to\mathbb{C}^\times$, one can define $L(s,\chi,L/K)$ as follows, called Artin's L-function.

Recall the exact sequence $1\to I_\mathfrak{p}\to D_\mathfrak{p}\to\mathrm{Gal}(l/k)\to 1$. Since $\mathrm{Gal}(l/k)$ is cyclic generated by Frobenius automorphism $x\to x^{|k|}$, let $\sigma_\mathfrak{p}$ be a fixed lift so that $\sigma_\mathfrak{p}I_\mathfrak{p}$ is the set of all lifts. When $\mathfrak{p}$ is unramified, $I_\mathfrak{p}=1$ and $\sigma_\mathfrak{p}$ is unique, and we denote it $(\frac{L/K}{\mathfrak{p}})$.

By assumption, L/K is abelian, let $\chi:\mathrm{Gal}(L/K)\to\mathbb{C}^\times$ be a character. If $K=\mathbb{Q}$, we may view it as a Dirichlet character, and hence view it as a function on $\mathbb{N}$, hence a function on the set of integral ideals of $\mathbb{Q}$. In this more general case, we may however define a function χ^* on the set of integral ideals as follows:

$$\chi^*(\mathfrak{p})=\frac{\chi(\sigma_\mathfrak{p})\sum_{\tau\in I_\mathfrak{p}}\chi(\tau)}{e_\mathfrak{p}}=\chi(\sigma_\mathfrak{p})\cdot\langle\chi,\mathbb{1}\rangle_{I_\mathfrak{p}},$$

and extend it to $\chi^*(\mathfrak{a})$ multiplicatively. We have the following properties:

(1) the definition of χ^* does not depend on the choice of $\sigma_\mathfrak{p}$;

(2) If $I_\mathfrak{p}\not\subseteq\ker(\chi)$, then χ is not trivial on $I_\mathfrak{p}$, and $\chi^*(\mathfrak{p})=0$ by Schur orthogonality relation;

(3) If $I_\mathfrak{p}\subset\ker(\chi)$, then $\chi^*(\mathfrak{p})=\chi(\sigma_\mathfrak{p})$. In particular, if $\mathfrak{p}$ is unramified, we have

$$\chi^*(\mathfrak{p})=\chi((\frac{L/K}{\mathfrak{p}})).$$

The character χ^* is an analogue of the primitive character inducing χ in Dirichlet case. As an example, let us assume $K=\mathbb{Q}$ and let $N\ge 1$ be such that $K\subset\mathbb{Q}(\zeta_N)$ and hence view $\chi:G\to\mathbb{C}^\times$ as a Dirichlet character of $(\mathbb{Z}/N\mathbb{Z})^\times$. Let d be the conductor of χ, i.e. χ factors through

$$(\mathbb{Z}/N\mathbb{Z})^\times\twoheadrightarrow(\mathbb{Z}/d\mathbb{Z})^\times\to\mathbb{C}^\times,$$

then $d|N$ and $d=N$ if and only if χ is primitive. Note that if $p\nmid d$, then $\chi(p)=\chi^*(p)$, while if $p|N$ and $p\nmid d$, then

$$\chi(p)=0,\quad\chi^*(p)\neq 0.$$

Let us assume $p|N$ and $p\nmid d$. Then p is unramified in $\mathbb{Q}(\zeta_d)$ but ramified in $\mathbb{Q}(\zeta_N)$. So we see

$$I_p\subset\ker\left((\mathbb{Z}/N\mathbb{Z})^\times\to(\mathbb{Z}/d\mathbb{Z})^\times\right)\subset\ker(\chi),$$

and (3) says that $\chi^*(p) \neq 0$.

As in $K = \mathbb{Q}$ case, we extend χ^* to a function on all integral ideals of K, and define

$$L(s, \chi, L/K) = \sum_{\mathfrak{a}} \frac{\chi^*(\mathfrak{a})}{N(\mathfrak{a})^s}, \quad \Re(s) > 1.$$

We can prove the following facts for $L(s, \chi, L/K)$:

- For $\Re(s) > 1$, $L(s, \chi, L/K)$ converges and extends to the whole plane; it is entire if $\chi \neq \chi_0$.
- $\zeta_L(s) = \prod_{\chi \in \hat{G}} L(s, \chi, L/K) = \zeta_K(s) \prod_{\chi \neq \chi_0} L(s, \chi, L/K)$.

We can now prove Theorem 12.3.3.

Proof. We want to show that

$$\lim_{s \to 1} \frac{\sum_{\mathfrak{p} \in A(\sigma)} N(\mathfrak{p})^{-s}}{\log \zeta_K(s)} = \frac{1}{n}.$$

First we need an expression for the condition $\mathfrak{p} \in A(\sigma)$, i.e. $(\frac{L/K}{\mathfrak{p}}) = \sigma$. Note the identity (for given $\mathfrak{p}$ and $\sigma \in G$)

$$\sum_{\chi \in \widehat{G}} \chi(\sigma^{-1}) \chi\big((\frac{L/K}{\mathfrak{p}})\big) = \begin{cases} n & \mathfrak{p} \in A(\sigma) \\ 0 & \text{else} \end{cases}$$

and that $\chi^*(\mathfrak{p}) = \chi\big((\frac{L/K}{\mathfrak{p}})\big)$ for all unramified $\mathfrak{p}$, we get

$$\sum_{\mathfrak{p} \in A(\sigma)} N(\mathfrak{p})^{-s} = \sum_{\mathfrak{p}} \sum_{\chi \in \widehat{G}} \chi(\sigma^{-1}) \frac{\chi^*(\mathfrak{p})}{N(\mathfrak{p})^s} + O(1).$$

On the other hand, as before, we have (using Euler product formula and Taylor series of log)

$$\log L(s, \chi, L/K) = \sum_{\mathfrak{p}} \sum_{m \geq 1} \frac{\chi^*(\mathfrak{p})^m}{m N(\mathfrak{p})^{ms}} = \sum_{\mathfrak{p}} \frac{\chi^*(\mathfrak{p})}{N(\mathfrak{p})^s} + g(s, \chi)$$

where $\lim_{s \to 1} g(s, \chi)$ exists. Hence

$$T(s) := \frac{1}{n} \sum_{\chi \in \widehat{G}} \chi(\sigma^{-1}) \log L(s, \chi, L/K) = \frac{1}{n} \sum_{\chi \in \widehat{G}} \chi(\sigma^{-1}) \sum_{\mathfrak{p}} \frac{\chi^*(\mathfrak{p})}{N(\mathfrak{p})^s} + O(1) = \sum_{\mathfrak{p} \in A(\sigma)} \frac{1}{N(\mathfrak{p})^s}.$$

However, if $\chi \neq \chi_0$, $L(s, \chi, L/K)$ is holomorphic at $s = 1$, so

$$T(s) = \frac{1}{n} \log \zeta_K(s) + O(1)$$

and the result follows.

$\square$

12.3.2 General case

Theorem 12.3.6. *(Chebatyrev density theorem) Let L/K be a Galois extension of number fields with $G = \mathrm{Gal}(L/K)$. Let C be a conjugacy class in G with $c = |C|$, and*

$$A = \{\mathfrak{p} \subset \mathcal{O}_K | \mathfrak{p} \text{ unramified } (\frac{L/K}{\mathfrak{p}}) = C\}.$$

Then $\delta(A) = c/n$, where $n = [L : K]$.

Here, for $\mathfrak{p}$ unramified, write $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_g$, then the $(\frac{L/K}{\mathfrak{P}_i}) \in G$ lie in the same conjugacy class; we denote this class simply by $(\frac{L/K}{\mathfrak{p}})$.

Proof. Let $\mathfrak{p}$ be unramified. Given a conjugacy class C, and $\sigma \in C$, let $H = \langle\sigma\rangle$ and $M = L^H$, the intermediate field. If $\mathfrak{P} \subset \mathcal{O}_L$ is a prime ideal above $\mathfrak{p}$ such that Frob, let $\mathfrak{q} = \mathfrak{P} \cap \mathcal{O}_M$. Then $D_{\mathfrak{P}} = H$, so that

$$\mathfrak{q}\mathcal{O}_L = \mathfrak{P}, \quad f(\mathfrak{P}/\mathfrak{q}) = |H|, \quad f(\mathfrak{q}/\mathfrak{p}) = 1.$$

In particular, for any such $\mathfrak{q}$, $N(\mathfrak{q}) = N(\mathfrak{p})$ and $(\frac{L/M}{\mathfrak{q}}) = \sigma$.

If we write $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_g$ (unramified), then we claim that there are in total

$$r := [C_G(\sigma) : |H|]$$

primes $\mathfrak{P}_i$ such that $\mathrm{Frob}_{\mathfrak{P}_i} = \sigma$.

Proof: Indeed, assume $\mathfrak{P}_1$ is such a prime (always exists because $\mathrm{Frob}_{\mathfrak{P}_i} \in C$), then for $\mathfrak{P}_i$ let $\tau \in G$ be such that $\mathfrak{P}_i = \tau\mathfrak{P}_1$, then $\mathrm{Frob}_{\mathfrak{P}_i} = \tau\sigma\tau^{-1}$ is equal to σ if and only if $\tau \in C_G(\sigma)$. On the other hand, $\tau\mathfrak{P}_1 = \mathfrak{P}_1$ if and only if $\tau \in D_{\mathfrak{P}_1} = H$. This proves the claim.

Now, we want to estimate $\sum_{\mathfrak{p},(\frac{L/K}{\mathfrak{p}})=C} N(\mathfrak{p})^{-s}$. We fix an element $\sigma \in C$ and there are r prime ideals $\mathfrak{q}$ such that $(\frac{L/M}{\mathfrak{q}}) = \sigma$, so there is a $r : 1$ correspondence between primes $\mathfrak{q} \subset \mathcal{O}_M$ with $(\frac{L/M}{\mathfrak{q}}) = \sigma$ and primes $\mathfrak{p} \subset \mathcal{O}_K$ with $(\frac{L/K}{\mathfrak{p}}) = C$. Hence

$$\sum_{\mathfrak{p},(\frac{L/K}{\mathfrak{p}})=C} N(\mathfrak{p})^{-s} = \frac{1}{r} \sum_{\mathfrak{q},(\frac{L/M}{\mathfrak{q}})=\sigma} N(\mathfrak{q})^{-s}.$$

However, L/M is an abelian extension of degree $|H|$, so

$$\sum_{\mathfrak{q},(\frac{L/M}{\mathfrak{q}})=\sigma} N(\mathfrak{q})^{-s} \sim \frac{1}{|H|} \log \frac{1}{s-1},$$

and therefore

$$\delta(A) = \frac{1}{r} \cdot \frac{1}{|H|} = \frac{1}{|C_G(\sigma)|} = \frac{c}{n}.$$

□

W12: Exercise

Determine the Dirichlet density of the set $\{p | 2 \text{ is cubic residue mod } p\}$.