2-Torsion in Ideal Class-Groups

Jan Bednarski, Tudor Ciurca, Davide Gallo
Supervised by Lucas Mann

PROMYS Europe 2017

Contents

1 Introduction

After the traumatic realization that uniqueness of factorization into irreducible holds in some rings of integers but not in others, mathematicians took steps to develop more insightful theories. Kummer had the bright idea that if he could not factorize a number uniquely in a given ring of integers, then perhaps he could extend the ring to a bigger one in which the factorization is possible and unique. He called the new elements to be added to extend the ring in such a way *ideal numbers*. Dedekind looked at the same ideas from a different direction instead. He introduced in ring theory the notion of *ideal*, a term arising from the correspondence with ideal numbers.

It turns out that although factorization might fail for numbers, an elegant theory of unique factorization can be developed for ideals. In this theory, the essential building blocks are *prime ideals*. We want to find a quantitative measure of how *non-unique* factorization can be though. Here comes the notion of *class-group*, with the *class-number* being its corresponding size. Intuitively, the larger the class-number, the more complicated the possibilities for non-uniqueness become.

The importance of the class-number can only be hinted at here. Many deep and delicate results in the theory of numbers are related to arithmetic properties of the class-number, or to algebraic properties of the class-group. The goal of this project is to study a case where things are somewhat well understood: the case of *2-power torsion* in the class-groups of quadratic fields.

2 Background

We are going to start our journey by assembling some definitions and proving some preliminary results which will help us achieve our two initial goals of describing the prime factorization of ideals and constructing the ideal class-group. Throughout this section (and, indeed, the whole project) *ring* will mean commutative ring with unity.

2.1 Number Fields and Algebraic Integers

The first concepts which will need to be introduced are *number field* and *algebraic integer*.

Definition 2.1. A number field K is a field of the form $\mathbb{Q}(\alpha_1, ..., \alpha_n)$ where the α_is are algebraic numbers.

Definition 2.2. The minimal polynomial f_α of an algebraic number α is the monic polynomial of least degree among all the polynomials in $\mathbb{Q}[x]$ having α as a root.

The fact that fields of such form are indeed fields is definitely not obvious and needs to be proven. We stow these background results to the supplement at the end of this paper to be able to move more quickly to the actual results we want to present.

In this research project we will focus on quadratic fields of the form $\mathbb{Q}(\sqrt{d})$ where d is a square-free integer.

Definition 2.3. We call an element $\delta \in \mathbb{C}$ an algebraic integer if it is in the zero set of a monic polynomial $f(x) \in \mathbb{Z}[x]$.

Definition 2.4. The ring of integers $\mathcal{O}_K$ of a number field K is the ring of all the algebraic integers in K.

Again, the ring of integers of a number field turns out to be a ring. Here we are going to prove a basic result about $\mathbb{Z}$ to provide an example of what we are trying to talk about.

Proposition 2.1. *The ring of algebraic integers of $\mathbb{Q}$ is $\mathbb{Z}$.*

Proof. First of all, any rational integer n has the minimal polynomial $x - n$ and because it is monic we get that n is an algebraic integer in $\mathbb{Q}$. Now, let us take any rational number $\alpha = \frac{p}{q}$ where p, q are coprime integers with $q > 0$ such that α is an algebraic integer in $\mathbb{Q}$. Then there is a polynomial

$$f(x) = x^k + a_{k-1}x^{k-1} + \ldots + a_0$$

with $a_0, \ldots, a_{k-1} \in \mathbb{Z}$ such that

$$f(\alpha) = \left(\frac{p}{q}\right)^k + a_{k-1}\left(\frac{p}{q}\right)^{k-1} + \ldots + a_0 = 0.$$

Multiplying this equation by q^k we obtain $p^k = -a_{k-1}p^{k-1}q - \ldots - a_0q^k$, from which we get that $q \,|\, p^k$. Since p and q are coprime and q positive, it follows that $q = 1$. Therefore, $\alpha = p \in \mathbb{Z}$. □

The reader might now ask what happens if we consider different number fields. In the case we care about, the case of quadratic number fields, things work out rather neatly. Here we have a first useful result.

Lemma 2.2. *Let d be a square-free integer. Then the algebraic integers in $\mathbb{Q}(\sqrt{d})$ are:*

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}\frac{1+\sqrt{d}}{2} & \textit{if } d \equiv 1 \pmod 4 \\ \mathbb{Z}\sqrt{d} & \textit{if } d \not\equiv 1 \pmod 4. \end{cases}$$

Proof. Every element $\alpha \in \mathbb{Q}[(\sqrt{d})$ is of the form $\alpha = r + s\sqrt{d}$ where $r, s \in \mathbb{Q}$. Hence we may write

$$\alpha = \frac{a + b\sqrt{d}}{c}$$

where $a, b, c \in \mathbb{Z}$ and $(a, b, c) = 1$. Now α is an algebraic integers if the coefficients in the minimal polynomial

$$\Big(x - \Big(\frac{a + b\sqrt{d}}{c}\Big)\Big)\Big(x - \Big(\frac{a - b\sqrt{d}}{c}\Big)\Big)$$

are integers. We want

$$\frac{a^2 - b^2d}{c^2} \in \mathbb{Z} \text{ and } \frac{2a}{c} \in \mathbb{Z}.$$

Now we must have either $c = 1$ or $c = 2$. If c and a share a common factor p then by the first equation $p \,|\, b$, because d is square-free, against our assumption $(a, b, c) = 1$.

Let's concentrate on the case $c = 2$. Then a and b are both odd and $\frac{a^2-b^2d}{4} \in \mathbb{Z}$. Hence

$$a^2 - b^2 d \equiv 0 \pmod 4.$$

This is only possible if $d \equiv 1 \pmod 4$. Conversely, for $d \equiv 1 \pmod 4$ and a, b odd we have α is an algebraic integers, because our previous argument holds. To sum up:

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

□

We may now wonder whether the ring of integers $\mathcal{O}_K$ of number fields $K = \mathbb{Q}(\sqrt{d})$ have unique prime factorization. It is worth noticing that counterexamples in rings such as $\mathbb{Z}[\sqrt{-3}]$, e.g.

$$(1 + \sqrt{-3})(1 - \sqrt{-3}) = 2 \cdot 2,$$

shouldn't bother us much. We now know indeed that ring of integers $\mathcal{O}_K$ for $K = \mathbb{Q}(\sqrt{-3})$ is actually $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ and not $\mathbb{Z}[\sqrt{-3}]$.

It turns out there are actually number fields whose ring of integers indeed do not have unique prime factorization. It is easy to prove unique prime factorization when we have an efficient division algorithm. This happens for

$$d = -11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73.$$

It is an open question whether there exist finitely many such values.

Example. In the ring of integers $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ of the number field $K = \mathbb{Q}(\sqrt{-5})$ all the factors of the factorization $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ are indeed irreducible.

For an element $a + b\sqrt{-5} \in \mathcal{O}_K$ for the norm we have

$$N(a + b\sqrt{-5}) = a^2 + 5b^2.$$

Hence the norms of our 4 elements in the two factorizations are 4, 9, 6 and 6 respectively. If two of them were not to be an irreducible element then there would exist $p, q \in \mathcal{O}_K$ such that $2 = pq$, leading to $4 = N(2) = N(p)N(q) \implies N(p)$ and $N(q) = \pm 2$. Similarly there would exist $r, s \in \mathcal{O}_K$ such that $3 = rs$, leading to

$$9 = N(3) = N(r)N(s) \implies N(r) = \pm 3 \text{ and } N(s).$$

This all sums up to the existence of integer solutions to the equation

$$a^2 + 5b^2 = \pm 2 \text{ or } \pm 3.$$

Such solutions do not exist. Thus all elements are irreducible. In the ring $\mathbb{Z}[\sqrt{-5}]$ unique prime factorization does not hold.

We might still have unique prime factorization without a division algorithm though. This happens for

$$d = -19, -43, -67, -163.$$

These are the *only* negative integers (together with the ones listed above) for which unique prime factorization holds true.

2.2 Ideals

To fix the issue of rings which don't have unique factorization in the usual sense we introduce the notion of *ideals*.

Definition 2.5. A subset I of a ring R is said to be an ideal in R if it satisfies the following two properties: (i) $\forall\ a, b \in I$ we have $a + b \in I$ (I is an additive subgroup of R); (ii) $\forall\ r \in R$ we have $rI \subseteq I$.

Definition 2.6. An ideal $\mathfrak{p}$ is prime if $\forall\ a, b \in R$ we have that $ab \in \mathfrak{p}$ implies either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

Definition 2.7. If $a_1, \dots, a_n$ are elements of R then $(a_1, \dots, a_n)$ is defined to be the set $\{a_1 r_1 + \cdots + a_n r_n : r_i \in R\}$.

The reader is invited to check that $(a_1, \dots, a_n)$ is indeed an ideal.

Definition 2.8. If an ideal I is equal to (a) for some $a \in R$ we say I is principal.

Definition 2.9. If I and J are two ideals then $IJ = \{\sum a_i b_i : a_i \in I, b_i \in J\}$.

The reader is invited to check that also IJ is still an ideal.

Proposition 2.3. *All ideals I in $\mathbb{Z}$ are principal.*

Proof. The case $I = (0)$ is boring. Suppose $I \neq (0)$. Since both s and $-s$ belong to I by definition there also exists a positive integer in our ideal. We choose the smallest positive element d in I and try to prove that all the other elements in I are multiples of d.
Take any $a \in I$ and let $a = qd + r$, where $q, r \in \mathbb{Z}$ and $0 \leq r < d$. Since $a \in I$ and $qd \in I$ also

$$r = a - qd \in I.$$

But d was supposed to be a smallest element. Therefore $r = 0$ and $a = qd$. Hence $I = (d)$. □

Corollary 2.4. *The sum of two ideals (a) and (b) in $\mathbb{Z}$ is $(a) + (b) = (\gcd(a, b))$.*

We then conclude with two more definitions. Here we just gave a general idea of what we are talking about, further results about ideals will be proven in future sections.

Definition 2.10. If K is a number field and $I \subseteq \mathcal{O}_K$ is a non-zero ideal then $\mathcal{O}_K/I$ is the set of all the equivalence classes under the relation $a \equiv b \pmod{I}$ if and only if $b - a \in I$.

Definition 2.11. We define the *norm* of a non-zero ideal $I \subseteq \mathcal{O}_K$ to be $N(I) = \left|\mathcal{O}_K/I\right|$.

2.3 Class-Group

Now that we have concluded our endless list of definitions about ideals we can actually move on to the definition of the *class-group.* Finally we will prove the equivalence of some fundamental statements involving unique prime factorization of elements and the size of the class-group. Further details and more in-deep results will be left to the following section.

Definition 2.12. Let K be a number field and I and J be ideals in $\mathcal{O}_K$. Define $I \sim J$ if and only if there exist $a, b \in \mathcal{O}_K$ such that $aI = bJ$.

Again it is easy to show this is indeed an equivalence relation.

Definition 2.13. The set of equivalence classes under the above equivalence relation is called the class-group of K and denoted $cl(K)$ or $cl(\mathcal{O}_K)$.

Our next goals will be showing that $cl(K)$ is actually a group and eventually that $|\,cl(K)\,|$ is finite. To achieve this we need to mention an appealing feature of ideals.

Assumption. *Let K be a number field and $\mathcal{O}_K$ be its ring of integers. If I is a non-zero ideal in $\mathcal{O}_K$ then I admits a unique prime factorization.*

Proposition 2.5. *Let K be a quadratic field. Then for any ideal $I \subseteq \mathcal{O}_K$ there exists an ideal $I' \subseteq \mathcal{O}_K$ and a rational integer k such that $II' = (k)$.*

Proof. Let $I \subseteq \mathcal{O}_K$ be an ideal. Suppose $I = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_i$ where $\mathfrak{p}_i$ are prime ideals (not necessarily different). Consider the ideal $\bar{I}$ generated by the conjugates of the generators of I. Then

$$I\bar{I} = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_i \cdot \bar{\mathfrak{p}_1}\bar{\mathfrak{p}_2} \dots \bar{\mathfrak{p}_i} = \mathfrak{p}_1\bar{\mathfrak{p}_1} \cdot \mathfrak{p}_2\bar{\mathfrak{p}_2} \cdot \dots \cdot \mathfrak{p}_n\bar{\mathfrak{p}_n}.$$

Since $\mathfrak{p}\bar{\mathfrak{p}} = N(\mathfrak{p})$, by Proposition 8.1, the equation above then becomes

$$I\bar{I} = (N(\mathfrak{p}_1))(N(\mathfrak{p}_2)) \dots (N(\mathfrak{p}_n)) = (N(I)),$$

which is clearly a principal ideal generated by $k = N(I) \in \mathbb{Z}$. □

In the following sections we might mention the notion of *Dedekind domain.* It is worth providing a definition. In this project we will just use the fact that a ring of integers $\mathcal{O}_K$ is indeed a Dedekind domain.

Definition 2.14. An integral domain R is said to be a Dedekind domain if it satisfies the following properties: (i) R is Noetherian; (ii) R is integrally closed; (iii) every nonzero prime ideal in R is maximal.

It is not necessary to fully understand this definition. It just allows us to present our results in a more general way. We might rephrase our previous statement about unique prime factorization of ideals as follows.

Assumption. *Let R be a Dedekind domain. If I is a non-zero ideal in R then I admits a unique prime factorization.*

This allows us to conclude this sections with the following two results. More details about these proofs can be found in the following section. Here the main purpose is just to give a general feeling of what we will be dealing with.

Proposition 2.6. *The ring of integers $\mathcal{O}_K$ has unique factorization if and only if every ideal in $\mathcal{O}_K$ is principal.*

Proof of $\Leftarrow$. Follows immediately from the fact that ideals factors uniquely.

Proof of $\mapsto$. Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$. Since $N(\mathfrak{p}) = \left|\mathcal{O}_K/\mathfrak{p}\right|$, we have $m \cdot N(\mathfrak{p}) \in \mathfrak{p}$ for any element $m \in \mathcal{O}_K$. Hence $\mathfrak{p} \mid N(\mathfrak{p})$. Now let us factorize $N(\mathfrak{p})$ into irreducible elements in $\mathcal{O}_K$ and notice that we can write $\big(N(\mathfrak{p})\big)$ as the product of the principal ideals generated by such irreducible elements. Since $\mathfrak{p}$ is prime and our factorization is unique, $\mathfrak{p} \mid (q_i)$ for some ideal generated by prime factor of $N(p)$. Hence $\mathfrak{p} = (q_i)$ and both the ideals are prime. In particular $\mathfrak{p}$ is principal. □

Proposition 2.7. *Every ideal in $\mathcal{O}_K$ is principal if and only if $cl(K)$ is trivial.*

Proof of $\Leftarrow$. Suppose any two ideals are equivalent. Then there always exist an element $a \in \mathcal{O}_K$ and a principal ideal (b) such that $a \cdot I = (b)$. Therefore $b = a \cdot i$ for some $i \in I$. Hence $a \cdot I = a \cdot (i)$ and $I = (i)$.

Proof of $\mapsto$. Suppose every ideal is principal. Given any two ideals $I = (a)$ and $J = (b)$ clearly we have $bI = aJ$. Hence they to belong the same class. Thus $cl(K) = \{1\}$. □

3 Norm of Ideals

Here we will prove some more in-deep results about the *norm* of ideals which will turn out to be really useful in future sections. If the reader is already familiar with these concepts the section might also be skipped as a whole to jump to the actual aim of our project.

Definition 3.1. If R is a ring and $I \subseteq R$ is a non-zero ideal then $N(I)$ is the size of R/I.

We have already defined the concept of norm in the previous sections. Here we generalized the concept to any ring R. In other words the norm $N(I)$ of an ideal $I \subseteq R$ is the number of equivalence classes in the quotient ring R/I. In particular, the ideal norm is multiplicative.

We start with a basic result. We discover without much surprise that modding out a ring by a non-principal ideal is the same as modding out the ring by each of the ideal generators in turn.

Proposition 3.1. *Let R be a ring and $I, J \subset R$ be ideals. Then $(R/I)/(J/(J \cap I)) \cong (R/J)/(I/(J \cap I)) \cong R/(I + J)$.*

Proof. It is sufficient to show that $(R/I)/(J/(J \cap I)) \cong R/(I+J)$. Let

$$\psi : R \mapsto (R/I)/(J/(J \cap I))$$

be the homomorphism. Then $I \subseteq \ker\psi$ and $J \subseteq \ker\psi$. Since $\ker\psi$ is an ideal, it is closed under addition. So $I + J \subseteq \ker\psi$.

It turns out that $I+J$ is in fact the kernel of ψ. Any element not in $I+J$ can be written as $k+a$ for $k \in (I+J)$ and $a \in R/(I+J)$. We can further decompose k into $i+j$ and require $i \in I/(I \cap J)$ and $j \in J/(I \cap J)$. Then $(i+j)+a$ is mapped to $j+a$ by the first quotient and then to a by the second quotient. So $k+a$ belongs to the kernel if and only if $a=0$.

On the other hand, the kernel of the homomorphism

$$\mu : R \mapsto R/(I+J)$$

is $I+J$. Hence the kernels are the same. Thus by the First Isomorphism Theorem we have $(R/I)/(J/(J \cap I)) \cong R/(I+J)$. □

We are now able to prove the generalization of CRT for generic rings. This allows us to prove the first actual result about the norm of ideals.

Theorem 3.2. *Let R be a ring and $I, J \subset R$ be ideals such that $I+J=R$. Then $R/(IJ) \cong R/I \times R/J$.*

Proof. The kernel of $\psi : R \mapsto R/(IJ)$ is clearly IJ. Let μ be the homomorphism

$$\mu : R \mapsto R/I \times R/J$$

such that $\mu(x) = (x \pmod I,\ x \pmod J)$. Since $I + J = (1)$, there always exist $a \in I, b \in J$ such that $a+b=1$. It follows that there is always a solution $x = as + br$ to the system of congruences

$$x \equiv r \pmod I \wedge x \equiv s \pmod J.$$

This solution is unique modulo IJ. If two elements $a_1s + b_1r$ and $a_2s + b_2r$ are equivalent in $R/I \times R/J$ then they are also equivalent in R/I and R/J. Hence $(a_1 - a_2)s + (b_1 - b_2)r$ belongs to both I and J. So it belongs to IJ. Therefore the two elements are also equivalent in $R/(IJ)$.

The kernel of μ consists of elements $r \in R$ that map to $(0 \pmod I,\ 0 \pmod J)$. It follows that $r \equiv 0 \pmod{IJ}$ is the unique solution to such congruences. So $\ker\mu = IJ = \ker\psi$. Since the kernels of the functions are the same, the images of the homomorphisms must be isomorphic by the First Isomorphism Theorem, and so we have $R/(IJ) \cong R/I \times R/J$. □

Corollary 3.3. *Let R be a ring and $I, J \subset R$ be ideals such that $I+J=R$. Then $N(IJ) = N(I)N(J)$.*

Proof. We just showed $R/(IJ) \cong R/I \times R/J$. Thus

$$|\,R/(IJ)\,| = |\,R/I \times R/J\,| = |\,R/I\,| \times |\,R/J\,|.$$

This is indeed the definition of norm. Hence $N(IJ) = N(I)N(J)$. □

We can now move on trying to extend this result to the general case. We will here start using the notion of *Dedekind domain.* Since any ring of integers $\mathcal{O}_{\mathcal{K}}$ of a number field K is indeed such a domain, in our case this is equivalent to considering the by-now-familiar ring $\mathcal{O}_K$.

Proposition 3.4. *Let R be a Dedekind domain and $\mathfrak{p} \subset R$ be a prime ideal. Then $\mathfrak{p}^n/\mathfrak{p}^{n+1} \cong R/\mathfrak{p}$.*

Proof. First of all $\mathfrak{p} \neq R$. So $\mathfrak{p}^{n+1} \neq \mathfrak{p}^n$. Hence there is an element $b \in \mathfrak{p}^n/\mathfrak{p}^{n+1}$, $b \neq 0$. Let ψ be the homomorphism

$$\psi : R/\mathfrak{p} \mapsto \mathfrak{p}^n/\mathfrak{p}^{n+1}$$

such that $\psi(a) = ab$. Since

$$\psi(a) = 0 \implies ab \in \mathfrak{p}^{n+1},$$

we have $\ker\psi = \mathfrak{p}$. Since b is not an element of $\mathfrak{p}^{n+1}$, we have $\mathfrak{p}^{n+1} \nmid (b)$. Hence

$$\mathfrak{p}^{n+1} \,|\, (a)(b) \implies \mathfrak{p} \,|\, (a) \implies a \equiv 0 \text{ in } R/\mathfrak{p}.$$

We now show that ψ is injective. We have

$$\psi(x) = \psi(y) = by = bx \implies b(x-y) \equiv 0 \implies (x-y) \in \ker\psi \implies x \equiv y.$$

We now show that ψ is surjective, and hence ψ is an isomorphism. Suppose it is not. Then b does not generate the whole $\mathfrak{p}^n/\mathfrak{p}^{n+1}$ under addition. So

$$(\mathfrak{p}^n/\mathfrak{p}^{n+1})/((b)/(b) \cap \mathfrak{p}^{n+1})) \cong \mathfrak{p}^n/(\mathfrak{p}^{n+1} + (b))$$

is non-trivial. In other words $(b) + \mathfrak{p}^{n+1} \neq \mathfrak{p}^n$. But

$$(b) \subset \mathfrak{p}^n \implies (b) = I \cdot \mathfrak{p}^n$$

for some ideal I. Hence $\mathfrak{p}^n(I + \mathfrak{p}) \neq \mathfrak{p}^n \implies I + \mathfrak{p} \neq R$. Since $\mathfrak{p}$ is a prime ideal, we have

$$\mathfrak{p} \,|\, I \implies \mathfrak{p}^{n+1} \,|\, (b),$$

which is a contradiction. □

Corollary 3.5. *Let R be a Dedekind domain and $\mathfrak{p} \subset R$ be a prime ideal. Then $N(\mathfrak{p}^n) = N(\mathfrak{p})^n$.*

Proof. Consider the ring R and the ideals $\mathfrak{p}^n, \mathfrak{p}^{n+1}$ as additive commutative groups. We have

$$\mathfrak{p}^{n+1} \subset \mathfrak{p}^n \subset R$$

and by the First Isomorphism Theorem we get

$$\frac{R/\mathfrak{p}^{n+1}}{\mathfrak{p}^n/\mathfrak{p}^{n+1}} \cong R/\mathfrak{p}^n.$$

Hence

$$\frac{|\, R/\mathfrak{p}^{n+1}\,|}{|\,\mathfrak{p}^n/\mathfrak{p}^{n+1}\,|} = |\, R/\mathfrak{p}^n\,| \implies \frac{|\, R/\mathfrak{p}^{n+1}\,|}{|\, R/\mathfrak{p}\,|} = |\, R/\mathfrak{p}^n\,| \implies |\, R/\mathfrak{p}\,|\,|\, R/\mathfrak{p}^n\,| = |\, R/\mathfrak{p}^{n+1}\,|.$$

Therefore

$$N(\mathfrak{p}^{n+1}) = N(\mathfrak{p}^n)N(\mathfrak{p}).$$

We can inductively assume that the claim is true for all exponents of $\mathfrak{p}$ up to and including n to use the same argument and extend our claim to the exponent $n+1$. We clearly have $N(\mathfrak{p}^1) = N(\mathfrak{p})$ as a base case. □

Finally we are able to prove that the norm is multiplicative. This fact will be widely used in future proofs.

Proposition 3.6. *Let R be a ring and $I, J \subset R$ be ideals. Then $N(IJ) = N(I)N(J)$.*

Proof. Let the product IJ decompose into the prime ideals $\prod_{i=1}^n \mathfrak{p}_i^{e_i}$. Each pair of prime ideals in the decomposition is clearly coprime. We have $\mathfrak{p}_i^{e_i} + \mathfrak{p}_j^{e_j} = R$ for $i \neq j$. Thus by Corollary 3.3 we get

$$N(IJ) = \prod_{i=1}^{n} N(\mathfrak{p}_i^{e_i}).$$

This by Corollary 3.5 can be decomposed as $N(IJ) = \prod_{i=1}^n N(\mathfrak{p}_i)^{e_i}$. The ideal norm is multiplicative. We essentially have $N(IJ) = N(I)N(J)$. □

This achieves the main aim of this section. Now we state some more simple observations that mainly follow as corollaries of previous results.

Proposition 3.7. *Let R be a ring and $I \subseteq R$ be an ideal. Then $N(I) = 1 \iff I = R$.*

Proof of $\Leftarrow$. Clear. $I = R \implies N(I) = |\, R/R\,| = 1$.

Proof of implies. If $N(I) = |\, R/I\,| = 1$ then every element from R is mapped to the same equivalence class 0. In other words $a - 0 = a \in I \;\forall\; a \in R \implies I = R$. □

Corollary 3.8. *Let K be a quadratic field and $I \subseteq \mathcal{O}$ be an ideal. Suppose $I = (p)$ for a rational prime p. Then I factors into at most 2 prime ideals.*

Proof. We have $N\big((p)\big) = p^2$. Hence every ideal that properly divides (p) must have norm that divides p. Thus either (p) is a prime ideal or it factors into exactly 2 prime ideals with norm p. □

Corollary 3.9. *Let R be a Dedekind domain and $\mathfrak{p} \subset R$ be a prime ideal. Then for each $a \in \mathfrak{p}$ we must have $N(\mathfrak{p}) \,|\, N(a)$.*

4 Computing the Class-Group

4.1 Lattices

We now take a small detour to prove a few results about lattices. We will focus here on quadratic number fields $K = \mathbb{Q}(\sqrt{d})$ where d is a square-free integer $d < 0$. We can view ideals in K as lattices in the complex plane. The results we are going to provide will turn out to be really useful to prove facts about the ideal class-group.

Definition 4.1. Given a a bounded subset R of the plane $\mathbb{C}$:

(i) We call R *convex* if for all $a, b \in R$, for any c on the line segment joining a to b we have $c \in R$.

(ii) We call R *centrally symmetric* if for all $p \in R$ we have $-p \in R$.

Recall that a lattice $L \in \mathbb{C}$ can either be $\{0\}$ or must be generated by one or two vectors. We are here just considering the cases where $d > 0$, meaning that there will always be an imaginary component, so it is always the case with two vectors, and note also that such vectors constitute the lattice basis for L.

Will hereafter denote by $\Delta(L)$ the area of the fundamental parallelogram of the lattice $L \subset \mathbb{C}$ and by V_R the volume of a convex centrally symmetric region $R \subset \mathbb{C}$.

Theorem 4.1 (Minkowski)**.** *Let L be a lattice in C and $R \subset \mathbb{C}$ be a convex and centrally symmetric region such that $V_R > 4\Delta(L)$. Then R must contain a lattice point other than the origin.*

4.2 Minkowski's Bounds

Proposition 4.2. *Let $K = \mathbb{Q}(\sqrt{d})$ be a number field with $d < 0$ being a square-free integer and $\mathcal{O}_K = \mathbb{Z}[\alpha] = \{a + b\alpha : (a, b) \in \mathbb{Z}^2\}$ be its ring of integers. Let $I \subseteq \mathcal{O}_K$ be an ideal and $L \subset \mathbb{Z} \times \alpha\mathbb{Z}$ be the lattice generated by I in $\mathbb{Z} \times \alpha\mathbb{Z} \subset \mathbb{C}$. Then $\Delta(L) = \det L = \Big|\mathbb{Z}[\alpha]/I\Big| = N(I)$.*

Proposition 4.3. *Let $I \subseteq \mathcal{O}_K$ be an ideal. Then $\Delta(I) = kN(I)$ for some $k \in \mathbb{R}$.*

Proof. Let $I \subseteq \mathcal{O}_K$ be an ideal. In a quadratic number field $K = \mathbb{Q}(\sqrt{d})$ we have that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ where either $\alpha = \sqrt{d}$ or $\alpha = \frac{1+\sqrt{d}}{2}$ and $\mathbb{Z}[\alpha] = \{a + b\alpha : (a, b) \in \mathbb{Z}^2\}$. Let $L \subset \mathbb{Z} \times \alpha\mathbb{Z}$ be the lattice generated by I in $\mathbb{Z} \times \alpha\mathbb{Z} \subset \mathbb{C}$. Let f be the scaling function

$$f : \mathbb{Z} \times \alpha\mathbb{Z} \mapsto \mathbb{Z}^2$$

such that

$$f\big((a,b\alpha)\big)=(a,b).$$

Let $L':=f(L)$. Hence $\Delta(I)=\Delta(L)=\delta\Delta(L')$ where either $\delta=\sqrt{|d|}$ or $\delta=\frac{1+\sqrt{|d|}}{2}$. Therefore we have $\delta\Delta(L')=\delta N(I)$. □

Lemma 4.4. *Let $I\subseteq\mathcal{O}_K$ be an ideal. Then there always exist an element $a\in I$ such that $N(a)<cN(I)$ for some (possibly different) $c\in\mathbb{R}$.*

Proof. Define the convex and central symmetric region

$$\mathcal{K}:=\{a\in\mathbb{C}:|a|^2<cN(I)\}$$

for a constant $c\in\mathbb{R}$ yet to be defined. Then $\mathcal{K}$ is a circle of radius $\sqrt{cN(I)}$ with $V_{\mathcal{K}}=\pi\sqrt{cN(I)}^2=\pi cN(I)$.

Suppose now

$$V_{\mathcal{K}}>4\Delta(I)=4\delta N(I)$$

where either $\delta=\sqrt{|d|}$ or $\delta=\frac{1+\sqrt{|d|}}{2}$ as in the proposition above. Then $c>\frac{4\alpha}{\pi}$. Put $c>\frac{4\alpha}{\pi}$. Then by Theorem 4.1 there exist $a\in I$ such that $a\in\mathcal{K}$, $a\neq 0$. In particular

$$N\big((a)\big)=|a|^2<cN(I).$$

Now $(a)\subset I\implies I\,|\,(a)\implies\exists$ an ideal $J\in\mathcal{O}_K$ such that $(a)=IJ$. Hence $I\sim J^{-1}$ and

$$N(IJ)=N(I)N(J)\implies N(a)=N(I)N(J)\implies N(J)<c.$$

In particular for c properly chosen we have $N(J)<\frac{4\alpha}{\pi}$. □

Such results can also be generalized to real quadratic fields. We can define the notion of *discriminant* and sum up everything as follows.

Definition 4.2. Let $K=\mathbb{Q}(\sqrt{d})$ be a number field and $\mathcal{O}_K=\mathbb{Z}[\alpha]$ be its ring of integers. Then we say the *discriminant* D_K of K is the discriminant of the minimal polynomial $f_\alpha\in\mathbb{Z}[x]$ of the algebraic integer α.

Lemma 4.5. *Each ideal class in the class-group $cl(K)$ contains an ideal with norm at most $\mathcal{M}_K$ with:*

$$\mathcal{M}_K=\sqrt{|D_K|}\cdot\begin{cases}\frac{2}{\pi} & \textit{if } D<0\\ \frac{1}{2} & \textit{if } D>0.\end{cases}$$

We can now compute the class-group easily by only checking those ideals $I\subseteq\mathcal{O}_K$ such that $N(I)<c$. Every ideal I contains a rational integer, namely $N(I)$, so that can find every prime ideal by factoring rational primes. We then just need to factor rational primes $p<\mathcal{M}_K$. Please now pause and ponder on how powerful this tool is. By factoring a *handful* of principal ideals we can compute the class-group of the number field and, for example, among other things, check whether the ring of integers has unique prime factorization.

Example. We compute the class-group $cl(K)$ of $K = \mathbb{Q}(\sqrt{-5})$.

For $d = \sqrt{-5}$ we have $D_K = -20$ and $\mathcal{M}_K = \frac{2\sqrt{20}}{\pi} < 3$. We then just have to factor the principal ideal generated by 2. We find

$$(2) = (2,\, 1 + \sqrt{-5})^2.$$

Now $(2) \sim (1)$ and clearly $(2) \not\sim (2,\, 1 + \sqrt{-5})$ in the class-group. We then have

$$cl(\mathbb{Q}(\sqrt{-5})) = \{(1),\, (2, 1 + \sqrt{-5})\}.$$

Incidentally we notice $|cl(\mathbb{Q}(\sqrt{-5}))| = 2 \neq 1$. In the ring $\mathbb{Z}[\sqrt{-5}]$ unique prime factorization does not hold.

Here is a table displaying the structure of class groups for $\mathcal{O}_{\mathbb{Q}(n)}$ for square-free integers $n = -2$ to -22:

n	class number	class group	n	class number	class group
-2	1	–	-13	2	C_2
-3	1	–	-14	4	C_4
-5	2	C_2	-15	2	C_2
-6	2	C_2	-17	4	C_4
-7	1	–	-19	1	–
-10	2	C_2	-21	4	$C_2 \times C_2$
-11	1	–	-22	2	C_2

Table 1: Examples of class groups

5 Prime Factorization of Ideals

We know that an ideal $I \in R$ is prime if and only if R/I is an integral domain. In this section we will exploit an isomorphism between the ring $\mathbb{Z}[\alpha]$ and the ring of polynomials $\mathbb{Z}[x]/f_\alpha$ in order to extend our understanding of this fact. In this section f_α will denote the minimal polynomial of α in $\mathbb{Z}[x]$. Our results will allow for both a quicker and more systematic method of studying ideal factorization.

Lemma 5.1. *There is an isomorphism* $\mathbb{Z}[x]/f_\alpha \cong \mathbb{Z}[\alpha]$ *induced by* $\psi : f(x) \mapsto f(\alpha)$.

Proof. We can extend the domain of ψ such that

$$\psi : \mathbb{Z}[x] \mapsto \mathbb{Z}[\alpha].$$

Now ψ is clearly surjective as every element $e \in \mathbb{Z}[\alpha]$ can be written as

$$\sum_{i=0}^{n} k_i \alpha^i$$

for some integers k_i and a natural number n. The kernel of this map is the ideal generated by f_α in $\mathbb{Z}[x]$ because

$$f(\alpha) = 0 \iff f_\alpha | f.$$

Then by the First Isomorphism Theorem, it follows that $\mathbb{Z}[x]/f_\alpha \cong \mathbb{Z}[\alpha]$. □

We will make use of the results proved earlier to demonstrate a fundamental result in quadratic number fields.

Theorem 5.2 (Dedekind's Criterion)**.** *Let* $K = \mathbb{Q}(\sqrt{d})$ *be a quadratic number field. Consider the ring of integers* $\mathcal{O}_K = \mathbb{Z}[\delta]$ *where* δ *is the primitive element of* $\mathcal{O}_K$*. Let* p *be a rational prime and* $(p) \subset \mathcal{O}_K$ *be the principal ideal generated by* p *in* $\mathcal{O}_K$*. Let* f_δ *be the minimal polynomial of* δ *in* $\mathbb{Z}[x]$*. Suppose* f_δ *decomposes as* $(x+a)(x+b)$ *in* $\mathcal{O}_K/(p)$ *for some non-zero* $a, b \in \mathcal{O}_K/(p)$*. Then we have the unique factorization in prime ideals* $(p) = (p, a+\delta)(p, b+\delta)$.

Proof. We start by showing that $(p) \supset (p, \delta + a)(p, \delta + b)$. Since

$$(p, \delta + a)(p, \delta + b) = (p^2,\, p\delta + pa,\, p\delta + pb,\, \delta^2 + (a+b)\delta + ab)$$

and p divides each generator the claim follows. We now try to show that $p \in (p, a+\delta)(p, b+\delta)$.

1. If $a \neq b$ then we have $(p\delta + pa) - (p\delta + pb) = p(a-b)$ in the ideal. Hence

$$(p, (a-b)) = 1 \implies \exists\, x, y \in \mathbb{Z} : p \cdot (xp + y(a-b)) = p.$$

2. If $a = b$ then we need to consider the two cases $f_\delta = x^2 - d$ and $f_\delta = x^2 - x - \frac{d-1}{4}$ separately:

   a) If $\delta = \sqrt{d}$ then we have

   $$f_\delta = x^2 - d \equiv x^2 + 2ax + a^2$$

   and so either $p \,|\, a$ or $p = 2$ by comparing coefficients.

   In the first scenario we have $a \equiv 0 \pmod{p}$. Our factorization is $(p^2, p\sqrt{d},\, d)$. Also

   $$-d \equiv a^2 \implies p \,|\, d$$

and we may write $d = pk$ where $k \not\equiv 0 \pmod{p}$. From $(p,k) = 1$ it follows that

$$\exists\, x, y \in \mathbb{Z} : p \cdot (xp + yk) = p.$$

In the second scenario we have $p = 2$ and $a \not\equiv 0 \pmod{p}$. Then

$$x^2 + 2ax + a^2 \equiv (x+1)^2 \pmod{2}.$$

Our factorization is $(4,\ 2 + 2\sqrt{d},\ d + 1 + 2\sqrt{d})$. We have

$$(d + 1 + 2\sqrt{d}) - (2 + 2\sqrt{d}) = d - 1.$$

In this case $d \equiv 2, 3 \pmod{4}$, and so

$$a \not\equiv 0 \pmod{2} \implies d \not\equiv 0 \pmod{2} \implies d \equiv 3 \pmod{4}.$$

Hence

$$(d-1, 4) = 2 \implies \exists\, x, y \in \mathbb{Z} : (x(d-1) + 4y) = 2.$$

b) If $\delta = \frac{1+\sqrt{d}}{2}$ then we have

$$f_\delta = x^2 - x - \frac{d-1}{4} \equiv x^2 + 2ax + a^2.$$

Therefore by comparing coefficients

$$2a \equiv 1 \text{ and } a^2 \equiv -\frac{d-1}{4} \implies 4a^2 \equiv 1 \text{ and } 4a^2 \equiv 1 - d \implies -d \equiv 0 \pmod{p}.$$

Hence

$$p|d \implies x^2 - x - \frac{d-1}{4} \equiv x^2 - x + \frac{1}{4} \equiv (x - \frac{1}{2})^2 \equiv (x - \frac{p+1}{2})^2.$$

Since p is an odd prime our factorization here becomes $(p^2, \frac{-p^2+p\sqrt{d}}{2}, \frac{p^2+d-2p\sqrt{d}}{4})$. We now have

$$4(\frac{-p^2 + p\sqrt{d}}{2} + \frac{p^2 + d - 2p\sqrt{d}}{4}) = 4\frac{-p^2 + d}{4} = d - p^2.$$

Now p divides d but d is square-free and we may write $d = pk$ where $k \not\equiv 0 \pmod{p}$. Hence

$$(p,k) = 1 \implies \exists\, x, y \in \mathbb{Z} : p \cdot (xp + yk) = p.$$

We just showed that $(p) \supset (p, \delta + a)(p, \delta + b)$ and $(p) \subset (p, \delta + a)(p, \delta + b)$. Thus we have the unique factorization in prime ideals $(p) = (p, a + \delta)(p, b + \delta)$. □

Now we will introduce some terminology in order to distinguish the cases of prime ideals.

Definition 5.1. Given a principal ideal $(p) \subset \mathcal{O}_K$ generated by a rational prime p:

(i) We say p is *inert* in $\mathcal{O}_K$ if (p) is also a prime ideal in R.

(ii) We say p *splits* in $\mathcal{O}_K$ if (p) is the product of two distinct prime ideals.

(iii) We say p is *ramified* in $\mathcal{O}_K$ if (p) is the square of a prime ideal.

Theorem 5.3. *Let (p) be an ideal in $\mathbb{Q}(\sqrt{d})$ generated by an integral prime. Let $\mathcal{O}_K$ be the ring of integers of $\mathbb{Q}(\sqrt{d})$. Then we have the following conditions for the factorization of (p):*

1. *The prime p is inert if and only if $\left(\frac{d}{p}\right) = -1$ and $p \nmid disc(\mathbb{Q}(\sqrt{d}))$.*
2. *The prime p splits if and only if $\left(\frac{d}{p}\right) = 1$ and $p \nmid disc(\mathbb{Q}(\sqrt{d}))$.*
3. *The prime p is ramified if and only if $p \mid disc(\mathbb{Q}(\sqrt{d}))$.*

Proof. Firstly, all factors of (p) are of the form $(p, n+\alpha)$ where $n \in \mathbb{Z}$ due to Dedekind's Criterion. We are going to prove the three parts of the theorem separately.

1. To prove this case, it is sufficient to prove cases $2, 3$.
2. Suppose that (p) splits as $(p, m+\alpha)(p, n+\alpha)$ where $m \neq n$. Then

$$p \,|\, (mn + (m+n)\alpha + \alpha^2).$$

We now apply reverse map from Lemma 5.1. If $d \equiv 2, 3 \pmod 4$ we have

$$x^2 + (m+n)x + mn \equiv x^2 - d \pmod p,$$

which leads to $m + n \equiv 0 \pmod p$ and so $-d \equiv mn \equiv -m^2 \pmod p$, which implies that d is a quadratic residue modulo p as required. If $d \equiv 1 \pmod 4$ we have

$$x^2 + (m+n)x + mn \equiv x^2 - x - \frac{d-1}{4} \pmod p,$$

which leads to $m + n \equiv -1$ and $1 - d \equiv 4mn \pmod p$. Now

$$1 - d \equiv 4m(-m-1) \equiv -4m^2 - 4m \implies d \equiv (2m+1)^2$$

and so d is a quadratic residue modulo p as required.

We now prove the other direction. If d is a quadratic residue modulo p then there exists an element $k \in \mathbb{Z}$ such that $k^2 \equiv d \pmod p$. If $d \equiv 2, 3 \pmod 4$ then

$$x^2 - d \equiv (x+k)(x-k) \pmod p$$

and so (p) splits in $\mathcal{O}_K$. If $d \equiv 1 \pmod 4$ then

$$x^2 - x - \frac{d-1}{4} \equiv (x - \frac{1}{2})^2 - (\frac{k}{2})^2 \equiv (x - \frac{1+k}{2})(x - \frac{1-k}{2}) \pmod p$$

and again (p) splits in $\mathcal{O}_K$.

3. We showed in that if (p) factors as a square of the form $(p, k+\alpha)^2$, then (i) we require $p|d$ in the case $d \equiv 1 \pmod 4$, or (ii) we require $p \mid d \vee p = 2$ otherwise.

   Conversely, if $d \equiv 1 \pmod 4$ and $p \mid D_{\mathbb{Q}(\sqrt{d})}$ then $p \mid d$ and

   $$x^2 - x - \frac{d-1}{4} \equiv x^2 - x + \frac{1}{4} \equiv \big(x - \frac{p-1}{2}\big)^2 \pmod p$$

   so that (p) ramifies.

   We now prove the other direction. If $d \equiv 2, 3 \pmod 4$ and $p \mid D_{\mathbb{Q}(\sqrt{d})}$ then either $p \mid d$ or $p = 2$. In the first case $x^2 - d \equiv x^2 \pmod p$, and so (p) ramifies.

   In the second case $p = 2$, and (i) if $2|d$ then

   $$x^2 - d \equiv x^2 \pmod p$$

   which is similar to the first case, or (ii) otherwise

   $$x^2 - d \equiv x^2 + 2x + 1 \equiv (x+1)^2 \pmod p$$

   and again (p) ramifies. □

Whilst proving the previous theorems we managed to specify to a higher degree of precision how the prime ideals in a quadratic number field look like. We will now present a table which summarizes these results. This table will be referenced in future chapters where we require explicit use of prime ideals. Note that the split and ramified prime ideals are not necessarily non-principal but for simplicity we will leave them in this form.

$\overline{d} \pmod 4$	1	2	3
p is inert	(p)	(p)	(p)
p is ramified	$(p, \frac{-p+\sqrt{d}}{2})$	$(p, \sqrt{d})$	$(p, \sqrt{d})$
p splits	$(p, a + \frac{\pm 1+\sqrt{d}}{2})$	$(p, \pm a + \sqrt{d})$	$(p, \pm a + \sqrt{d})$
$p = 2$	(2)	$(2, \sqrt{d})$	$(2, 1+\sqrt{d})$

Table 2: Prime ideals in quadratic number fields

6 Computing the 2-Torsion

In this section we want to construct a map which will help us compute the degree of 2-torsion in the class-group. This will be our main result. We will focus here only on the case $d < 0$. First of all we need to go through some technical details to ensure that such a map is well-defined and that it exists. We then prove a sufficient condition for norm of an element of an ideal to be a quadratic residue modulo D_K. This will only work in the cases $d \equiv 1, 3 \pmod 4$.

Lemma 6.1. *Let $d \equiv 1, 3 \pmod 4$ and $\alpha \in \mathcal{O}_K$ such that $(N(\alpha), D_K) = 1$. Then $\left(\frac{N(\alpha)}{D_K}\right) = 1$.*

Proof. Consider the case $d \equiv 1 \pmod 4$, where $D_K = d$. Then let $\alpha = x + y\frac{1+\sqrt{d}}{2}$ for some $x, y \in \mathbb{Z}$, in which case

$$N(\alpha) = x^2 + xy + \frac{1-d}{4}y^2 = (x + \frac{y}{2})^2 - \frac{dy^2}{4}.$$

Since $d \equiv 1 \pmod 2$, then 2 must be a unit in $\mathbb{Z}/d\mathbb{Z}$. Hence

$$(x + \frac{y}{2})^2 - d(\frac{y}{2})^2 \equiv (x + \frac{y}{2})^2 \pmod d$$

as $\frac{y}{2} \in \mathbb{Z}/d\mathbb{Z}$. Therefore $N(\alpha)$ is a quadratic residue modulo $d = D_K$.

Consider now the case $d \equiv 3 \pmod 4$, where $D_K = 4d$. Then let $\alpha = x + y\sqrt{d}$ for some $x, y \in \mathbb{Z}$, in which case

$$N(\alpha) = x^2 - dy^2.$$

Since $x^2 - dy^2 \equiv x^2 \pmod d$, then $N(\alpha)$ clearly is a quadratic residue modulo d. Let us now have a look at the congruence of (x^2, y^2) modulo 4. We have the following possible cases:

1. $(0, 0) \implies N(\alpha) \equiv 0 - 3 \cdot 0 \equiv 0 \pmod 4 \implies 4|(N(\alpha), D_K)$, which is a contradiction;
2. $(1, 1) \implies N(\alpha) \equiv 1 - 3 \cdot 1 \equiv 2 \pmod 4 \implies 2|(N(\alpha), D_K)$, which is a contradiction;
3. $(0, 1) \implies N(\alpha) \equiv 0 - 3 \cdot 1 \equiv 1 \pmod 4$;
4. $(1, 0) \implies N(\alpha) \equiv 1 - 3 \cdot 0 \equiv 1 \pmod 4$.

Hence $N(\alpha) \equiv 1 \pmod 4$. So it is a quadratic residue modulo 4. Since $(4, d) = 1$, then $N(\alpha)$ is also a quadratic residue modulo $4d = D_K$. □

We will from now on just consider the number fields $K = \mathbb{Q}(\sqrt{d})$ with $d \equiv 1, 3 \pmod 4$. We want to show that every ideal $I \subseteq \mathcal{O}_K$ contains an element i for which the quotient $\frac{N(i)}{NI}$ is coprime to D_K. We will also identify examples and provide a useful and handy table of such elements. All this work is required for the well-definability of the map we want to construct.

Lemma 6.2. *Let $d \equiv 1, 3 \pmod 4$ and $K = \mathbb{Q}(\sqrt{d})$. Then for any ideal $I \subset \mathcal{O}_K$ there exists an element $i \in I$ such that $(\frac{N(i)}{N(I)}, D_K) = 1$.*

Proof. Let us first prove this for primes. We will then extend to any other ideal. We will make use of our table of prime ideals from the previous section.

Suppose $d \equiv 1 \pmod 4$. We have $D_K = d$.

1. Consider any inert prime ideal $\mathfrak{p} = (p)$. Now choose $i = p \in \mathfrak{p}$ so that $\frac{N(i)}{N(\mathfrak{p})} = 1$. Clearly $(1, d) = 1$.

2. Consider any ramified prime ideal $\mathfrak{p} = (p, \frac{-p+\sqrt{d}}{2})$. Now choose $i = -p + \sqrt{d} \in \mathfrak{p}$ so that $N(i) = p^2 - d$. Every prime dividing d divides either p or $\frac{d}{p}$, but can't divide both, because d is square-free. Hence $(\frac{N(i)}{N(\mathfrak{p})}, d) = (p - \frac{d}{p}, d) = 1$.

3. Consider any split prime ideal $\mathfrak{p} = (p, a + \frac{\pm 1+\sqrt{d}}{2})$. Now choose $i = p \in \mathfrak{p}$. Then $\frac{N(i)}{N(\mathfrak{p})} = p$ and also $p \nmid D_K$. Hence $(p, d) = 1$.

4. In this case the ideal (2) is inert. We pick $i = 2 \in (2)$ so that $\frac{N(i)}{N((2))} = 1$. Clearly $(1, d) = 1$.

Suppose now $d \equiv 3 \pmod 4$. We have $D_K = 4d$.

1. Consider any inert prime ideal $\mathfrak{p} = (p)$. Now choose $i = p \in \mathfrak{p}$ so that $\frac{N(i)}{N(\mathfrak{p})} = 1$. Clearly $(1, 4d) = 1$.

2. Consider any ramified prime ideal $\mathfrak{p} = (p, \sqrt{d})$. Now choose $i = 2p + \sqrt{d} \in \mathfrak{p}$ so that $N(i) = 4p^2 - d$. Every prime dividing d divides either $4p$ or $\frac{d}{p}$, but can't divide both. In this case p is odd and so $2 \nmid 4p - \frac{d}{p}$. Hence $(\frac{N(i)}{N(\mathfrak{p})}, d) = (4p - \frac{d}{p}, 4d) = 1$.

3. Consider any split prime ideal $\mathfrak{p} = (p, \pm a + \sqrt{d})$. Now choose $i = p \in \mathfrak{p}$. Then $\frac{N(i)}{N(\mathfrak{p})} = p$ and also $p \nmid D_K$. Hence $(p, 4d) = 1$.

4. In this case the ideal (2) ramifies as $\mathfrak{p}^2 = (2, 1 + \sqrt{d})^2$. We pick $i = 1 + \sqrt{d} \in \mathfrak{p}$ so that $N(i) = 1 - d \equiv 2 \pmod 4$. Then $\frac{N(i)}{N(\mathfrak{p})} = \frac{1-d}{2}$ and also every prime dividing d cannot divide $\frac{1-d}{2}$ because $\frac{1-d}{2}$ is odd. Hence $(\frac{1-d}{2}, 4d) = 1$.

We have proven the statement for all prime ideals. Now we show that this property is multiplicative. Let $I, J \subset \mathcal{O}_K$ be two ideals with $i \in I$ and $j \in J$ such that

$$(\frac{N(i)}{N(I)}, D_K) = 1 \text{ and } (\frac{N(j)}{N(J)}, D_K) = 1.$$

Then the ideal IJ contains ij so that $\frac{N(ij)}{N(IJ)} = \frac{N(i)}{N(I)} \cdot \frac{N(j)}{N(J)}$ which satisfies

$$(\frac{N(i)}{N(I)} \cdot \frac{N(j)}{N(J)}, D_K) = 1.$$

Hence this property follows for all ideals in $\mathcal{O}_K$. □

Now we can define the map itself and show that it is well-defined.

Lemma 6.3. *Let $K = \mathbb{Q}(\sqrt{d})$ with $d \equiv 1, 3 \pmod 4$. Then there exists a well-defined group homomorphism $g : cl(\mathcal{O}_K) \mapsto (\mathbb{Z}/D_K\mathbb{Z})^\times/((\mathbb{Z}/D_K\mathbb{Z})^\times)^2$ such that the class $\overline{I}$ is mapped to $\frac{N(i)}{N(I)}$ for some element i in some ideal $I \in \overline{I}$ satisfying the property $(\frac{N(i)}{N(I)}, D_K) = 1$.*

Proof. We need to prove that g is well-defined. First of all we show that the choice of element in an ideal does not affect the image of a class. Let I be an ideal and $a, b \in I$ be two possible candidates satisfying the condition $(\frac{N(i)}{N(I)}, D_K) = 1$. Then $\bar{I}$ turns out to be mapped both to $\frac{N(a)}{N(I)}$ and $\frac{N(b)}{N(I)}$. These are the same in $(\mathbb{Z}/D_K\mathbb{Z})^\times/((\mathbb{Z}/D_K\mathbb{Z})^\times)^2$ if and only if

$$\frac{N(a)}{N(I)} \Big/ \frac{N(b)}{N(I)} = \frac{N(a)}{N(b)} \in ((\mathbb{Z}/D_K\mathbb{Z})^\times)^2.$$

Now both $N(a)$ and $N(b)$ are quadratic residues modulo D_K and then are mapped to $((\mathbb{Z}/D_K\mathbb{Z})^\times)^2$. But $((\mathbb{Z}/D_K\mathbb{Z})^\times)^2$ is an abelian group and therefore $\frac{N(a)}{N(b)}$ is also a quadratic residue modulo D_K and it is congruent to 1 in $(\mathbb{Z}/D_K\mathbb{Z})^\times/((\mathbb{Z}/D_K\mathbb{Z})^\times)^2$.

We now need to show that the choice of ideal does not affect the image of a class. Let $\mathfrak{a}, \mathfrak{b} \in \bar{I}$ be two ideals in the same class with $m \in \mathfrak{a}$ and $n \in \mathfrak{b}$ as elements satisfying the required condition as above. There exist elements $x, y \in \mathcal{O}_K$ such that $(x)\mathfrak{a} = (y)\mathfrak{b}$. Then $\bar{I}$ turns out to be mapped both to $\frac{N(m)}{N(\mathfrak{a})}$ and $\frac{N(n)}{N(\mathfrak{b})}$. These are the same in $(\mathbb{Z}/D_K\mathbb{Z})^\times/((\mathbb{Z}/D_K\mathbb{Z})^\times)^2$ if and only if their quotient lies in $((\mathbb{Z}/D_K\mathbb{Z})^\times)^2$. We have

$$\frac{N(m)}{N(\mathfrak{a})} = \frac{N(xm)}{N((x)\mathfrak{a})} = \frac{N(xm)}{N((y)\mathfrak{b})}$$

and so

$$\frac{N(m)}{N(\mathfrak{a})} \Big/ \frac{N(n)}{N(\mathfrak{b})} = \frac{N(xm)}{N((y)\mathfrak{b})} \Big/ \frac{N(n)}{N(\mathfrak{b})} = \frac{N(xm)}{N(yn)}.$$

But xm and yn are just elements of $\mathcal{O}_K$ and therefore their norms are quadratic residues modulo D_K. We reach the same conclusion as above.

We finally have to show that g is a group homomorphism. It is sufficient to show that

$$g(\bar{I}\bar{J}) = g(\bar{I})g(\bar{J})$$

because the other conditions have been met. Assume we have $a \in I\ in \bar{I}$ and $b \in J\ in \bar{J}$ being chosen such that $(\frac{N(a)}{N(I)}, D_K) = 1$ and $(\frac{N(b)}{N(J)}, D_K) = 1$. Clearly $g(\bar{I}\bar{J}) = \frac{N(ab)}{N(IJ)}$ by the definition of multiplication for $ab \in IJ$ such that $(\frac{N(ab)}{N(IJ)}, D_K) = 1$ as explained before. However

$$\frac{N(ab)}{N(IJ)} = \frac{N(a)}{N(I)} \cdot \frac{N(b)}{N(J)} = g(\bar{I})g(\bar{J})$$

and so g is indeed a well-defined group homomorphism. □

So what are we going to do with this well-defined map? The class-group is a mysterious object so far, and so any map that could potentially unravel its mysteries should be studied. In particular, we will learn that he kernel of g is $cl(\mathcal{O}_\mathcal{K})^2$. This will tell us a lot about the 2-torsion in the class-group once we understand the image of the map, which is what we are going to do now.

6.1 Finding the Image

Proposition 6.4. *Let $K = \mathbb{Q}(\sqrt{d})$ with $d \equiv 1, 3 \pmod 4$. Then $(\mathbb{Z}/D_K\mathbb{Z})^\times/((\mathbb{Z}/D_K\mathbb{Z})^\times)^2 \cong \prod_{p_i^{e_i}|D_K}(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times/((\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times)^2 \cong (\mathbb{Z}/2\mathbb{Z})^{\omega(D_K)}$ where e_i is maximum power of p_i dividing D_K and $\omega(D_K)$ is the number of distinct prime factors of D_K.*

Proof. In order to show that

$$\prod_{p_i^{e_i}|D_K}(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times/((\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times)^2 \cong (\mathbb{Z}/2\mathbb{Z})^{\omega(D_K)}$$

it is sufficient prove

$$(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times/((\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times)^2 \cong (\mathbb{Z}/2\mathbb{Z})$$

for any prime p_i dividing D_K.

In D_K the exponents e_i always equal 1. The one exception in the case $d \equiv 3 \pmod 4$ is the exponent of 2 which is 2. In that particular case we have

$$(\mathbb{Z}/4\mathbb{Z})^\times/((\mathbb{Z}/4\mathbb{Z})^\times)^2 \cong (1,3)/(1) \cong (1,3) \cong \mathbb{Z}/2\mathbb{Z}$$

and we are still good.

Now we can assume $e_i = 1$. The quadratic residues $((\mathbb{Z}/p_i\mathbb{Z})^\times)^2$ form an Abelian group and we can consider the multiplication table for quadratic residues and quadratic non-residues:

$\times$	QR	QNR
QR	QR	QNR
QNR	QNR	QR

We can see that these classes form a structure which is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ with the quadratic residues being mapped to 0 and the quadratic non-residues being mapped to 1. Note that $((\mathbb{Z}/p_i\mathbb{Z})^\times)^2$ is the kernel of this map and by the First Isomorphism Theorem we have

$$(\mathbb{Z}/p_i\mathbb{Z})^\times/((\mathbb{Z}/p_i\mathbb{Z})^\times)^2 \cong (\mathbb{Z}/2\mathbb{Z}).$$

We will require an additional map μ to represent this isomorphism, which we define by:

$$\mu(\left(\frac{a}{p_i}\right)) = \begin{cases} 0 & \text{if } \left(\frac{a}{p_i}\right) = 1 \\ 1 & \text{if } \left(\frac{a}{p_i}\right) = -1. \end{cases}$$

We will extend μ so that $(\mathbb{Z}/4\mathbb{Z})^\times/((\mathbb{Z}/4\mathbb{Z})^\times)^2$ is also included as a potential domain. Here the image is defined in the same way as above. Now we have an isomorphism

$$\mathbb{Z}/D_K\mathbb{Z} \cong \prod_{p_i^{e_i}|D_K} \mathbb{Z}/p_i^{e_i}\mathbb{Z}$$

which sends $a \in \mathbb{Z}/D_K\mathbb{Z}$ to $(a \pmod{p_1^{e_1}}, ..., a \pmod{p_{\omega(D_K)}^{e_{\omega(D_K)}}})$. Since a is a unit in $\mathbb{Z}/D_K\mathbb{Z}$ if and only if it is a unit in each of $\mathbb{Z}/p_i^{e_i}\mathbb{Z}$, this is still an isomorphism when we restrict the groups to units. Hence $(\mathbb{Z}/D_K\mathbb{Z})^\times \cong \prod_{p_i^{e_i}|D_K}(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times$.

On the other hand, a is a quadratic residue modulo D_K if and only if it is a quadratic residue modulo each of the $p_i^{e_i}$ dividing D_K. Hence can restrict both the image and the domain further, quotienting by the quadratic residues. Therefore we have an isomorphism

$$\phi : \mathbb{Z}/D_K\mathbb{Z})^\times/((\mathbb{Z}/D_K\mathbb{Z})^\times)^2 \mapsto \prod_{p_i^{e_i}|D_K} (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times/((\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times)^2$$

which sends $a \in \mathbb{Z}/D_K\mathbb{Z})^\times/((\mathbb{Z}/D_K\mathbb{Z})^\times)^2$ to $((\frac{a}{p_1^{e_1}}), ..., (\frac{a}{p_{\omega(D_K)}^{e_{\omega(D_K)}}}))$. □

Over the next three results we will demonstrate that the image of the map g is in fact isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{\omega(D_K)-1}$.

Lemma 6.5. *We have $\mu(\phi(im(g))) \subset S$ where $S := \{a \in (\mathbb{Z}/2\mathbb{Z})^{\omega(D_K)} | \sum_{e\in a} e \equiv 0 \pmod 2\}$.*

Proof. We can think of S as the coordinates in $(\mathbb{Z}/2\mathbb{Z})^{\omega(D_K)}$ such that the sum of the individual components of each coordinate is even. How does the pre-image of S under μ look like? It consists of all sets of coordinates in $\{-1, 1\}^{\omega(D_K)}$ such that there are an even number of instances of -1. In other words we claim that every element a in the image of g is a QNR over an even number of primes p_i (and 4 in the case $d \equiv 3 \pmod 4$). This occurs if and only if $\prod_{p_i^{e_i}|D_K} (\frac{a}{p_i^{e_i}}) = 1$. Keep this condition in mind as we will prove it for every such element a which originated from a prime ideal under g. This is sufficient given that g is a group homomorphism and the prime ideal classes generate the ideal class-group.

Recall the isomorphism

$$\phi : (\mathbb{Z}/D_K\mathbb{Z})^\times/((\mathbb{Z}/D_K\mathbb{Z})^\times)^2 \mapsto \prod_{p_i^{e_i}|D_K} (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times/((\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times)^2$$

which has been previously explained. It is the composition of homomorphisms

$$\phi_i : (\mathbb{Z}/D_K\mathbb{Z})^\times/((\mathbb{Z}/D_K\mathbb{Z})^\times)^2 \mapsto (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times/((\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times)^2$$

which send a to $(\frac{a}{p_i^{e_i}})$.

Remember how we found the image of every prime ideal under g in Lemma 6.2? Now we will see how these elements map under these components of ϕ. We denote by q_i the integral prime from which the prime ideal originates from. The following table summarizes the images under ϕ_j for a corresponding prime p_j dividing d, ϕ_4 corresponding to 4 in the case $4 \,|\, D_K$ and ϕ_i in the ramified case where $q_i = p_i$.

$\overline{d}$	prime type	image under g	image under ϕ_j	image under ϕ_i	image under ϕ_4
1	$\left(\frac{d}{q_i}\right) = -1$	1	1	N/A	N/A
1	$\left(\frac{d}{q_i}\right) = 0$	$q_i - d/q_i$	$\left(\frac{q_i}{p_j}\right)$	$\left(\frac{d/q_i}{q_i}\right)$	N/A
1	$\left(\frac{d}{q_i}\right) = 1$	q_i	$\left(\frac{q_i}{p_j}\right)$	N/A	N/A
1	$p = 2$	1	1	N/A	N/A
3	$\left(\frac{d}{q_i}\right) = -1$	1	1	N/A	$\left(\frac{q_i}{4}\right)$
3	$\left(\frac{d}{q_i}\right) = 0$	$4q_i - d/q_i$	$\left(\frac{q_i}{p_j}\right)$	$\left(\frac{d/q_i}{q_i}\right)$	$\left(\frac{d/q_i}{4}\right)$
3	$\left(\frac{d}{q_i}\right) = 1$	q_i	$\left(\frac{q_i}{p_j}\right)$	N/A	$\left(\frac{q_i}{4}\right)$
3	$p = 2$	$\frac{1-d}{2}$	$\left(\frac{2}{p_j}\right)$	N/A	$\left(\frac{2}{d}\right)$

Table 3: Image of prime ideals under g and ϕ

We have to show that every element represented by a prime ideal in $cl(\mathcal{O}_K)$ is mapped to S under $g \circ \phi \circ \mu$. If you remembered, this is equivalent to showing that the image under g is a QNR over an even number of primes (or 4 in the case $d \equiv 3 \pmod 4$).

Firstly we consider the case $d \equiv 1 \pmod 4$. Let $D_K = \prod_j^n p_j$ for primes p_j. We require $\prod_j^n \left(\frac{q_i}{p_j}\right) = 1$ for primes p_j. We enumerate through the rows of the table.

1. 1 is mapped to S because it is a QR over each of the primes p_j.
2. In this case the image under ϕ is in S if

   $$\prod_j^n \left(\frac{q_i}{p_j}\right) = \left(\frac{d/q_i}{q_i}\right) \prod_{j,j\neq i}^n \left(\frac{q_i}{p_j}\right) = \prod_{j,j\neq i}^n \left(\frac{q_i}{p_j}\right)\left(\frac{p_j}{q_i}\right) = 1$$

   because $\frac{d}{q_i}$ consists of the product of all primes dividing d not equal to q_i. This is equivalent to showing that

   $$\prod_{j,j\neq i}^n (-1)^{(\frac{p_j-1}{2})(\frac{q_i-1}{2})} = 1.$$

   We have $d \equiv 1 \pmod 4$ and so there must be an even number of primes $p_j \equiv 3 \pmod 4$.

   If $q_i \equiv 1 \pmod 4$ then $(-1)^{(\frac{p_j-1}{2})(\frac{q_i-1}{2})} = 1$ for all p_j.

   If $q_i \equiv 3 \pmod 4$ then an even number of $(-1)^{(\frac{p_j-1}{2})(\frac{q_i-1}{2})}$ are -1 so that the product is 1.
3. In this case $\left(\frac{d}{q_i}\right) = \prod_j^n \left(\frac{q_i}{p_j}\right) = 1$.
4. 1 is mapped to S because it is a QR over each of the primes p_j.

Secondly we consider the case $d \equiv 3 \pmod 4$. Let $D_K = 4\prod_j^n p_j$ for primes p_j. We require $\left(\frac{q_i}{4}\right)\prod_j^n \left(\frac{q_i}{p_j}\right) = 1$ for primes p_j. We enumerate through the rows of the table.

1. 1 is mapped to S because it is a QR over each of the primes p_j as well as over 4.

2. In this case the image under ϕ is in S if

$$\left(\frac{q_i}{4}\right)\prod_j^n \left(\frac{q_i}{p_j}\right) = \left(\frac{q_i}{4}\right)\left(\frac{d/q_i}{q_i}\right)\prod_{j,j\neq i}^n \left(\frac{q_i}{p_j}\right) = \left(\frac{q_i}{4}\right)\prod_{j,j\neq i}^n \left(\frac{q_i}{p_j}\right)\left(\frac{p_j}{q_i}\right) = 1$$

   by similar reasoning as above. This is equivalent to showing that

$$\left(\frac{q_i}{4}\right)\prod_{j,j\neq i}^n (-1)^{(\frac{p_j-1}{2})(\frac{q_i-1}{2})} = 1.$$

   We have $d \equiv 3 \pmod 4$ and so there must be an odd number of primes $p_j \equiv 3 \pmod 4$.

   If $q_i \equiv 1 \pmod 4$ then $(-1)^{(\frac{p_j-1}{2})(\frac{q_i-1}{2})} = 1$ for all p_j and $\left(\frac{q_i}{4}\right) = 1$.

   If $q_i \equiv 3 \pmod 4$ then an odd number of $(-1)^{(\frac{p_j-1}{2})(\frac{q_i-1}{2})}$ are -1 so that the product is -1. However this is multiplied by $\left(\frac{q_i}{4}\right) = -1$ and so the whole product is 1.

3. In this case the image is in S if

$$\left(\frac{q_i}{4}\right)\prod_j^n \left(\frac{q_i}{p_j}\right) = 1.$$

   In the case $q_i \equiv 1 \pmod 4$ we have $\left(\frac{d}{q_i}\right) = \prod_j^n \left(\frac{q_i}{p_j}\right) = 1$. Additionally, $\left(\frac{q_i}{4}\right) = 1$ and so the whole product is 1. In the case $d \equiv 3 \pmod 4$ we have $-\left(\frac{d}{q_i}\right) = \prod_j^n \left(\frac{q_i}{p_j}\right) = -1$ and $\left(\frac{q_i}{4}\right) = -1$ and so the whole product is 1.

4. In this case the image of the ideal class of 2 is in S if

$$\left(\frac{2}{d}\right)\prod_j^n \left(\frac{2}{p_j}\right) = \prod_j^n (\left(\frac{2}{p_j}\right))^2 = 1.$$

   That is true as it is a product of squares which must equal 1.

We have shown that all prime ideals chosen are mapped to the set S. Since this mapping is a group homomorphism, and the prime ideals generate the class-group, it must be true that the images of all ideals lie in S. Hence $\mu(\phi(im(g))) \subset S$. □

Now we prove the other direction, that for every element in S there exists an element in the class-group that maps to it under $g \circ \phi \circ \mu$. We are assuming a pretty powerful theorem, the proof is not at all slick. However it is the most efficient approach given that we have classified the images of all prime ideals.

Lemma 6.6. *We have $im(g) \cong S$ via the isomorphism $\phi \circ \mu$.*

Proof. By applying Theorem 8.7 for each congruence $p \equiv a \pmod{b}$ there is a prime p satisfying it as long as $(a, b) = 1$. Then for each $s \in \mu^{-1}(S)$ there is an element $a \in (\mathbb{Z}/D_K\mathbb{Z})^\times$ that is mapped to s under ϕ. Hence we can construct primes p that map to each element $s \in S$ under $\phi \circ \mu$.

Now we need to calculate $\left(\frac{D_K}{p}\right)$ for such primes in order to make sure that there is a prime ideal $\mathfrak{p}$ that maps to p under g.

Let $D_K = \prod_i^n p_i$ as before for primes p_i. Then $\left(\frac{D_K}{p}\right) = \prod_i^n \left(\frac{p}{p_i}\right)$. Since we picked p so that an even number of $\left(\frac{p}{p_i}\right)$ produce -1 we have $\left(\frac{D_K}{p}\right) = 1$ and so p splits in $\mathcal{O}_K$ and its split ideals can map to p under g.

Therefore every element in S has an element in $cl(\mathcal{O}_K)$ that maps to it. □

The final missing piece for constructing the image of g is to show that the group S is isomorphic to a much more easily defined group.

Lemma 6.7. *Let S be the set defined earlier. Then S is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{\omega(D_K)-1}$.*

Proof. S is clearly a group because it is an image of a group $cl(\mathcal{O}_K)$ under group homomorphisms $g \circ \phi \circ \mu$. Define $\lambda : S \mapsto (\mathbb{Z}/2\mathbb{Z})^{\omega(D_K)-1}$ by truncating the last digit of an element $a \in S$. This is clearly a homomorphism because the individual binary digits of a do not interact and so any truncation of the digits will still form a group. Additionally the first $\omega(D_K)-1$ digits can be chosen arbitrarily so that the last digit acts as a deterministic check digit to make sure the number of 1's is even. This ensures both surjectivity and injectivity and so λ is an isomorphism. □

6.2 Finding the Kernel

Lemma 6.8. *Let J be an ideal such that $N(J)$ is a QR modulo D_K, d is a QR modulo $N(J)$ and $(N(J), D_K) = 1$. Then there exists an element $a \in \mathcal{O}_K$ such that $N((a)J)$ is a perfect square.*

Proof. We separate the cases into $d \equiv 1 \pmod 4$ and $d \equiv 3 \pmod 4$ because of the different definition of norm.

Consider $d \equiv 3 \pmod 4$. The norm of an arbitrary element in $\mathcal{O}_K$ is of the form $x^2 - dy^2$ for integers x, y. Hence we are looking for a solution in integers (x, y, z) to

$$N(J)(x^2 - dy^2) = z\dot{}2$$

Clearly $N(J)|z^2$, and by clearing squared factors from both we reduce the equation to $x^2 - dy^2 = cz^2$, where c is the square-free part of $N(J)$. Note that c is a quadratic residue modulo d due to the reduction of squares. Similarly d is a QR modulo c and $(c, D_F) = 1$.

By using Theorem 8.8 there exists such a solution in integers (x, y, z).

Consider $d \equiv 1 \pmod 4$. The norm of an arbitrary element is of the form $x^2 + xy + \frac{1-d}{4}y^2$ for integers x, y. Hence we are looking for a solution in integers (x, y, z) to

$$N(J)(x^2 + xy + \frac{1-d}{4}y^2) = z^2.$$

This is equivalent to $N(J)(4x^2 + 4xy + (1-d)y^2) = 4z^2$, which factorizes as

$$N(J)((2x+y)^2 - dy^2) = (2z)^2,$$

and by canceling squares from $N(J)$ we get $c((2x+y)^2 - dy^2) = (2z)^2$ where $c|z$. This is also equivalent to $(2x+y)^2 = 4cz^2 + dy^2$. The integers $4c, d$ satisfy the same conditions as in the previous case.

By using Theorem 8.8 there exists such a solution in integers $(2x+y, z, y)$.

We just need to show that x is an integer in this case. If y is odd then we have

$$4cz^2 + dy^2 \equiv 1 \equiv (2x+y)^2 \pmod 4$$

and so $2x + y$ is odd. This implies $2x$ is even and we are done. If y is even then we have

$$4cz^2 + dy^2 \equiv 0 \equiv (2x+y)^2 \pmod 4$$

and so $2x + y$ is even. This implies $2x$ is even and we are done. □

Lemma 6.9. *Recall the definition of the map g from previous results. Then* $\ker(g) = (cl(K))^2$. *In other words if $\frac{N(i)}{N(I)} \in \left(\mathbb{Z}/D_K)^\times\right)^2$ then $I \in (cl(K))^2$.*

Proof. Let $I \subseteq \mathcal{O}_K$ be an ideal and $i \in I$ in such a way that $\frac{N(i)}{N(I)} \in \left(\mathbb{Z}/D_K)^\times\right)^2$. Define $J = (i)I^{-1}$ such that

$$N(J) = \frac{N(i)}{N(I)} \in \left(\mathbb{Z}/D_K)^\times\right)^2.$$

Note that $J = I^{-1}$ in the class-group. Clearly $I \in (cl(K))^2$ if and only if $J \in (cl(K))^2$. We only need to show $J \in (cl(K))^2$.

Suppose $J = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_\mathfrak{n}$ for some prime ideals $\mathfrak{p}_i$. Then

$$(N(J)) = \mathfrak{p}_1\bar{\mathfrak{p}_1} \cdot \mathfrak{p}_2\bar{\mathfrak{p}_2} \cdot \dots \cdot \mathfrak{p}_n\bar{\mathfrak{p}_n} = (N(\mathfrak{p}_1))(N(\mathfrak{p}_2))\dots(N(\mathfrak{p}_n)) = (p_1)(p_2)\dots(p_n)$$

for some rational primes p_i.

Since every principal ideal is a square in the class-group, we can assume J doesn't contain any principal ideals in its factorization.

Suppose $\mathfrak{p}_\mathfrak{i} = \bar{\mathfrak{p}_\mathfrak{i}}$ for some $1 \leq i \leq n$. Then $p = \mathfrak{p}_\mathfrak{i}\bar{\mathfrak{p}_\mathfrak{i}}$ would be a ramified prime and then $p \mid D_K$. But $p|N(J)$ and then $(N(J), D_K) \neq 1$. Which contradicts

$$N(J) = \frac{N(i)}{N(I)} \in \left(\mathbb{Z}/D_K)^\times\right)^2.$$

Hence all the principal ideals (p_i) in the factorization above split. In other words $\left(\frac{p_i}{D_K}\right) = 1$ for each $1 \leq i \leq n$. Then $N(J)$ is a quadratic residue modulo D_K.

By applying Quadratic reciprocity we get $\left(\frac{D_K}{p_i}\right) = \left(\frac{d}{p_1}\right) = 1$ for each $1 \leq i \leq n$. Then d is also a quadratic residue modulo $N(J)$.

By applying Lemma 6.8 then there exist an element $a \in \mathcal{O}_K$ such that $N\big((a)J\big)$ is a perfect square.

Put $J' = (a)J$. Now we have

$$N(J') = J'\bar{J}' = (k)^2$$

for some $k \in \mathbb{Z}$. But J' and $\bar{J}'$ are coprime. Hence also J' is a square. Since

$$J' \sim J \sim I$$

in the class-group we finally get $I \in (cl(K))^2$. □

We have been able to understand both the kernel of the map g and its image. Then the result we found can be summed up by the formula

$$cl(\mathcal{O}_K)/cl(\mathcal{O}_K)^2 \cong (\mathbb{Z}/2\mathbb{Z})^{\omega(D_K)-1}.$$

In other words the degree of 2-torsion in the class-group is

$$|cl(\mathcal{O}_K)[2]| = |\{I \in cl(K) : I^2 = (1)\}| = \omega(D_K) - 1.$$

7 Conclusion

The failure of the uniqueness of factorization into irreducibles in some rings prompted us to study the ideals and ideal class-group. At first we developed some algebraic background - we explored the rings of algebraic integers and proved some of their properties. We managed to discover various results concerning ideals, such as the fact that norm of ideals is multiplicative.

At this point we were ready to try to understand the class-group. To compute it, we used Minkowski‘s theorem and some deep facts about ideals. But it turned out, that to perform these computations more efficiently we can use the isomorphism $\mathbb{Z}[x]/f_\alpha \cong \mathbb{Z}[\alpha]$ to get a powerful tool to factorize ideals, namely Dedekind‘s Criterion. We summarized our results by discovering the way the prime ideals factor. An unexpected fact was the substancial role of quadratic residues in this issue. Having done all of this, we thoroughly studied the structure of class-groups what allowed us to state a few conjectures.

At last, we got down to the main problem of our project - computing the degree of 2-torsion in the ideal class-group for imaginary quadratic fields. We constructed a well-defined group homomorphism $g : cl(\mathcal{O}_K) \mapsto (\mathbb{Z}/D_K\mathbb{Z})^\times/((\mathbb{Z}/D_K\mathbb{Z})^\times)^2$ such that the class $\overline{I}$ is mapped to $\frac{N(i)}{N(I)}$ for some element i in some ideal $I \in \overline{I}$ satisfying the property $(\frac{N(i)}{N(I)}, D_K) = 1$. Using quadratic reciprocity we found the image of prime ideals under this map. Then we explored the kernel of g, which with the previous result about the image implied the following property of the degree of 2-torsion:

$$|cl(\mathcal{O}_K)[2]| = |\{I \in cl(K) : I^2 = (1)\}| = \omega(D_K) - 1$$

It turns out that these results can also be extended to real quadratic fields, by introducing the notion of *narrow class-group.*

One can also try to focus on different kind of fields, such as $F(\sqrt{(-\alpha\pi)})$ where α, π are totally positive and π is a prime number, or also $F(\sqrt[3]{(\alpha)})$ and $F(\sqrt[3]{(\alpha\pi)})$... Unfortunately problems in this area range from speculative to almost completely open though.

8 Algebraic Supplement

In this section we mention, without proof, some theorems and statements that were assumed in this project.

Proposition 8.1. *Let K be a quadratic field, and let $\mathfrak{I} \subset \mathcal{O}_K$ be a non-zero ideal. Let $\overline{\mathfrak{I}}$ be the conjugate ideal of $\mathfrak{I}$. Here the generators of $\overline{\mathfrak{I}}$ are the conjugates of the generators of $\mathfrak{I}$. Then we have $\overline{\mathfrak{I}}\mathfrak{I} = (N(\mathfrak{I})) = N((\overline{\mathfrak{I}}))$.*

Proposition 8.2. *Let $\alpha \in \mathcal{O}_K$. Then each polynomial $g \in \mathbb{Q}[x]$ such that $g(\alpha) = 0$ is divisible by the minimal polynomial of α.*

Lemma 8.3 (Gauss). *Let $\alpha \in K$. Then $\alpha \in \mathcal{O}_K$ if and only if the minimal polynomial $f_\alpha \in \mathbb{Q}[x]$ of α is also monic polynomial in $\mathbb{Z}[x]$.*

Theorem 8.4 (First Isomorphism Theorem). *Let R, S be rings and $\phi : R \mapsto S$ be a ring homomorphism. Then $R/ker(\phi) \cong S$.*

Theorem 8.5 (Third Isomorphism Theorem). *Let G be an abelian group with subgroups H, I such that $I \subset H \subset G$. Then $\frac{G/I}{H/I} \cong G/H$.*

Proposition 8.6. *Let (i) be a principal ideal in a Dedekind domain R. Then $N((i)) = |R/(i)| = N(i)$.*

Theorem 8.7 (Dirichlet's Theorem on Arithmetic Progressions). *There are infinitely many primes p satisfying the congruence $p \equiv a \pmod{b}$ as long as $(a, b) = 1$ and a, b are positive integers.*

Theorem 8.8 (Legendre). *The equation $x^2 = by^2 + cz^2$ has a solution in integers (x, y, z) if b and c are quadratic residues modulo each other and $(b, c) = 1$.*

We also provide some useful definitions in the case the reader is not familiar with the following concepts.

Definition 8.1. Let $a \in \mathbb{Z}$ and P be an odd rational prime. We define the *Jacobi symbol* as:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a QR modulo } p, \\ -1 & \text{if } a \text{ is a QNR modulo } p. \end{cases}$$

Remark. If a, b, m are integers then we have

$$\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right) \text{ and } \left(\frac{m}{ab}\right) = \left(\frac{m}{a}\right)\left(\frac{m}{b}\right).$$

Remark. If a, b, m are integers such that $a \equiv b \pmod{m}$ then we have

$$\left(\frac{a}{m}\right) = \left(\frac{b}{m}\right).$$