ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Genus Theory

Student Seminar in Number Theory: L-Functions

Filip Kovacevic, Greg Weiler

November 30, 2021

Organiser: Dr. Markus Schwagenscheidt

Department of Mathematics, ETH Zürich

Contents

Chapter 1

Recapitulations & Preliminaries

Let us begin by recalling some notions necessary for the understanding (and perhaps enjoyment) of the later chapters. Our principal source is [1], mainly chapter 12.

We shall work over an arbitrary quadratic field K, i.e. $K = \mathbb{Q}(\sqrt{d})$ for $d \in \mathbb{Z}$ square-free (w.l.o.g.). Any number $\lambda \in K$ can then be uniquely represented as $\lambda = \alpha + \beta\sqrt{d}$ for $\alpha, \beta \in \mathbb{Q}$. The **conjugate** of λ is defined as $\lambda' := \alpha - \beta\sqrt{d}$. We call $N(\lambda) := \lambda\lambda'$ the **norm** and $tr(\lambda) := \lambda + \lambda'$ the **trace** of λ.

Definition 1.1 (Discriminant of a quadratic Field) *The **discriminant** D of K is defined as*

$$D := \begin{cases} 4d & \text{if } d \equiv 2, 3 \bmod 4, \\ d & \text{if } d \equiv 1 \bmod 4. \end{cases}$$

Definition 1.2 (Characters) *A **character** on a finite group G is a group homomorphism*

$$\chi : G \to \mathbb{C}^\times.$$

*The characters on G form a group $\hat{G}$, the so-called **dual** of G, under pointwise multiplication and inversion. The neutral element of $\hat{G}$ is denoted by χ_0 and called the **principal character**. In other words, χ_0 is a group homomorphism $\chi : G \to \mathbb{C}^\times$ satisfying $\forall g \in G : \chi(g) = 1$.*

*The characters for $m \in \mathbb{Z}_{>0}$, $G = (\mathbb{Z}/m\mathbb{Z})^\times = \{n \pmod m \mid (n, m) = 1\}$ are called **Dirichlet characters of modulus m.***

*A Dirichlet character χ of modulus m is called **primitive** if it cannot be obtained from a Dirichlet character χ' of strictly smaller modulus $m' \mid m$ in the following way:*

$$\chi : (\mathbb{Z}/m\mathbb{Z})^\times \xrightarrow{(\bmod m')} (\mathbb{Z}/m'\mathbb{Z})^\times \xrightarrow{\chi'} \mathbb{C}^\times.$$

Definition 1.3 (Dirichlet L-Series) *Let $s \in \mathbb{C}$ and χ a Dirichlet character of modulus m. Then the **Dirichlet L-series** L corresponding to χ is defined as follows:*

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

For $\sigma := Re(s) > 1$, Dirichlet L-series admit the following ***Euler product*** *representation:*

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

Definition 1.4 (Fundamental Discriminant) *A* ***fundamental discriminant*** *(now in the context of quadratic forms) is an integer D such that one of the following two conditions holds:*

$$D \equiv 1 \ mod\ 4 \ and \ D \ is \ square\text{-}free\ ,$$
$$D = 4m \ for \ m \equiv 2,3 \ mod\ 4 \ and \ m \ square\text{-}free\ .$$

Definition 1.5 (Prime Discriminant) *We call* ***prime discriminant*** *any number in the following list:*

$$-4, 8, -8, p\ (p \equiv 1\ (mod\ 4)\ prime), -p\ (p \equiv 3\ (mod\ 4)\ prime).$$

Fact 1.6 *Every fundamental discriminant D admits a unique decomposition into prime discriminants.*

To each fundamental discriminant D one can associate a primitive Dirichlet character of modulus $|D|$ denoted by χ_D.

If $D = D_1 \dots D_k$ is the decomposition of D into prime discriminants, then $\chi_D = \chi_{D_1} \cdots \chi_{D_k}$.

Definition 1.7 (Discriminant of a binary quadratic Form) *Recall that a* ***binary quadratic form*** *f is a homogeneous polynomial in two variables with integer coefficients, e.g. $f(x,y) = ax^2 + bxy + cy^2$ for $a, b, c \in \mathbb{Z}$.*

If a, b and c are globally coprime, f is called ***primitive****. An arbitrary b.q.f. differs from a primitive b.q.f. by a factor equal to the gcd of its coefficients.*

The ***discriminant*** *D of f is then defined as $D := b^2 - 4ac$.*

Fact 1.8 *A b.q.f. with negative discriminant is either globally positive or globally negative on all non-zero pairs of integers. In the former case, the b.q.f. is called* ***positive definite****, in the latter case it is called* ***negative definite****.*

Definition 1.9 (Class Number) *Recall that two binary quadratic forms f and f' are called* ***equivalent*** *if there exists $A \in SL(2,\mathbb{Z})$ such that for*

$$\begin{pmatrix} x' \\ y' \end{pmatrix} := A \begin{pmatrix} x \\ y \end{pmatrix}$$

it holds that $f'(x,y) = f(x',y')$. This is in fact an equivalence relation on the set of binary quadratic forms.

Recall further that the discriminant D is constant in each equivalence class.

The ***class number*** *$h(D)$ is defined as follows:*

$$h(D) := \begin{cases} the\ nr.\ of\ classes\ of\ primitive\ b.q.f.'s\ of\ discriminant\ D & if\ D > 0, \\ the\ nr.\ of\ classes\ of\ positive\text{-}definite\ primitive\ b.q.f.'s\ of\ discriminant\ D & if\ D < 0. \end{cases}$$

Definition 1.10 (Ring of Integers) *The **ring of integers** of K is defined as the subset of numbers in K that are roots of monic polynomials with integer coefficients. It is denoted in general by $\mathcal{O}_K$. Since we're working over a fixed quadratic field, we simply write $\mathcal{O}$.*

Example 1.11 $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.

Fact 1.12 *Let $\lambda \in K$. Then $\lambda \in \mathcal{O}$ if and only if $N(\lambda) \in \mathbb{Z}$ and $tr(\lambda) \in \mathbb{Z}$.*

Definition 1.13 (Ideals) *An **integral ideal** of $\mathcal{O}$ is a finitely generated additive subgroup $\mathfrak{a}$ of $\mathcal{O}$ such that*

$$\forall \lambda \in \mathcal{O}\ \forall a \in \mathfrak{a} : \lambda a \in \mathfrak{a}, \tag{1.1}$$

or more briefly $\mathcal{O}\mathfrak{a} = \mathfrak{a}$.

*For $0 \neq \xi \in \mathcal{O}$, the integral ideal defined as $(\xi) := \mathcal{O}\xi = \{\lambda\xi \mid \lambda \in \mathcal{O}\}$ is called the **principal ideal** generated by ξ. The brackets for principal ideals may be omitted when confusion is unlikely.*

*A **fractional ideal** of K s a finitely generated additive subgroup $\mathfrak{a}$ of K (instead of $\mathcal{O}$) satisfying (1.1), i.e. $\mathcal{O}\mathfrak{a} \subset \mathfrak{a}$.*

*Note that the definition of an integral ideal is a special case of the definition of a fractional ideal. For this reason, fractional ideals may sometimes be referred to simply as **ideals** (of K).*

*The **conjugate** $\mathfrak{a}'$ of an ideal $\mathfrak{a}$ is defined as $\mathfrak{a}' := \{a' \mid a \in \mathfrak{a}\}$.*

*Given two ideals $\mathfrak{a}$ and $\mathfrak{b}$, we say that $\mathfrak{a}$ **divides** $\mathfrak{b}$ and write $\mathfrak{a} \mid \mathfrak{b}$ if there exists an integral ideal $\mathfrak{c}$ such that $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$.*

*We call **prime ideal** an integral ideal that is only divisible by $\mathcal{O}$ and by itself.*

Fact 1.14 *For every fractional ideal $\mathfrak{a}$, there exists an $n \in \mathbb{Z}_{\geq 0}$ such that $n\mathfrak{a}$ is an integral ideal.*

Fact 1.15 *For $\xi \in K$ and $\mathfrak{a}$ a fractional ideal, we have*

$$\mathfrak{a} \mid (\xi) \iff \xi \in \mathfrak{a}.$$

Fact 1.16 *The ring of integers $\mathcal{O}$ is a so-called **Dedekind domain**, meaning that every non-zero ideal of $\mathcal{O}$ can be uniquely decomposed into a product of prime ideals.*

Recall for $\sigma > 1$ the **Riemann zeta function**:

$$\zeta(s) = \sum_n \frac{1}{n^s} = \prod_p \frac{1}{(1 - p^{-s})}$$

. The above formula stems from the existence of a unique prime factor decomposition of any natural number. Though this property may not hold in general for the numbers of K, it does for its ideals. We therefore formulate the following definition:

Definition 1.17 (Dedekind Zeta Function) *The **Dedekind zeta function** is given by*

$$\zeta_K(s) := \sum_{0 \neq \mathfrak{a}\ ideal\ of\ K} \frac{1}{N(\mathfrak{a})^s}.$$

Definition 1.18 (Norms) *The **norm of a number** $\lambda \in K$ is defined as $N(\lambda) = \lambda\lambda' \in \mathbb{Z}$.*

*The **norm of an integral ideal** $\mathfrak{a}$ is defined as $N(\mathfrak{a}) := [\mathscr{O} : \mathfrak{a}] \in \mathbb{Z}_{\geq 0}$, where we view $\mathscr{O}$ and $\mathfrak{a}$ as Abelian groups.*

*The **norm of a fractional ideal** $\mathfrak{b}$ is defined as $N(\mathfrak{b}) := \frac{1}{n^2}N(n\mathfrak{b}) \in \mathbb{Q}$, where $n \in \mathbb{N}$ is chosen sucht that $n\mathfrak{b}$ is an integral ideal.*

Fact 1.19 *Each of these norms is multiplicative. Further useful properties of the ideal norm include*

$$N((\xi)) = |N(\xi)|,$$

$$(N(\mathfrak{a})) = \mathfrak{a}\mathfrak{a}'.$$

Fact 1.20 *The fractional ideals form a group $\mathfrak{I}$ under multiplication. The existence of inverses is guaranteed by the previous fact via $\mathfrak{a}^{-1} = N(\mathfrak{a})^{-1}\mathfrak{a}'$.*

Definition 1.21 (Equivalence of Ideals) *Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are called **equivalent** if there exists a $0 \neq \xi \in K$ such that*

$$\mathfrak{a} = (\xi)\mathfrak{b}.$$

*If in addition $N(\xi) > 0$, $\mathfrak{a}$ and $\mathfrak{b}$ are called **equivalent in the narrow sense**.*

We shall only use the latter type of equivalence and therefore at times omit to specify "in the narrow sense".

Definition 1.22 (Ideal Class Group) *We call **ideal class group** and denote by C the abelian group formed by the set of equivalence classes of ideals. In other words, the ideal class group is defined as the quotient*

$$C := \mathfrak{I}/\mathfrak{P},$$

where $\mathfrak{I}$ denotes the group of ideals and $\mathfrak{P}$ denotes its subgroup formed by the principal ideals.

Fact 1.23 *For a fundamental discriminant $0 < D \neq 1$ and $d = D$, there is a bijective correspondence between the equivalence classes of binary quadratic forms of discriminant D and the equivalence classes (in the narrow sense) of ideals of K. For $D < 0$, the same holds for positive-definite binary quadratic forms.*

In particular, $|C| = h(D)$.

Definition 1.24 (Ideal Class Character) *The characters of C are called **ideal class characters**. Equivalently, an **ideal class character** is a complex-valued function χ on the ideals of K such that:*

1. *$\chi(\mathfrak{a}\mathfrak{b}) = \chi(\mathfrak{a})\chi(\mathfrak{b})$ for all ideals $\mathfrak{a}, \mathfrak{b}$,*
2. *$\chi((\lambda)) = 1$ for all $\lambda \in K$ with $N(\lambda) > 0$.*

To each idea class character χ, we associate an L-series, namely

$$L_K(s,\chi) := \sum_{0\neq\mathfrak{a}\ principal} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s}.$$

By multiplicativity of χ, its Euler product representation is given by

$$L_K(s,\chi) = \prod_{\mathfrak{p}\ prime} (1-\frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s})^{-1}.$$

Definition 1.25 (Inert, ramified, split Primes) *Let $p \in \mathbb{Z}$ be a prime number.*

*If $(p) = \mathfrak{p}$ for $\mathfrak{p}$ a prime ideal with $N(\mathfrak{p}) = p^2$, we call p **inert**.*

*If $(p) = \mathfrak{p}^2$ for $\mathfrak{p}$ a prime ideal with $N(\mathfrak{p}) = p$, we call p **ramified**.*

*If $(p) = \mathfrak{p}_1\mathfrak{p}_2$ for $\mathfrak{p}_1 \neq \mathfrak{p}_2$ prime ideals with $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p$, we call p **split**.*

Fact 1.26 *Let $p \in \mathbb{Z}$ be a prime number. Then the decomposition of (p) into prime ideals happens along the following three cases:*

1. $(p) = \mathfrak{p}\mathfrak{p}' \iff \chi_D(p) = 1$,
2. $(p) = \mathfrak{p}^2 \iff \chi_D(p) = 0$,
3. $(p) = \mathfrak{p} \iff \chi_D(p) = -1$.

Furthermore, the Dedekind zeta function admits the decomposition

$$\zeta_K(s) = \zeta(s)L(s,\chi_D).$$

Chapter 2

Definitions and first Results

Even with knowledge of the elegant correspondence between classes of binary quadratic forms of discriminant D and classes of ideals from fact 1.23, the study of $h(D)$ remains highly complicated.

It was (of course) Gauss who discovered a different approach to this issue. When considering binary quadratic forms under *rational* equivalence, namely by requiring only $A \in SL(2,\mathbb{Q})$ instead of $A \in SL(2,\mathbb{Z})$ in definition 1.9, one can precisely determine the number of rational equivalence classes, say $h_{\mathbb{Q}}(D)$.

Gauss called the rational equivalence classes of binary quadratic forms *genera* and determined their number $h_{\mathbb{Q}}(D)$ to be exactly equal to 2^{t-1}, where t denotes the number of factors in the decomposition of D into prime discriminants. As we shall see in chapter 3, this result also holds insightful implications for $h(D)$.

Note that rational equivalence is truly weaker than the usual "integer" equivalence. Indeed, consider for $D = -23$ the b.q.f.'s

$$f(x,y) := x^2 + xy + 6y^2, \qquad g(x,y) := 2x^2 + xy + 3y^2.$$

Then f and g are rationally equivalent via

$$A := \begin{pmatrix} 1/2 & 1/2 \\ -3/2 & 1/2 \end{pmatrix},$$

they can however not be equivalent in the usual sense, since f evaluates to 1 for $(x,y) = (1,0)$ whereas for all pairs of integers $(x,y) \neq (0,0)$, one has

$$g(x,y) = 2(x + \frac{1}{4}y)^2 + \frac{23}{8}y^2 > 1.$$

Our path towards Gauss' results shall however differ slightly from the one laid out above: remembering the correspondence between classes of binary quadratic forms of discriminant D and classes of ideals, we shall define genera on the set of ideal classes instead of working on the set of binary quadratic forms.

To our great delight, both definitions shall turn out to be equivalent in the following sense: genera of ideal classes will correspond to rational equivalence classes of b.q.f.'s,

while ideal classes will correspond to integer equivalence classes of b.q.f.'s (see remark 2.11).

Let now K be a quadratic field (as before) and C its group of ideal classes (in the narrow sense).

Definition 2.1 (Genus Character) *We call **genus characters** the $\{\pm 1\}$-valued characters of C, i.e. the group homomorphisms*

$$\chi : C \to \{\pm 1\}.$$

The genus characters form a subgroup of the dual $\hat{C}$ of C.

Definition 2.2 (Genus) *We say that two ideal classes A_1 and A_2 belong to the same **genus** if for all genus characters χ it holds*

$$\chi(A_1) = \chi(A_2).$$

Proposition 2.3 *(Equivalent Characterisation, Part 1)*
If two ideal classes in C differ by a square in C, they belong to the same genus.

Proof. For a character χ, note that:

$$\begin{aligned}\chi(C) \subset \{\pm 1\} &\iff \forall A \in C : \chi(A)^2 = 1 \\ &\iff \forall A \in C : \chi(A^2) = 1 \\ &\iff \forall A_1, A_2 \in C : \chi(A_1 A_2^2) = \chi(A_1),\end{aligned}$$

where the first formula is simply the definition of genus character and the final formula states that for arbitrary ideal classes A_1, A_2 from C, A_1 and $A_1 A_2^2$ belong to the same genus. □

Proposition 2.4 *(Group of Genus Characters)*
Let C^2 denote the subgroup $\{A^2 \mid A \in C\}$ of C. The group formed by the genus characters is isomorphic to $\widehat{C/C^2}$.

Proof. We want to show that $\widehat{C/C^2} = \{\bar{\chi} : C/C^2 \to \mathbb{C}^\times\}$ (where $\bar{\chi}$ is understood to be a group homomorphism) is isomorphic to the group of genus characters.

Note first that $\widehat{C/C^2} = \{\bar{\chi} : C/C^2 \to \{\pm 1\}\}$.

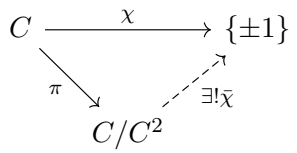
Indeed, $B \in C/C^2 \implies ord(B) \leq 2$. Clearly, $ord(B) = 1 \implies \bar{\chi}(B) = 1$. On the other hand, for $ord(B) = 2$, $1 = \bar{\chi}(B^2) = \bar{\chi}(B)^2 \implies \bar{\chi}(B) \in \{\pm 1\}$.

Recall now from the proof of proposition 2.3 that for a character χ,

$$\chi(C) \subset \{\pm 1\} \iff \forall A \in C : \chi(A^2) = 1.$$

Equivalently, χ is a genus character if and only if $C^2 \subset Ker(\chi)$).

We thus obtain the desired isomorphism between $\widehat{C/C^2}$ and the group of genus characters via the universal property of the factor group, i.e. for every χ there exists exactly one $\bar{\chi}$ such that the following diagram commutes:



This concludes the proof. □

Proposition 2.5 *(Equivalent Characterisation, Part 2) If two ideal classes in C belong to the same genus, then they differ by a square in C (i.e. the converse of proposition 2.3 is true).*

Proof. Let A_1, A_2 be ideal classes in the same genus, i.e. $\chi(A_1) = \chi(A_2)$ for every genus character χ. We want to show the existence of a $B \in C$ such that $A_1 = A_2 B^2$.

Dividing both sides of these equations by $\chi(A_2)$ respectively A_2 and writing $A := A_1/A_2$, this reduces to proving the following:

$$\chi(A) = 1 \text{ for every genus character } \chi \implies A \text{ is a square in } C.$$

Identifying the group of genus characters with $\widehat{C/C^2}$ using the isomorphism from the previous proposition, consider the sum

$$\sum_{\bar{\chi} \in \widehat{C/C^2}} \bar{\chi}(A).$$

By assumption, the genus character χ corresponding to $\bar{\chi}$ takes the value 1 on A, so each summand must be equal to 1. In particular, the sum does not vanish.

However, character orthogonality implies that the sum vanishes unless A is neutral in C/C^2, i.e. if A is a square.

□

Corollary 2.6 *(Equivalent Characterisation) Two ideal classes $A_1, A_2 \in C$ belong to the same genus if and only if A_1 and A_2 differ by a square in C.*

Proposition 2.7 *(Genus Group)*
The genera form a group isomorphic to C/C^2 which we call the ***genus group****.*

Proof. By the multiplicativity of characters, the group operation on C descends to the set of genera. The existence of an isomorphism between the genus group and C/C^2 follows from corollary 2.6. □

Recall that finite abelian groups are isomorphic to their dual, that C is abelian and that $|C| = h(D) < \infty$. We therefore find that $C/C^2 \cong \widehat{C/C^2}$.

By the preceding propositions, the dual of the genus group is thus isomorphic to the group of genus characters. Furthermore, the number of genera is equal to the number of genus characters. Since C/C^2 is a finite abelian group of index 2, this number is a power of 2 by the structure theorem for finitely generated abelian groups. This idea will be developed further in the proof of corollary 3.3.

Let us now turn to a closer investigation of the genus group.

Definition 2.8 (Principal Genus) *The unit of the genus group is called the* ***principal genus****.*

Remark 2.9 *From corollary 2.6, it follows that the principal genus is formed by the squares of ideal classes. More precisely, by the definition of equivalence, an ideal* $\mathfrak{a}$ *belongs to the principal genus if and only if* $\mathfrak{a} = (\lambda)\mathfrak{b}^2$ *for an ideal* $\mathfrak{b}$ *and a* $\lambda \in K$ *with* $N(\lambda) > 0$*.*

The following theorem is an attempt to highlight the naturality of the at first perhaps artificial notion of genera.

Theorem 2.10 *("Naturality" of the Definition of Genus)*

(i) Two fractional ideals $\mathfrak{a}$ *and* $\mathfrak{b}$ *are in the same genus if and only if there exists a* $\lambda \in K$ *with* $N(\lambda) > 0$ *such that*

$$N(\mathfrak{a}) = N(\lambda)N(\mathfrak{b}). \tag{2.1}$$

(ii) A natural number n *is the norm of a number* $\lambda \in K$ *if and only if it is the norm of an integral ideal from the principal genus.*

Proof. Ad (i):

Ad "⇒": Let first $\mathfrak{a}$ and $\mathfrak{b}$ be ideals in the same genus. Using the definition of equivalence as in remark 2.9 along with corollary 2.6, we deduce the existence of an ideal $\mathfrak{c}$ and a number $\mu \in K$ with $N(\mu) > 0$ such that

$$\mathfrak{a} = (\mu)\mathfrak{c}^2\mathfrak{b}.$$

Using known properties of the norm from fact 1.19, we find

$$N(\mathfrak{a}) = |N(\mu)|N(\mathfrak{c})^2N(\mathfrak{b}).$$

Note that by definition of the norm, $N(\mathfrak{c}) \neq 0$ and thus $N(\mu)N(\mathfrak{c})^2 > 0$. Furthermore, since $N(\mathfrak{c}) \in \mathbb{Q}$, we have that $0 < N(\mathfrak{c})^2 = N(\mathfrak{c})N(\mathfrak{c})' = N(N(\mathfrak{c})) = N((N(\mathfrak{c})))$.

Using the multiplicativity of the norm for ideals and the properties of principal ideal multiplication, we may therefore rewrite the factor $N(\mu)N(\mathfrak{c})^2$ as

$$0 < N((\mu))N((N(\mathfrak{c}))) = N((\mu)(N(\mathfrak{c}))) = N((\mu N(\mathfrak{c}))) = |N(\mu N(\mathfrak{c}))| = N(\mu N(\mathfrak{c})).$$

Thus $N(\mathfrak{a}) = N(\mu N(\mathfrak{c}))N(\mathfrak{b})$, in other words (2.1) holds with $\lambda = \mu N(\mathfrak{c})$.

Ad "$\Leftarrow$": Assume now that (2.1) holds for two ideals $\mathfrak{a}$ and $\mathfrak{b}$. Our goal is to show that $\mathfrak{a}$ belongs to the genus of $\mathfrak{b}$.

Note that by dividing by $N(\mathfrak{b})$ on both sides, we may w.l.o.g. replace $\mathfrak{a}$ by $\mathfrak{a}\mathfrak{b}^{-1}$. It is therefore enough to show

$$N(\mathfrak{a}) = N(\lambda),\ \lambda \in K,\ N(\lambda) > 0 \implies \mathfrak{a} \text{ lies in the principal genus.} \tag{2.2}$$

Applying the same trick again, now for $N(\lambda)$ instead of $N(\mathfrak{b})$, we may replace $\mathfrak{a}$ by $(\lambda^{-1})\mathfrak{a}$ and thus assume that $\lambda = 1$, i.e. $N(\mathfrak{a}) = 1$ in (2.2).

We now claim the following:

$$N(\mathfrak{a}) = 1 \implies \text{there exists an integral ideal } \mathfrak{b} \text{ s.t. } \mathfrak{a} = \mathfrak{b}/\mathfrak{b}' \tag{2.3}$$

(recall that $\mathfrak{b}' = \{b' \mid b \in \mathfrak{b}\}$ denotes the conjugate ideal of $\mathfrak{b}$).

This claim implies (2.2). Indeed, using fact 1.19, in particular that $\mathfrak{b}\mathfrak{b}' = (N(\mathfrak{b}))$, it follows from remark 2.9 that

$$\mathfrak{a} = (N(\mathfrak{b})^{-1})\mathfrak{b}^2$$

lies in the principle genus (as we already calculated for $\mathfrak{c}$ in the first part of the proof, $N(N(\mathfrak{b})^{-1}) = N(\mathfrak{b}^{-1})N(\mathfrak{b}^{-1})' = N(\mathfrak{b}^{-1})^2 > 0$).

Let us now prove claim (2.3). Consider the unique factorisation of $\mathfrak{a}$ into prime ideals. As recalled in fact 1.26, there are three kinds of prime factors:

1. $\mathfrak{p}_i$ with $\mathfrak{p}_i \neq \mathfrak{p}_i'$ and $N(\mathfrak{p}_i) = p_i$ for a split prime p_i,
2. $\mathfrak{q}_j$ with $\mathfrak{q}_j = \mathfrak{q}_j'$ and $N(\mathfrak{q}_j) = q_j^{k_j}$ for $k_j = 1$ and a ramified prime q_j,
3. $\mathfrak{q}_j$ with $\mathfrak{q}_j = \mathfrak{q}_j'$ and $N(\mathfrak{q}_j) = q_j^{k_j}$ for $k_j = 2$ and an inert prime q_j.

Keeping these three options in mind, we write

$$\mathfrak{a} = (\prod_i {\mathfrak{p}_i}^{a_i} {\mathfrak{p}_i'}^{b_i})(\prod_j {\mathfrak{q}_j}^{c_j}) \text{ for } a_i, b_i, c_i \in \mathbb{Z}.$$

Taking the norm on both sides, we obtain $1 = N(\mathfrak{a}) = \prod_i p_i^{a_i+b_i} \prod_j q_j^{k_j c_j}$. Since prime factorisation in $\mathbb{Q}$ is unique, this implies that $a_i + b_i = 0$ for all i and $c_j = 0$ for all j. Setting

$$\mathfrak{b} := \prod_{a_i>0} {\mathfrak{p}_i}^{a_i} \prod_{b_i>0} {\mathfrak{p}_i'}^{b_i}$$

then yields (substituting $\tilde{a_i} := a_i - b_i$):

$$\mathfrak{b}/\mathfrak{b}' = \frac{\prod_{a_i>0} {\mathfrak{p}_i}^{a_i} \prod_{b_i>0} {\mathfrak{p}_i'}^{b_i}}{\prod_{a_i>0} {\mathfrak{p}_i'}^{a_i} \prod_{b_i>0} {\mathfrak{p}_i}^{b_i}} = \prod_{\tilde{a_i}+\tilde{b_i}=0} {\mathfrak{p}_i}^{\tilde{a_i}} {\mathfrak{p}_i'}^{\tilde{b_i}} = \mathfrak{a},$$

which is precisely claim (2.3) and therefore concludes the proof of (i).

Ad (ii):

Ad "$\Leftarrow$": Let $\mathfrak{a}$ be an integral ideal in the principal genus and assume that $n = N(\mathfrak{a})$. Since (1) lies in the principal genus (e.g. by remark (2.9)), we may plug $\mathfrak{b} = (1)$ into (2.1), which yields $n = N(\mathfrak{a}) = N(\lambda)N((1)) = N(\lambda)$.

Ad "$\Rightarrow$": Assume now that there exists a $\lambda \in K$ with $n = N(\lambda)$. By separating the prime ideals of positive and negative exponents in its prime ideal decomposition, write (λ) as $\mathfrak{a}/\mathfrak{b}$ for coprime integral ideals $\mathfrak{a}$ and $\mathfrak{b}$ (meaning $(\mathfrak{a}, \mathfrak{b}) = (1)$, where $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$, see also definition 1.13). From $n = |N(\lambda)| = N(\mathfrak{a}/\mathfrak{b}) = N(\mathfrak{a})/N(\mathfrak{b})$ we deduce $N(\mathfrak{b}) \mid N(\mathfrak{a})$.

We finally claim the following:

$$\exists \mathfrak{c} \text{ integral} : \mathfrak{a} = \mathfrak{b}'\mathfrak{c} \text{ (i.e. } \mathfrak{b}' \mid \mathfrak{a}). \tag{2.4}$$

Note that this implies "$\Rightarrow$". Indeed, we find using claim (2.4) that

$$n = N(\lambda) = N(\mathfrak{a}/\mathfrak{b}) = N(\mathfrak{b}'\mathfrak{c}/\mathfrak{b}) = N(\mathfrak{b}')/N(\mathfrak{b})N(\mathfrak{c}) = N(\mathfrak{c}),$$

where we used that $N(\mathfrak{b}') = \mathfrak{b}'\mathfrak{b} = \mathfrak{b}\mathfrak{b}' = N(\mathfrak{b})$. A simple application of (2.2) then yields that $\mathfrak{c}$ lies in the principal genus.

Let us now prove claim (2.4) and thereby theorem 2.10. By the same argument and with the same notation as in the proof of claim (2.3), we can write

$$\mathfrak{b} = (\prod_i \mathfrak{p}_i{}^{a_i}\mathfrak{p}_i'^{b_i})(\prod_j \mathfrak{q}_j{}^{c_j}) \text{ for } a_i, b_i, c_i \in \mathbb{Z}_{\geq 0},$$

now with non-negative powers by definition of $\mathfrak{b}$. Taking the norm, we find $N(\mathfrak{b}) = \prod_i p_i^{a_i+b_i} \prod_j q_j^{k_j c_j}$ with $k_j \in \{1, 2\}$. Since $N(\mathfrak{b}) \mid N(\mathfrak{a})$ and since $\mathfrak{q}_\mathfrak{j}{}^{c_j}$ is the only ideal with norm $q_j^{k_j c_j}$, we must have $\mathfrak{q}_\mathfrak{j}{}^{c_j} \mid \mathfrak{a}$ for every j. From $(\mathfrak{a}, \mathfrak{b}) = (1)$, it then follows that $c_j = 0$ for every j.

Analogously, we cannot have $a_i > 0$ and $b_i > 0$ at the same time, i.e. at least one of them must be 0 for every i. Consider w.l.o.g. the case $a_i > 0$: again, $N(\mathfrak{b}) \mid N(\mathfrak{a})$ implies that $p_i^{a_i} \mid N(\mathfrak{a})$. Since $(\mathfrak{a}, \mathfrak{b}) = (1)$, we must therefore have that $\mathfrak{p}_i'^{a_i}$ appears in the prime ideal decomposition of $\mathfrak{a}$. Repeating this argument for every i yields $\mathfrak{b}' \mid \mathfrak{a}$, i.e. claim (2.4).

□

Remark 2.11 *It can be shown using theorem 2.10 that two ideal classes belong to the same genus if and only if the corresponding quadratic forms are rationally equivalent, i.e. via a matrix in $SL(2, \mathbb{Q})$.*

Remark 2.12 *Theorem 2.10 highlights the difference between ideal classes and genera. Indeed, for ideals $\mathfrak{a}, \mathfrak{b}$, we find the following:*

$$\begin{aligned} \mathfrak{a}, \mathfrak{b} \textit{ in the same ideal class} &\iff \mathfrak{a} = (\lambda)\mathfrak{b}, N(\lambda) > 0, \\ \mathfrak{a}, \mathfrak{b} \textit{ in the same genus} &\iff N(\mathfrak{a}) = N((\lambda)\mathfrak{b}), N(\lambda) > 0, \end{aligned}$$

where the first equivalence is simply the definition of a (narrow) ideal class and the second follows immediately from (i) in theorem 2.10 using known properties of the norm.

For $n \in \mathbb{N}$, we further find:

$$\begin{aligned} n = N(\mathfrak{a}),\ \mathfrak{a}\ \textit{principal},\ \mathfrak{a} \in \textit{principal ideal class} \quad &\Longleftrightarrow \quad n = N(\lambda), \lambda \in \mathscr{O}, \\ n = N(\mathfrak{a}),\ \mathfrak{a}\ \textit{principal},\ \mathfrak{a} \in \textit{principal genus} \quad &\Longleftrightarrow \quad n = N(\lambda), \lambda \in K, \end{aligned}$$

where the first equivalence is a rephrasing of the definition of a principal ideal, and the second is just (ii) from theorem 2.10.

Let us now gently conclude this chapter with a small addendum to theorem 2.10.

Proposition 2.13 *(2.3 for numbers)*
The following holds:

$$\lambda \in K,\ N(\lambda) = 1 \implies \exists \mu \in \mathscr{O} : \lambda = \mu/\mu'. \tag{2.5}$$

Proof. If $\lambda = -1$, define $\mu := \sqrt{d}$. Then $\mu \in \mathscr{O}$ since it solves $x^2 - d$, and $\mu/\mu' = \sqrt{d}/-\sqrt{d} = -1$.

Otherwise, pick $\mu_0 := \lambda + 1 \neq 0$ and note that $N(\mu_0) = \lambda + \lambda' + 2 = tr(\mu_0) \in \mathbb{Q}$. Pick $m \in \mathbb{Z}$ such that $m(\lambda + \lambda' + 2) \in \mathbb{Z}$ and define $\mu := m\mu_0$. By fact 1.12, $N(\mu) = m^2 N(\mu_0) \in \mathbb{Z}$ and $tr(\mu) = m \cdot tr(\mu_0) \in \mathbb{Z}$ imply that $\mu \in \mathscr{O}$. Finally, note that

$$\lambda\mu' = \lambda m\mu_0' = m\lambda(\lambda' + 1) = m(N(\lambda) + \lambda) = m(1 + \lambda) = m\mu_0 = \mu,$$

i.e. $\lambda = \mu/\mu'$. □

Having established our basic genus-theoretic approach to the matter at hand, we shall now proceed to the previously foreshadowed results of Gauss. In chapter 3, an elegant classification of genus characters will yield these and more.

Chapter 3

Classification of genus Characters

In this chapter, we denote the L-series $L(s, \chi_D)$ by $L_D(s)$. In particular, for $D = 1$, $\chi_D = \chi_0$ and we obtain $L_D(s) = \zeta(s)$. For $D \neq 1$ the discriminant of a quadratic field K, we write

$$\zeta_K(s) = \zeta(s)L_D(s). \tag{3.1}$$

Theorem 3.1 *Let D be the discriminant of a quadratic field K. There is a bijective correspondence between the genus characters of K and the partitions $D = D' \cdot D''$ of D into a product of two fundamental discriminants (up to commutation and including the partition $D = 1 \cdot D$).*

In particular, the genus character corresponding to the partition $D = D' \cdot D''$ is given for prime ideals $\mathfrak{p}$ by

$$\chi(\mathfrak{p}) = \begin{cases} \chi_{D'}(N(\mathfrak{p})), if(N(\mathfrak{p}), D') = 1, \\ \chi_{D''}(N(\mathfrak{p})), if(N(\mathfrak{p}), D'') = 1, \end{cases} \tag{3.2}$$

and for arbitrary ideals $\mathfrak{a} = \mathfrak{p}_1^{n_1} \dots \mathfrak{p}_k^{n_k}$ by

$$\chi(\mathfrak{a}) = \chi(\mathfrak{p}_1)^{n_1} \dots \chi(\mathfrak{p}_k)^{n_k}, \tag{3.3}$$

where $\mathfrak{p}_i$ are prime ideals and $n_i \in \mathbb{Z}$ for $1 \leq i \leq k$.

Furthermore, the L-series of χ is given by

$$L_K(s, \chi) = L_{D'}(s)L_{D''}(s). \tag{3.4}$$

Remark 3.2 *For the trivial partition $D' = 1$, $D'' = D$, one obtains $\chi = \chi_0$, thus (3.4) reduces to (3.1), in particular $L_K(s, \chi) = \zeta_K(s)$.*

First, we'll state a corollary of the theorem, which gives us more insight on the class number, based on the nature of the discriminant.

Corollary 3.3 *Let t be the number of prime discriminants in the decomposition of D. Then the group C/C^2 is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{t-1}$. In particular, $2^{t-1} \mid h(D)$ and $h(D)$ is odd if and only if D is a prime discriminant.*

Proof. (Corollary 3.3) Let $D = D_1 \dots D_t$ be the decomposition of D to prime discriminants. We then have 2^{t-1} total number of different decompositions $D = D' \cdot D''$, since that is the number of decompositions of a set $\{D_1, \dots D_t\}$ as a disjoint union of two subsets. On the other hand, we know that the number of genus characters is equal to the order of the group $|C/C^2|$, which is equal to the number of decompositions of D to prime disciminants, according to the theorem (3.1). Now, since C/C^2 is Abelian, and of exponent 2, we can conclude that it is isomorphic to the group $(\mathbb{Z}/2\mathbb{Z})^r$ and since $|C/C^2| = 2^{t-1}$ we can conclude that $r = t - 1$. Furthermore, as we have that $|C/C^2| = |C|/|C^2|$ and $|C| = h(D)$ we can see that $h(D) = 2^{t-1}|C^2|$ which gives us that $2^{t-1} \mid h(D)$. This gives us the first direction of the equivalence, notably:

$$h(D) \text{ odd } \implies t = 1$$

The other direction follows from the fact that if D is a prime discriminant it implies $t = 1$, which in turn gives us $|C| = |C^2| \implies C = C^2$. However, it cannot be that $2 \mid C$ since then, using the structure theorem we would get $C \cong \mathbb{Z}_{2^k} \times G$, for some natural number $k > 0$ and Abelian group G. Then the element $(1, 0) \neq 2k$ for any $k \in C$, so $(1, 0) \notin C^2$, which would be a contradiction. Finally, we have:

$$t = 1 \iff 2 \nmid h(D) \tag{3.5}$$

which is the final claim in the corollary.

□

Proof. (Theorem 3.1)

To make the proof more clear, it will be broken down into 4 parts:

i) χ is a well defined genus character determined by equations (3.2) and (3.3).

ii) For every χ the equation (3.4) holds.

iii) There are 2^{t-1} different genus characters constructed in this way, where t denotes the number of prime discriminants in the decomposition of D.

iv) There do not exist any other genus characters other than the ones constructed.

i) Firstly, we check that χ is well defined as a function. When $\mathfrak{p}$ is a prime ideal , we know that $N(\mathfrak{p})$ (further denoted with $N\mathfrak{p}$) is a power of a prime and $(D', D'') = 1$. . We have that it holds:

$$(N\mathfrak{p}, D') = 1 \vee (N\mathfrak{p}, D'') = 1$$

Now if it holds that $(N\mathfrak{p}, D') = 1$ and $(N\mathfrak{p}, D'') = 1$, we need to verify that $\chi_{D'}(N\mathfrak{p}) = \chi_{D''}(N\mathfrak{p})$, or equivalently $\chi_{D'}(N(\mathfrak{p})) \cdot \chi_{D''}(N\mathfrak{p}) = 1$. We also have that

$$(N\mathfrak{p}, D') = 1 \wedge (N\mathfrak{p}, D'') = 1 \Rightarrow (N\mathfrak{p}, D) = 1$$

Using the theorem 1 from chapter 11 in [1] we have 2 possibilities: either $N\mathfrak{p} = p^2$ with $\chi_D(p) = -1$, or $N\mathfrak{p} = p$ with $\chi_D(p) = 1$. In the first case, we have that (using multiplicativity of the character)

$$\chi_{D'}(N\mathfrak{p}) = \chi_{D'}(p^2) = \chi_{D'}(p)^2 = 1 = \chi_{D''}(N\mathfrak{p})$$

In the second case, we have that (using the multiplicativity of the Legendre symbol)

$$\chi_{D'}(N\mathfrak{p})\chi_{D''}(N\mathfrak{p}) = \chi_{D'}(p)\chi_{D''}(p) = \chi_D(p) = 1$$

Now we have proven that χ is a well-defined function, so it's left to prove that it indeed is a genus character. Since from equations (3.2) and (3.3) we can clearly see that it is multiplicative with the codomain of ± 1, only thing that is left to show is that it sends the neutral element of the ideal class group to the neutral element of $\{\pm 1\}$. More precisely, we want:

$$\chi(\,(\lambda)\,) = 1, (\lambda \in K, N(\lambda) > 0) \tag{3.6}$$

Firstly we will prove (3.6) only for the λ such that $N(\lambda)$ is coprime with D' (or equivalently D''). Using (3.2) We have that $\chi(\,(\lambda)\,) = \chi_{D'}(N(\lambda))$. Let $D' = \prod_i D_i$ be the decomposition of the fundamental discriminant to prime discriminants (which is unique). Since we have that $\chi_{D'} = \prod_i \chi_{D_i}$, it is sufficient to show that

$$\chi_{D_i}(N(\lambda)) = 1$$

We will break this down to cases depending on D_i; either $D_i = \pm p = 1 (\text{mod } 4)$ where p is prime, or $D_i = -4$, 8 or -8. In the first case, we have:

$$\lambda = \frac{a + b\sqrt{D}}{2}, \ (a, b \in \mathbb{Z} \text{ of same parity})$$

$$4N(\lambda) = 4 \cdot \frac{a^2 - b^2 D}{4} = a^2 (\text{mod } p), \text{where } p \nmid a \text{ since } N(\lambda) \text{ coprime with D'},$$

therefore,

$$\chi_{D_i}(4N(\lambda)) = \chi_{D_i}(a^2) = 1, \text{ since } \chi_{D_i}(4) = 1 \text{ we have that } \chi_{D_i}(N(\lambda)) = 1$$

In the other case, where $D_i = 4$, or respectively 8, -8, we can write D as $4d$ with $d = 3 \,(\text{mod } 4)$, respectively $d = 2 \,(\text{mod } 8)$, $d = 6 \,(\text{mod } 8)$. Then we get:

$$\begin{aligned} D_i = -4 &\Rightarrow N(\lambda) = m^2 - n^2 d, d = 3 \,(\text{mod } 4) \\ &\Rightarrow N(\lambda) = 0, 1, 2 \,(\text{mod } 4) \\ &\Rightarrow N(\lambda) = 1 \,(\text{mod } 4) \\ &\Rightarrow \chi_{-4}(N(\lambda)) = 1 \end{aligned}$$

$$\begin{aligned} D_i = 8 &\Rightarrow N(\lambda) = m^2 - n^2 d, d = 2 \,(\text{mod } 8) \\ &\Rightarrow N(\lambda) = 0, 1, 2, 4, 6, 7 \,(\text{mod } 4) \\ &\Rightarrow N(\lambda) = 1, 7 \,(\text{mod } 4) \\ &\Rightarrow N(\lambda) = 0 \,(\text{mod } 4) \\ &\Rightarrow \chi_8(N(\lambda)) = 1 \end{aligned}$$

$$\begin{aligned} D_i = -8 \Rightarrow N(\lambda) &= m^2 - n^2 d, d = 6 \,(\text{mod } 8) \\ &\Rightarrow N(\lambda) = 0, 1, 2, 3, 4, 6 \,(\text{mod } 8) \\ &\Rightarrow N(\lambda) = 1, 3 \,(\text{mod } 4) \\ &\Rightarrow N(\lambda) = 0 \,(\text{mod } 4) \\ &\Rightarrow \chi_{-8}(N(\lambda)) = 1 \end{aligned}$$

Note that $2 \nmid N(\lambda)$ was used here, due to the $N(\lambda)$ being coprime with D'. Now we can take λ to be an arbitrary element of $\mathscr{O}$, and write:

$$(\lambda) = \mathfrak{p}_1 \dots \mathfrak{p}_r \mathfrak{b}$$

where $\mathfrak{p}_i$ are prime ideals that divide D and $\mathfrak{b}$ is coprime with D. For every i we can find an ideal $\mathfrak{a}_i$ in the idealclass of $\mathfrak{p}_i^{-1}$ such that it is coprime with D. Now for every i we have that $\mathfrak{a}_i\mathfrak{p}_i$ is a principle ideal that is coprime with either D' or D'' (since every prime factor of D can show up only in either D' or D'', but not both). Using previosly proven case, we get:

$$\chi(\mathfrak{a}_i\mathfrak{p}_i) = 1, \text{ for every i}$$

Now we can write out

$$(\lambda) = (\mathfrak{p}_1\mathfrak{a}_1) \dots (\mathfrak{p}_r\mathfrak{a}_r)(\mathfrak{b}\mathfrak{p}_1^{-1} \dots \mathfrak{p}_r^{-1})$$

where $(\mathfrak{b}\mathfrak{p}_1^{-1} \dots \mathfrak{p}_r^{-1})$ is also a principle ideal coprime with D (as it is a product of ideals coprime with D) which lastly gives us

$$\chi((\mathfrak{b}\mathfrak{p}_1^{-1} \dots \mathfrak{p}_r^{-1})) = 1$$

This gives us

$$\chi((\lambda)) = 1$$

which is what we set out to prove.

ii) Writing out $L_K(s, \chi)$ with the Euler product, we get:

$$L_K(s,\chi) = \prod_{\mathfrak{p}} \left(1 - \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}\right)^{-1} = \prod_{p} \prod_{\mathfrak{p}|p} \left(1 - \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}\right)^{-1} \tag{3.7}$$

where the first product is over all rational prime numbers p, and the second one over all prime ideals $\mathfrak{p}$ that devide p. On the other hand we have that the Euler product of $L_{D'}$ and $L_{D''}$ gives:

$$L_{D'}(s)L_{D''}(s) = \prod_{p} \left(1 - \frac{\chi_{D'}(p)}{p^s}\right)^{-1} \left(1 - \frac{\chi_{D''}(p)}{p^s}\right)^{-1} \tag{3.8}$$

It will be shown that all the corresponding factors in the product in (3.7) and (3.8) are the equal. We break this proof down to 3 cases, based on the theorem 1, chapter 11 from [1]:

Case 1: $\chi_D(p) = 1, p = \mathfrak{p}\mathfrak{p}'$ where we have $\mathfrak{p}$ coprime with both D' and D'' (because otherwise we would get $\chi_D(p) = 0$). Using (3.2) gives us:

$$\chi(\mathfrak{p}) = \chi_{D'}(N\mathfrak{p}) = \chi_{D'}(p) = \chi_{D''}(p)$$

Likewise, we have $\chi(\mathfrak{p}') = \chi_{D'}(p) = \chi_{D''}(p)$, which gives us

$$\prod_{\mathfrak{p}|p} \left(1 - \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}\right)^{-1} = \left(1 - \frac{\chi_{D'}(p)}{p^s}\right)^{-1} \left(1 - \frac{\chi_{D''}(p)}{p^s}\right)^{-1}$$

Case 2: $\chi_D(p) = -1, p = \mathfrak{p}$. We have now that $N(\mathfrak{p}) = p^2$, therefore $\chi(\mathfrak{p}) = 1$. On the other hand, we have that $\chi_{D'}(p)\chi_{D''}(p) = \chi_D(p) = -1$, so one of the $\chi_{D'}(p)$, $\chi_{D''}(p)$ takes the value of $+1$, whereas the other -1. Consequently:

$$\begin{aligned}\prod_{\mathfrak{p}|p} \left(1 - \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}\right)^{-1} = \left(1 - \frac{1}{p^{2s}}\right)^{-1} &= \left(1 - \frac{1}{p^s}\right)^{-1} \left(1 + \frac{1}{p^s}\right)^{-1} \\ &= \left(1 - \frac{\chi_{D'}(p)}{p^s}\right)^{-1} \left(1 + \frac{\chi_{D''}(p)}{p^s}\right)^{-1}\end{aligned}$$

Case 3: $\chi_D(p) = 0$, $p = \mathfrak{p}^2$. We have that p devides either D' or D'', and so if for example $p \mid D''$, then $(p, D') = 1$ and so according to (3.2) is $\chi(\mathfrak{p}) = \chi_{D'}(p)$. Therefore it follows:

$$\begin{aligned}\prod_{\mathfrak{p}|p} \left(1 - \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}\right)^{-1} &= \left(1 - \frac{\chi_{D'}(p)}{p^s}\right)^{-1} \\ &= \left(1 - \frac{\chi_{D'}(p)}{p^s}\right)^{-1} \left(1 - \frac{\chi_{D''}(p)}{p^s}\right)^{-1}\end{aligned}$$

since $\chi_{D''}(p) = 0$.
Having all the cases covered, we can conclude that the equality between 3.7 and 3.8 holds.

iii) Let $D = D_1 \dots D_t$ be the decomposition of D to prime discriminats and lets us denote with χ_i the genus character corresponding to the decomposition $D = (D_i) \cdot (D_1 \dots D_{i-1} D_{i+1} \dots D_t)$. We then have that for any decomposition of $D = D' \cdot D''$, where $D'' = D_{i_1} D_{i_2} \dots D_{i_s}$, the corresponding character χ is equal to $\chi_{i_1}\chi_{i_2} \dots \chi_{i_s}$. In other words, the characters that we have created from the corresponding decomposition form a group, with the generators $\chi_1 \dots \chi_t$ and relations $\chi_i^2 = 1$ and $\prod_i \chi_i = 1$ (this can be verified by doing calculations and breaking down to cases similar to the ones in proof of i)). To conclude that group is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{t-1}$ and that it therefore has 2^{t-1} elements, we need to prove that no other relation in the group holds. In other words, it suffices to show that the only character that is trivial arises from the decomposition where either $D' = 1$ or $D'' = 1$. That, however, follows directly from (3.4), since for D' and $D'' \neq 1$ we have that functions $L_{D'}(s)$ and $L_{D''}(s)$ are holomorphic in the point $s = 1$, so $s = 1$ is not a pole of $L_k(s, \chi)$ and therefore χ cannot be a trivial character.

iv) As we have seen in the proof of the corollary, there is 2^r genus characters, where $2^r = |C/C^2|$. All that we need to prove now is that $r \leq t-1$. To further simplify the proof, we are going to look at the following exact sequence:

$$0 \to I \xrightarrow{i} C \xrightarrow{Sq} C \xrightarrow{\pi} C/C^2 \to 0\,,$$

where $I = Ker(Sq)$, and $Sq : C \to C$ is the square function, $Sq(A) = A^2$. Since all the groups are finite, using isomorphism theorem and Lagrange's theorem, we have that $|I| = |C/C^2|$. This means that instead of looking at $|C/C^2|$ we can look at all ideal classes s.t. A^2. Using that $A^{-1} = A'$, we further get

$$A \in I \iff A^2 = 1 \iff A = A^{-1} \iff A = A'$$

We will call the ideal classes that satisfy this condition *ambiguous*. It suffices to show that there are at most 2^{t-1} ambiguous ideal classes.
Let us observe first that in every ambiguous ideal class there is an ideal $\mathfrak{a}$ s.t. $\mathfrak{a}' = \mathfrak{a}$. To prove this observation, we will be using (2.5): Let $\mathfrak{a} \in A$ be an arbitrary ideal, then we have $\mathfrak{a}' \in A' = A$ and $\mathfrak{a}' = (\lambda)\mathfrak{a}$ with $\lambda \in K, N(\lambda) = 1$. Now using (2.5) we have that $\lambda = \frac{\mu}{\mu'}$, $\mu \in \mathscr{O}$ and $N(\mu) > 0$ (If K is imaginary then this is fulfilled anyways; If K is real, we can pick positive λ, so that $N(\mu) = \mu\mu' = \lambda\mu'^2 \geq 0$). Finally, this gives us the ideal $(\mu)\mathfrak{a}$ equal to its conjugate.

We choose such an ideal $\mathfrak{a} = \mathfrak{a}'$ from the ambiguous class A. After multiplying it with a suitable rational number we can get that $\mathfrak{a}$ is a whole and primitive ideal (no integer > 1 devises it). However, there are only 2^t whole, primitive, ambiguous ideals, namely those of the form

$$\mathfrak{p}_1{}^{i_1} \dots \mathfrak{p}_t{}^{i_t} \qquad (i_1, \dots, i_t \in \{0, 1\}), \tag{3.9}$$

where $\mathfrak{p}_i$ $(i = 1 \dots t)$ is the prime ideal that divides D_i. To see this, we recall the theorem 1, chapter 11 from [1] and look at all 3 cases. Firstly, such an ideal $\mathfrak{a}$ is not divisible by prime ideal $\mathfrak{p}$, $\mathfrak{p} = (p)$ for p inert (because then it would divisible by the natural number p). Also, there could not be a prime ideal $\mathfrak{p}$ in $\mathfrak{a}$ s.t. $\mathfrak{p} \neq \mathfrak{p}'$, $\mathfrak{p}\mathfrak{p}' = (p)$ (then $\mathfrak{p}' \mid \mathfrak{a}' = \mathfrak{a}$ would imply $p = \mathfrak{p}\mathfrak{p}' \mid \mathfrak{a}$, which would contradict $\mathfrak{a}$ being primitive). We thus have that $\mathfrak{a}$ contains only prime ideals $\mathfrak{p}$ such that $\mathfrak{p}^2 = (p)$ for p a ramified prime (also $\chi_D(p) = 0$, so $\mathfrak{p} \mid D$) at most to the power of one (since $\mathfrak{p}^2 = p \Rightarrow \mathfrak{p}^2 \nmid \mathfrak{a}$), from which we get our formula in 3.9. Every ambiguous ideal class $A \in I$ contains at least one of the 2^t ideals in 3.9, so we can conclude that $2^r \leq 2^t$ and if we are to find, among these 2^t ideals from 3.9, one principle ideal $\mathfrak{a} \neq 1$ we would be done (since we already know that $2^r \geq 2^{t-1}$). We now break into cases depending on the sign of the discriminant D.

Case 1: If $D < 0$, then we have

$$\mathfrak{p}_1^2 \dots \mathfrak{p}_t^2 = \prod_{p|D} p = \begin{cases} D, & if\ D \equiv 1 \pmod 4 \\ 2d, & if D = 4d,\ d \equiv 3 \pmod 4 \\ d, & if D = 4d,\ d \equiv 2 \pmod 4 \end{cases}$$

from which it follows

$$\begin{aligned}(\sqrt{D}) &= \mathfrak{p}_1 \dots \mathfrak{p}_t \text{ if } D \equiv 1 \pmod 4 \\ (\sqrt{d}) &= \mathfrak{p}_2 \dots \mathfrak{p}_t \text{ if } D = 4d\,, d \equiv 3 \pmod 4 \\ (\sqrt{D}) &= \mathfrak{p}_1 \dots \mathfrak{p}_t \text{ if } D = 4d\,, d \equiv 2 \pmod 4\end{aligned} \tag{3.10}$$

In the second equation of (3.10) we have numbered them in that way since $\mathfrak{p}_1$ is a prime devisor of 2. Since the left side of the equations in (3.10) are principle ideals we have found a non-trivial relation between $\mathfrak{p}_\mathfrak{i}$ in C.

Case2: If $D > 0$ then the equations of (3.10) still apply, however the left side does not necessarily need to be a principle ideal in the narrow sense, since $\sqrt{D}$(respectively $\sqrt{d}$) now have negative norm. However, we can still fix this by finding a unit ε with negative norm. We would then have that $\varepsilon\sqrt{D}$ ($\varepsilon\sqrt{D}$) would be the generator of the said principle ideal with positive norm, and then the same conclusion as in Case 1 would follow. Thus, let us suppose otherwise, that there is no unit of negative norm and take a fundamental unit ε with positive norm (we can normalize it to have $\varepsilon\varepsilon' = 1$) and let us set $\mu := (\varepsilon - 1)\sqrt{D}$. Then we have:

$$\mu' = -\varepsilon'\sqrt{D} + \sqrt{D} = (1 - \varepsilon^{-1})\sqrt{D} = \varepsilon^{-1}\mu$$

hence $(\mu) = (\mu')$. We can write (μ) as $n\mathfrak{a}$ for $n \in \mathbb{N}$ and $\mathfrak{a}$ primitive, and now since $\mathfrak{a} = \mathfrak{a}'$, $\mathfrak{a}$ must be among the ideals in (3.9). We cannot have $\mathfrak{a} = 1$, since then $(\mu) = (n)$ and since ε generates the group of units in $\mathscr{O}$

$$\mu = \pm n\varepsilon^r \quad (r \in \mathbb{Z})$$

so therefore

$$\varepsilon = \frac{\mu}{\mu'} = \frac{n\varepsilon^r}{n\varepsilon^{-r}} = \varepsilon^{2r}$$

which is a contradiction with ε being the fundamental unit (generator of the unit group which is of rank 1, according to Dirchlet's unit theorem). We now have the that $\mathfrak{a} = (n^{-1}\mu)$, and since $N(n^{-1}\mu) > 0$ we have found the non-trivial relation for the ideals in (3.9) we have been looking for. This concludes the proof.

□

Remark 3.4 *Using the theorem 3.1 we are now able to describe the structure of the group C/C^4.*

Using the structure theorem we have that $C/C^4 \cong G = (\mathbb{Z}/2\mathbb{Z})^{t-1-s} \times (\mathbb{Z}/4\mathbb{Z})^s$ (where $C/C^2 \simeq (\mathbb{Z}/2\mathbb{Z})^{t-1}$). Here, to see that the sum of exponents is t-1 we use the fact that there needs to be 2^{t-1} elements of order 2. To find s we look at the following equality which stems from counting the appropriate elements in G that are a square, and squared give the identity:

$$2^s = \#\{A \in C \mid A^2 = 1,\, A = B^2 \text{ for some } B \in C\} \tag{3.11}$$

which gives $2^s = ker(Sq) \cap Im(Sq)$. We can fully describe these groups according to the theorem (3.1), where all elements of $ker(Sq)$ are represented by (3.9), and exactly so twice. Furthermore, $Im(Sq)$ consists of elements $A \in C$ s.t. $\chi(A) = 1$ for all genus characters χ (here we've used the proposition 2.3). This means we know how to determine s by calculating the values of χ_i of the ideals in (3.9). This result can be formulated as follows:

Corollary 3.5 *Let $\varepsilon_{ij} \in \mathbb{Z}/2\mathbb{Z}$, $1 \leq i, j \leq t$ be such that*

$$(-1)^{\varepsilon_{ij}} = \chi_i(\mathfrak{p}_j) = \begin{cases} \chi_{D_i}(p_j), & if\ i \neq j \\ \prod_{k \neq i} \chi_{D_k}(p_i), & if\ i = j \end{cases}$$

where $p_j = N(\mathfrak{p}_j)$. Then we have that C/C^4 is isomorphic to the group $(\mathbb{Z}/2\mathbb{Z})^{t-1-s} \times (\mathbb{Z}/4\mathbb{Z})^s$, where $t - 1 - s$ is the rank of the matrix $E = (\varepsilon_{i,j})_{1 \leq i,j \leq t}$ over the field $\mathbb{Z}/2\mathbb{Z}$.

Proof. To see this, we can first write out an arbitrary ideal $\mathfrak{a}$ that is in $Ker(Sq)$ using 3.9 as

$$\mathfrak{a} = {\mathfrak{p}_1}^{i_1} \dots {\mathfrak{p}_t}^{i_t} \qquad (i_1, \dots, i_t \in \{0, 1\})$$

and form a vector $v \in (\mathbb{Z}/2\mathbb{Z})^t$, $v = (i_1, i_2 \dots i_t)$ that corresponds to the ideal $\mathfrak{a}$. We are now looking for all $\mathfrak{a}$ that take value 1 for all χ, which it is equivalent to taking value of 1 on all the generators χ_i. Furthermore, we can restate this requirement to having all the corresponding vectors v satisfy $Ev = 0$, since $\chi_i(\mathfrak{a}) = 1$ is equivalent to there being an even number of j such that $\chi_i(\mathfrak{p}_j) = -1$ which the aforementioned condition enforces. As we know there are 2^{s+1} number of such vectors (2^s corresponidng to different ideal classes and each is counted twice), so that gives us the rank of E to be $t - (s + 1)$ which is what we set out to prove. □

Corollary 3.6 *We can further describe the structure of discriminants for certain values of ideal class number modulus 4. Namely,*

$$\begin{aligned} h(D) = \pm 1\ (mod\ 4) &\iff D = -4,\ +8,\ -8,\ +p,\ -q, \\ h(D) = 2\ (mod\, 4) &\iff D = +4q,\ \pm 8p\,(p = 5\ (mod\ 8),\ +8q \\ &\qquad -8q\ (q = \ 3(mod\ 8)), \\ &\qquad +pp_1\ (for\ (\frac{p_1}{p}) = -1), \\ &\qquad -pq\ (for\ (\frac{q}{p}) = -1), +qq_1 \\ h(D) = 0, otherwise \end{aligned}$$

Proof. First case of $h(D) = \pm 1\ (mod\ 4)$ is already proven in the corollary 3.3, as D can only take values of prime discriminants. Second case $h(D) = 2\ (mod\, 4)$ is actually new, and here we can note that there must be two prime discriminants in the decomposition of D, due to the corollary 3.3. Below we will just do the proof that D cannot take the form of $D = -4p$, as all these results follow the same algorithm. Using the method from remark 3.4 we calculate $\chi_i(p_j)$ or in our case we

need to calculate $\chi_{-4}(p)$ and $\chi_p(-4)$. Since we have that $\chi_p(-1) = 1$, using the multiplicativity of characters we get $\chi_p(-4) = 1 = (-1)^0 \implies \varepsilon_{11} = 0 \ \wedge \ \varepsilon_{21} = 0$. Furthermore, we have $\chi_{-4}(p) = 1$ from the definition of χ_{-4}, which again gives us $\varepsilon_{21} = 0 \wedge \varepsilon_{22}$. Finally, we get that the matrix $[\varepsilon_{ij}]$ is of rank 0, so according to the remark 3.4 we have that s=1. This now gives us that C/C^4 is isomorphic to $\mathbb{Z}/4\mathbb{Z}$ which in turn gives us $4 \mid h(D)$. $\square$

Bibliography

[1] Zagier D.B. *Zetafunktionen und quadratische Körper*. Springer, 1981.