Royal Institute of Technology
Stockholm University

Master thesis

Counting Class Numbers

Tobias Magnusson

supervised by
Pär Kurlberg

January 4, 2018

Acknowledgements

Firstly, I would like to thank my supervisor Pär Kurlberg for suggesting such a rich problem for me to study.

Secondly, I would like to thank my classmates for their support, and in particular Simon Almerström-Przybyl and Erin Small.

Thirdly, I would like to thank Federico Pintore for answering important questions concerning his PhD thesis.

Finally, and most importantly, I would like to thank my wife for her patience with my mathematical obsessions.

Abstract

The following thesis contains an extensive account of the theory of class groups. First the form class group is introduced through equivalence classes of certain integral binary quadratic forms with a given discriminant. The sets of classes is then turned into a group through an operation referred to as "composition". Then the ideal class group is introduced through classes of fractional ideals in the ring of integers of quadratic fields with a given discriminant. It is then shown that for negative fundamental discriminants, the ideal class group and form class group are isomorphic. Some concrete computations are then done, after which some of the most central conjectures concerning the average behaviour of class groups with discriminant less than X – the Cohen-Lenstra heuristics – are stated and motivated. The thesis ends with a sketch of a proof by Bob Hough of a strong result related to a special case of the Cohen-Lenstra heuristics.

Att räkna klasstal

Följande mastersuppsats innehåller en utförlig redogörelse av klassgruppsteori. Först introduceras formklassgruppen genom ekvivalensklasser av en typ av binära kvadratiska former med heltalskoefficienter och en given diskriminant. Mängden av klasser görs sedan till en grupp genom en operation som kallas "komposition". Därefter introduceras idealklassgruppen genom klasser av kvotideal i heltalsringen till kvadratiska talkroppar med given diskriminant. Det visas sedan att formklassgruppen och idealklassgruppen är isomorfa för negativa fundamentala diskriminanter. Några konkreta beräkningar görs sedan, efter vilka en av de mest centrala förmodandena gällande det genomsnittliga beteendet av klassgrupper med diskriminant mindre än X – Cohen-Lenstra heuristiken – formuleras och motiveras. Uppsatsen avslutas med en skiss av ett bevis av Bob Hough av ett starkt resultat relaterat till ett specialfall av Cohen-Lenstra heuristiken.

Contents

Chapter 1

Introduction

The study of class numbers goes back to Joseph-Louis Lagrange (1736-1813) and in particular to his work Recherches d'Arithmétique, in which he studied the representation of integers by binary quadratic forms $ax^2 + bxy + cy^2$, with integer coefficients a, b, c.

Definition 1. Let f be a binary quadratic form and let m be an integer. Then f is said to represent m if there exists integers x, y such that $f(x, y) = m$.

In particular he noticed the following fundamental fact.

Proposition 1. Let f, F be binary quadratic forms. Then f and F represent the same set of integers whenever there exists integers $\alpha, \beta, \gamma, \delta$ with $\alpha\delta - \beta\gamma = \pm 1$ and

$$F(X, Y) = f\left(\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} X \\ Y \end{pmatrix}\right),$$

where X, Y are indeterminates.

Proof. Say that f represents an integer m, with $f(A, B) = m$ for integers A, B. We have that

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}^{-1} = \frac{1}{\alpha\delta - \beta\gamma}\begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix},$$

is an integer matrix, and thus F represents m, with

$$F(A^{-1}\begin{pmatrix} A \\ B \end{pmatrix}) = f(AA^{-1}\begin{pmatrix} A \\ B \end{pmatrix}) = f(A, B) = m.$$

Conversely, it is easy to see that if F represents m then f represents m too. $\square$

Forms that are related through a matrix transformation as above, later came to be called equivalent. This term was introduced by Carl Friedrich Gauß (1777-1855), whom we shall return to shortly. Lagrange also noticed that such transformations preserve discriminants.

Definition 2. Let $f(x, y) = ax^2 + bxy + cy^2$ be a binary quadratic form. Then $\Delta_f = b^2 - 4ac$ is called the discriminant of f.

In other words, Lagrange noticed the following property.

Proposition 2. Let F, f be equivalent forms. Then $\Delta_F = \Delta_f$.

Proof. Covered in the sequel. $\square$

He thus understood that the equivalence of binary quadratic forms is an equivalence relation in the modern sense on the set of binary quadratic forms with a given discriminant. Therefore the set of binary quadratic forms with a given discriminant, can be partitioned into classes, and the number of such classes later came to be called the class number.

Lagrange further discovered the following result. [Wei06, p. 321].

Proposition 3. Every form $ax^2 + bxy + cy^2$ is equivalent to a form $Ax^2 + Bxy + Cy^2$ where $|B| \leq |A|, |C|$.

Clearly there can only be finitely many forms with a given discriminant that satisfy such a bound, and therefore we have the following important result.

Corollary 1. The class number is finite.

To actually compute the class number, one only has to list all forms satisfying the bound, and then remove superfluous forms. One is then left with a list of forms, each contained in one and only one class.

The story continues with Adrien-Marie Legendre (1752-1833), and in particular with his work Essai sur la Théorie des Nombres. In this essay Legendre noted that if one has two binary quadratic forms f, f' given by

$$f(X, Y) = aX^2 + 2bXY + cY^2$$
$$f'(X', Y') = a'X'^2 + 2b'X'Y' + c'Y'^2,$$

then it is possible to find bilinear forms B, B' and a quadratic form $F(U, V) = AU^2 + 2BUV + CV^2$, such that

$$f(X, Y)f'(X', Y') = F(B(X, Y; X', Y'), B'(X, Y; X', Y')).$$

Furthermore, Legendre seems to have taken for granted that the above product induced a well-defined binary operation on the set of equivalence classes (with respect to Lagrange's notion of equivalence) of binary quadratic forms with a given discriminant. [Wei06, p. 334] This is by no means obvious, and was clarified greatly by the next actor in our story – Gauß.

Gauß' most important contribution to theory of class numbers and one of the most important contributions to number theory in general was his work Disquisitiones Arithmeticæ [Gau01]. In it he replaced Lagrange's notion of equivalence with the appropriate one, only allowing $\alpha\delta - \beta\gamma = 1$, generalized Legendre's operation to what he called the "law of composition", and proved that the set of classes of forms with a given discriminant forms with the composition law a finite abelian group – now called the (form) class group. Furthermore, he formulated three central conjectures.

Conjecture 1. Let $h(d)$ be the class number of the discriminant d. Then $h(d) \to \infty$ as $d \to -\infty$.

Conjecture 2. Gauß made lists of negative discriminants with class number 1, 2, and 3, and believed them to be complete.

Conjecture 3. There are infinitely many positive discriminants with class number 1.

The first conjecture was proven in 1934 by Hans Heilbronn. The second conjecture was proven for class number 1 in 1952 by Kurt Heegner, for class number 2 in 1971 by Alan Baker and Harold Stark, for class number 3 by Oesterlé in 1985, and for class numbers ≤ 100 by Mark Watkins in 2004. The last conjecture is still open.

Disquisitiones was hugely influential, but Gauß' composition law was considered by many to be prohibitively complicated. It was simplified in 1851 by Johann Peter Gustav Lejeune Dirichlet (1805-1859) who also made many other contributions to number theory and is often considered to be the founder of the field of analytic number theory.

One of Dirichlet's most ardent admirers was his student Richard Dedekind (1831-1916). Dedekind reformulated the theory of class numbers in terms of abstract algebra and in particular in terms of what is now known as quadratic field extensions. He noticed that the (ideal) class group appears as a set of equivalence classes of (fractional) ideals in the ring of integers of a quadratic field extension. This greatly simplified the theory, at the cost of making it more abstract.

In this thesis, I give a detailed account of the class group from the point of view of binary quadratic forms and from the point of view of quadratic fields. In particular, I focus on class groups of forms with negative discriminant, or equivalently, imaginary quadratic fields. The reader will be introduced to a series of conjectures which are the spiritual successors to Gauß' conjectures – the heuristics by Henri Cohen and Hendrik Lenstra. Among these is a prediction about the average size of the k-torsion subgroup of class groups with discriminant d satisfying $0 < -d < X$. The thesis ends with a sketch of a proof by Bob Hough that this prediction holds for the case $k = 3$.

If the reader has further interest in the historical background, please see André Weil's excellent book [Wei06].

Chapter 2

Preliminaries

In this chapter I introduce the form class group and the ideal class group, and prove that they are isomorphic. The reader is assumed to be acquainted with the group $\mathrm{SL}_2(\mathbb{Z})$ and have a rudimentary understanding of how it acts on the upper half plane

$$\mathbb{H} = \{z \in \mathbb{C} : \Im(z) > 0\},$$

and especially fundamental domains of the orbit space $\mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$. Should the reader need a refresher, I recommend the part on elliptic modular forms in [RBvdG+08].

The exposition is largely in the spirit of [Bue89] and [Pin15] for the form class group, and [Neu13], [Coh00] and the notes [Conb, Cona] for the ideal class group.

2.1 Binary quadratic forms

Definition 3. A binary quadratic form Q is a bivariate homogeneous polynomial of degree 2 with integer coefficients. In other words,

$$Q(x, y) = ax^2 + bxy + cy^2,$$

where $a, b, c \in \mathbb{Z}$. We often write (a, b, c) as an abbreviation. We'll also treat "binary quadratic form", "quadratic form", and "form" as synonyms, unless otherwise noted.

Definition 4. Let $Q = (a, b, c)$ be a form. Then the number $\Delta_Q = b^2 - 4ac$ is called the discrimant of Q.

Definition 5. Let $Q = (a, b, c)$ be a form. If $\gcd(a, b, c) = 1$, we say that Q is primitive.

Definition 6. Let Q be a form. If $\Delta_Q > 0$, we say that Q is indefinite. If $\Delta_Q < 0$, we say that Q is definite.

Notice that if a form $Q = (a, b, c)$ is definite, then $ac > \frac{b^2}{4}$ so that in particular a, c have the same signs.

Definition 7. Let $Q = (a, b, c)$ be a definite form. If $a > 0$ (and $c > 0$) we say that Q is positive definite. If $a < 0$ (and $c < 0$) we say that Q is negative definite.

For $D < 0$, let $\mathfrak{Q}_D$ denote the set of primitive positive definite quadratic forms with discriminant D. Let further

$$\phi : \mathfrak{Q}_D \times \mathrm{SL}_2(\mathbb{Z}) \to \mathfrak{Q}_D,$$

be defined by

$$\phi(Q, \gamma) = Q \circ \gamma.$$

Proposition 4. The map ϕ is well-defined and a (right) group action.

Proof. Let $f = (a, b, c) \in \mathfrak{Q}_D$, and $\gamma = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. We see that

$$\begin{aligned}
\phi(f)(x, y) &= (f \circ \gamma)(x, y) \\
&= f(\alpha x + \beta y, \gamma x + \delta y) \\
&= (a\alpha^2 + b\alpha\gamma + c\gamma^2)x^2 + (b(\alpha\delta + \beta\gamma) + 2(a\alpha\beta + c\gamma\delta))xy + (a\beta^2 + b\beta\delta + c\delta^2)y^2.
\end{aligned}$$

And so $\phi(f)$ is indeed a quadratic form. Furthermore, we see that

$$\begin{aligned}
\Delta_{\phi(f)} &= \alpha\beta\gamma\delta(-2b^2 + 8ac) + \alpha^2\delta^2(b^2 - 4ac) + \beta^2\delta^2(b^2 - 4ac) \\
&= \Delta_f \det(\gamma)^2 = \Delta_f.
\end{aligned}$$

And so $\phi(f)$ is definite. Let now $\gamma_1, \gamma_2 \in \mathrm{SL}_2(\mathbb{Z})$. We then have that

$$\begin{aligned}
\phi(f, \gamma_1\gamma_2) &= f \circ \gamma_1\gamma_2 \\
&= (f \circ \gamma_1) \circ \gamma_2 = \phi(\phi(f, \gamma_1), \gamma_2),
\end{aligned}$$

and clearly $\phi(f, I) = f \circ I = f$. It only remains to verify that $\phi(f, \gamma)$ is primitive positive definite for every $f \in \mathfrak{Q}_D$ and $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. To see this, recall that $\mathrm{SL}_2(\mathbb{Z})$ is (freely) generated by

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

and hence by the above we only have to verify that $\phi(f, S)$ and $\phi(f, T)$ are primitive positive definite. We see that

$$\phi(f, T) = (a, b + 2a, a + b + c),$$

and

$$\phi(f, S) = (c, -b, a).$$

Since the first coefficients are positive, we have that $\phi(f, S)$ and $\phi(f, T)$ are positive definite. Finally we see that

$$\gcd(a, b + 2a, a + b + c) = \gcd(a, a + b, a + b + c) = \gcd(a, a + b, c) = \gcd(a, b, c) = 1,$$

and

$$\gcd(c, -b, a) = \gcd(a, b, c) = 1,$$

so that they also are primitive. We are done. □

Since ϕ is a group action we write $f.\gamma$ as a shorthand for $\phi(f, \gamma)$.
The group action induces an equivalence relation.

Definition 8. Let $Q_1, Q_2 \in \mathfrak{Q}_D$. We say that Q_1 and Q_2 are equivalent, and write $Q_1 \sim Q_2$, if there exists an element $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $Q_2 = Q_1.\gamma$.

We have that $\sim$ is an equivalence relation and we denote the set of equivalence classes $\mathfrak{Q}_D/\sim$ by $H(D)$. Of special interest is $|H(D)|$, which is denoted by $h(D)$ and is called the *class number*.

Remark 1. If $(*, b_1, *) \sim (*, b_2, *)$ then $b_1 \equiv_2 b_2$, so that $\frac{b_1+b_2}{2}$ is an integer. Here and in the sequel, the notation $a \equiv_n b$ for integers a, b and n denotes congruence modulo n, in other words $n \mid a - b$.

Theorem 1. Let $D < 0$. Then the class number $h(D)$ is finite.

We'll prove the theorem by selecting appropriate representatives for each equivalence class of forms in $H(D)$, and in doing so putting $H(D)$ in one-to-one correspondence with a set that is obviously finite.

Definition 9. Let $Q=(a,b,c)$ be a binary quadratic form. Then the (unique) root $\frac{-b+\sqrt{D}}{2a}$ of $Q(z,1)=0$ in $\mathbb{H}$ is called the principal root of Q and is denoted by $\mathfrak{z}_Q$.

Lemma 1. The map $\mathfrak{z}_{-}:\mathfrak{Q}_D\to\mathbb{H}$ defined by $Q\mapsto\mathfrak{z}_Q$ is injective.

Proof. Let $Q_1=(a_1,b_1,c_1),Q_2=(a_2,b_2,c_2)\in\mathfrak{Q}_D$ satisfy $\mathfrak{z}_{Q_1}=\mathfrak{Q}_2$. Then

$$\frac{-b_1}{2a_1}=\frac{-b_2}{2a_2},$$

and

$$\frac{\sqrt{|D|}}{2a_1}=\frac{\sqrt{|D|}}{2a_2}.$$

The last equation gives that $a_1=a_2$, whence the first equation gives that $b_1=b_2$. Finally we have that

$$c_1=\frac{b_1^2-D}{4a_1}=\frac{b_2^2-D}{4a_2}=c_2,$$

whence $Q_1=Q_2$, and we are done. □

Recall now that $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathbb{H}$ through linear fractional transformations. In other words if $\tau\in\mathbb{H}$ and $\gamma=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\mathrm{SL}_2(\mathbb{Z})$ we have the action

$$\gamma(\tau)=\frac{a\tau+b}{c\tau+d}.$$

Recall also that every equivalence class in $\mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$ has a unique representative in the (semi-closed) fundamental domain, defined by

$$\begin{gathered}\tilde{\mathcal{F}}_1=\{z\in\mathbb{H}:-\frac{1}{2}\leq\Re(z)<\frac{1}{2}\text{ and }|z|>1\\ \text{or}\\ -\frac{1}{2}\leq\Re(z)\leq 0\text{ and }|z|=1\}.\end{gathered}$$

Lemma 2. Let $\gamma=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\mathrm{SL}_2(\mathbb{Z})$ and $f=(a,b,c)\in\mathfrak{Q}_D$. Then $\mathfrak{z}_{f.\gamma}=\gamma^{-1}(\mathfrak{z}_f)$.

Proof. Since $\mathfrak{z}_{f.\gamma}\in\mathbb{H}$ we only have to verify that $f.\gamma(\gamma^{-1}(\mathfrak{z}_f),1)=0$. This is straightforward.

$$\begin{aligned}f.\gamma(\gamma^{-1}(\mathfrak{z}_f),1)&=f.\gamma\left(\frac{d\mathfrak{z}_f-b}{-c\mathfrak{z}_f+a},1\right)\\&=f\left(\frac{ad\mathfrak{z}_f-ab+b(-c\mathfrak{z}_f+a)}{-c\mathfrak{z}_f+a},\frac{cd\mathfrak{z}_f-bc+d(-c\mathfrak{z}_f+a)}{-c\mathfrak{z}_f+a}\right)\\&=f\left(\frac{\mathfrak{z}_f}{-c\mathfrak{z}_f+a},\frac{1}{-c\mathfrak{z}_f+a}\right)\\&=\frac{f(\mathfrak{z}_f,1)}{(-c\mathfrak{z}_f+a)^2}=0.\end{aligned}$$

□

We now introduce the set of reduced forms.

Definition 10. The set

$$\mathfrak{Q}_D^{\mathrm{red}}=\{(a,b,c)\in\mathfrak{Q}_D:-a<b\leq a<c\text{ or }0\leq b\leq a=c\},$$

is called the set of reduced (primitive positive definite) forms.

Lemma 3. Let $Q = (a, b, c) \in \mathfrak{Q}_D$. Then $Q \in \mathfrak{Q}_D^{\mathrm{red}}$ if and only if $\mathfrak{z}_Q \in \tilde{\mathcal{F}}_1$.

Proof. We have that
$$\Re(\mathfrak{z}_Q) = -\frac{b}{2a},$$
and
$$|\mathfrak{z}_Q|^2 = \frac{b^2 - D}{4a^2} = \frac{c}{a}.$$
Furthermore, we have that $\mathfrak{z}_Q \in \tilde{\mathcal{F}}_1$ if and only if
$$-\frac{1}{2} \leq -\frac{b}{2a} < \frac{1}{2} \text{ and } \frac{c^2}{a^2} > 1$$
$$\text{or}$$
$$-\frac{1}{2} \leq -\frac{b}{2a} \leq 0 \text{ and } \frac{c^2}{a^2} = 1.$$
Which is true if and only if
$$-a < b \leq a \text{ and } c > a$$
$$\text{or}$$
$$0 \leq b \leq a \text{ and } c = a,$$
if and only if $(a, b, c) \in \mathfrak{Q}_D^{\mathrm{red}}$. The lemma has been proved. □

Lemma 4. Let $Q_c \in H(D)$. Then $|Q_c \cap \mathfrak{Q}_D^{\mathrm{red}}| = 1$. In other words, every class of forms in $H(D)$ has a unique representative in $\mathfrak{Q}_D^{\mathrm{red}}$.

Proof. Let Q be a representative of Q_c, so that $[Q] = Q_c$. Let $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ be such that $\gamma^{-1}(\mathfrak{z}_Q) \in \tilde{\mathcal{F}}_1$. Then $\mathfrak{z}_{Q.\gamma} \in \tilde{\mathcal{F}}_1$ and so $Q.\gamma \in \mathfrak{Q}_D^{\mathrm{red}}$. Hence $Q.\gamma \in Q_c \cap \mathfrak{Q}_D^{\mathrm{red}}$ and we have proved existence.

Let $Q_1, Q_2 \in \mathfrak{Q}_c \cap \mathfrak{Q}_D^{\mathrm{red}}$. Then $\mathfrak{z}_{Q_1}, \mathfrak{z}_{Q_2} \in \tilde{\mathcal{F}}_1$. We also have that $Q_1 \sim Q_2$ and hence $\mathfrak{z}_{Q_1} = \gamma . \mathfrak{z}_{Q_2}$ for some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. But since $\tilde{\mathcal{F}}_1$ is a fundamental domain, we must have that $\gamma = I$, and so $\mathfrak{z}_{Q_1} = \mathfrak{z}_{Q_2}$. Since $\mathfrak{z}_-$ is injective, we conclude that $Q_1 = Q_2$, and we have proved uniqueness. □

By the above, we have that $h(D) = |\mathfrak{Q}_D^{\mathrm{red}}|$. We can now prove theorem 1.

Proof of theorem 1. Let $(a, b, c) \in \mathfrak{Q}_D^{\mathrm{red}}$. Then $|b| \leq a \leq c$, and so $-b^2 \geq -a^2$. This implies that $|D| = 4ac - b^2 \geq 3a^2$ whence
$$a \leq \sqrt{\frac{|D|}{3}},$$
and as a consequence
$$-\sqrt{\frac{|D|}{3}} \leq b \leq \sqrt{\frac{|D|}{3}}.$$
The number of possible values for a and b is thus finite, and since c is determined (through D) by the choice of a and b, we are done. □

2.2 Composition law

Hereafter D denotes a negative integer unless otherwise noted.

We now introduce the composition law. It turns $H(D)$ into a group – the *class group*. To simplify the exposition we define the law on pairs of *united* forms.

Definition 11. Let $f = (a_1, b_1, c_1), g = (a_2, b_2, c_2) \in \mathfrak{Q}_D$. If $\gcd(a_1, a_2, \frac{b_1+b_2}{2}) = 1$, we say that f and g are united.

Note that

$$b_1^2 - b_2^2 = 4(a_1c_1 - a_2c_2),$$

and so $b_1 \equiv_2 b_2$ whence $b_1 + b_2 \equiv_2 0$, as is implicit in the definition.

Lemma 5. Let $f = (a, b, c) \in \mathfrak{Q}_D$. Then for any nonzero integer m there exists relatively prime integers x, y such that $\gcd(f(x, y), m) = 1$.

Proof. Let $m \in \mathbb{Z}$ be arbitrary and put

$$\begin{aligned} P &= \text{product of primes } p \text{ such that } p \mid m,\ p \mid a, \text{ and } p \mid c \\ Q &= \text{product of primes } p \text{ such that } p \mid m,\ p \mid a, \text{ and } p \nmid c \\ R &= \text{product of primes } p \text{ such that } p \mid m,\ p \nmid a, \text{ and } p \mid c \\ S &= \text{product of primes } p \text{ such that } p \mid m,\ p \nmid a, \text{ and } p \nmid c. \end{aligned}$$

Evidently these numbers are mutually relatively prime. In particular $\gcd(Q, RS) = 1$. Now, let p be a prime divisor of m. Then $p \mid P, Q, R$ or S.

If $p \mid P$ we have that $p \mid aQ^2$ and $p \mid c(RS)^2$. But since f is primitive we have that $p \nmid b$, and by construction $p \nmid Q, R$ and S. Hence $p \nmid bQRS$ and thus $p \nmid f(Q, RS)$.

If $p \mid Q$ we have that $p \mid aQ^2$ and $p \mid bQRS$. But $p \nmid c$ and $p \nmid RS$ by construction, and so $p \nmid c(RS)^2$. Hence $p \nmid f(Q, RS)$.

If $p \mid R$ we have that $p \mid c(RS)^2$ and $p \mid bQRS$. But $p \nmid a$ and $p \nmid Q$ by construction, and so $p \nmid aQ^2$. Hence $p \nmid f(Q, RS)$.

If $p \mid S$ we have that $p \mid c(RS)^2$ and $p \mid bQRS$. But $p \nmid a$ and $p \nmid Q$ by construction, and so $p \nmid aQ^2$. Hence $p \nmid f(Q, RS)$.

It follows that $f(Q, RS)$ and m have no common prime divisors, whence $\gcd(f(Q, RS), m) = 1$ and we are done. □

Lemma 6. Let $f \in \mathfrak{Q}_D$, r be a nonzero integer, and x, y be relatively prime integers such that $f(x, y) = r$. Then there exists integers s, t such that $f \sim (r, s, t)$.

Proof. By the extended Euclidean algorithm we have that there exists integers z, w such that $xw - yz = 1$. Hence

$$f \sim f.\begin{pmatrix} x & z \\ y & w \end{pmatrix} = (ax^2 + bxy + cy^2, b(xw + yz) + 2(axz + cyw), az^2 + bzw + cw^2) = (r, s, t),$$

and we are done. □

Proposition 5. Let $f = (a_1, b_1, c_1), g = (a_2, b_2, c_2) \in \mathfrak{Q}_D$. Then there exists an $h \in \mathfrak{Q}_D$ such that $h \sim g$ and f and h are united.

Proof. By lemma 5, there exists relatively prime integers x, y such that $(g(x, y), a_1) = 1$. By lemma 6 there exists a form $h = (g(x, y), s, t)$ such that $g \sim h$.

We have that $\gcd(a_1, g(x, y), \frac{b_1+s}{2}) = 1$, and thus f and h are united. □

Proposition 6. Let $f = (a_1, b_1, c_1), g = (a_2, b_2, c_2) \in \mathfrak{Q}_D$. If f and g are united, then there exists integers B, C with B unique modulo $2a_1a_2$ such that

$$\begin{aligned} B &\equiv_{2a_1} b_1 \\ B &\equiv_{2a_2} b_2 \\ C &= \frac{B^2 - D}{4a_1a_2}, \end{aligned}$$

and as a consequence

$$f \sim (a_1, B, a_2 C)$$
$$g \sim (a_2, B, a_1 C).$$

Proof. Since f and g are united we have that

$$\gcd(a_1, a_2, \frac{b_1+b_2}{2}, 2a_1a_2) = 1,$$

and so there exists integers l_1, l_2, l_3, l such that

$$l_1 a_1 + l_2 a_2 + l_3 \frac{b_1+b_2}{2} + 2l a_1 a_2 = 1.$$

Notice also that since $b_1 \equiv_2 b_2$ we have that $b_1 b_2 + D \equiv_2 0$, and

$$a_1 a_2 b_1 \equiv_{2a_1a_2} a_1 a_2 b_2,$$

and since $a_1 D \equiv_{4a_1a_2} a_1 b_2^2$ and $a_2 D \equiv_{4a_1a_2} a_2 b_1^2$, we have that

$$a_1 \frac{D+b_1b_2}{2} \equiv_{2a_1a_2} a_1 b_2 \frac{b_1+b_2}{2}, \text{ and}$$
$$a_2 \frac{D+b_1b_2}{2} \equiv_{2a_1a_2} a_2 b_1 \frac{b_1+b_2}{2}.$$

Put now

$$B = l_1 a_1 b_2 + l_2 a_2 b_1 + l_3 \frac{D+b_1b_2}{2}.$$

Then

$$\begin{aligned} a_1 B &\equiv_{2a_1a_2} (l_1 a_1 b_2) a_1 + (l_2 a_1 b_2) a_2 + (l_3 a_1 b_2) \frac{b_1+b_2}{2} \\ &= a_1 b_2 (l_1 a_1 + l_2 a_2 + l_3 \frac{b_1+b_2}{2}) \\ &= a_1 b_2 (1 - 2l a_1 a_2) \equiv_{2a_1a_2} a_1 b_2, \end{aligned} \tag{2.1}$$

and similarly

$$a_2 B \equiv_{2a_1a_2} a_2 b_1. \tag{2.2}$$

We have furthermore that

$$\begin{aligned} \frac{b_1+b_2}{2} B &= l_1 a_1 b_2 \frac{b_1+b_2}{2} + l_2 a_2 b_1 \frac{b_1+b_2}{2} + l_3 \frac{D+b_1b_2}{2} \frac{b_1+b_2}{2} \\ &= \frac{D+b_1b_2}{2} (l_1 a_1 + l_2 a_1 + l_3 \frac{b_1+b_2}{2}) \\ &\equiv_{2a_1a_2} \frac{D+b_1b_2}{2}. \end{aligned} \tag{2.3}$$

The congruences (2.1) and (2.2) are equivalent to $B \equiv_{2a_1} b_1$ and $B \equiv_{2a_2} b_2$, respectively. Hence

$$B^2 - (b_1+b_2)B + b_1 b_2 = (B - b_1)(B - b_2) \equiv_{4a_1a_2} 0,$$

and thus

$$B^2 \equiv_{4a_1a_2} (b_1+b_2)B - b_1 b_2.$$

Moreover, congruence (2.3) is equivalent to

$$(b_1 + b_2)B \equiv_{4a_1a_2} D + b_1b_2,$$

so that $B^2 \equiv_{4a_1a_2} D$.

We can now finish the proof. Let $C = \frac{B^2-D}{4a_1a_2}$. There exists integers δ_1 and δ_2 such that $B = b_1 + 2a_1\delta_1$ and $B = b_2 + 2a_2\delta_2$. This implies that

$$\begin{aligned} a_2C &= \frac{B^2 - D}{4a_1} = a_1\delta_1^2 + b_1\delta_1 + c_1, \text{ and} \\ a_1C &= \frac{B^2 - D}{4a_2} = a_2\delta_2^2 + b_2\delta_2 + c_2, \end{aligned}$$

and so we conclude that

$$\begin{aligned} f.T^{\delta_1} &= (a_1, B, a_1\delta_1^2 + b_1\delta_1 + c_1) = (a_1, B, a_2C), \text{ and} \\ g.T^{\delta_2} &= (a_2, B, a_2\delta_2^2 + b_2\delta_2 + c_2) = (a_2, B, a_1C), \end{aligned}$$

whence we are done with existence. From the above, it is clear that the system

$$\begin{aligned} a_1B &\equiv_{2a_1a_2} a_1b_2 \\ a_2B &\equiv_{2a_1a_2} a_2b_1 \\ \frac{b_1 + b_2}{2}B &\equiv_{2a_1a_2} \frac{D + b_1b_2}{2}, \end{aligned}$$

is equivalent to the system in the proposition. Say now that we have two solutions B, B' to this system. Then

$$\begin{aligned} 2a_1a_2 &\mid a_1(B - B') \\ 2a_1a_2 &\mid a_2(B - B') \\ 2a_1a_2 &\mid \frac{b_1 + b_2}{2}(B - B'), \end{aligned}$$

and since $\gcd(a_1, a_2, (b_1 + b_2)/2) = 1$ we see that $2a_1a_2 \mid B - B'$ by the extended Euclidean algorithm. □

Lemma 7. Let

$$\mathfrak{D}_1 = \{(f, g) \in \mathfrak{Q}_D^2 : \exists a_1, a_2, B, C.\, f = (a_1, B, a_2C) \text{ and } g = (a_2, B, a_1C)\},$$

and let $\circ_1 : \mathfrak{D}_1 \to \mathfrak{Q}_D$ be defined by

$$(a_1, B, a_2C) \circ_1 (a_2, B, a_1C) = (a_1a_2, B, C).$$

Then $\circ_1$ is well-defined.

Proof. Say $(a_1, B, a_2C) = (a_1', B', a_2'C')$ and $(a_2, B, a_1C) = (a_2', B', a_1'C')$. Then $a_1 = a_1'$, $a_2 = a_2'$, $B = B'$ and $a_1C = a_1'C' = a_1C'$. But since $a_1 > 0$, we get that $C = C'$, and so $(a_1a_2, B, C) = (a_1'a_2', B', C')$. Moreover we have that $a_1, a_2 > 0$ and so $a_1a_2 > 0$. Finally it is clear that the discriminant of (a_1a_2, B, C) is the same as e. g. (a_2, B, a_1C), whence we are done. □

Lemma 8. Let

$$\mathfrak{D}_2 = \{(f, g) \in \mathfrak{Q}_D^2 : f \text{ and } g \text{ united}\},$$

and let $\circ_2 : \mathfrak{D}_2 \to H(D)$ be defined by

$$(a_1, b_1, c_1) \circ_2 (a_2, b_2, c_2) = [(a_1, B, a_2C) \circ_1 (a_2, B, a_1C)],$$

where B and C are any integers as in proposition 6. Then $\circ_2$ is well-defined.

Proof. Suppose we have two solutions B, C and B', C' to the system in proposition 6. We want to show that $(a_1a_2, B', C') \sim (a_1a_2, B, C)$. We have that $B' \equiv_{2a_1a_2} B$ and so $B' = B + 2a_1a_2l$ for some integer l. We see that
$$(a_1a_2, B', C').S^l = (a_1a_2, B, a_1a_2l^2 + B'l + C'),$$
Put $X = a_1a_2l^2 + B'l + C'$. Since the discriminant is preserved, we have that $D = B^2 - 4a_1a_2C = B^2 - 4a_1a_2X$ and thus $X = C$. Hence $(a_1a_2, B', C') \sim (a_1a_2, B, C)$ and we are done. $\square$

Definition 12. Let $(f, g) \in \mathfrak{Q}_D^2$ be a pair of forms. Then $(f', g') \in \mathfrak{Q}_D^2$ is said to be a uniting of (f, g) if $f' \sim f$, $g' \sim g$, and f' and g' are united.

Remark 2. By proposition 5 we have that for any $(f, g) \in \mathfrak{Q}_D^2$ there exists a uniting of (f, g).

Lemma 9. Let $f = (a_1, b_1, c_1), g = (a_2, b_2, c_2) \in \mathfrak{Q}_D$. Then $f \sim g$ if and only if there exists integers α and γ such that
$$\begin{aligned} a_1\alpha^2 + b_1\alpha\gamma + c_1\gamma^2 &= a_2 \\ 2a_1\alpha + (b_1 + b_2)\gamma &\equiv_{2a_2} 0 \\ (b_1 - b_2)\alpha + 2c_1\gamma &\equiv_{2a_2} 0. \end{aligned} \tag{2.4}$$

Proof. Recall that $f \sim g$ if and only if there exists integers $\alpha, \beta, \gamma, \delta$ such that
$$\begin{aligned} a_1\alpha^2 + b_1\alpha\gamma + c_1\gamma^2 &= a_2 \\ b_1(\alpha\delta + \beta\gamma) + 2(a_1\alpha\beta + c_1\gamma\delta) &= b_2 \\ a_1\beta^2 + b_1\beta\delta + c_1\delta^2 &= c_2 \\ \alpha\delta - \beta\gamma &= 1. \end{aligned} \tag{2.5}$$

Suppose now that $f \sim g$. Then the first equation of (2.4) is immediate. We further have that
$$2a_1\alpha + (b_1 + b_2)\gamma - 2a_2\delta = 2\alpha a_1(1 + \beta\gamma - \alpha\delta) + \gamma b_1(1 + \beta\gamma - \alpha\delta) = 0,$$
and
$$(b_1 - b_2)\alpha + 2c_1\gamma + 2a_2\beta = \alpha b_1(1 + \beta\gamma - \alpha\delta) + 2\gamma c_1(1 + \beta\gamma - \alpha\delta) = 0.$$
Hence the second and third equations of (2.4) are satisfied.

Suppose now that equations (2.4) hold. Then the first equation of (2.4) holds, so we only need to find integers β, δ such that the the last three equations of (2.5) hold. Inspired by the above, we put
$$\delta = \frac{2a_1\alpha + (b_1 + b_2)\gamma}{2a_2},$$
and
$$-\beta = \frac{(b_1 - b_2)\alpha + 2c_1\gamma}{2a_2}.$$
Then
$$\alpha\delta - \beta\gamma = \frac{a_1\alpha^2 + b_1\alpha\gamma + c_1\gamma^2}{a_2} = 1,$$
and
$$b_1(\alpha\delta + \beta\gamma) + 2(a_1\alpha\beta + c_1\gamma\delta) = b_2\frac{a_1\alpha^2 + b_1\alpha\gamma + c_1\gamma^2}{a_2} = b_2,$$
Finally, we have that
$$4a_2(a_1\beta^2 + b_1\beta\delta + c_1\delta^2) = (a_1\alpha^2 + b_1\alpha\gamma + c_1\gamma^2)(b_2^2 - b_1^2 + 4a_1c_1) = 4a_2c_2,$$
where in the last step we used that $\Delta_f = \Delta_g = D$, and so
$$4a_2c_2 = b_2^2 - D = b_2^2 - b_1^2 + 4a_1c_1.$$
$\square$

Lemma 10. Let $\circ_3 : \mathfrak{Q}_D^2 \to H(D)$ be defined by

$$f \circ_3 g = f_u \circ_2 g_u,$$

where (f_u, g_u) is any uniting of f and g. Then $\circ_3$ is well-defined.

Proof. Suppose we have two unitings $(f_u, g_u), (f_v, g_v)$ of f and g. We want to show that $f_u \circ_2 g_u = f_v \circ_2 g_v$. Write

$$\begin{aligned} f_u &= (a_1, b_1, c_1) \sim (a_1, B, a_2C) \\ g_u &= (a_2, b_2, c_2) \sim (a_2, B, a_1C) \\ f_v &= (a_1', b_1', c_1') \sim (a_1', B', a_2'C') \\ g_v &= (a_2', b_2', c_2') \sim (a_2', B', a_1'C'), \end{aligned}$$

where B, C and B', C' are some integers on the same form as in proposition 6. Then

$$\begin{aligned} f_u \circ_2 g_u &= [(a_1a_2, B, C)] \\ f_v \circ_2 g_v &= [(a_1'a_2', B', C')], \end{aligned}$$

Hence we are done if we can show that $(a_1a_2, B, C) \sim (a_1'a_2', B', C')$. We notice first that $f \sim f_u \sim f_v$ and $g \sim g_u \sim g_v$, so that

$$\begin{aligned} (a_1, B, a_2C) &\sim (a_1', B', a_2'C') \\ (a_2, B, a_1C) &\sim (a_2', B', a_1'C'). \end{aligned}$$

Applying lemma 9, we have that there exists integers x_1, y_1, x_2, y_2 such that

$$\begin{aligned} a_1x_1^2 + Bx_1y_1 + a_2Cy_1^2 &= a_1' \\ 2a_1x_1 + (B + B')y_1 &\equiv_{2a_1'} 0 \\ (B - B')x_1 + 2a_2Cy_1 &\equiv_{2a_1'} 0 \\ a_2x_2^2 + Bx_2y_2 + a_1Cy_2^2 &= a_2' \\ 2a_2x_2 + (B + B')y_2 &\equiv_{2a_2'} 0 \\ (B - B')x_2 + 2a_1Cy_2 &\equiv_{2a_2'} 0. \end{aligned}$$

If we can find integers X, Y such that

$$\begin{aligned} a_1a_2X^2 + BXY + CY^2 &= a_1'a_2' \\ 2a_1a_2X + (B + B')Y &\equiv_{2a_1'a_2'} 0 \\ (B - B')X + 2CY &\equiv_{2a_1'a_2'} 0, \end{aligned}$$

we are done. Put

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & -C \\ 0 & a_1 & a_2 & B \end{pmatrix} \begin{pmatrix} x_1x_2 \\ x_1y_2 \\ y_1x_2 \\ y_1y_2 \end{pmatrix}.$$

We then have that

$$a_1'a_2' = (a_1x_1^2 + Bx_1y_1 + a_2Cy_1^2)(a_2x_2^2 + Bx_2y_2 + a_1Cy_2^2) = a_1a_2X^2 + BXY + CY^2.$$

It remains to verify the congruences. We have that[1]

$$2(a_1x_1 + \frac{B+B'}{2}y_1)(a_2x_2 + \frac{B+B'}{2}y_2) \equiv_{2a_1'a_2'} 2a_1a_2X + (B+B')Y,$$

and so $2a_1a_2X + (B+B')Y \equiv_{2a_1'a_2'} 0$. We also have that

$$\begin{aligned}
2a_1(\frac{B-B'}{2}X + CY) &\equiv_{2a_1'a_2'} 2(a_1x_1 + \frac{B+B'}{2}y_1)(\frac{B-B'}{2}x_2 + a_1Cy_2)\\
2a_2(\frac{B-B'}{2}X + CY) &\equiv_{2a_1'a_2'} 2(\frac{B-B'}{2}x_1 + a_2Cy_1)(a_2 + \frac{B+B'}{2}y_2)\\
(B-B')(\frac{B-B'}{2}X + CY) &\equiv_{2a_1'a_2'} 2(\frac{B-B'}{2}x_1 + a_2Cy_1)(\frac{B-B'}{2}x_2 + a_1Cy_2)\\
(B+B')(\frac{B-B'}{2}X + CY) &\equiv_{2a_1'a_2'} 2C(a_1x_1 + \frac{B+B'}{2}y_1)(a_2x_2 + \frac{B+B'}{2}y_2).
\end{aligned}$$

This yields that

$$a_1(\frac{B-B'}{2}X + CY) \equiv_{a_1'a_2'} a_2(\frac{B-B'}{2}X + CY) \equiv_{a_1'a_2'} 0,$$

and summing the last two congruences

$$B(\frac{B-B'}{2}X + CY) \equiv_{a_1'a_2'} 0.$$

Hence we have for any $k_1, k_2, k_3 \in \mathbb{Z}$ that

$$(k_1a_1 + k_2a_2 + k_3B)(\frac{B-B'}{2}X + CY) \equiv_{2a_1'a_2'} 0.$$

Notice now that $\gcd(a_1, a_2, B) \mid \gcd(a_1, B, a_2C) = 1$ so that $\gcd(a_1, a_2, B) = 1$. By the extended Euclidean algorithm we have that there exists $l_1, l_2, l_3 \in \mathbb{Z}$ such that $l_1a_1 + l_2a_2 + l_3C = 1$. Consequently

$$\frac{B-B'}{2}X + CY = (l_1a_1 + l_2a_2 + l_3B)(\frac{B-B'}{2}X + CY) \equiv_{a_1'a_2'} 0,$$

and we are done.

We conclude that $(a_1a_1, B, C) \sim (a_1'a_2', B', C')$ and so $f_u \circ_2 g_u = f_v \circ_2 g_v$. □

Proposition 7. Let $\circ : H(D)^2 \to H(D)$ be defined by

$$[f] \circ [g] = f \circ_3 g.$$

Then $\circ$ is well-defined.

Proof. Let $f_1 \sim f_2, g_1 \sim g_2 \in \mathfrak{Q}_D$, and let $(f_1^u, g_1^u), (f_2^u, g_2^u)$ be unitings of (f_1, g_1) and (f_2, g_2) respectively. We have that

$$f_1 \circ_3 g_1 = f_1^u \circ_2 g_1^u,$$

and

$$f_2 \circ_3 g_2 = f_2^u \circ_2 g_2^u.$$

We have that $f_2^u \sim f_2 \sim f_1$ and $g_2^u \sim g_2 \sim g_1$, and consequently (f_2^u, g_2^u) is a uniting of (f_1, g_1). Consequently

$$f_2^u \circ_2 g_2^u = f_1 \circ_3 g_1,$$

and we are done. □

[1] Use that $B'^2 = D + 4a_1'a_2'C' = B^2 - 4a_1a_2C + 4a_1'a_2'C'$.

Theorem 2. Let D be a negative integer. Then $(H(D), \circ)$ is a finite abelian group.

Proof. Let $F = [(a_1, b_1, c_1)], G, H \in H(D)$. By lemmas 5 and 6 there exists integers $a_2, a_3, b_2, b_3, c_2, c_3$ such that $G = [(a_2, b_2, c_3)]$, $H = [(a_3, b_3, c_3)]$ and

$$\gcd(a_2, 2a_1) = \gcd(a_3, 2a_1a_2) = 1.$$

Consequently

$$\gcd(a_1, a_2) = \gcd(a_1, a_3) = \gcd(a_2, a_3) = 1,$$

and so $(a_1, b_1, c_1), (a_2, b_2, c_2), (a_3, b_3, c_3)$ are pairwise united. We now have that

$$\begin{aligned}
(F \circ G) \circ H &= ((a_1, b_1, c_1) \circ_3 (a_2, b_2, c_2)) \circ H \\
&= ((a_1, b_1, c_1) \circ_2 (a_2, b_2, c_2)) \circ H \\
&= [(a_1, B, Ca_2) \circ_1 (a_2, B, Ca_1)] \circ H \\
&= [(a_1a_2, B, C)] \circ H \\
&= (a_1a_2, B, C) \circ_2 (a_3, b_3, c_3) \\
&= [(a_1a_2a_3, B', C')],
\end{aligned}$$

where B, B', C, C' are as in proposition 6. In particular

$$\begin{aligned}
B &\equiv_{2a_1} b_1 \\
B &\equiv_{2a_2} b_2 \\
B' &\equiv_{2a_1a_2} B \\
B' &\equiv_{2a_3} b_3.
\end{aligned}$$

This implies that

$$\begin{aligned}
B &\equiv_{2a_1} b_1 \\
B &\equiv_{a_2} b_2 \\
B' &\equiv_{2a_1a_2} B \\
B' &\equiv_{a_3} b_3,
\end{aligned}$$

which in turn implies that

$$\begin{aligned}
B' &\equiv_{2a_1} b_1 \\
B' &\equiv_{a_2} b_2 \\
B' &\equiv_{a_3} b_3.
\end{aligned}$$

Similarly, we have that

$$\begin{aligned}
F \circ (G \circ H) &= F \circ ((a_2, b_2, c_2) \circ_2 (a_3, b_3, c_3)) \\
&= F \circ [(a_2a_3, D, E)] \\
&= (a_1, b_1, c_1) \circ_2 (a_2a_3, D, E) \\
&= [(a_1a_2a_3, D', E')],
\end{aligned}$$

where D, D', E, E' are as in proposition 6. In particular we have as above that

$$\begin{aligned}
D &\equiv_{2a_2} b_2 \\
D &\equiv_{2a_3} b_3 \\
D' &\equiv_{2a_1} b_1 \\
D' &\equiv_{2a_2a_3} D.
\end{aligned}$$

This implies that

$$\begin{aligned} D &\equiv_{a_2} b_2 \\ D &\equiv_{a_3} b_3 \\ D' &\equiv_{2a_1} b_1 \\ D' &\equiv_{a_2a_3} D, \end{aligned}$$

which in turn implies that

$$\begin{aligned} D' &\equiv_{2a_1} b_1 \\ D' &\equiv_{a_2} b_2 \\ D' &\equiv_{a_3} b_3. \end{aligned}$$

By the Chinese remainder theorem, we have that $D' = B' + 2a_1a_2a_3\delta$ for some $\delta \in \mathbb{Z}$, and so

$$(a_1a_2a_3, B', C').T^\delta = (a_1a_2a_3, D', *) = (a_1a_2a_3, D', E').$$

We thus conclude that $F \circ (G \circ H) = (F \circ G) \circ H$ and so $\circ$ is associative.

With B, C the same as above, we also have that

$$F \circ G = [(a_1a_2, B, C)] = [(a_2a_1, B, C)] = G \circ F,$$

so that $\circ$ is commutative.

The form of the identity element depends on the residue of D modulo 4. If $D \equiv_4 0$, put $I = [(1, 0, -D/4)]$. Since (a_1, b_1, c_1) and $(1, 0, -D/4)$ are united, we find that

$$F \circ I = [(a_1, B, C)],$$

where B, C are any integers that satisfies

$$\begin{aligned} B &\equiv_{2a_1} b_1 \\ B &\equiv_2 0 \\ B^2 &\equiv_{4a_1} D \\ C &= \frac{B^2 - D}{4a_1}. \end{aligned}$$

Since $b_1^2 \equiv_4 0$, we have that $b_1 \equiv_2 0$, and hence $B = b_1$ and $C = \frac{b_1^2 - D}{4a_1} = c_1$ solve the system. Consequently

$$F \circ I = [(a_1, b_1, c_1)] = F,$$

and so I is the identity element.

If $D \equiv_4 1$, put $I = [(1, 1, (1 - D)/4)]$. Since (a_1, b_1, c_1) and $(1, 1, (1 - D)/4)$ are united, we find that

$$F \circ I = [(a_1, B, C)],$$

where B, C are any integers that satisfies

$$\begin{aligned} B &\equiv_{2a_1} b_1 \\ B &\equiv_2 1 \\ B^2 &\equiv_{4a_1} D \\ C &= \frac{B^2 - D}{4a_1}. \end{aligned}$$

Since $b_1^2 \equiv_4 1$, we have that $b_1 \equiv_2 1$, and hence $B = b_1$, $C = c_1$ is again a solution. Hence $F \circ I = F$, and so I is the identity element. Let henceforth I denote the identity element.

It remains to find inverses. Put $Q = [(c_1, b_1, a_1)]$. We have that $(a_1, c_1, \frac{b_1+b_1}{2}) = (a_1, b_1, c_1) = 1$, and so (a_1, b_1, c_1) and (c_1, b_1, a_1) are united. Hence

$$F \circ Q = [(a_1 c_1, B, C)],$$

where B, C are any integers such that

$$\begin{aligned} B &\equiv_{2a_1} b_1 \\ B &\equiv_{2c_1} b_1 \\ B^2 &\equiv_{4a_1c_1} D \\ C &= \frac{B^2 - D}{4a_1c_1}. \end{aligned}$$

Evidently $B = b_1$ and $C = 1$ will do. Hence

$$F \circ Q = [(a_1c_1, b_1, 1)] = [(a_1c_1, b_1, 1).S] = [(1, -b_1, a_1c_1)].$$

If $D \equiv_4 0$ we have that $b_1 \equiv_2 0$ and so $b_1 = 2\delta$ for some $\delta \in \mathbb{Z}$. Consequently

$$[(1, -b_1, a_1c_1)] = [(1, -b_1, a_1c_1).T^{\delta}] = [(1, 0, *)] = [(1, 0, -D/4)] = I.$$

If $D \equiv_4 1$ we have that $b_1 \equiv_2 1$ and so $b_1 = 2\delta + 1$ for some $\delta \in \mathbb{Z}$. Consequently

$$[(1, -b_1, a_1c_1)] = [(1, -b_1, a_1c_1).T^{\delta+1}] = [(1, 1, *)] = [(1, 1, (1-D)/4)] = I,$$

and we conclude that $H(D)$ is an abelian group. By theorem 1, it is finite, and so we are done. □

2.3 Number fields

We shall now adopt a different point of view – that of number fields.

Definition 13. We say that a field K containing $\mathbb{Q}$ which is finite-dimensional as a vector space over $\mathbb{Q}$ is a number field. The dimension of K over $\mathbb{Q}$ is called the degree of K and is denoted by $[K : \mathbb{Q}]$.

Proposition 8. Let K be a number field. Then there exists a number $\theta \in K$ such that $K = \mathbb{Q}(\theta)$. Such a number is called a primitive element of K.

Proof. See [ST01, p. 56] or [DF04, p. 509]. □

Definition 14. We say that a number field K of degree 2, i. e. $K = \mathbb{Q}(\sqrt{D})$, with D a square-free integer, is a quadratic (number) field. If $D < 0$ we say that K is a imaginary quadratic field, and if $D > 0$ we say that K is a real quadratic field.

Proposition 9. Let K be a number field and let $\alpha \in K$. Then there exists a unique non-zero monic polynomial $p \in \mathbb{Q}[x]$ such that $p(\alpha) = 0$, with smallest degree.

Proof. We first prove that α is zero of some monic polynomial $f \in \mathbb{Q}[x]$. Let $n = [K : \mathbb{Q}]$. Then the elements $1, \alpha, \dots, \alpha^n$ are $\mathbb{Q}$-linearly dependent, and hence there are numbers $a_i \in \mathbb{Q}$, not all zero, such that

$$a_n\alpha^n + \dots + a_1\alpha + a_0 = 0.$$

We may without loss of generality assume that $a_n \neq 0$, and so we put

$$f(x) = x^n + \frac{a_{n-1}}{a_n}x^{n-1} + \dots + \frac{a_1}{a_n}x + \frac{a_0}{a_n} \in \mathbb{Q}[x].$$

Let now S be the set of all non-zero monic polynomials in $\mathbb{Q}[x]$ that has α as a zero. We want to prove that S has unique minimal element with respect to the degree. The existence of a minimal element follows from the well-ordering principle. Suppose f, g are two minimal elements. Then $\deg(f) = \deg(g)$ because otherwise one of them would be non-minimal. By the division algorithm, we have that

$$f(x) = q(x)g(x),$$

for some $q \in \mathbb{Q}[x]$. Clearly $\deg(q) = 0$, and so q is constant. Since f, g are both monic, we must therefore have that $q = 1$, and we are done. □

Definition 15. Let K be a number field and let $\alpha \in K$. Then the polynomial of proposition 9 is called the minimal polynomial of α, and is denoted by $\operatorname{minpol}_\alpha$.

Remark 3. Evidently minimal polynomials are irreducible. Recall also that number fields are separable, in other words for any $\alpha \in K$, we have that $\operatorname{minpol}_\alpha$ has distinct zeros in $\overline{K}$.

Proposition 10. Let $K = \mathbb{Q}(\theta)$ be a number field of degree n. Then there are exactly n distinct embeddings $\sigma_i : K \to \mathbb{C}$ of K in $\mathbb{C}$. The elements $\sigma_i(\theta) = \theta_i$ are the distinct zeros in $\mathbb{C}$ of $\operatorname{minpol}_\theta$.

Proof. See [ST01, p. 38] or [DF04, p. 487]. □

Definition 16. Let K be a number field. We say that $\alpha \in K$ is an algebraic integer of K if there exists a monic polynomial $p \in \mathbb{Z}[x]$ such that $p(\alpha) = 0$. The set of algebraic integers of K is denoted by $\mathbb{Z}_K$.

Lemma 11. Let K be a number field. Then $\alpha \in K$ is an algebraic integer of K if and only if $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-module.

Proof. Suppose $\mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-module, say with generating set $\{g_1(\alpha), \ldots, g_n(\alpha)\}$ for some polynomials $g_1, \ldots, g_n \in \mathbb{Z}[x]$. Put $N = \max_{1 \le i \le n} g_i$. Evidently $\alpha^{N+1} \in \mathbb{Z}[\alpha]$ and hence there exists integers $k_1, \ldots, k_n$ such that

$$\alpha^{N+1} = \sum_{i=1}^{n} k_i g_i(\alpha).$$

Put therefore $p(x) = x^{N+1} - \sum_{i=1}^{n} k_i g_i(x)$. It is clear that $p \in \mathbb{Z}[x]$, and since $\deg(\sum_{i=1}^{n} k_i g_i(x)) = N$, we have that p is monic. Hence α is an algebraic integer.

Suppose now that α is an algebraic integer, say a zero of $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. I claim that $G = \{\alpha^{n-1}, \ldots, \alpha, 1\}$ is a generating set. To see this, let $\beta \in \mathbb{Z}[\alpha]$. Then

$$\beta = b_N \alpha^N + \cdots + b_1 \alpha + b_0.$$

If we can show that α^k is a $\mathbb{Z}$-combination of G for any non-negative integer k, we see from the above that we are done. Clearly, it is true whenever $k < n$, because then $\alpha^k \in G$. For $k \ge n$, we use induction. As for the base case, we see that

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_1\alpha - a_0,$$

and we are done with the base case. As for the inductive step, we let $k \ge n$ and assume that α^l is a $\mathbb{Z}$-combination of G whenever $l \le k$. We thus have that

$$\alpha^{k+1} = \alpha(k_0 + k_1\alpha + \cdots + k_{n-1}\alpha^{n-1}),$$

for some integers k_i. Consequently

$$\alpha^{k+1} = -k_{n-1}a_0 + (k_0 - k_{n-1}a_1)\alpha + (k_1 - k_{n-2}a_2)\alpha^2 + \cdots + (k_{n-2} - a_{n-1})\alpha^{n-1},$$

and we are done with the inductive step. □

Proposition 11. Let K be a number field. Then $\mathbb{Z}_K$ is a ring.

Proof. Let $\alpha, \beta \in \mathbb{Z}_K$. We only have to verify that $0, 1, -\alpha, \alpha\beta, \alpha + \beta \in \mathbb{Z}_K$. As for the first and second, note that 0 is a zero of $x \in \mathbb{Z}[x]$, and that 1 is zero of $x - 1 \in \mathbb{Z}[x]$. As for the third, let $p(x) \in \mathbb{Z}[x]$ be monic such that $p(\alpha) = 0$. Then clearly $-\alpha$ is a zero of $p(-x)$. As for the fourth, we may without loss of generality assume that $\beta \neq 0$. With p as before, let $n = \deg(p)$. Put $q(x) = \beta^n p(x/\beta)$ and notice that q is monic. Clearly $q(\alpha\beta) = 0$ and we are done.

The fifth is easy to prove with lemma 11. We have that $\mathbb{Z}[\alpha], \mathbb{Z}[\beta]$ are finitely generated $\mathbb{Z}$-modules and want to show that $\mathbb{Z}[\alpha+\beta]$ is a finitely generated $\mathbb{Z}$-module. Say that $\mathbb{Z}[\alpha]$ is generated by $G = \{g_1, \dots, g_n\}$ and that $\mathbb{Z}[\beta]$ is generated by $H = \{h_1, \dots, h_m\}$. I claim that $F = \{g_i h_j\}_{1 \leq i \leq n, 1 \leq j \leq m}$ generates $\mathbb{Z}[\alpha + \beta]$. As in the proof of the lemma, it is enough to show that $(\alpha+\beta)^n$ is a $\mathbb{Z}$-combination of F for any non-negative integer n. We have that

$$(\alpha + \beta)^n = \sum_{k=0}^{N} \binom{n}{k} \alpha^k \beta^{n-k},$$

and so it is enough to show that $\alpha^i \beta^j$ is a $\mathbb{Z}$-combination of F for any non-negative integers i, j. Clearly

$$\alpha^i \beta^j = (k_{i1} g_1 + \cdots + k_{in} g_n)(l_{j1} h_1 + \cdots + l_{jm} h_m) = \sum_{\substack{1 \leq r \leq n \\ 1 \leq s \leq m}} k_{ir} l_{js} g_r h_s,$$

and we are done. □

Definition 17. Let K be a number field. Then a fractional ideal I of $\mathbb{Z}_K$ is a subset of K on the form $I = \frac{1}{d} J$ where J is non-zero ideal of $\mathbb{Z}_K$ and $d \neq 0$ is an integer. The set of fractional ideals of $\mathbb{Z}_K$ is denoted by $\mathcal{I}(K)$.

Remark 4. Notice that I is a non-zero $\mathbb{Z}_K$-submodule of K such that there exists a non-zero integer d with dI an ideal of $\mathbb{Z}_K$. This can be taken as the definition of a fractional ideal.

Lemma 12. Let I be a $\mathbb{Z}_K$-submodule of K. Then I is an ideal of $\mathbb{Z}_K$ if and only if $I \subset \mathbb{Z}_K$.

Proof. If I is an ideal $\mathbb{Z}_K$, then obviously $I \subset \mathbb{Z}_K$. Suppose therefore that $I \subset \mathbb{Z}_K$. We have already that $(I, +)$ is a subgroup of $(K, +)$, and since $(\mathbb{Z}_K, +)$ also is a subgroup of $(K, +)$, we have that $(I, +)$ is a subgroup of $(\mathbb{Z}_K, +)$. Closure under multiplication by elements from $\mathbb{Z}_K$ follows by definition of being a $\mathbb{Z}_K$-module. □

Proposition 12. Let K be a number field, and let I be a $\mathbb{Z}_K$-submodule of K. It holds that I is a fractional ideal if and only if there exists a $d \in \mathbb{Z}_K \setminus \{0\}$ such that $dI \subset \mathbb{Z}_K$.

Proof. Suppose I is a fractional ideal. Then there exists a non-zero integer d such that dI is an ideal in $\mathbb{Z}_K$. Since also $d \in \mathbb{Z}_K$, and $dI \subset \mathbb{Z}_K$, we are done with one direction.

Suppose that $I \subset K$ satisfies that $dI \subset \mathbb{Z}_K$ for some $d \in \mathbb{Z}_K \setminus \{0\}$. Let $p = \mathrm{minpol}_d$ and put $n = \deg(p)$ and write $p(x) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_{n-1})(x - d)$. Note also that all $\alpha_i = 0$ for else p would be reducible. Now $d' = (-1)^n \alpha_1 \alpha_2 \dots \alpha_{n-1} d = [x^0] p \in \mathbb{Z}$, and by multiplicative closure, we have that $d' I \subset \mathbb{Z}_K$, and so $d' I \subset \mathbb{Z}_K$ is an ideal of $\mathbb{Z}_K$. □

Definition 18. Let $I, J \in \mathcal{I}(K)$. The product of I and J is defined to be

$$IJ = \{\sum_{i=1}^{n} a_i b_i : a_i \in I, b_i \in J, n \geq 1\}.$$

Proposition 13. Let $I, J \in \mathcal{I}(K)$. Then $IJ \in \mathcal{I}(K)$.

Proof. We have that $I = \frac{1}{d} I'$ and $J = \frac{1}{f} J'$, where I', J' are ideals in $\mathbb{Z}_K$. Hence

$$IJ = \{\frac{1}{df} \sum_{i=1}^{n} a_i b_i : a_i \in I', b_i \in J', n \geq 1\} = \frac{1}{df} I' J'.$$

Since $I' J'$ is an ideal in $\mathbb{Z}_K$, we are done. □

Remark 5. Notice that the product is commutative and for every $I \in \mathcal{I}(K)$ we have that $I\mathbb{Z}_K = I$.

Proposition 14. Let $A, B, C \in \mathcal{I}(K)$. Then $A(BC) = (AB)C$.

Proof. Let $x \in A(BC)$. Then $x = \sum_{i=1}^{n}\sum_{j=1}^{m_i} a_i b_{ij} c_{ij}$. For every i, j we see that $a_i b_{ij} c_{ij} = (a_i b_{ij}) c_{ij} \in (AB)C$, and hence by summation closure we have that $x \in (AB)C$. The converse is analogous and so we are done. $\square$

Definition 19. Let $I \in \mathcal{I}(K)$. If there exists a $J \in \mathcal{I}(K)$ such that $IJ = \mathbb{Z}_K$, we say that I is invertible.

The following notions are fundamental.

Definition 20. Let K be a number field of degree n over $\mathbb{Q}$, and let σ_i be the n distinct embeddings of K in $\mathbb{C}$. Then the characteristic polynomial C_α of α in K is

$$C_\alpha(x) = \prod_{i=1}^{n}(x - \sigma_i(\alpha)).$$

Furthermore, the trace $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$ of α in K is defined as

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = -[x^{n-1}]C_\alpha,$$

where the notation $[X]p$ denotes the coefficient of the term X in the expression p. The norm $\mathcal{N}_{K/\mathbb{Q}}(\alpha)$ of α in K is defined as

$$\mathcal{N}_{K/\mathbb{Q}}(\alpha) = (-1)^n[x^0]C_\alpha.$$

Remark 6. It is easy to see that the trace is $\mathbb{Q}$-linear, and that the norm is multiplicative.

Lemma 13. Let K be a number field of degree n and let $\alpha \in K$. Then $C_\alpha \in \mathbb{Q}[x]$. If furthermore $\alpha \in \mathbb{Z}_K$, then $C_\alpha \in \mathbb{Z}[x]$.

Proof. By proposition 8 we have that $K = \mathbb{Q}(\theta)$ for some $\theta \in K$. Recall that $\mathbb{Q}(\theta) = \mathbb{Q}[\theta]$ so that $\alpha = r(\theta)$ for some $r \in \mathbb{Q}[x]$ with $\deg(r) < n$.

We now see that $\sigma_i(\alpha) = \sigma_i(r(\theta)) = r(\theta_i)$, and hence the coefficients of C_α are symmetric polynomials $h_i \in \mathbb{Q}[\theta_1, \ldots, \theta_n]$. We have that any symmetric polynomial over $\mathbb{Q}$ is a polynomial over $\mathbb{Q}$ in the elementary symmetric polynomials of $\theta_1, \ldots, \theta_n$, and consequently the h_i are rational numbers.

The same argument shows that if $\alpha \in \mathbb{Z}_K$, then $C_\alpha \in \mathbb{Z}[x]$ $\square$

Proposition 15. Let K be a number field of degree n, σ_i be the n embeddings of K in $\mathbb{C}$, and $\{\alpha_j\}_{j=1}^n \subset K$. Then

$$\det((\sigma_i(\alpha_j))_{1\le i,j\le n})^2 = \det((\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j)_{1\le i,j\le n}).$$

This quantity is a rational number and is called the discriminant of $\{\alpha_j\}_{j=1}^n$ and is denoted by $d(\alpha_1, \ldots, \alpha_n)$. Furthermore $d(\alpha_1, \ldots, \alpha_n) = 0$ if and only if the α_js are linearly dependent over $\mathbb{Q}$.

Proof. See [Coh00, p. 163]. $\square$

Proposition 16. Let K be a number field, and let $n = [K : \mathbb{Q}]$. Then $\mathbb{Z}_K$ is a free $\mathbb{Z}$-module of rank n.

Proof. Let $(a_1, \ldots, a_n)$ be a basis of K over $\mathbb{Q}$. Since the a_i are algebraic, we have that there exists an integer b such that for all i we have that $ba_i \in \mathbb{Z}_K$. Let now $\phi : K \to \mathbb{Q}^n$ be defined by

$$\phi(x) = (\mathrm{Tr}_{K/\mathbb{Q}}(b_1 x), \ldots, \mathrm{Tr}_{K/\mathbb{Q}}(b_n x)).$$

Since the trace is $\mathbb{Q}$-linear, we have that ϕ is homomorphism of $\mathbb{Q}$-modules. We have further that if $x \in \mathbb{Z}_K$ then $C_x \in \mathbb{Z}[x]$, and so $\phi|_{\mathbb{Z}_K}$ is a homomorphism of $\mathbb{Z}$-modules from $\mathbb{Z}_K$ to $\mathbb{Z}^n$. By proposition 15, we have that ϕ is injective. We have further that $\phi(\mathbb{Z}_K)$ is an additive subgroup of $\mathbb{Z}^n$, and thus $\phi(\mathbb{Z}_K) \cong \mathbb{Z}^k$ for $k \le n$. This shows that $\mathbb{Z}_K \cong \phi(\mathbb{Z}_K)$ is a free $\mathbb{Z}$-module of rank $k \le n$. But since the $(b_1, \ldots, b_n)$ are linearly independent over $\mathbb{Q}$ and thus also over $\mathbb{Z}$, we find that $\mathrm{rank}(\mathbb{Z}_K) \ge n$. Consequently $\mathrm{rank}(\mathbb{Z}_K) = n$ and we are done. $\square$

Proposition 17. Let $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_n$ be bases of $\mathbb{Z}_K$. Then $d(\alpha_1, \ldots, \alpha_n) = d(\beta_1, \ldots, \beta_n)$.

Proof. See [Coh00, p. 164]. $\square$

Definition 21. Let K be a number field. Then the discriminant of K, denoted by $d(K)$, is the discriminant of any basis of $\mathbb{Z}_K$.

Lemma 14. Let K be a number field of degree n, and let I be any non-zero ideal of $\mathbb{Z}_K$. Then $|\mathbb{Z}_K/I| < \infty$.

Proof. Let $0 \neq \alpha \in I$. We have that $\mathcal{N}_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^n \sigma_i(\alpha)$, where the σ_i are the n embeddings. One of the σ_i is the identity, say without loss of generality that $\sigma_1 = \mathrm{id}$. Then $\mathcal{N}_{K/\mathbb{Q}}(\alpha) = \alpha \prod_{i=2}^n \sigma_i(\alpha)$. Clearly $\sigma_i(\alpha) \in \mathbb{Z}_K$ for all i, and thus $\mathcal{N}_{K/\mathbb{Q}}(\alpha) = \alpha\beta$ with $\beta \in \mathbb{Z}_K$. Putting $N = \mathcal{N}_{K/\mathbb{Q}}(\alpha)$ we thus have that $N \in I$, and so $(N) \subset I$. Therefore $\mathbb{Z}_K/I \subset \mathbb{Z}_K/(N)$.

By proposition 16, we have that $\mathbb{Z}_K \cong \mathbb{Z}^n$, and $(N) \cong N\mathbb{Z}^n$ as additive groups. Therefore $\mathbb{Z}_K/(N) \cong \mathbb{Z}^n/N\mathbb{Z}^n \cong (\mathbb{Z}/N\mathbb{Z})^n$, and we are done. $\square$

Definition 22. Let I be a non-zero ideal of $\mathbb{Z}_K$. Then the number $|\mathbb{Z}_K/I|$ is called the (absolute) norm of I, and is denoted by $\mathcal{N}(I)$. If $\alpha \in K$, we put $\mathcal{N}(aI) = |\mathcal{N}_{K/\mathbb{Q}}(a)|\mathcal{N}(I)$.

Proposition 18. Let $I \in \mathcal{I}(K)$, and let $n = [K : \mathbb{Q}]$. Then I is a free $\mathbb{Z}$-module of rank n.

Proof. Since non-integral fractional ideals are just non-zero multiples of integral ideals, we may assume that I is a non-zero integral ideal. We have that I is a $\mathbb{Z}$-submodule of the $\mathbb{Z}$-module $\mathbb{Z}_K$. Since $\mathbb{Z}$ is a PID, we have that I is free with rank k for some $k \leq n$. If $k < n$, we'd have that $|\mathbb{Z}_K/I| = \infty$, which contradicts lemma 14. Hence $k = n$ and we are done. $\square$

Proposition 19. Let $0 \neq P \subset \mathbb{Z}_K$ be a prime ideal. Then P is maximal.

Proof. By lemma 14 we have that $\mathbb{Z}_K/P$ is a finite integral domain and thus a field.[2] Hence P is maximal. $\square$

Lemma 15. Let $I \subset \mathbb{Z}_K$ be a non-zero ideal. Then I contains a product of non-zero prime ideals.

Proof. We will prove the lemma by induction on $|\mathbb{Z}_K/I|$. Assume the lemma is false, and let I be a non-zero ideal with minimal $|\mathbb{Z}_K/I|$ that doesn't contain a product of non-zero prime ideals. Clearly $\mathbb{Z}_K$ contains products of non-zero prime ideals, and thus $I \neq \mathbb{Z}_K$. Consequently $|\mathbb{Z}_K/I| \geq 2$. Moreover, we have that I cannot itself be a prime ideal, and thus there exists $x, y \notin I$ such that $xy \in I$. With these x, y we have that $(x) + I, (y) + I \supsetneq I$, and so $|\frac{\mathbb{Z}_K}{(x)+I}|, |\frac{\mathbb{Z}_K}{(y)+I}| < |\mathbb{Z}_K/I|$. We therefore have prime ideals $P_1, \ldots, P_r$ and $Q_1, \ldots, Q_s$ such that

$$P_1 \cdots P_r \subset (x) + I,$$

and

$$Q_1 \cdots Q_s \subset (y) + I.$$

Consequently

$$P_1 \cdots P_r Q_1 \cdots Q_r \subset ((x) + I)((y) + I) = (xy) + xI + yI + I^2 \subset I,$$

and we have a contradiction. $\square$

Lemma 16. Let $I \in \mathcal{I}(K)$, and put $\tilde{I} = \{x \in \mathbb{Z}_K : xI \subset \mathbb{Z}_K\}$. Then $\tilde{I} \in \mathcal{I}(K)$.

Proof. If $x, y \in \tilde{I}$ then $(x + y)I \subset xI + yI \subset \mathbb{Z}_K$ so that $x + y \in \tilde{I}$. If $d \in \mathbb{Z}_K$ and $x \in \tilde{I}$, then $(dx)I \subset d\mathbb{Z}_K \subset \mathbb{Z}_K$. It follows that $\tilde{I}$ is $\mathbb{Z}_K$-submodule of $\mathbb{Z}_K$.

Since $I \in \mathbb{Z}_K$, there exists a $d \in \mathbb{Z}_K \setminus \{0\}$ such that $dI \subset \mathbb{Z}_K$. Furthermore, since $I \neq 0$ there exists an element $x \in I$ such that $x \neq 0$. Consequently $dx \in \mathbb{Z}_K \setminus \{0\}$. Let now $y \in dx\tilde{I}$, then $y = dxy'$ for some $y' \in \tilde{I}$. Since $y' \in \tilde{I}$ we have that $y'x \in y'I \subset \mathbb{Z}_K$, and thus $y \in \mathbb{Z}_K$. Hence $dx\tilde{I} \subset \mathbb{Z}_K$ whence we conclude that $\tilde{I} \in \mathcal{I}(K)$, as desired. $\square$

[2] Let A be a finite integral domain, and let $0 \neq x \in A$. Consider the set $S = \{xa : a \in A\}$, and notice that since A is an integral domain, all the elements of S are distinct. Hence $S = A$, and thus there exists an element $y \in A$ such that $xy = 1$.

Lemma 17. Let $I \in \mathcal{I}(K)$. If I is invertible, then the inverse is unique and is given by $\tilde{I}$.

Proof. We first prove uniqueness. Say that J_1 and J_2 are inverses of I. Then

$$J_1 = J_1\mathbb{Z}_K = J_1(IJ_2) = (J_1I)J_2 = \mathbb{Z}_K J_2 = J_2,$$

and we have uniqueness.

Let now J be such that $IJ = \mathbb{Z}_K$. If $y \in J$, then $yI \subset IJ = \mathbb{Z}_K$ so that $y \in \tilde{I}$. Hence $J \subset \tilde{I}$. Multiplying by I we thus have that $\mathbb{Z}_K \subset \tilde{I}I$. If $x \in \tilde{I}$, then $xI \subset \mathbb{Z}_K$ and thus $\tilde{I}I \subset \mathbb{Z}_K$. Hence $\tilde{I}I = \mathbb{Z}_K$, and we are done. $\square$

Lemma 18. Let $P \subset \mathbb{Z}_K$ be a prime ideal. If $0 \neq A, B \subset \mathbb{Z}_K$ are ideals such that $P \supset AB$, then $P \supset A$ or $P \supset B$.

Proof. Say that $P \not\supset A$, and let $x \in A$ be such that $x \notin P$. Let $y \in B$, then $xy \in AB \subset P$ and so, using that P is prime, we have that $x \in P$ or $y \in P$. But we know that $x \notin P$ and so $y \in P$. We conclude that $B \subset P$. $\square$

Lemma 19. Let $\alpha \in K$. We have that $\alpha \in \mathbb{Z}_K$ if and only if there exists a non-zero finitely generated $\mathbb{Z}$-submodule A of K such that $\alpha A \subset A$.

Proof. Suppose $\alpha \in \mathbb{Z}_K$. Then $A = \mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-submodule of K, and clearly $\alpha A \subset A$.

Suppose A is a finitely generated $\mathbb{Z}$-module such that $\alpha A \subset A$. Let $\phi : A \to A$ be defined by $\phi(x) = \alpha x$. Since $\alpha A \subset A$ we see that ϕ is an endomorphism of $\mathbb{Z}$-modules. We have further that $\phi(A) = \alpha A \subset \mathbb{Z}A$, and so by proposition 2.4 of [AM94] we have that

$$\phi^n + a_1\phi^{n-1} + \cdots + a_n = 0,$$

where $a_i \in \mathbb{Z}$ for all i. We see that $\phi^n(\alpha) = \alpha^{n+1}$, and thus $\alpha \in \mathbb{Z}_K$ as claimed. $\square$

Lemma 20. Let $0 \neq P \subset \mathbb{Z}_K$ be a prime ideal. Then $\tilde{P}$ satisfies the following properties.

(i) $\mathbb{Z}_K \subsetneq \tilde{P}$

(ii) $P\tilde{P} = \mathbb{Z}_K$

Proof. It is immediate that $\mathbb{Z}_K \subset \tilde{P}$ and hence to show the first part we only need to show that $\tilde{P} \setminus \mathbb{Z}_K$ is non-empty. Let $0 \neq x \in P$. Then $(x) \subset P$. By lemma 15 we also have that

$$(x) \supset P_1 \cdots P_r,$$

for some non-zero prime ideals P_i. Let r be minimal. If $r = 1$, then $P \supset P_1$ and thus by maximality $P_1 = P$, so that $P = (x)$. It follows that $\tilde{P} = \frac{1}{x}\mathbb{Z}_K \neq \mathbb{Z}_K$.[3] We therefore assume that $r \geq 2$. Since $P \supset (x) \supset P_1 \cdots P_r$ we have that $P \supset P_i$ for some i, and thus by maximality $P = P_i$. Without loss of generality we have that $i = 1$. Hence $(x) \supset PP_2 \cdots P_r$. Since we picked r to be minimal, we have that $(x) \not\supset P_2 \cdots P_r$. Let therefore $y \in P_2 \cdots P_r$ be such that $y \notin (x)$. Now[4] $y/x \notin \mathbb{Z}_K$ and since also $yP \subset PP_2 \cdots P_r \subset (x)$, we have that $y/x \in \mathbb{Z}_K$. We thus conclude that $y/x \in \tilde{P} \setminus \mathbb{Z}_K$, whence (i) is proven.

As for (ii), let $x \in \tilde{P}$ be such that $x \notin \mathbb{Z}_K$. Evidently $xP \subset \mathbb{Z}_K$ and so $P \subset P + xP \subset \mathbb{Z}_K$. By maximality we thus have that $P + xP = \mathbb{Z}_K$ or $P + xP = P$. If the former holds, we have that $P + xP = P(\mathbb{Z}_K + x\mathbb{Z}_K) = \mathbb{Z}_K$ and so $\mathbb{Z}_K + x\mathbb{Z}_K$ is an inverse for P, whence by lemma 17 we have that $\tilde{P} = \mathbb{Z}_K + x\mathbb{Z}_K$. If the latter holds, we have that $xP \subset P$. But by proposition 18, we have that P is a finitely generated $\mathbb{Z}$-module, and thus by lemma 19 we have that $x \in \mathbb{Z}_K$. This is a contradiction, and thus we are done. $\square$

[3] For if they would be equal, then $x^{-1} \in \mathbb{Z}_K$, and thus $1 = x^{-1}x \in (x) = P$, whence $P = \mathbb{Z}_K$. But prime ideals are proper, and thus contradiction.

[4] For if this weren't so, then $y \in (x)$, and thus contradiction.

We have concluded that prime ideals of $\mathbb{Z}_K$ are invertible. Hence we write P^{-1} for the inverse of a non-zero prime ideal $P \subset \mathbb{Z}_K$.

Proposition 20. Let $I \subset \mathbb{Z}_K$ be an ideal different from 0 and $\mathbb{Z}_K$. Then I admits a factorization

$$I = P_1 \dots P_r,$$

into non-zero prime ideals P_i of $\mathbb{Z}_K$ which is unique up to the order of the factors.

Proof. We first concentrate on existence.

Let $r \geq 1$ be an integer. We are going to prove that if I contains a product of r prime ideals (which it does by lemma 15), then it is a product of prime ideals. As for the base case, say that $r = 1$. Then $I \supset P$, but since I is proper and P is maximal, we must have $I = P$, and so we are done.

Assume now that the statement holds for an integer $r > 1$, and say that $I \supset P_1 \dots P_{r+1}$ for some prime ideals P_i. Since I is proper, it is contained in a maximal ideal P. But then $P \supset P_1 \dots P_r$, whence we have as before that $P = P_i$ for some i. Hence we have $P_i \supset I \supset P_1 \dots P_{r+1}$. Multiplying by P_i^{-1}, we see that

$$\mathbb{Z}_K \supset P_i^{-1} I \supset P_1 \dots P_{i-1} P_{i+1} \dots P_{r+1}.$$

The first inclusion shows that $P_i^{-1} I$ is an ideal in $\mathbb{Z}_K$, and the second inclusion shows that it contains a product of r prime ideals. By the inductive assumption we thus have that

$$P_i^{-1} I = Q_1 \dots Q_n,$$

for some prime ideals Q_i. Multiplying by P_i, we get that

$$I = P_i Q_1 \dots Q_n,$$

and so we have proved existence.

We now concentrate on uniqueness. Say $I = P_1 \dots P_r = Q_1 \dots Q_s$. We can without loss of generality assume that $r \geq s \geq 1$. For every P_i, compare with the Q_j, and if they're equal, multiply the equation with P_i^{-1}. At the end of the process, we have that

$$P_{i_1} \dots P_{i_{r-s}} = \mathbb{Z}_K,$$

where $1 \leq i_1 \leq i_2 \leq \dots \leq i_{r-s} \leq r$. If $r > s$, we have a contradiction, because prime ideals are proper. Hence $r = s$, which means that every prime ideal was cancelled. In other words, we have that $P_i = Q_{\sigma(i)}$ for some permutation $\sigma \in S_r$. □

Proposition 21. Let $I \in \mathcal{I}(K)$. Then I is invertible with $I^{-1} = \tilde{I}$.

Proof. By lemma 17, it is enough to construct an inverse. We have that $I = \frac{1}{d} J$ for an integral ideal $J \subset \mathbb{Z}_K$, and a number $d \in \mathbb{Z}_K \setminus \{0\}$. If H is an inverse for J, we have that $(dH)(\frac{1}{d} J) = HJ = \mathbb{Z}_K$, so that dH is an inverse of I. Hence we only have to find an inverse of J.

If $J = \mathbb{Z}_K$, we have that $H = \mathbb{Z}_K$ is an inverse of J. If J is proper, we have by proposition 20 that $J = P_1 \dots P_r$ for prime ideals P_i. Let $H = P_1^{-1} \dots P_r^{-1}$. Since the product of ideals is commutative and associative, we see that $JH = P_1 P_1^{-1} \dots P_r P_r^{-1} = \mathbb{Z}_K$ so that H is an inverse of J. □

We have thus proved the following theorem.

Theorem 3. Let K be a number field. Then $\mathcal{I}(K)$ is an abelian group.

Definition 23. Let $I \in \mathcal{I}(K)$. Then I is principal if it is generated by one element. If I is generated by $g \in K \setminus \{0\}$, we write $I = (g)_{\mathbb{Z}_K}$. We also write $\mathcal{P}(K) = \{I \in \mathcal{I}(K) : I = (g)_{\mathbb{Z}_K} \text{ for some } g \in \mathbb{Z}_K\}$.

Proposition 22. Let $I \in \mathcal{I}(K)$. Then I is principal if and only if there exists a non-zero element $x \in \mathbb{Z}_K$, and an element $d \in \mathbb{Z}_K \setminus \{0\}$, such that $I = \frac{1}{d}(x)$.

Proof. Suppose that I is principal, say with generator $g \in I$. Since $I \in \mathcal{I}(K)$, we have that $dI = J$ for some ideal $J \subset \mathbb{Z}_K$ and $d \in \mathbb{Z}_K \setminus \{0\}$. We see that $dg \in J$ and thus $dg = x$ for some $x \in J \subset \mathbb{Z}_K$, and so $g = \frac{x}{d}$. If $y \in J$ is arbitrary, we thus have that $y = dfg$ for some $f \in \mathbb{Z}_K$. In other words $y = fx$, so that $J = (x)$.

If $I = \frac{1}{d}(x)$, then clearly $g = \frac{x}{d}$ generates I. We are done. □

Proposition 23. The set $\mathcal{P}(K)$ is a subgroup of $\mathcal{I}(K)$.

Proof. Let $I, J \in \mathcal{P}(K)$. We only need to show that $IJ \in \mathcal{P}(K)$. Say $I = (g)_{\mathbb{Z}_K}$ and $J = (h)_{\mathbb{Z}_K}$. I claim that $IJ = (gh)_{\mathbb{Z}_K}$. Let $x \in IJ$, then

$$x = \sum_{k=1}^{n} d_k g f_k h = (\sum_{k=1}^{n} d_k f_k) gh \in (gh)_{\mathbb{Z}_K}.$$

Let $x \in (gh)_{\mathbb{Z}_K}$. Then $x = agh$ for some $a \in \mathbb{Z}_K$. But $agh = (ag)(h) \in IJ$, and so we are done. □

Definition 24. The quotient group $\mathcal{I}(K)/\mathcal{P}(K)$ is denoted by $\mathrm{Cl}(K)$ and is called the ideal class group of K.

As for quadratic fields, it turns out that for negative so-called fundamental discriminants D, we have that $\mathrm{Cl}(\mathbb{Q}(\sqrt{D})) \cong H(D)$.

2.4 Equivalence

We now show the aforementioned isomorphism between the ideal class group and the form class group.

Proposition 24. Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field with d squarefree and $d \neq 1$. Let $1, \omega$ be an integral basis and $d(K)$ be the discriminant of K. Then if $d \equiv_4 1$ we can take $\omega = (1+\sqrt{d})/2$ and we have $d(K) = d$, while if $d \equiv_4 2$ or 3, we can take $\omega = \sqrt{d}$ and we have $d(K) = 4d$.

Proof. Since $\sqrt{d}$ is irrational or purely complex, we have that $\{1, \sqrt{d}\}$ and $\{1, (1+\sqrt{d})/2\}$ are linearly independent and hence we only have to show that they span $\mathbb{Z}_K$. To this end let $\alpha \in \mathbb{Z}_K$. If $\alpha \in \mathbb{Q}$ then the rational root theorem gives us that $\alpha \in \mathbb{Z}$ and we are done. If $\alpha \notin \mathbb{Q}$ then it is easy to see[5] that we can write

$$\alpha = \frac{j + k\sqrt{d}}{l},$$

with $\gcd(j, k, l) = 1$ and $k, l \neq 0$. Hence we get that α is a root of

$$B(t) = l^2t^2 - 2ljt + j^2 - k^2d,$$

and since $B(t) \in \mathbb{Z}[x]$ we get that $\mathrm{minpol}_\alpha \mid B$. Since B is of degree 2, we find that B is an integer multiple of minpol_α, whence

$$\mathrm{minpol}_\alpha = t^2 - \frac{2j}{l}t + \frac{j^2 - k^2d}{l^2}.$$

[5]There are unique numbers p_1, p_2, q_1, q_2 such that

$$\alpha = \frac{p_1}{q_1} + \frac{p_2}{q_2}\sqrt{d},$$

with $(p_1, q_1) = (p_2, q_2) = 1$. Let $l = \mathrm{lcm}(q_1, q_2)$ and write

$$\alpha = \frac{1}{l}\left(\frac{p_1 l}{q_1} + \frac{p_2 l}{q_2}\sqrt{d}\right).$$

Then

$$\gcd\left(\frac{p_1 l}{q_1}, \frac{p_2 l}{q_2}, l\right) = \gcd\left(\frac{p_1 l}{q_1}, \gcd\left(\frac{p_2 l}{q_2}, l\right)\right) = \gcd\left(\frac{p_1 l}{q_1}, \frac{l}{q_2}\right) = \gcd\left(\frac{l}{q_1}, \frac{l}{q_2}\right) = 1,$$

and we are done.

Thus we must have that $l \mid 2j$ and $l^2 \mid j^2 - k^2 d$. From the latter we have that there exists $l', l'' \in \mathbb{Z}$ such that

$$k^2 d = j^2 - l^2 l' = \gcd(j,l)^2 l'',$$

and hence $\gcd(j,l)^2 \mid k^2 d$. We further have that $\gcd(j,l,k) = \gcd(\gcd(j,l),k) = 1$ and so $\gcd(\gcd(j,l)^2, k^2) = 1$. We thus conclude that $\gcd(j,l)^2 \mid d$, whence $\gcd(j,l) = 1$ because d is squarefree. Hence we have that $l \mid 2$ and thus $l = 1$ or $l = 2$.

If $l = 2$, then $\gcd(j,2) = 1$ and so j is odd. This implies that $j^2 \equiv_4 1$, and hence $k^2 d \equiv_4 1$. This implies that $k^2 \equiv_4 1$, and so k is odd, and $d \equiv_4 1$. We conclude that if $d \not\equiv_4 1$, then $l = 1$ and so $\alpha = j + k\sqrt{d} \in (1, \sqrt{d})_{\mathbb{Z}}$.

If however $d \equiv_4 1$ we put $\omega = \frac{1+\sqrt{d}}{2}$, and notice that $\sqrt{d} = 2\omega - 1$. If $l = 1$, then $\alpha = j - k + 2k\omega \in (1,\omega)_{\mathbb{Z}}$. If $l = 2$, then

$$\alpha = \frac{2j' + 1 + (2k'+1)\sqrt{d}}{2} = j' + k' - 1 + 3\omega \in (1,\omega)_{\mathbb{Z}},$$

where $j', k' \in \mathbb{Z}$.

We are done with the integral basis, and let us therefore focus on the discriminant. By proposition 15 we only have to compute $\mathrm{Tr}_{K/\mathbb{Q}}(1)$, $\mathrm{Tr}_{K/\mathbb{Q}}(\omega)$, and $\mathrm{Tr}_{K/\mathbb{Q}}(\omega^2)$. If $\omega = \sqrt{d}$, we have that[6]

$$\begin{aligned} C_1(x) &= x^2 - 2x + 1 \\ C_\omega(x) &= x^2 - d \\ C_{\omega^2}(x) &= x^2 - 2dx + d^2, \end{aligned}$$

whence $\mathrm{Tr}_{K/\mathbb{Q}}(1) = 2$, $\mathrm{Tr}_{K/\mathbb{Q}}(\omega) = 0$, and $\mathrm{Tr}_{K/\mathbb{Q}}(\omega^2)$. This gives us that $d(1,\omega) = 4d$, as claimed.

If $\omega = (1+\sqrt{d})/2$, we have that $C_1(x)$ is unchanged, and

$$\begin{aligned} C_\omega(x) &= x^2 - x + \frac{1-d}{4} \\ C_{\omega^2}(x) &= x - \frac{1+d}{2}x - \left(\frac{1-d}{4}\right)^2, \end{aligned}$$

whence $\mathrm{Tr}_{K/\mathbb{Q}}(1) = 2$, $\mathrm{Tr}_{K/\mathbb{Q}}(\omega) = 1$, and $\mathrm{Tr}_{K/\mathbb{Q}}(\omega^2) = \frac{1+d}{2}$. It follows that $d(1,\omega) = d$, and we are done. □

Definition 25. An integer d is called a fundamental discriminant if d is the discriminant of a quadratic field K. In other words $d \neq 1$ and either $d \equiv_4 1$ and is squarefree or $d \equiv_4 0$, and $d/4$ is squarefree with $d/4 \equiv_4 2$ or 3.

Proposition 25. Let Q be a binary quadratic form and let d be a fundamental discriminant. If $\Delta_Q = d$, then Q is primitive.

Proof. We prove the proposition by contradiction. Suppose that $\Delta_Q = d$ and that $g = \gcd(a,b,c) > 1$. Then $b = gb'$, $a = ga'$ and $c = gc'$ for some $a', b', c' \in \mathbb{Z}$. Thus

$$d = b^2 - 4ac = g^2 b'^2 - 4g^2 a'c' = g^2(b'^2 - 4a'c'),$$

and so d is not square-free. Hence $d \equiv_4 0$ and $d/4$ is square-free. If g is odd, then $4 \mid b'^2 - 4a'c'$, and so

$$d/4 = g^2 \frac{b'^2 - 4a'c'}{4},$$

but since $g \geq 3$, we then have that $d/4$ is not square-free. If g is even, the fact that $d/4$ is square-free gives us that $g = 2$, and so $d/4 = b'^2 - 4a'c'$. But then $d/4 \equiv_4 0$ or 1. □

[6]Recall that $C_\alpha(x) = (x - \sigma_1(\alpha))(x - \sigma_2(\alpha))$ where σ_i are the embeddings of the primitive element into $\mathbb{C}$; in our case $\sigma_1(\sqrt{d}) = \sqrt{d}$ and $\sigma_2(\sqrt{d}) = -\sqrt{d}$.

If K is a quadratic field we will write $K = \mathbb{Q}(\sqrt{d})$ where d is a fundamental discriminant, and $\omega = (d+\sqrt{d})/2$. Clearly then $\{1, \omega\}$ is an integral basis, and $d = d(K)$. We will also write $\mathrm{Cl}(d) = \mathrm{Cl}(K)$.

Theorem 4. Let d be a negative fundamental discriminant. Then the maps

$$\psi_{FI}(a,b,c) = (a, \frac{-b+\sqrt{d}}{2})_{\mathbb{Z}},$$

and

$$\psi_{IF}(A) = \frac{\mathcal{N}_{K/\mathbb{Q}}(x\omega_1 - y\omega_2)}{\mathcal{N}(A)},$$

where $A = (\omega_1, \omega_2)_{\mathbb{Z}}$ with[7]

$$\frac{\omega_2\sigma(\omega_1) - \omega_1\sigma(\omega_2)}{\sqrt{d}} > 0,$$

induce inverse homomorphisms from $H(d)$ to $\mathrm{Cl}(d)$.

To prove this theorem, we need some lemmas. In the sequel, discriminants are negative.

Lemma 21. Let $I \subset \mathbb{Z}_K$ be an integral ideal. Then I has a $\mathbb{Z}$-basis $\{a, \beta\}$ where $a \in \mathbb{Z}$ and $\beta \in \mathbb{Z}_K$.

Proof. By lemma 16 we have that I has a $\mathbb{Z}$-basis $\{\alpha_1, \alpha_2\}$ for some $\alpha_i \in \mathbb{Z}_K$. We also have that

$$\alpha_1 = a_1 + b_1\omega$$
$$\alpha_2 = a_2 + b_2\omega,$$

where without loss of generality we may assume that $b_1 \geq b_2$. Notice that for any integers $k, x, y \in \mathbb{Z}$ we have that

$$\alpha_1 x + \alpha_2 y = \alpha_1(x+ky) + (\alpha_2 - k\alpha_1)y = (\alpha_1 - k\alpha_2)x + \alpha_2(kx+y),$$

and hence also $\{\alpha_1, \alpha_2 - k\alpha_1\}$ and $\{\alpha_1 - k\alpha_2, \alpha_2\}$ are bases for I. This fact allows us to use the Euclidean algorithm on b_1, b_2, giving the following basis for I.

$$\{a, b + \gcd(b_1, b_2)\omega\}$$

Where a, b are integers. Clearly we may assume that $a \geq 0$, and since the rank of I is 2, we in fact have that $a \neq 0$. Subtracting multiples of a from b, we can therefore also assume that $0 \leq b < a$. □

Lemma 22. Let $I \subset \mathbb{Z}_K$ be an integral ideal with a $\mathbb{Z}$-basis $\{a, b + c\omega\}$ where $a \in \mathbb{Z}$ and $\beta \in \mathbb{Z}_K$. If m is an integer such that $m \in I$, then $a \mid m$.

Proof. We have that $m = ax + (b + c\omega)y$ for unique $x, y \in \mathbb{Z}$. Evidently $y = 0$ and thus the result. □

Lemma 23. Let $I \subset \mathbb{Z}_K$ be an integral ideal. Then I has a unique $\mathbb{Z}$-basis $\{a, b + c\omega\}$ where $a, b, c \in \mathbb{Z}$, and $a > 0$, $0 \leq b < a$, and $0 < c \leq a$.

Proof. From the proof of lemma 21 we have integers a, b, c such that $\{a, b + c\omega\}$ is a basis, and such that a and b satisfy the above conditions. Say that we have two such bases, $\{a, b + c\omega\}$ and $\{a', b' + c'\omega\}$. Then by lemma 22 we have that $a = a'k_1$ and $a' = ak_2$ for some $k_i \in \mathbb{Z}$. Hence $a = ak_1k_2$ whence $k_1 = k_2 = \pm 1$, but as $a > 0$ we must have $k_1 = k_2 = 1$. This proves that a is unique.

Say that we have two bases, $\{a, b + c\omega\}$ and $\{a, b' + c'\omega\}$, with a, b, c, b', c' satisfying the conditions. Then there are integers x, y, x', y' such that

$$b' + c'\omega = ax + (b + c\omega)y, \text{ and}$$
$$b + c\omega = a'x' + (b' + c'\omega)y'.$$

[7] Here σ denotes the non-trivial embedding.

Since $1, \omega$ is an integral basis we find that

$$\begin{aligned} ax + by &= b' \\ c' &= cy \\ a'x' + b'y' &= b \\ c &= c'y. \end{aligned}$$

The second and fourth equations imply that $yy' = 1$ and so $y = y' = \pm 1$. But since $c, c' > 0$ we cannot have that $y = -1$. Hence we conclude from the first equation that $ax = b' - b$. Since $-a < b' - b < a$ we must have that $x = 0$. Hence $b = b'$ and $c = c'$, and we have proved uniqueness.

It remains to show that we can pick c to satisfy $0 < c \leq a$. As is clear from the proof of lemma 21, we can pick c to satisfy $c \geq 0$. Furthermore, we have that $a\omega \in I$ and so $a\omega = ax + (b + c\omega)y$ for some $x, y \in \mathbb{Z}$. Since $1, \omega$ is integral basis, we conclude that $cy = a$ and so $0 < c \leq a$. □

Lemma 24. Let $I \subset \mathbb{Z}_K$ be an integral ideal, and let $\{a, b + c\omega\}$ be the unique basis of lemma 23. Then $\mathcal{N}(I) = ac$, where $\mathcal{N}(I)$ is the norm of definition 22.

Proof. We have to show that $|\mathbb{Z}_K/I| = ac$. To this end, let $\alpha \in \mathbb{Z}_K/I$. Then

$$\begin{aligned} \alpha &= x + y\omega + I \\ &= (x - \lfloor y/c \rfloor b) + (y \bmod c) + I \\ &= ((x - \lfloor y/c \rfloor b) \bmod a) + (y \bmod c) + I. \end{aligned}$$

Hence any element of $\mathbb{Z}_K/I$ can be written $x + y\omega + I$ where $0 \leq x < a$ and $0 \leq y < c$. Suppose now that $x_1 + y_1\omega + I = x_2 + y_2\omega + I$ where both x_1, x_2, y_1, y_2 satisfy the bounds. Say, without loss of generality, that $y_1 \geq y_2$, and put $x_3 = x_1 - x_2$ and $y_3 = y_1 - y_2$. Then $0 \leq y_3 < c$ and

$$x_3 + y_3\omega = k_1 a + k_2(b + c\omega),$$

for some $k_1, k_2 \in \mathbb{Z}$. Hence $x_3 = k_1 a + k_2 b$ and $y_3 = k_2 c$. The latter gives that $k_2 = 0$, whence the former given $k_1 = 0$. Hence $x_3 = y_3 = 0$. This gives uniqueness.

There are thus a choices for x, and c choices for y. Yielding in total ac possible choices for $x + y\omega$. □

Proposition 26. Let $I \subset \mathbb{Z}_K$ be an integral ideal with basis $\{\alpha_1, \alpha_2\}$. Then

$$\mathcal{N}(I) = \left| \frac{\alpha_2\sigma(\alpha_1) - \alpha_1\sigma(\alpha_2)}{\sqrt{d}} \right|.$$

Proof. If $\{\beta_1, \beta_2\}$ is another basis for I, we have that

$$\begin{aligned} \beta_1 &= x_{11}\alpha_1 + x_{12}\alpha_2 \\ \beta_2 &= x_{21}\alpha_1 + x_{22}\alpha_2, \end{aligned}$$

for integers x_{ij} such that $\det((x_{ij})_{1 \leq i,j \leq 2}) = \pm 1$. Put $X = (x_{ij})_{1 \leq i,j \leq n}$. We then see that

$$\frac{\beta_2\sigma(\beta_1) - \beta_1\sigma(\beta_2)}{\sqrt{d}} = \det(X)\frac{\alpha_2\sigma(\alpha_1) - \alpha_1\sigma(\alpha_2)}{\sqrt{d}},$$

and so we can assume that $\alpha_1 = a$ and $\alpha_2 = b + c\omega$, with a, b, c as in lemma 23. We see that

$$(b + c\omega)a - a(b + c\sigma(\omega)) = ac\sqrt{d},$$

and thus the result follows from lemma 24. □

Lemma 25. Let $I \subset \mathbb{Z}_K$ be an integral ideal, and let $\{a, b + c\omega\}$ be the unique basis of lemma 23. Then $c \mid a$ and $c \mid b$.

Proof. Let $d = \gcd(a, c)$. Then $d = ak_1 + ck_2$ for some integers k_i. We have that $ak_1\omega \in I$ and hence

$$ak_1\omega + (b + c\omega)k_2 = d\omega + bk_2 \in I.$$

Therefore

$$d\omega + bk_2 = ax + (b + c\omega)y,$$

for integers x, y. Hence $d = cy$, and thus $c \mid d \mid a$. It remains to show that $c \mid b$. Notice that $\omega^2 = l_1 + l_2\omega$, and hence

$$I \ni (b + c\omega)\omega = cl_1 + (b + cl_2)\omega,$$

and so $b + cl_2 = cy$ for an integer y. Hence $c \mid b$, and we are done. $\square$

Lemma 26. Let I, J be integral ideals such that $I \supset J$. Then $\mathcal{N}(I) \mid \mathcal{N}(J)$.

Proof. By Noether's third isomorphism theorem we have that

$$\frac{\mathbb{Z}_K/J}{I/J} \cong \mathbb{Z}_K/I,$$

and so

$$\frac{\mathcal{N}(J)}{|I/J|} = \mathcal{N}(I),$$

whence the lemma. $\square$

Lemma 27. Let I be an integral ideal. Then for any $x \in I$ we have that $\mathcal{N}(I) \mid \mathcal{N}_{K/\mathbb{Q}}(x)$.

Proof. Clearly $\mathcal{N}((x)) = |\mathcal{N}_{K/\mathbb{Q}}(x)|$ and since $(x) \subset I$, lemma 26 gives the lemma. $\square$

We can now prove theorem 4.

Proof of theorem 4. Let $f = (a_1, b_1, c_1)$ and $g = (a_2, b_2, c_2)$. We first prove that if $g = f.\gamma$ for some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, then $\psi_{FI}(f) = \alpha\psi_{FI}(g)$ for some $\alpha \in K^\times$.

Put $\tau = (-b_1 + \sqrt{d})/(2a_1)$ and notice that $\tau = \mathfrak{z}_f$. Notice further that

$$\frac{-b_2 + \sqrt{d}}{2a_2} = \mathfrak{z}_g = \gamma^{-1}(\mathfrak{z}_f) = \frac{\delta\tau - \beta}{-\gamma\tau + \alpha}.$$

It is also easy to see that

$$a_2 = a_1\mathcal{N}_{K/\mathbb{Q}}(-\gamma\tau + \alpha).$$

We now see that

$$(1, \mathfrak{z}_g)_{\mathbb{Z}} \subset \frac{1}{-\gamma\tau + \alpha}(1, \tau)_{\mathbb{Z}}.$$

Let $z \in (1, \mathfrak{z}_g)_{\mathbb{Z}}$. Then for some integers $x, y \in \mathbb{Z}$ we have that

$$z = x + y\tau' = \frac{x(-\gamma\tau + \alpha) + y(\delta\tau - \beta)}{-\gamma\tau + \alpha} = \frac{\alpha x - \beta y + (-\gamma x + \delta y)\tau}{-\gamma\tau + \beta} \in \frac{1}{-\gamma\tau + \beta}(1, \tau)_{\mathbb{Z}},$$

where the last step follows from that

$$\begin{pmatrix} \alpha & -\beta \\ -\gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

We conclude that

$$\psi_{FI}(a_2, b_2, c_2) = a_2(1, \mathfrak{z}_g)_{\mathbb{Z}} = \frac{a_2}{-\gamma\tau + \beta}(1, \tau)_{\mathbb{Z}} = \sigma(-\gamma\tau + \alpha)\psi_{FI}(a_1, b_1, c_1).$$

Let now $A_1 = (\omega_1, \omega_2)_{\mathbb{Z}}$ where[8]

$$\frac{\omega_2\sigma(\omega_1) - \omega_1\sigma(\omega_2)}{\sqrt{d}} > 0,$$

and let $A_2 = (\tau_1, \tau_2)_{\mathbb{Z}}$. We prove that if $A_2 = \alpha A_1$ for some $\alpha \in K^\times$, then $\psi_{IF}(A_1) = \psi_{IF}(A_2).\gamma$ for some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. We have that

$$\frac{\tau_2\sigma(\tau_1) - \tau_1\sigma(\tau_2)}{\sqrt{d}} = \mathcal{N}_{K/\mathbb{Q}}(\alpha)\frac{\omega_2\sigma(\omega_1) - \omega_1\sigma(\omega_2)}{\sqrt{d}} > 0,$$

where the inequality follows from that $d < 0$ and so $\mathcal{N}_{K/\mathbb{Q}}(\alpha) > 0$. We further have that

$$\psi_{IF}(A_2) = \frac{\mathcal{N}_{K/\mathbb{Q}}(x\tau_1 - y\tau_2)}{\mathcal{N}(A_2)} = \frac{\mathcal{N}_{K/\mathbb{Q}}(\alpha)\mathcal{N}_{K/\mathbb{Q}}(x\omega_1 - y\omega_2)}{|\mathcal{N}_{K/\mathbb{Q}}(\alpha)|\mathcal{N}_{K/\mathbb{Q}}(A_1)} = \mathrm{sgn}(\mathcal{N}_{K/\mathbb{Q}}(\alpha))\psi_{IF}(A_1) = \psi_{IF}(A_1).$$

We now need to verify that given that (a_1, b_1, c_1) is primitive positive definite, then $\psi_{FI}(a_1, b_1, c_1)$ is a fractional ideal, and that given that A is a fractional ideal in K, then $\psi_{IF}(A)$ is a primitive positive definite quadratic form. The former is obvious and so we only concern ourselves with the latter.

Let A be a fractional ideal, so that $A = \frac{1}{k}B$ where $k \in \mathbb{Z}_K \setminus \{0\}$ and B is an integral ideal. Write $B = (\omega_1, \omega_2)_{\mathbb{Z}}$ with ω_i satisfying the criterion. Then

$$\psi_{IF}(A) = \frac{\mathcal{N}_{K/\mathbb{Q}}(1/k)\mathcal{N}_{K/\mathbb{Q}}(x\omega_1 - y\omega_2)}{|\mathcal{N}_{K/\mathbb{Q}}(1/k)|\mathcal{N}(B)} = \frac{\mathcal{N}_{K/\mathbb{Q}}(x\omega_1 - y\omega_2)}{\mathcal{N}(B)}.$$

We further see that

$$\mathcal{N}_{K/\mathbb{Q}}(x\omega_1 - y\omega_2) = \mathcal{N}_{K/\mathbb{Q}}(\omega_1)x^2 - (\mathcal{N}_{K/\mathbb{Q}}(\omega_1 + \omega_2) - \mathcal{N}_{K/\mathbb{Q}}(\omega_1) - \mathcal{N}_{K/\mathbb{Q}}(\omega_2))xy + \mathcal{N}_{K/\mathbb{Q}}(\omega_2)y^2.$$

By lemma 27 we thus have that $\psi_{IF}(A)$ has integer coefficients. Since $d < 0$, we have that $\mathcal{N}_{K/\mathbb{Q}}(\omega_1) > 0$. It thus remains to show that $\psi_{IF}(A)$ has discriminant d. Indeed, since d is fundamental we have then by proposition 25 that $\psi_{IF}(A)$ is primitive. We have that

$$\begin{aligned}
\Delta_{\psi_{IF}(A)} &= \frac{1}{\mathcal{N}(B)^2}(\mathcal{N}_{K/\mathbb{Q}}(\omega_1 + \omega_2) - \mathcal{N}_{K/\mathbb{Q}}(\omega_1) - \mathcal{N}_{K/\mathbb{Q}}(\omega_2))^2 - \frac{4\mathcal{N}_{K/\mathbb{Q}}(\omega_1\omega_2)}{\mathcal{N}(B)^2} \\
&= \frac{1}{\mathcal{N}(B)^2}\left((\sigma(\omega_1)\omega_2 + \omega_1\sigma(\omega_2))^2 - 4\omega_1\omega_2\sigma(\omega_1)\sigma(\omega_2)\right) \\
&= \frac{1}{\mathcal{N}(B)^2}\left((\sigma(\omega_1)\omega_2)^2 + 2\sigma(\omega_1)\omega_2\omega_1\sigma(\omega_2) + (\omega_1\sigma(\omega_2))^2 - 4\omega_1\omega_2\sigma(\omega_1)\sigma(\omega_2)\right) \\
&= \frac{1}{\mathcal{N}(B)^2}(\sigma(\omega_1)\omega_2 - \omega_1\sigma(\omega_2))^2 \\
&= \frac{1}{\mathcal{N}(B)^2}(\sqrt{d}\mathcal{N}(B))^2 = d,
\end{aligned}$$

where in the last step we used lemma 26 and the criterion on the ω_i.

We now arrive at the next step of the proof. Proving that the maps induced by ψ_{FI} and ψ_{IF} are inverses. Put $\omega_1 = a$ and $\omega_2 = \frac{-b+\sqrt{d}}{2}$. Then clearly $\omega_i \in \mathbb{Z}_K$ and furthermore

$$\frac{\omega_2\sigma(\omega_1) - \omega_1\sigma(\omega_2)}{\sqrt{d}} = a.$$

[8]We have that $A_1 = (1/d)A'$ for some $d \in \mathbb{Z}_K \setminus \{0\}$. By lemma 25 there are unique integers a, b, c such that $\{a, b + c\omega\}$ is a $\mathbb{Z}$-basis for A'. It is easy to see that $\omega_1 = a/d$ and $\omega_2 = (b + c\omega)/d$ satisfies the criterion.

So that if (a,b,c) is a primitive positive definite form of discriminant d, then $\mathcal{N}(A) = a$ and

$$\begin{aligned}
\psi_{IF}(\psi_{FI}(a,b,c)) &= \psi_{IF}((a, \frac{-b+\sqrt{d}}{2})_{\mathbb{Z}}) \\
&= \frac{\mathcal{N}_{K/\mathbb{Q}}(xa - y\left(\frac{-b+\sqrt{d}}{2}\right))}{\mathcal{N}(A)} \\
&= \frac{1}{\mathcal{N}(A)}(a^2x^2 + abxy + \frac{y^2}{4}(b^2-d)) \\
&= ax^2 + bxy + y^2\frac{b^2-d}{4a} \\
&= ax^2 + bxy + cy^2.
\end{aligned}$$

If A is a fractional ideal with basis $\{\omega_1, \omega_2\}$ satisfying the criterion, then

$$\begin{aligned}
\psi_{FI}(\psi_{IF}(A)) &= \psi_{FI}\left(\frac{\mathcal{N}_{K/\mathbb{Q}}(x\omega_1 - y\omega_2)}{\mathcal{N}(A)}\right) \\
&= \left(\frac{\mathcal{N}_{K/\mathbb{Q}}(\omega_1)}{\mathcal{N}(A)}, \frac{\frac{\omega_2\sigma(\omega_1)+\omega_1\sigma(\omega_2)}{\mathcal{N}(A)} + \sqrt{d}}{2})\right)_{\mathbb{Z}} \\
&= \left(\frac{\mathcal{N}_{K/\mathbb{Q}}(\omega_1)}{\mathcal{N}(A)}, \frac{\sigma(\omega_1)\omega_2}{\mathcal{N}(A)}\right)_{\mathbb{Z}} \\
&= \frac{\sigma(\omega_1)}{\mathcal{N}(A)}A,
\end{aligned}$$

so that the induced maps indeed are inverses.

We finally arrive at the last step of the proof. Proving that ψ_{FI} is a group homomorphism. In other words, we want to prove that

$$\psi_{FI}([(a_1, B, a_2C)] \circ [(a_2, B, a_1C)]) = \psi_{FI}([a_1, B, a_2C])\psi_{FI}([a_2, B, a_1C]),$$

where a_1, a_2, B, C are as in proposition 6. The right hand side is clearly equal to

$$(a_1a_2, \frac{-B+\sqrt{d}}{2})_{\mathbb{Z}},$$

whereas the left hand side is equal to

$$\left(a_1a_2, a_1\frac{-B+\sqrt{d}}{2}, a_2\frac{-B+\sqrt{d}}{2}, \left(\frac{-B+\sqrt{d}}{2}\right)^2\right)_{\mathbb{Z}}.$$

We have that

$$\left(\frac{-B+\sqrt{d}}{2}\right)^2 = \frac{B^2+d-2B\sqrt{d}}{4} = -B\frac{-B+\sqrt{d}}{2} - a_1a_2C,$$

and thus

$$\left(a_1a_2, a_1\frac{-B+\sqrt{d}}{2}, a_2\frac{-B+\sqrt{d}}{2}, \left(\frac{-B+\sqrt{d}}{2}\right)^2\right)_{\mathbb{Z}} = \left(a_1a_2, a_1\frac{-B+\sqrt{d}}{2}, a_2\frac{-B+\sqrt{d}}{2}, -B\frac{-B+\sqrt{d}}{2}\right)_{\mathbb{Z}}.$$

Since $\gcd(a_1, a_2, B) = 1$ we have by the extended Euclidean algorithm that

$$\left(a_1 a_2, a_1 \frac{-B+\sqrt{d}}{2}, a_2 \frac{-B+\sqrt{d}}{2}, -B\frac{-B+\sqrt{d}}{2}\right)_{\mathbb{Z}} = (a_1 a_2, \frac{-B+\sqrt{d}}{2})_{\mathbb{Z}},$$

and we are done. $\square$

Chapter 3

Computation

We now have a firm theoretical grasp of what the class group is, but we have yet to see it "in the wild". I shall therefore give some computational examples.

3.1 Brute force

The brute force method of computing the class group $H(d)$ for a negative fundamental discriminant d consists of simply enumerating all reduced forms with discriminant d, and then making a Cayley table using Dirichlet composition combined with a reduction of the compound. Since we know that $H(d)$ is a finite abelian group, we can then enumerate the finite abelian groups with order $h(d)$ and compare them to the Cayley table of $H(d)$.

I use this method below on three fundamental discriminants, namely -19, -95, and -228.

Example 1. Let $d = -19$, and suppose that (a, b, c) is a reduced form of discriminant d. Then

$$0 < a \leq \sqrt{\frac{19}{3}},$$

so that

$$0 < a \leq 2.$$

We further have that $-2 \leq b \leq 2$. Since $b^2 - 4ac = -19$ we immediately see that $b \neq 0$, and thus we are left with the following candidates

$$\begin{gathered}(1, \pm 2, *)\\(1, \pm 1, *)\\(2, \pm 1, *)\\(2, \pm 2, *).\end{gathered}$$

Since $c = (19 + b^2)/(4a)$ we eliminate all but the mutually opposite forms $(1, \pm 1, *)$. But clearly only one of these is reduced, namely $(1, 1, *) = (1, 1, 5)$. In conclusion $H(-19) = \{[(1, 1, *)]\} \cong C_1$ and so $h(-19) = 1$.

Not very exhilarating, but -19 is one of only 9 negative fundamental discriminants d for which $h(d) = 1$. The others are $-3, -4, -7, -8, -11, -43, -67$, and -163. This is the content of the theorem by Heegner, which was mentioned in the introduction.

Example 2. Let $d = -95$, and suppose that (a, b, c) is a reduced form with discriminant d. Then

$$0 < a \leq 5,$$

and

$$-5 \leq b \leq 5$$

For the same reason as before, we have that $b \neq 0$. Enumerating the candidates and eliminating those who are not forms with[1] discriminant d or are not reduced, we are left with the following list of reduced forms.

$$\begin{aligned}&(1,1,24)\\&(2,\pm 1,12)\\&(3,\pm 1,8)\\&(4,\pm 1,6)\\&(5,5,6)\end{aligned}$$

Hence $h(d) = 8$.

We now compute the Cayley table of $H(d)$. The computations are straightforward (albeit technical) and are therefore omitted.

$\circ$	$(1,1,24)$	$(2,1,12)$	$(2,-1,12)$	$(3,1,8)$	$(3,-1,8)$	$(4,1,6)$	$(4,-1,6)$	$(5,5,6)$
$(1,1,24)$	$(1,1,24)$	$(2,1,12)$	$(2,-1,12)$	$(3,1,8)$	$(3,-1,8)$	$(4,1,6)$	$(4,-1,6)$	$(5,5,6)$
$(2,1,12)$	$(2,1,12)$	$(4,1,6)$	$(1,1,24)$	$(4,-1,6)$	$(5,5,6)$	$(3,-1,8)$	$(2,-1,12)$	$(3,1,8)$
$(2,-1,12)$	$(2,-1,12)$	$(1,1,24)$	$(4,-1,6)$	$(5,5,6)$	$(4,1,6)$	$(2,1,12)$	$(3,1,8)$	$(3,-1,8)$
$(3,1,8)$	$(3,1,8)$	$(4,-1,6)$	$(5,5,6)$	$(4,1,6)$	$(1,1,24)$	$(2,-1,12)$	$(3,-1,8)$	$(2,1,12)$
$(3,-1,8)$	$(3,-1,8)$	$(5,5,6)$	$(4,1,6)$	$(1,1,24)$	$(4,-1,6)$	$(3,1,8)$	$(2,1,12)$	$(2,-1,12)$
$(4,1,6)$	$(4,1,6)$	$(3,-1,8)$	$(2,1,12)$	$(2,-1,12)$	$(3,1,8)$	$(5,5,6)$	$(1,1,24)$	$(4,-1,6)$
$(4,-1,6)$	$(4,-1,6)$	$(2,-1,12)$	$(3,1,8)$	$(3,-1,8)$	$(2,1,12)$	$(1,1,24)$	$(5,5,6)$	$(4,1,6)$
$(5,5,6)$	$(5,5,6)$	$(3,1,8)$	$(3,-1,8)$	$(2,1,12)$	$(2,-1,12)$	$(4,-1,6)$	$(4,1,6)$	$(1,1,24)$

By the fundamental theorem of finite abelian groups, we have the following candidates for $H(d)$

$$\begin{aligned}&C_8\\&C_4 \times C_2\\&C_2 \times C_2 \times C_2,\end{aligned}$$

where C_n is an abbreviation for $\mathbb{Z}/n\mathbb{Z}$. As we shall see later, there are good reasons to first compare $H(d)$ with groups of low rank. Hence we start with C_8. Using the table we see that $[(2,1,12)]$ generates $H(d)$, and hence $H(d) \cong C_8$.

It turns out that for the most time, $H(d)$ is cyclic. The heuristics by Cohen and Lenstra do in fact imply that approximately 97.757% of odd order class groups with negative fundamental discriminants are cyclic. The following is an example of when the class group is not cyclic.

Example 3. Let $d = -228$ and suppose that (a, b, c) is a reduced form with discriminant d. Then $0 < a \leq 8$ and $-8 \leq b \leq 8$. Proceeding as before, we are left with the following list of reduced forms.

$$\begin{aligned}&(1,0,57)\\&(2,2,29)\\&(3,0,19)\\&(6,6,11)\end{aligned}$$

Hence $h(d) = 4$.

[1] Or somewhat sloppily, those who have non-integral c.

Computing the Cayley table of $H(d)$ we get the following.

$\circ$	$(1,0,57)$	$(2,2,29)$	$(3,0,19)$	$(6,6,11)$
$(1,0,57)$	$(1,0,57)$	$(2,2,29)$	$(3,0,19)$	$(6,6,11)$
$(2,2,29)$	$(2,2,29)$	$(1,0,57)$	$(6,6,11)$	$(3,0,19)$
$(3,0,19)$	$(3,0,19)$	$(6,6,11)$	$(1,0,57)$	$(2,2,29)$
$(6,6,11)$	$(6,6,11)$	$(3,0,19)$	$(2,2,29)$	$(1,0,57)$

By the fundamental theorem of finite abelian groups, we have that $H(d)$ is isomorphic to either C_4 or $C_2 \times C_2$. It is however clear from the Cayley table that every element has order ≤ 2, and so $H(d) \cong C_2 \times C_2$.

3.2 On elements with order less than or equal to two

In the last example, we saw that every element in the class group had order less than or equal to two. We can in fact rather easily determine the exact number of elements in the class group with such an order.

The approach below is based on [Cox13, pp. 47-48].

Proposition 27. Let $d < 0$ be a fundamental discriminant and let r be the number of odd primes dividing d. Define the number μ depending on d as follows: if $d \equiv_4 1$ then $\mu = r$, and if $d \equiv_4 0$ then $\mu = r + 1$. Then $H(d)$ has exactly $2^{\mu-1}$ elements of order less than or equal to 2.

For example, when $d = -228$, we see that the number of elements with order ≤ 2 is equal to $2^2 = 4$. Using this with the fact that $h(d) = 4$ we thus have another way to conclude that $H(d) \cong C_2 \times C_2$.

To prove the proposition, we need a lemma.

Lemma 28. A form $(a,b,c) \in \mathfrak{Q}_d^{\text{red}}$ has order less than or equal to 2 in $H(d)$ if and only if $b = 0$, or $a = b$, or $a = c$.

Proof. We have that $[(a,b,c)]^2 = 1_{H(d)}$ if and only if $[(a,b,c)] = [(a,b,c)]^{-1} = [(a,-b,c)]$ if and only if $(a,b,c) \sim (a,-b,c)$. Since (a,b,c) is reduced we have that

$$-a < b < a < c, \text{ or } -a < b = a < c, \text{ or } 0 \leq b \leq a = c.$$

In the first case, it holds that $-a < -b < a$ so that also $(a,-b,c)$ is reduced. This can be the case if and only if $(a,b,c) = (a,-b,c)$ which holds if and only if $b = 0$.

In the second case, it holds that $(a,a,c).S = (a,-a,c)$, so that $(a,b,c) \sim (a,-b,c)$.

In the third case, it holds that $(a,b,a).T = (a,-b,a)$, so that $(a,b,c) \sim (a,-b,c)$. The lemma has been proved. $\square$

Proof of proposition 27. Let first $d \equiv_4 1$, with d square-free. We'll find a bijection $f : A \to B$ where

$$A = \{b > 0 : \exists k \in \mathbb{Z}.\, k > b, d = -bk\}, \text{ and}$$
$$B = \{(a,b,c) \in \mathfrak{Q}_d^{\text{red}} : b = 0, \text{ or } a = b, \text{ or } a = c\}.$$

Clearly $|A| = 2^{r-1}$ so that if f exists, then $|B| = 2^{r-1}$. Notice also that $b \neq 0$ for else we would have that $d \equiv_4 0$. Hence we have that

$$B = \{(a,b,c) \in \mathfrak{Q}_d^{\text{red}} : a = b, \text{ or } a = c\}.$$

Put now

$$f(b) = \begin{cases} (b,b,c) & \text{if } b < c \\ (c, 2c-b, c) & \text{if } b \geq c, \end{cases}$$

where $c = (b+k)/4$. We first prove that f has the stated co-domain. If $b < c$ we have that $-b < b \leq b < c$ so that (b, b, c) is reduced. If $b > c$ we have that $2c - b < c$ and since

$$2c - b = \frac{b+k}{2} - b = \frac{k-b}{2} > 0,$$

we have that $(c, 2c-b, c)$ is reduced. Furthermore, we see that $(b, b, c).ST = (c, 2c-b, c)$ and that

$$\Delta_{(b,b,c)} = b^2 - 4bc = b^2 - b(b+k) = -bk = d.$$

This shows that f indeed has the stated co-domain. It is easy to see that f is injective, and hence we only need to show that it is surjective. Let $(a, b, c) \in B$, then $a = b$ or $a = c$. Say first that $a = b$, so that $(a, b, c) = (b, b, c)$. Then $d = -b(4c - b)$ and since the form is positive definite and reduced, we have that $0 < b \leq c < 2c$, so that $0 < b < 4c - b$. This implies that $b \in A$, so that $f(b) = (b, b, \frac{4c-b+b}{4}) = (b, b, c)$. Say now that $a = c$, so that $(a, b, c) = (c, b, c)$. Since $0 \leq b \leq c$ we have that $2c - b < 2c + b$, so that $2c - b \in A$. We also have that $2c - b < c$, so that

$$f(b) = (2c - b, 2c - b, c).ST = (c, b, c).$$

This proves that f is surjective, and hence we have proven that $|B| = 2^{\mu-1}$.

Let now $d = -4n$ with n square-free and $n \equiv_4 1$ or 2. Suppose also for simplicity that $d \neq -4$. This means that

$$B = \overbrace{\{(a, b, c) \in \mathfrak{Q}_d^{\text{red}} : b = 0\}}^{B_1} \sqcup \overbrace{\{(a, b, c) \in \mathfrak{Q}_d^{\text{red}} : a = b, \text{ or } a = c\}}^{B_2}.$$

Adopting the bijective proof above, we find that $|B_2| = 2^{r-1}$ (see also [Cox13, p. 48]). Say that $(a, b, c) \in B_1$, then $n = ac$. Since $\gcd(a, c) = 1$, $a, c > 0$, and $a < c$ there are 2^{r-1} choices for a. We conclude that $|B_1| = 2^{r-1}$, so that $|B| = 2 \cdot 2^{r-1} = 2^r = 2^{\mu-1}$. We have thus proven the theorem. □

3.3 Dirichlet's class number formula

Of theoretical interest, but of little use for practical computation, is following exact formula for the class number, first published by Dirichlet in 1839.

Proposition 28. Let $d < 0$ be a fundamental discriminant and put

$$L_d(s) = \sum_{n \geq 1} \frac{(d/n)}{n^s},$$

for $\Re(s) > 1$, where (d/n) is the Jacobi symbol. Then there exists an analytic continuation of L_d to all of $\mathbb{C}$ such that

$$\Lambda_d(s) = \Lambda_d(1 - s),$$

where

$$\Lambda_d(s) = |d/\pi|^{\frac{s+1}{2}} \Gamma(\frac{s+1}{2}) L_d(s).$$

Proof. See [Dav00, pp. 35-42, and pp. 65-72]. □

Theorem 5. Let $d < 0$ be a fundamental discriminant. Then

$$h(d) = \frac{w(d)|d|^{1/2}}{2\pi},$$

where

$$w(d) = \begin{cases} 2 & \text{if } d < -4 \\ 4 & \text{if } d = -4 \\ 6 & \text{if } d = -3 \end{cases}.$$

Proof. See [Dav00, pp. 43-53]. ☐

One can use the functional equation of $L_d(s)$ to deduce the following proposition.

Proposition 29. Let $d < -4$ be a fundamental discriminant. Then

$$h(d) = \sum_{n \geq 1} \left(\frac{d}{n}\right) \left(\operatorname{erfc}\left(n\sqrt{\frac{\pi}{|d|}}\right) + \frac{\sqrt{|d|}}{\pi n} \exp(-\pi n^2/|d|)\right),$$

where

$$\operatorname{erfc} = \frac{2}{\sqrt{\pi}} \int_x^\infty e^{-t^2} \mathrm{d}t,$$

is known as the complementary error function.

Proof. See [Coh00, p. 233]. ☐

The above proposition yields the following efficient way to compute $h(d)$.

Corollary 2. Let $d < -4$ be a fundamental discriminant. Then $h(d)$ is the closest integer to the nth partial sum of the series in proposition 29, where

$$n = \left\lfloor \sqrt{\frac{|d| \log |d|}{2\pi}} \right\rfloor.$$

Proof. See [Coh00, p. 234]. ☐

3.4 Better algorithms

The brute-force method is obviously quite slow. For computing the class group in practice, there are far better methods. Cohen covers many, if not most, of the algorithms for computing class groups in [Coh00, chapter 5.4]. All of these algoritms are implemented in the computer algebra system PARI/GP [Thea], which was originally developed by Cohen. In particular one can use the module `qfbclassno` to compute the class number using the probabilistic "Baby Step Giant Step" method of Daniel Shanks [Coh00, algorithm 5.4.10] and the module `quadclassunit` to compute class groups using Kevin McCurley's sub-exponential algorithm [Coh00, algorithm 5.5.2] (for negative discriminants) and Johannes Buchmann's sub-exponential algorithm [Coh00, algorithm 5.9.2] (for positive discriminants). There is also the module `qfbred` for reducing quadratic forms using [Coh00, algorithm 5.4.2] and the module `qfbnucomp` for composing them using [Coh00, algorithm 5.4.9].

Many of these modules can be used through the module `BinaryQF` in the computer algebra system SageMath [Theb].

Chapter 4

Cohen-Lenstra heuristics

In this chapter I will motivate and formulate Henri Cohen and Hendrik Lenstra's heuristics for imaginary quadratic fields – closely following Cohen's book [Coh00, section 5.10, pp. 289-293] and Cohen and Lenstra's paper [CHa].

4.1 Motivation

Upon investigating experimental data on $h(d)$ for negative fundamental discriminants d, one notices that

(A) If p is a small odd prime, the proportion of fundamental discriminants d for which $p \mid h(d)$ is significantly greater than the expected $1/p$. If $p = 3$, it is around 43%, if $p = 5$ it is around 23.5%, and so on.

(B) Looking at the odd part[1] of the class group, cyclic groups seem to form the overwhelming majority.

The starting point is observation (B). What could explain it? By the below lemma and proposition, a possible candidate is the size of the automorphism group.

Lemma 29. Let G be a finite abelian group. Then $|\mathrm{Aut}(G)| \geq \phi(|G|)$, where ϕ is Euler's totient function.

Proof. We first assume that G is a p-group. Then it is well-known that $\mathrm{Aut}(G)$ acts transitively on the set X of elements of largest order. Therefore, by the orbit-stabilizer theorem, we see that $|\mathrm{Aut}(G)| = |X|l$ for some positive integer l. We have that there at most $|G|/p$ elements of smaller order, and therefore $|X| \geq |G|(1 - \frac{1}{p}) = \phi(|G|)$. It follows that $|\mathrm{Aut}(G)| \geq \phi(|G|)$.

If G is not a p-group, it is by the fundamental theorem of finite abelian groups a product of p-groups. In other words, we have that

$$G \cong A_1 \times \cdots \times A_n,$$

where $|A_i| = p_i^{k_i}$ for distinct primes p_i and positive k_i. We thus have that

$$|\mathrm{Aut}(G)| \geq |\mathrm{Aut}(A_1)| \cdots |\mathrm{Aut}(A_n)| \geq \phi(|A_1|) \cdots \phi(|A_n|) = \phi(|A_1| \cdots |A_n|) = \phi(|G|),$$

where in the last step we used that ϕ is multiplicative. □

Proposition 30. Let G be a cyclic group. Then for any abelian group H such that $|H| = |G|$, we have that $|\mathrm{Aut}(G)| \leq |\mathrm{Aut}(H)|$.

Proof. Since G is cyclic, we have that $|\mathrm{Aut}(G)| = \phi(|G|)$. By lemma 29 we see that $\phi(|G|) = \phi(|H|) \leq |\mathrm{Aut}(H)|$, and we are done. □

[1]Subgroups of elements of odd order.

So cyclic groups have the smallest automorphism group. If G is an abelian group, we employ the notation G_o for its odd part. Motivated by the proposition, we guess that isomorphism classes of abelian groups G have a "weight" proportional to $1/|\mathrm{Aut}(G)|$, as this would imply that non-cyclic groups occur more rarely.

Definition 26. Let f be a function defined on the isomorphism classes of finite abelian groups of odd order. We say that the average of f is[2]

$$M(f) = \lim_{x\to\infty} \frac{\displaystyle\sum_{0<-D\le x}^{\flat} f(H(d)_o)}{\displaystyle\sum_{0<-d\le x}^{\flat} 1},$$

given that the limit exists. If f is the characteristic function of a property P, we call $M(f)$ the probability that P holds.

Conjecture 4. Let f be a function defined on the isomorphism classes of finite abelian groups of odd order. Then

$$M(f) = \lim_{x\to\infty} \frac{\sum_{|G|\le x} f(G_o)/|\mathrm{Aut}(G)|}{\sum_{|G|\le x} 1/|\mathrm{Aut}(G)|},$$

where the sums are to be taken over isomorphism classes.

Using quite a few auxiliary results which are outside of the scope of this thesis (see [CHb] for details) and assuming conjecture 4, one can deduce the following.

Theorem 6. For any odd prime p and any integer r including $r=\infty$, set $(p)_r = \prod_{k=1}^{r}(1-p^{-k})$, and let $C = \prod_{k\ge 2}\zeta(k) \approx 2.29486$. Let also d be a negative fundamental discriminant, and $r_p(G)$ denote the p-rank of an abelian group G. Then if conjecture 4 is true it holds that

(A) The probability that $H(d)_o$ is cyclic is equal to

$$\frac{\zeta(2)\zeta(3)}{3(2)_\infty C\zeta(6)} \approx 0.977575.$$

(B) If p is an odd prime, the probability that $p \mid h(d)$ is equal to

$$f(p) = 1-(p)_\infty.$$

For example $f(3)\approx 0.43987$, $f(5)\approx 0.23967$, and $f(7)\approx 0.16320$.

(C) If p is an odd prime, the average of $p^{r_p(H(d))}$ is 2.

Proof. See [CHb]. $\square$

Remark 7. As for (C), note that $p^{r_p(H(d))} = |H(d)[p]|$, where $G[p]$ denotes the p-torsion subgroup of an abelian group G, and so (C) can be equivalently stated as

$$\sum_{0<-d<X}^{\flat} |H(d)[p]| \sim 2\sum_{0<-d<X}^{\flat} 1.$$

Putting $p=3$ this is a famous theorem by Harold Davenport and Hans Heilbronn. We sketch a proof of a sharper version of this theorem in the next chapter.

[2]The notation $\sum^{\flat}$ indicates that the sum is taken over fundamental discriminants.

Chapter 5

Average cardinality of torsion subgroups

Let d be a negative fundamental discriminant, and let $H_p(d)$ or $\mathrm{Cl}_p(d)$ denote the set of elements of order p in the form class group $H(d)$ or ideal class group $\mathrm{Cl}(d)$, respectively. From conjecture 4 and by noticing that $|H_p(d)| = |H(d)[p]| - 1$, we have that

$$\sum_{0<-d<X}^{\flat} |H_p(d)| \sim \sum_{0<-d<X}^{\flat} 1. \tag{5.1}$$

In [Hou10], Bob Hough proves (5.1) for $p = 3$ by first making a broader prediction in terms of equidistribution. In fact, he is able to prove something stronger, namely the following theorem.

Theorem 7. Let $X > 0$, then

$$\sum_{0<-d<X}^{\flat} |H_3(d)| = c_1 X + c_2 X^{5/6} + o(X^{5/6}),$$

where $c_1, c_2 \in \mathbb{R}$ are constants with $c_1 > 0$ and $c_2 < 0$.

This theorem has also been proved by Manjul Bhargava et al. [BST13], and Frank Thorne et al. [TT13], but with different techniques. In the sequel, we give a rough outline of Hough's proof of theorem 7. The analytical details are omitted, as they are well beyond the scope of this thesis.

5.1 Background

Let $[I] \in \mathrm{Cl}(d)$ and recall from theorem 4 that there exists a unique class of forms $[(a, b, c)] \in H(d)$ for which

$$[I] = [(a, \frac{-b + \sqrt{d}}{2})].$$

We thus have a one-to-one correspondence between ideal classes and points in $\mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$ given by

$$[I] \leftrightarrow [\mathfrak{z}_{(a,b,c)}].$$

Definition 27. Let $[I] \in \mathrm{Cl}(d)$ and let $\psi : H(d) \to \mathrm{Cl}(d)$ be the isomorphism induced from the maps in theorem 4. Let $Q \in \psi^{-1}([I])$ be arbitrary. Then the point in the fundamental domain $\mathcal{F}$ of the modular surface $\mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$ corresponding to the class $[\mathfrak{z}_Q]$ is called the CM-point of $[I]$, and is denoted by $\mathfrak{z}_{[I]}$.

As a starting point Hough took the following theorem of William Duke [Duk88] and Yuri V. Linnik [Lin68], here in the formulation of [Duk].

Theorem 8. Suppose that $K \in C^\infty(\mathbb{H})$ is $\mathrm{SL}_2(\mathbb{Z})$-invariant and bounded on $\mathbb{H}$. Then as $d \to -\infty$ with d a fundamental discriminant,

$$\frac{\sum_{z \in \mathfrak{z}_{\mathrm{Cl}(d)}} K(z)}{\sum_{z \in \mathfrak{z}_{\mathrm{Cl}(d)}} 1} \to \int_{\mathbb{H}/\mathrm{SL}_2(\mathbb{Z})} K(z) \mathrm{d}\mu(z),$$

where $\mathrm{d}\mu(z) = \frac{3}{\pi}\frac{\mathrm{d}x\mathrm{d}y}{y^2}$, and $\mathfrak{z}_{\mathrm{Cl}(d)}$ is the set of all CM-points of ideal classes in $\mathrm{Cl}(d)$.

In analogy with this theorem, and based on visual evidence, Hough formulates the following conjecture.

Conjecture 5. Let K be a continuous function of compact support on the fundamental domain $\mathcal{F}$ of the modular surface. For each odd $k > 1$ we have that

$$\lim_{X\to\infty} \frac{\sum^{\flat}_{0<-d<X} \sum_{[I]\in H_k(d)} K(\mathfrak{z}_{[I]})}{\sum^{\flat}_{0<-d<X} 1} = \int_{\mathcal{F}} K(z)\mathrm{d}\mu(z),$$

where $\mathrm{d}\mu$ is the same measure as in theorem 8.

Hough is able to prove conjecture 5 for the case $k = 3$, and establishes partial results towards the conjecture for larger k. The latter is however beyond the scope of this thesis.

Remark 8. The result of Hough does indeed imply (5.1). Simply put $K(z) = 1$ for $z \in \mathcal{F}$ and the rest by interpolation from 0.

Instead of working with CM points of ideal classes in $\mathrm{Cl}(d)$, Hough works with so-called Heegner points of primitive ideals with classes in $\mathrm{Cl}(d)$. These points of view turn out to be equivalent.

Definition 28. Let $A \subset \mathbb{Z}_K$ be an ideal. We say that A is primitive if there exists no prime $p \in \mathbb{Z}$ and no ideal $B \subset \mathbb{Z}_K$ such that $A = (p)B$. If $k > 1$ is odd we use the notation $P_k(d)$ to denote primitive ideals with classes in $\mathrm{Cl}_k(d)$.

Proposition 31. If $A \subset \mathbb{Z}_K$ is a primitive (integral) ideal, we can write $A = (\mathcal{N}(A), b + \omega)$, where b is uniquely determined by

$$-\frac{\mathcal{N}(A)}{2} < b \leq \frac{\mathcal{N}(A)}{2},$$

and

$$b + \omega \in A.$$

Proof. Recall that by lemma 23 we have a unique basis $\{a, b + c\omega\}$ for A, where $a > 0$, $0 \leq b < a$, $0 < c \leq a$, and $\mathcal{N}(A) = ac$. It is easy to see that A is primitive iff $c = 1$, whence we have the basis $\{\mathcal{N}(A), b + \omega\}$. It is easy to see from the proof that $-a/2 < b \leq a/2$ still uniquely determines b. □

Definition 29. Let $A = (\mathcal{N}(A), b + \sqrt{d})$ be primitive, with b as in proposition 31. Then the point $\mathfrak{z}_A = \frac{b+\sqrt{d}}{\mathcal{N}(A)}$ (which lies in $(-1/2, 1/2] + i\mathbb{R}^+$) is called the Heegner point of A.

Proposition 32. The collection of Heegner points of primitive ideals of class $[A]$ are exactly the images of the CM point $\mathfrak{z}_{[A]}$ in the various fundamental domains for $\mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$ with the strip $(-1/2, 1/2] + i\mathbb{R}^+$.

Proof. See [IK04, C. 22]. □

Corollary 3. The equidistribution of CM-points within $\mathcal{F}$ is equivalent to the equidistribution of the corresponding Heegner points in $(-1/2, 1/2] + i\mathbb{R}^+$.

We now introduce some notation. Given an integrable function f on $\mathbb{R}^+$ let its Mellin transform $\tilde{f}$ be defined (when absolutely convergent) by $\tilde{f}(s) = \int_0^\infty f(x)x^{s-1}\mathrm{d}x$ where $s \in \mathbb{C}$, and be analytic continuation elsewhere, let ϵ denote arbitrarily small positive parameters, and let $A \ll B$ denote $A = O(B)$.

Hough's main result can be given quantitatively as follows.

Theorem 9. Let $k \geq 3$ be odd, and let $\phi, \psi \in C^\infty(\mathbb{R}^+)$ with ϕ of compact support and ψ supported in $[1, \infty)$ with $\psi \equiv 1$ on a neighborhood of ∞. Let $T = T(X)$ be a parameter and put $\psi_T(y) = \psi(\frac{y}{T})$. For T in the range $X^{\frac{1}{2}-\frac{1}{k-2}+\epsilon} < T < X^{\frac{1}{2}-\frac{1}{k}+\epsilon}$ we have that

$$\sum_{\substack{d\equiv_4 2\\ \text{square-free}}} \phi\left(\frac{d}{X}\right) \sum_{A\in P_k(-4d)} \psi_T(\Im \mathfrak{z}_A) \Big/ \sum_{\substack{d\equiv_4 2\\ \text{square-free}}} \phi\left(\frac{d}{X}\right)$$
$$= \frac{3}{\pi T}\int_0^\infty \psi(y)\frac{\mathrm{d}y}{y^2} + \frac{\pi^2}{2}c_k \frac{\tilde{\phi}\left(\frac{1}{2}+\frac{1}{k}\right)}{\tilde{\phi}(1)} X^{\frac{1}{k}-\frac{1}{2}}$$
$$+ O\left(\frac{X^{\frac{k}{4}-1+\epsilon}}{T^{\frac{k}{2}}}\right) + O\left(X^{\frac{1}{2k-2}-\frac{1}{2}+\epsilon}\right),$$

where

$$c_k = \frac{\Gamma(\frac{1}{2}-\frac{1}{k})\zeta(1-\frac{2}{k})}{k\pi^{3/2}\Gamma(1-\frac{1}{k})}(1 - 2^{\frac{1}{k}} + 2^{1-\frac{1}{k}}) \prod_{\substack{p\geq 3\\ \text{prime}}} \left[1 + \frac{1}{p+1}\left(\frac{1}{p^{\frac{1}{k}}} - \frac{1}{p^{1-\frac{2}{k}}} - \frac{1}{p^{1-\frac{1}{k}}} - \frac{1}{p}\right)\right].$$

Remark 9. Since $\zeta(1-\frac{2}{k}) < 0$ we have that $c_k < 0$.

Remark 10. Notice that the theorem only covers discriminants of the form $-4d$ where $d > 0$, $d \equiv_4 2$ and d is square-free. Hough's method works for the other two cases (see proposition 24) with minor modifications.

The equidistribution setting gives us a pretty geometric interpretation of the negative secondary main term. Namely, if $A \in P_k(d)$ then A^k is principal, so that $A^k = (x + y\sqrt{-d})$ for some $x, y \in \mathbb{Z}$, with $y \neq 0$ since A is primitive. Consequently $\mathcal{N}(A^k) = \mathcal{N}(A)^k = x^2 + dy^2 \geq d$ so that $\mathcal{N}(A) \geq d^{\frac{1}{k}}$ and thus

$$\Im(\mathfrak{z}_A) = \frac{\sqrt{d}}{\mathcal{N}(A)} \leq d^{\frac{1}{2}-\frac{1}{k}}.$$

Therefore there are no Heegner points in the set $T = \{z \in (-1/2, 1/2] + i\mathbb{R}^+ : \Im(z) > X^{\frac{1}{2}-\frac{1}{k}}\}$. Hence we expect

$$\frac{\sum^\flat_{0<-d<X} \sum_{A\in P_k(d)} K(\mathfrak{z}_A)}{\sum^\flat_{0<-d<X} 1},$$

to asymptotically behave like

$$\int_{(-1/2,1/2]+i\mathbb{R}^+} K(z)\mathrm{d}\mu(z) - \int_T K(z)\mathrm{d}\mu(z).$$

We have that $\mathrm{Vol}_\mu(T) = \frac{3}{\pi}X^{\frac{1}{k}-\frac{1}{2}}$, and thus we have a heuristic justification for the negative secondary main term $\frac{\pi^2}{2}c_k\frac{\tilde{\phi}(\frac{1}{2}+\frac{1}{k})}{\tilde{\phi}(1)}X^{\frac{1}{k}-\frac{1}{2}}$.

In the following section I will sketch a proof of theorem 9 following Hough. Theorem 7 is then by corollary 3 an easy consequence.

5.2 Set-up

From basic Fourier analysis, we have the following theorem.

Proposition 33. Let $C_c(S)$ ($C_c^\infty(S)$) denote the space of continous (smooth) functions defined on S with compact support. The linear span of function of the form

$$e(fx)\psi(y), \quad f \in \mathbb{Z}, \psi \in C_c^\infty(\mathbb{R}^+),$$

is dense (with respect to the supremum-norm) in $C_c(\mathbb{R}/\mathbb{Z} \times \mathbb{R}^+)$.

Proof. Take the Fourier series in the first variable and apply (say) theorem 1.4.2 of [DM72]. □

With this in mind, we only have to prove the theorem for functions $K(x,y) = e(fx)\psi(y)$ with $f \in \mathbb{Z}$ and $\psi \in C_c^\infty(\mathbb{R}^+)$. The rest follows from linearity.

The most central piece of the proof is the following parameterization of primitive ideals A such that $A \neq 1$ and $[A^k] = [1]$.

Proposition 34. Let $d \equiv_4 2$ be square-free and $k \geq 3$ be odd. The set

$$\{(l,m,n,t) \in (\mathbb{Z}^+)^4 : lm^k = l^2n^2 + t^2 d, \gcd(lmn, t) = 1\},$$

is in bijection with primitive ideal pairs $\{A, \overline{A}\}$ with $A \neq 1$ and A^k principal. Explicitly, the ideals $A, \overline{A}$ are given as $\mathbb{Z}$-modules by

$$A = (lm, lnt^{-1} + \sqrt{-d})_{\mathbb{Z}} \quad \overline{A} = (lm, -lnt^{-1} + \sqrt{-d})_{\mathbb{Z}},$$

where $\mathcal{N}(A) = lm$ and t^{-1} is the inverse of t modulo m.

In order to prove the proposition, we need an alternative characterization of primitive ideals. It is based on the behaviour of the principal ideals $(p) \subset \mathbb{Z}_K$ for $p \in \mathbb{Z}$ prime.

Proposition 35. Let as usual $K = \mathbb{Q}(\sqrt{d})$, with d fundamental, let $\omega = \frac{d+\sqrt{d}}{2}$, and let p be a prime number. Then

(i) If $p \mid d$, then p is ramified and we have $(p) = P^2$ where $P = (p) + (\omega)$, except when $p = 2$ and $d \equiv_{16} 12$ in which case $P = (p) + (1+\omega)$.

(ii) If $(d/p) = -1$, then p is inert and we have $(p) = P$ a prime ideal in $\mathbb{Z}_K$.

(iii) If $(d/p) = 1$, then p is split and we have $(p) = P\overline{P}$ with $P = (p) + (\omega - \frac{d+b}{2})$ where b is any solution to $b^2 \equiv_{4p} d$, and where $\overline{P} = \{\overline{a} : a \in P\}$ is the conjugate ideal.

Proof. See [Coh00, p. 219]. □

Keeping in mind that (see chapter 2.3) ideals in $\mathbb{Z}_K$ have unique prime ideal factorization, we make the following definition.

Definition 30. Let d be a fundamental discriminant. The ideal

$$\mathfrak{d} = \prod_{\substack{P \mid (d) \\ P \text{ prime ideal}}} P,$$

is called the different of d.

With the different of d, we can give the alternative characterization.

Proposition 36. Let $A \subset \mathbb{Z}_K$ be an ideal. Then A is primitive iff $A = LB$ with $L \mid \mathfrak{d}$, $(B, \mathfrak{d}) = (1)$ and $(B, \overline{B}) = (1)$.

Proof. Evidently A is primitive iff it has no inert primes, any prime ideal resulting from ramification only occurs once, and for prime ideals P resulting from splitting it only contains one of P or $\overline{P}$; in its prime ideal factorization.

Proposition 35 gives us that $\mathfrak{d}$ only contains primes that result from ramification. These primes are not inert, since if a prime ideal P resulting from ramification of a prime $q \mid d$ would be inert then $P^2 = (p)^2 = (p^2) = (q)$ for some prime p, but this is a contradiction. They also cannot have resulted from the splitting of a prime, because if a prime ideal P resulting from ramification of a prime $q \mid d$ would resulting from the splitting of a prime p, then $P\overline{P} = (p)$ and $P^2 = (q)$ so that $(p^2) = (P\overline{P})^2 = (q^2)$. Thus $p = q$ and so $P = \overline{P}$, which contradicts the assumption that P resulted from the splitting of a prime.

Furthermore, the condition $(B, \mathfrak{d}) = (1)$ is equivalent to B not consisting of any prime ideal resulting from ramification, and the condition $(B, \overline{B}) = (1)$ implies that B has no inert primes, and that if $P \mid B$ results from splitting, then only one of P and $\overline{P}$ occurs in the factorization of B. Thus it is easy to see that if $A = LB$ with L and B satisfying the criteria, then A is primitive.

Conversely, if A is primitive, we have that $A = P_1^{k_1} \dots P_r^{k_r}$. Clearly prime ideals resulting from ramification can only occur once in the factorization, because if some P_i resulting from ramification of $q \mid d$ occurs $k_i \geq 2$ times, we have that $P_i^{k_i} = (q)Q$ for some ideal Q, and so A is not primitive. Grouping all prime ideals resulting from ramification together in the prime ideal factorization of A, we then see that $A = LB$ for some $L \mid \mathfrak{d}$. The conditions on B follow from arguing as before. $\square$

We can now prove the parameterization.

Proof of proposition 34. Let $A \neq (1)$ be primitive with A^k principal. By proposition 36 we have that there exists ideals H, B so that $A = HB$ and $H \mid \mathfrak{d}$, $(B, \mathfrak{d}) = (1)$, and $(B, \overline{B}) = (1)$. We have that $B \neq 1$ because otherwise $A = H$ so that[1] $[H]^k = [H^k] = [H] = [1]$ and thus $H = (1)$, which leads to the contradiction $A = (1)$. Now since $k-1$ is even, we have that $A^k H^{-(k-1)} = HB^k$ is principal, say

$$HB^k = (x + t\sqrt{-d}).$$

Since HB^k is on the form given in proposition 36 we also see that it is primitive. Put $m = \mathcal{N}(B)$ and $l = \mathcal{N}(H)$ and notice that $l \mid d$, and l is square-free. Taking the norm of HB^k we see that

$$lm^k = x^2 + t^2 d,$$

and consequently $l \mid x$, whence we can write $x = ln$ and we get $m^k = ln^2 + t^2 l'$ where $l' = d/l$. Since HB^k is primitive we further see that $\gcd(t, ln) = 1$, so that also $\gcd(n, t) = 1$. It is moreover the case that $\gcd(m, t) = 1$ because if $p \mid \gcd(m, t)$ then $p^2 \mid m^k - t^2 l' = ln^2$ so that $p \mid \gcd(ln, t) = 1$ which is a contradiction.

Finally, since HB^k is primitive, we have that $n, t \neq 0$. Multiplying by -1 if necessary, we may assume that $t > 0$. By replacing A with $\overline{A}$ if necessary, we may also assume that $n > 0$.

We have now shown how, given an ideal pair $\{A, \overline{A}\}$ we can get a quadruple $(l, m, n, t) \in (\mathbb{Z}_+)^4$ satisfying $lm^k = l^2 n^2 + t^2 d$ and $\gcd(lmn, t) = 1$. Suppose conversely we are given a quadruple $(l, m, n, t) \in (\mathbb{Z}_+)^4$ satisfying the conditions. Then clearly $l \mid lm^k - l^2 n^2 = t^2 d$ so that from co-primality $l \mid d$. This gives us that l is square-free. I further claim that $\gcd(m, n) = 1$. Indeed, if $p \mid (m, n)$ then from co-primality, we have that $p \nmid t$ and thus $p^2 \mid \frac{lm^k - l^2 n^2}{t^2} = d$, which is a contradiction. From $\gcd(m, n) = 1$ we conclude[2] that $\gcd(m, d) = 1$. Write now $(ln + t\sqrt{-d}) = HC$ with $H \mid \mathfrak{d}$ and $(C, \mathfrak{d}) = (1)$. Then $(lm^k) = (l)(m^k) = H^2 C\overline{C}$.

[1] Here we use that k is odd, say $k = 2k' + 1$ and that H consists of prime ideals resulting from ramification. This means that $H^{2k'}$ is principal whence obviously $[H^k] = [H]$.

[2] For the sake of readability, we prove this in a footnote. Say that $p \mid (m, d)$, then $p \mid m$ and $p \mid d$ so $p \mid l^2 n^2$ and thus $p \mid l$ or $p \mid n$. If $p \mid n$ then $p \mid (m, n)$ which is a contradiction. Thus we have that $p \mid l$. This implies that $p \mid m^k - ln^2$ and so $p \mid t^2 \frac{d}{l}$, but from co-primality we have that $p \nmid t$ and so $p \mid \frac{d}{l}$. Then $p \mid (l, \frac{d}{l}) = 1$ and we have a contradiction.

Since $(m,l) \mid (m,d) = 1$ we have that $(l) = H^2$ and $C\overline{C} = (m^k)$. We also have that C divides $(ln + t\sqrt{-d})$ and $(C, \mathfrak{d}) = (1)$, whence also $(C, \overline{C}) = (1)$. Therefore there exists an ideal B such that $C = B^k$. Since also $(B, \overline{B}) = (1)$ and $(B, \mathfrak{d}) = (1)$ we conclude that B is primitive. Put now $A = HB$. Then $\overline{A} = H\overline{B}$, and clearly $A, \overline{A}$ are primitive. Furthermore

$$A^k = H^k B^k = (H^2)^{\frac{k-1}{2}} HC = (l)^{\frac{k-1}{2}} (ln + t\sqrt{-d}),$$

is principal. This completes the bijection.

Now let A be the ideal in the pair $\{A, \overline{A}\}$ which satisfies $n, t > 0$. We want to give A explicitly as a $\mathbb{Z}$-module. Since A is primitive, we can write $A = (\mathcal{N}(A), b + \sqrt{-d})_{\mathbb{Z}}$ and from the bijection we see that $\mathcal{N}(A) = lm$. It thus only remains to find b modulo lm. We have that

$$A^2 = (l^2m^2, lmb + lm\sqrt{-d}, b^2 - d + 2b\sqrt{-d})_{\mathbb{Z}},$$

but from the bijection we also have that $A^2 = (l)B^2$. Hence we must have that $l \mid b^2 - d$ so that $l \mid b^2$ and since l is square-free, $l \mid b$. Write therefore $b = lb'$. Since $lm \in A$, we have that lm^2 and $lmb' + m\sqrt{-d} \in B^2$. This implies that the ideal

$$A(B^2)^{\frac{k-3}{2}} B^2 = (l)^{-\frac{k-1}{2}} A^k = (ln + t\sqrt{-d}),$$

contains $(lm)(lm^2)^{\frac{k-3}{2}}(lmb' + m\sqrt{-d})$. In other words, there are integers x, y such that

$$l^{\frac{k+1}{2}} m^{k-1} b' + l^{\frac{k-1}{2}} m^{k-1}\sqrt{-d} = (ln + t\sqrt{-d})(x + y\sqrt{-d}),$$

multiplying by m and using that $lm^k = (ln + t\sqrt{-d})(ln - t\sqrt{-d})$, we see that

$$(ln - t\sqrt{-d})(l^{\frac{k-1}{2}} b' + l^{\frac{k-3}{2}} \sqrt{-d}) = mx + my\sqrt{-d}.$$

Expanding and equating coefficients, we get

$$m \mid l^{\frac{k-1}{2}}(n - tb'),$$

so that $n \equiv_m tb'$. Multiplying by the inverse t^{-1} of t modulo m, and then by l, we get $lm \mid b - lnt^{-1}$, whence we are done. $\square$

We can now end this thesis by giving a rough sketch of how to prove theorem 9.

5.3 Proof sketch

Using proposition 31, we see that the sum in theorem 9 can be written as

$$\mathscr{S}_X = \sum_{\substack{d \equiv_4 2 \\ |\mu(d)|=1}} \phi\left(\frac{d}{X}\right) \sum_{\substack{A \in P_k(-4d) \\ A = (a, b+\sqrt{-d})_{\mathbb{Z}}}} \psi\left(\frac{\sqrt{d}}{Ta}\right),$$

where $\mu(n)$ is the Möbius function.[3] We now have that

$$\mathscr{S}_X = \sum_{\substack{d \equiv_4 2 \\ |\mu(d)|=1}} \phi\left(\frac{d}{X}\right) \sum_{\substack{(1) \neq A \text{ primitive} \\ [A]^k = [1] \in \mathrm{Cl}(-4d) \\ A = (a, b+\sqrt{-d})_{\mathbb{Z}}}} \psi\left(\frac{\sqrt{d}}{Ta}\right),$$

[3]Defined by $\mu(n) = 0$ if n is divisible by the square of a prime, and by $\mu(p_1 p_2 \dots p_r) = (-1)^r$ for distinct primes p_i.

because while criterion $[A]^k = [1]$ implies that the class $[A]$ has order **dividing** k, the conditions on T and the support of ψ make sure that classes with order less than k do not appear. Introducing the parameterization from proposition 34 we get

$$\mathscr{S}_X = \sum_{\substack{l,m,t\in\mathbb{Z}^+,n\in\mathbb{Z}\\ \mathscr{C}_1}} \phi\left(\frac{lm^k - l^2n^2}{t^2X}\right)\psi\left(\frac{\sqrt{lm^k - l^2n^2}}{lmtT}\right),$$

where $\mathscr{C}_1$ represents the conditions

$$\gcd(lmn,t) = 1,\ lm^k - l^2n^2 \equiv_{4t^2} 2t^2, \text{ and } |\mu(\frac{lm^k - l^2n^2}{t^2})| = 1.$$

Notice that the latter two conditions correspond to the conditions $d \equiv_4 2$ and d is square-free. We shall introduce the last condition in a clever way. Let N be an integer and consider the sum

$$\sum_{s^2|N}\mu(s).$$

Say that the prime factorization of N is $N = p_1^{2k_1+l_1}\dots p_r^{2k_r+l_r}$ with $l_i \in \{0,1\}$, and put $q = p_1^{k_1}\dots p_r^{k_r}$ and $r = p_1^{l_1}\dots p_r^{l_r}$. Say now that $s^2 \mid N$. Then s consists of the same primes as N, and thus $s^2 = p_1^{2s_1}\dots p_r^{2s_r}$. Hence $s_i \le k_i + \frac{l_i}{2}$, but since the s_i are integers we have that $s_i \le k_i$, which means that $s \mid q$. Hence

$$\sum_{s^2|N}\mu(s) = \sum_{s|q}\mu(s) = [q = 1],$$

where $[\cdot]$ is the Iverson-bracket.[4] But $q = 1$ iff N is square-free, and hence

$$|\mu(\frac{lm^k - l^2n^2}{t^2})| = \sum_{s^2|\frac{lm^k - l^2n^2}{t^2}}\mu(s).$$

This means that

$$\mathscr{S}_X = \sum_{\substack{l,m,t\in\mathbb{Z}^+,n\in\mathbb{Z}\\ \mathscr{C}_2}} \phi\left(\frac{lm^k - l^2n^2}{t^2X}\right)\psi\left(\frac{\sqrt{lm^k - l^2n^2}}{lmtT}\right) \times \sum_{s^2|\frac{lm^k - l^2n^2}{t^2}}\mu(s),$$

where $\mathscr{C}_2$ are the same conditions as $\mathscr{C}_1$ except square-freeness. What makes this clever is that the sum can be split over s at a parameter Z which then makes it possible to write $\mathscr{S}_X = \mathscr{M} + \mathscr{E}$ where $\mathscr{M}$ is a main term and $\mathscr{E}$ is an error term. Namely

$$\mathscr{M} = \sum_{\substack{l,m,t\in\mathbb{Z}^+,n\in\mathbb{Z}\\ \mathscr{C}_2}} \phi\left(\frac{lm^k - l^2n^2}{t^2X}\right)\psi\left(\frac{\sqrt{lm^k - l^2n^2}}{lmtT}\right) \times \sum_{\substack{s^2|\frac{lm^k - l^2n^2}{t^2}\\ s\le Z}}\mu(s),$$

and

$$\mathscr{E} = \sum_{\substack{l,m,t\in\mathbb{Z}^+,n\in\mathbb{Z}\\ \mathscr{C}_2}} \phi\left(\frac{lm^k - l^2n^2}{t^2X}\right)\psi\left(\frac{\sqrt{lm^k - l^2n^2}}{lmtT}\right) \times \sum_{\substack{s^2|\frac{lm^k - l^2n^2}{t^2}\\ s> Z}}\mu(s).$$

Through an array of analytical tools, Hough is finally able to evaluate the main term,

[4]Let P be a statement. Then $[P] = 0$ if P is true, and $[P] = 1$ if P is false.

Proposition 37. Let $k \geq 3$ and let c_k be the same constant as before. Then for $Z \ll T^{\frac{k}{4}} X^{\frac{1}{2}-\frac{k}{8}-\epsilon}$ we have that

$$\mathscr{M} = \frac{6}{\pi^3}\tilde{\phi}(1)\tilde{\psi}(-1)\frac{X}{T} + \psi(\infty)\tilde{\phi}\left(\frac{1}{2}+\frac{1}{k}\right) c_k X^{\frac{1}{2}+\frac{1}{k}} + O\left(X^{\frac{1}{2}+\frac{1}{2k-2}+\epsilon}\right) + O\left(X^{1+\epsilon}T^{-1}Z^{-1}\right) + O\left(X^{\frac{k}{4}+\epsilon}T^{-\frac{k}{2}}\right).$$

and estimate the error term

Proposition 38. We have that

$$\mathscr{E} \ll \frac{X^{1+\epsilon}}{TZ} + \frac{X^{\frac{k}{4}+\epsilon}}{T^{\frac{k}{2}}}.$$

By Mellin inversion one obtains that

$$\sum_{\substack{d \equiv_4 2 \\ d \text{ square-free}}} \phi\left(\frac{d}{X}\right) = \frac{2}{\pi^2}\tilde{\phi}(1) + O\left(X^{1/2}\right),$$

so proving theorem 9 is now only a matter of picking the right Z. Letting $Z = T^{\frac{k}{4}} X^{\frac{1}{2}-\frac{k}{8}-\epsilon}$ it can be shown that

$$\mathscr{E} \ll \frac{X^{\frac{k}{4}+\epsilon}}{T^{\frac{k}{2}}} + X^{\frac{1}{2}+\frac{1}{2k-2}+\epsilon},$$

and thus the theorem is proved.

Bibliography

[AM94] M.F. Atiyah and I.G. MacDonald. *Introduction To Commutative Algebra*. Addison-Wesley Series in Mathematics. Avalon Publishing, 1994.

[BST13] Manjul Bhargava, Arul Shankar, and Jacob Tsimerman. On the Davenport-Heilbronn theorems and second order terms. *Inventiones Mathematicae*, 193(2):439–499, 2013.

[Bue89] D.A. Buell. *Binary Quadratic Forms: Classical Theory and Modern Computations*. Springer, 1989.

[CHa] H. Cohen and Lenstra H.W. Heuristics on class groups. In Cohn H. Chudnovsky D.V., Chudnovsky G.V. and Nathanson M.B., editors, *Lecture Notes in Mathematics 1052, Number Theory*, pages 26–36. Springer.

[CHb] H. Cohen and Lenstra H.W. Heuristics on class groups of number fields. In Cohn H. Chudnovsky D.V., Chudnovsky G.V. and Nathanson M.B., editors, *Lecture Notes in Mathematics 1068, Number Theory*, pages 33–62. Springer.

[Coh00] H. Cohen. *A Course in Computational Algebraic Number Theory*. Graduate Texts in Mathematics. Springer Berlin Heidelberg, 2000.

[Cona] K. Conrad. Factoring in quadratic fields. `http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/quadraticgrad.pdf`. Unpublished expository paper, accessed 2017-12-27.

[Conb] K. Conrad. Ideal factorization. `http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/idealfactor.pdf`. Unpublished expository paper, accessed 2017-12-27.

[Cox13] David A. Cox. *Primes of the form* $x^2 + ny^2$. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013. Fermat, class field theory, and complex multiplication.

[Dav00] Harold Davenport. *Multiplicative number theory*, volume 74 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2000. Revised and with a preface by Hugh L. Montgomery.

[DF04] D.S. Dummit and R.M. Foote. *Abstract Algebra*. Wiley, 2004.

[DM72] H. Dym and H.P. McKean. *Fourier Series and Integrals*. Probability and mathematical statistics. Academic Press, 1972.

[Duk] W. Duke. An introduction to the linnik problems. In Andrew Granville and Zeév Rudnick, editors, *Equidistribution in number theory*, pages 197–216. Springer.

[Duk88] W. Duke. Hyperbolic distribution problems and half-integral weight maass forms. *Inventiones Mathematicae*, 92(1):73–90, 1988.

[Gau01] Gauß C.F., Waterhouse, W.C. (ed.) and Clarke, A.A. (trans.). *Disquisitiones Arithmeticæ*. Springer-Verlag, 1986 (originally 1801).

[Hou10] B. Hough. Equidistribution of bounded torsion CM points. *ArXiv e-prints*, May 2010.

[IK04] H. Iwaniec and E. Kowalski. *Analytic Number Theory*. Number v. 53 in American Mathematical Society colloquium publications. American Mathematical Society, 2004.

[Lin68] Y. V. Linnik. *Ergodic properties of algebraic fields*. Springer-Verlag, Berlin, 1968.

[Neu13] J. Neukirch. *Algebraic Number Theory*. Grundlehren der mathematischen Wissenschaften. Springer Berlin Heidelberg, 2013.

[Pin15] F. Pintore. *Binary quadratic forms, elliptic curves and Schoof's algorithm*. PhD thesis, University of Trento, 5 2015.

[RBvdG+08] K. Ranestad, J.H. Bruinier, G. van der Geer, G. Harder, and D. Zagier. *The 1-2-3 of Modular Forms: Lectures at a Summer School in Nordfjordeid, Norway*. Universitext. Springer Berlin Heidelberg, 2008.

[ST01] I. Stewart and D. Tall. *Algebraic Number Theory and Fermat's Last Theorem: Third Edition*. AK Peters Series. Taylor & Francis, 2001.

[Thea] The PARI Group. PARI/GP. `https://pari.math.u-bordeaux.fr/`. Version 2.9.3, 2017-06-05.

[Theb] The SageMath Group. SageMath module BinaryQF. `https://github.com/sagemath/sagelib/blob/master/sage/quadratic_forms/binary_qf.py`. Source code at GitHub repository, accessed 2018-01-01.

[TT13] Takashi Taniguchi and Frank Thorne. Secondary terms in counting functions for cubic fields. *Duke Mathematical Journal*, 162(13):2451–2508, 2013.

[Wei06] A. Weil. *Number Theory: An approach through history From Hammurapi to Legendre*. Modern Birkhäuser Classics. Birkhäuser Boston, reprint, 2006.