The Ideal Class Group

Andrei Lapets
lapets@fas.harvard.edu

January 09, 2006

Abstract

We present a concise and self-contained definition of the ideal class group, which is useful for proving facts about zero sets of Diophantine equations, and discuss a few relevant key facts. We approach this by first assembling some preliminary definitions regarding algebraic integers, and subsequently delving into several useful results about lattices, including Minkowski's lemma. Then, returning to our goal, we construct the ideal class group for the ring of integers in an imaginary quadratic field. Finally, applying the facts we have accumulated, we prove that the group is always finite and analyze a few examples.

1 Background and Definitions

Below, we assemble some definitions which will help us achieve our two initial goals of describing the prime factorization of ideals and constructing the ideal class group, and inform our examples further below. The notion of an imaginary quadratic number field underlies the structure of the ideal class group.

1.1 Imaginary Quadratic Number Fields

Definition 1. We define a field F as being an *imaginary quadratic number field* if $F = \mathbb{Q}[\sqrt{d}]$, where $\mathbb{Q}[\sqrt{d}]$ is the field consisting of all complex numbers of the form $a + b\sqrt{d}$ such that $a, b \in \mathbb{Q}$ and the constant $d \in \mathbb{Z}$ satisfies $d < 0$.

In general, only square-free values of d are of interest; otherwise, we can easily factor the square out of d and include the square's root in b.

1.2 The Ring of Integers in $\mathbb{Q}[\sqrt{d}]$

Definition 2. We call an element $\delta \in \mathbb{C}$ an *algebraic integer* if it is in the zero set of a monic polynomial $f(x) \in \mathbb{Z}[x]$.

The above condition is satisfied if any only if the coefficients of the monic irreducible polynomial $f(x)$ over $\mathbb{Q}$ are integers [Artin 11.6.7], and so, because we are concerned only with the field $\mathbb{Q}[\sqrt{d}]$ with $d < 0$, we need only those integers δ which are in the zero set of a monic *quadratic* polynomial $f(x) \in \mathbb{Z}[x]$. Note that such a condition indeed accounts for all algebraic integers in $\mathbb{Q}[\sqrt{d}]$. We now want to determine explicitly the set R of all algebraic integers in $\mathbb{Q}[\sqrt{d}]$.

Claim 3 *The set R of all algebraic integers in $\mathbb{Q}[\sqrt{d}]$ is such that either*

(i) $R = \mathbb{Z} + \mathbb{Z}\sqrt{d}$ *if* $d \equiv 2 \mod 4$ *or* $d \equiv 3 \mod 4$, *or*

(ii) $R = \mathbb{Z} + \mathbb{Z}\frac{\sqrt{d}+1}{2}$ *if* $d \equiv 1 \mod 4$.

Proof. Consider an element $n \in R \subset F$. It must be the case that n is of the form $n = a + b\sqrt{d}$. If $b = 0$, $a \in \mathbb{Z} \Rightarrow n \in \mathbb{Z}$. Because any rational zero of a monic polynomial with integer coefficients must be an integer, we see that when $b = 0$, n is an integer if and only if it is an algebraic integer.

We now assume $b \neq 0$, which means n must be a zero of $f(x) = (x - (a + b\sqrt{d}))(x - (a - b\sqrt{d})) = x^2 - 2ax + (a^2 - db^2)$. Note that if there exists another polynomial $g(x)$ for which n is a zero, it must have as another root $\overline{n}$, which means $g(x)$ must have $f(x)$ as a factor. Thus, $f(x)$ is the *unique* monic quadratic polynomial for which n is in the zero set.

We now see that the two coefficients of $f(x)$, $2a$ and $a^2 - db^2$, must be integers. It is clear that $a, b \in \mathbb{Z} \Rightarrow n \in \mathbb{Z}$. We assume that $d \equiv 1 \bmod 4$ and that $2a, 2b \in \mathbb{Z}$. If we write $a = \frac{1}{2}a_1$ and $b = \frac{1}{2}b_1$ where a_1 and b_1 are odd, we have $a_1^2 - db_1^2 \equiv (\pm 1)^2 - (\pm 1)^2 \cdot 1 \equiv 0 \bmod 4$, so $a^2 - db^2 = \frac{1}{4}(a_1^2 - db_1^2) \in \mathbb{Z}$, and since we assumed $d \equiv 1 \bmod 4$, this is as expected.

Now assume that n is an algebraic integer. This means by definition that $2a \in \mathbb{Z}$, and so either $a \in \mathbb{Z}$, in which case $b^2 d \in \mathbb{Z}$, and (since d is square-free) $b \in \mathbb{Z}$, or $2a \in \mathbb{Z}$. In the latter case, let $a = \frac{1}{2}a_1$ again, and note that

$$4a^2 \in \mathbb{Z} \text{ and } a^2 - db^2 \in \mathbb{Z} \implies 4b^2 d \in \mathbb{Z} \text{ but } db^2 \notin \mathbb{Z} \implies 2b \in \mathbb{Z} \text{ but } b \notin \mathbb{Z}.$$

Since n is an algebraic integer, $a^2 - db^2 \in \mathbb{Z}$, so

$$a^2 - db^2 \equiv 0 \bmod 4 \iff d \equiv 1 \bmod 4,$$

since $a^2 \equiv db^2 \bmod 4$, and the only quadratic residue modulo 4 is 1. □

Claim 4 *R is a subring of $\mathbb{Q}[\sqrt{d}]$.*

Proof. By Claim 3, $R = \mathbb{Z} + \mathbb{Z}\delta$ for appropriate δ. For $n, m \in \mathbb{Z}$, consider the polynomial

$$f(x) = x^2 + nx + m \in \mathbb{Z}[x].$$

It is clear that if $\delta = \sqrt{d}$, δ is in the zero set of $f(x)$ for appropriate n, m, and so it is in R. Likewise, if $\delta = \frac{\sqrt{d}+1}{2}$, it is also in the zero set for appropriate n, m, as is evident from the quadratic equation. Thus, R is in fact a subring of $\mathbb{Q}[\sqrt{d}]$. □

Definition 5. We call R the *ring of integers* in our imaginary quadratic field.

Definition 6. We define the *discriminant* D of $\mathbb{Q}[\sqrt{d}]$ as the discriminant of the irreducible polynomial $f(x)$ for which δ is in the zero set. This means that $D = 4d$ if $d \equiv 2$ or $d \equiv 3$ modulo 4, since then $f(x) = x^2 - d$, and $D = d$ if $d \equiv 1 \bmod 4$, since then $f(x) = x^2 - x + \frac{1}{4} - \frac{1}{4}d$.

We define a norm N over $\mathbb{Q}[\sqrt{d}]$ in the usual manner, where given any $\gamma = a + b\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$, $N(\gamma) = \gamma\overline{\gamma} = a^2 - db^2$. Because conjugation is an automorphism of $\mathbb{C}$, N is multiplicative.

Lemma 7 (Main) *Let R be the ring of (algebraic) integers in $\mathbb{Q}[\sqrt{d}]$ as above. For any ideal $I \subset R$, there exists I' such that $II' = (k)$, where (k) is the principal ideal generated by some $k \in \mathbb{Z}$ and $I' = \overline{I}$.*

Proof. The case where I is the zero ideal is trivial. We note that the complex conjugate $\overline{I}$ of an ideal is generated by the complex conjugates of the generators of I, and thus it is also an ideal. Because $I \subset R$ and R is of the form $\mathbb{Z} + \mathbb{Z}\delta$, it must be the case that $I = (\gamma_1, \gamma_2)$ for some $\gamma_1, \gamma_2 \in I$ [Artin 12.4.11], and from this we have

$$\overline{I} = (\overline{\gamma_1}, \overline{\gamma_2}).$$

By definition, the four products $\gamma_1\overline{\gamma_1}$, $\gamma_1\overline{\gamma_2}$, $\overline{\gamma_1}\gamma_2$, and $\gamma_2\overline{\gamma_2}$ generate $I\overline{I}$, and by definition of our norm, we know that $\gamma_1\overline{\gamma_1}$ and $\gamma_2\overline{\gamma_2}$ are integers, since they are their own conjugates. Also, $\gamma_1\overline{\gamma_2} + \overline{\gamma_1}\gamma_2$ is its own conjugate. Thus, all three of these values are integers.

($\subset$) We want to show that there exists k such that $(k) \subset I\overline{I}$. Let k be the greatest common divisor of the above three integers. Clearly, k can be written as a linear combination of these integers with linear coefficients, which means $k \in I\overline{I}$, which means $(k) \subset I\overline{I}$, since any element of (k) has k as a factor.

($\supset$) We now want to show that any element in $I\overline{I}$ is also in (k). We note that $\frac{\gamma_1\overline{\gamma_1}}{k} \in \mathbb{Z}$, and $\frac{\gamma_2\overline{\gamma_2}}{k} \in \mathbb{Z}$ by the fact that k is a factor. We consider the equation $f(x) = x^2 - rx + s$ where $r = \frac{\gamma_1\overline{\gamma_2} + \overline{\gamma_1}\gamma_2}{k}$ and $s = \frac{\gamma_1\overline{\gamma_2}}{k} \cdot \frac{\gamma_2\overline{\gamma_1}}{k} = \frac{\gamma_1\overline{\gamma_1}}{k} \cdot \frac{\gamma_2\overline{\gamma_2}}{k}$. Because $r, s \in \mathbb{Z}$, we know by our definition of algebraic integers that

$$\frac{\gamma_1\overline{\gamma_2}}{k} \in \mathbb{Z} \text{ and } \frac{\gamma_2\overline{\gamma_1}}{k} \in \mathbb{Z}.$$

Thus, $(k) \supset I\overline{I}$, so $I\overline{I} = (k)$ is a principal ideal. $\square$

2 Lattices and Minkowski's Lemma

We take a small detour to prove a few results, this time about lattices. We will see in the last section that ideals in our ring of algebraic integers R can be viewed as lattices, and that the below results

can be utilized to prove facts about the ideal class group. We will focus specifically on lattices in the plane $\mathbb{C} \simeq \mathbb{R}^2$, as this will make more intuitive the relationship between $R \subset \mathbb{Q}[\sqrt{d}]$ for $d < 0$ and lattices in $\mathbb{C}$.

Definition 8. We consider S, a bounded subset of the plane $\mathbb{C}$.

(i) We call S *convex* if for all $a, b \in S$, for any c on the line segment joining a to b, it is the case that $c \in S$.

(ii) We call S *centrally symmetric* if for any $p \in S$, it is the case that $-p \in S$.

By (i) and (ii) above, we see that $0 \in S$, unless $S = \emptyset$, since the line joining any pair of points p and $-p$ must pass through the origin.

Recall that a lattice L in $\mathbb{R}^2 \simeq \mathbb{C}$ must be either $\{0\}$, or it must be generated by either one vector or two linearly independent vectors; since it is always the case that $d < 0$, there will be an imaginary component, and so we only consider the latter case with two vectors, and note that these vectors constitute the lattice basis for $L \subset \mathbb{C}$. We denote by $P = P_L$ a parallelogram defined using the two elements of the lattice basis for L, and $\Delta(L)$ will refer to the area of any such P.

Lemma 9 *Let $S \subset \mathbb{C}$ be convex and centrally symmetric, and assume that* $\text{Area}(S) > \Delta(L)$. *There exists $\gamma \in L$ such that $S \cap (S + \gamma) \neq \emptyset$.*

Proof. Let P be any parallelogram as defined above. We can translate this parallelogram by any $\gamma \in L$ to obtain $P + \gamma$, and any such translation results in a new parallelogram which overlaps with P only along its edge. The set S is bounded, so we can assume we can list the translated parallelograms which it overlaps as $P + \gamma_1, ..., P + \gamma_m$. Let

$$S = \bigcup_{i=1}^{m} S_i = \bigcup_{i=1}^{m} S \cap (P + \gamma_i).$$

We can shift the S_i back to P by setting $\forall i$, $S_i' = S_i - \gamma_i$ such that $S_i' \subset P$. By assumption,

$$\text{Area}(S) = \sum_{i=1}^{m} \text{Area}(S_i) = \sum_{i=1}^{m} \text{Area}(S_i') > \Delta(L) = \text{Area}(P),$$

which means that some of the sets S_i' must overlap. Let $\gamma = \gamma_i - \gamma_j$ for $j \neq i$ such that $S_i' \cap S_j' \neq \emptyset$. Then, $S \cap (S + \gamma) \neq \emptyset$. □

We now have a useful tool to help us easily prove Minkowski's Lemma.

Lemma 10 (Minkowski) *Let L be a lattice in $\mathbb{C}$, and let $S \subset \mathbb{C}$ be convex and centrally symmetric. If* $\text{Area}(S) > 4\Delta(L)$, *then S must contain a lattice point other than* 0.

Proof. Define another convex set S' such that

$$S' = \{p \mid 2p \in S\}.$$

Note that S' is also centrally symmetric, and clearly it is still convex. Note also that $\text{Area}(S') = \frac{1}{4}\text{Area}(S)$, which by our assumption means that $\text{Area}(S') > \Delta(L)$. We can now choose γ as in Lemma 9, and consider any point $p \in S' \cap (S' + \gamma)$. We see that

$$p \in S' + \gamma \quad \text{and} \quad p - \gamma \in S',$$

and because S' is centrally symmetric,

$$(\gamma - p) \in S'.$$

The midpoint of the line segment between p and $(\gamma - p)$ is $\frac{1}{2}\gamma$, which must also be in S' by convexity. Thus, by definition of S', $\gamma \in S$ where $\gamma \neq 0$. $\square$

Proposition 11 *Any lattice $L \subset \mathbb{C}$ contains a nonzero vector γ such that $|\gamma|^2 \leq \frac{4}{\pi}\Delta(L)$.*

Proof. Consider $S \subset \mathbb{C}$, a circle of radius r around the origin. Provided that

$$\text{Area}(S) = \pi r^2 > 4\Delta(L) \iff r^2 > \frac{4}{\pi}\Delta(L), \tag{1}$$

Lemma 10 guarantees a nonzero lattice point $\gamma \in S$, and since S is a circle, $|\gamma|^2 < r^2$. Thus, given any arbitrarily small $\varepsilon > 0$ so that (1) is satisfied, there must exist nonzero γ such that $|\gamma|^2 \leq \frac{4}{\pi}\Delta(L) + \varepsilon$. We note that the number of lattice points in any bounded region is necessarily finite, so there must exist such a γ for a sufficiently small ε. $\square$

Finally, we consider two lattices $K \subset L \subset \mathbb{C}$ with lattice bases (k_1, k_2) and (l_1, l_2) for K and L, respectively.

Lemma 12 *If $K \subset L$ are lattices in $\mathbb{C}$, then $[L : K] = \frac{\Delta(K)}{\Delta(L)}$.*

Proof. Because the lattice K is a *subset* of L, there must exist positive integers n and m such that $k_1 = nl_1$ and $k_2 = ml_2$. Thus, we can shift the lattice K up to n times along the line parallel to one basis vector, and up to m times along the line parallel to the other basis vector; in other words, $L/K \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Thus,

$$[L : K] = nm.$$

Note also that a single parallelogram of the lattice K, P_K, can "contain" nm copies of the parallelogram P_L such that each copy of P_K overlaps only at edges with the other copies. Thus,

$$\text{Area}(P_K) = nm \cdot \text{Area}(P_L) \iff \Delta(K) = nm\Delta(L).$$

Clearly,

$$\Delta K = [L : K]\Delta(L) \iff [L : K] = \frac{\Delta(K)}{\Delta(L)},$$

which is the desired result. □

Lemma 13 *Let $I \subset J \subset \mathbb{C}$ be lattices. There are only finitely many lattices K between I and J such that $I \subset K \subset J$.*

Proof. Let (γ_1, γ_2) be a lattice basis for I, and let $P \equiv P_I$ be a parallelogram with vertices 0, γ_1, γ_2, $\gamma_1 + \gamma_2$. The bounded subset $P \subset \mathbb{C}$ contains only finitely many elements of J [Artin 5.4.12] because J is a discrete subgroup of $\mathbb{C}$, so if any K exists such that $I \subset K \subset J$, there are finitely many possibilities for $S = K \cap P$. Given any $\lambda \in K$, there must exist $\gamma \in I$ such that $(\lambda - \gamma) \in P$, and thus [Artin 5.4.14] in S. This means that $I + S = K$, which means I and S determine K completely, and so there can exist only finitely many such K. □

3 The Ideal Class Group

3.1 Ideals and Factorization

Let R be the ring of algebraic integers in $\mathbb{Q}[\sqrt{d}]$, as usual.

Lemma 14 *Given nonzero ideals I and J such that $I \subset J \subset R$, there exists an ideal $K \subset R$ such that $I = JK$. Additionally, if $IK \subset IJ$, then $K \subset J$, and if $IJ = IK$, then $J = K$.*

Proof. By Lemma 7, $\exists n \in \mathbb{Z}$ such that $J\overline{J} = (n)$, and so $I\overline{J} \subset J\overline{J} \subset (n)$. Note that $(\frac{1}{n})I\overline{J} \subset R$ is an ideal of R, since $I\overline{J} \subset R$ is an ideal of R. Let $K = (\frac{1}{n})I\overline{J}$ be this ideal, so that $JK = (\frac{1}{n})IJ\overline{J} = I$.

For the second portion, we can note that

$$IK \subset IJ \implies nK = I\overline{I}K \subset I\overline{I}J = nJ \implies K \subset J.$$

Additionally, note that

$$IJ = IK \iff IJ \subset IK \text{ and } IK \subset IJ \implies J \subset K \text{ and } K \subset J \iff J = K,$$

as desired. □

Theorem 1 *Let R be the ring of algebraic integers in $\mathbb{Q}[\sqrt{d}]$ as above. Every non-trivial ideal $I \subset R$ is*

(i) a product of prime ideals, and

(ii) can be factored uniquely up to the ordering of the factors.

Proof.

(i) We want to show that every non-trivial ideal $I \subset R$ is a product of prime ideals. Assume I is not itself prime. This means that I cannot be a maximal ideal, which means there exists a *proper* ideal $I' \subsetneq R$ such that $I \subsetneq I'$. Then there exists J such that

$$I = I'J \implies I \subset J.$$

Note that $I \neq J$, as then $R = I'$, which is a contradiction of our assumption that I' is a proper ideal. As we will see in the application of Lemma 20 in the next section, there exist finitely many ideals between I and R, so this process eventually terminates, if repeated. Note that the factors must be maximal for the process to terminate, which means they are prime.

(ii) Assume that there exist two factorizations of $I \subset R$ such that

$$I = P_1 \cdots P_n = Q_1 \cdots Q_m,$$

where all P_i and Q_i are prime ideals in R. We know that P_n divides I, so it divides $Q_1 \cdots Q_m$. Because all ideals in the factorization are prime, it must be equivalent to one of the Q_i. Re-order the Q_i so that $i = m$. By 14, we can now cancel P_n and Q_m to obtain

$$P_1 \cdots P_{n-1} = Q_1 \cdots Q_{m-1}.$$

We can continue this process, and by induction, we will see that the two factorizations are in fact identical up to re-ordering. □

3.2 Definition of the Ideal Class Group

Note that given any two nonzero ideals $I, J \subset R$, if there exist $\alpha, \beta \in R$ such that $\alpha I = \beta J$, we can find $\lambda = \alpha^{-1}\beta \in \mathbb{Q}[\sqrt{d}]^\times$ such that $I = \lambda J$. We construct an equivalence relation of ideals in R based on this:

$$I \sim J \text{ if and only if } \exists \lambda \in \mathbb{Q}[\sqrt{d}]^\times \text{ such that } I = \lambda J.$$

We can verify that this is indeed an equivalence relation:

(i) $I = I$ because $1 \in \mathbb{Q}[\sqrt{d}]^\times$ and $I = 1 \cdot I$;

(ii) $I = J \Rightarrow J = I$ because $\exists \lambda \in \mathbb{Q}[\sqrt{d}]^\times \Rightarrow \exists \lambda^{-1} \in \mathbb{Q}[\sqrt{d}]^\times$ such that $J = \lambda^{-1} I$;

(iii) $I = J$ and $J = K$ implies $I = K$ because given $I = \lambda_1 J$ and $J = \lambda_2 K$, we know that $I = (\lambda_1 \lambda_2) K$.

Claim 15 *Note that given this definition, for any ideal $I \in \langle R \rangle$, there exists λ such that $I = \lambda R$, which means $I = (\lambda)$, so I is a principal ideal.* □

Theorem 2 *The equivalence classes of ideals in R defined by our equivalence relation $\sim$ form an abelian group $\mathcal{C}$ under the law of composition $\cdot$ defined by*

$$\langle I \rangle \cdot \langle J \rangle = \langle IJ \rangle$$

where for some ideals $I, J \in \mathcal{C}$, IJ denotes multiplication of the ideals.

Proof. We first show that the group operation $\cdot$ is well defined. Assume $I, I', J, J' \in R$ are such that $I \sim I'$ and $J \sim J'$. We see that for some $\lambda_1, \lambda_2 \in F^\times$,

$$I' = \lambda_1 I \text{ and } J' = \lambda_2 J \implies I'J' = (\lambda_1 \lambda_2) IJ \implies IJ \sim I'J'.$$

By associativity and commutativity of multiplication of ideals, the law of composition must also be commutative and associative. Inverses exist by Lemma 7, because we can always find some ideal I' such that $II' = (n)$ for some element $n \in R$, and since $\forall J \in \langle R \rangle, J \sim (n)$, $\langle R \rangle$ is the identity element in $\mathcal{C}$. □

Definition 16. We define the *ideal class group* for the ring of integers in an imaginary quadratic number field as $\mathcal{C}$.

3.3 Finiteness

We will now apply our results about lattices from the previous section to show that $\mathcal{C}$ is always finite. We consider the ring R as usual. We note that there is a natural imbedding of $\mathbb{Q}[\sqrt{d}]$ into $\mathbb{C}$ because $d < 0$, as $\mathbb{Q}[\sqrt{d}] \subset \mathbb{C}$. We also know by Claim 3 that $R = \mathbb{Z} + \mathbb{Z}\delta$ for appropriate δ, which means

Claim 17 *the ring R forms a lattice over $\mathbb{C}$.*

In order to measure the area $\Delta(R)$, we note that

$$\Delta(R) = \frac{1}{2}\sqrt{|D|},$$

since $D = 4d$ if $d \equiv 2, 3 \bmod 4$, which means $\Delta(R) = \frac{\sqrt{4d}}{2} = \sqrt{d}$, and $D = d$ if $d \equiv 1 \bmod 4$, which means $\Delta(R) = \frac{\sqrt{d}}{2}$, which is consistent with what we might expect, since in the latter case the

parallelogram is only half the area of the one in the former case. We may also use Lemma 7 to take the norm of an ideal I so that $N(I) = n$ if $I\overline{I} = (n)$. Since N is multiplicative, $N(I)N(J) = N(IJ)$.

Lemma 18 *Let n be an integer and $I \subset R$ be an ideal. Then $[R : nI] = n^2[R : I]$.*

Proof. Since $nI \subset I \subset R$, by Lemma 12, $[R : nI] = [R : I][I : nI]$, and because I is a lattice, nI is simply the same lattice scaled by a factor of n, so clearly $[I : nI] = n^2$. □

Lemma 19 *For any nonzero ideal $I \subset R$, $[R : I] = N(I)$.*

Proof. Consider a prime ideal $P \subset R$. By results regarding primes in the Gaussian integers [Artin 11.5], we know that either there is an integer p such that $P = (p)$, or there is p such that $P\overline{P} = (p)$.

In the latter case, $N(P) = p$. Note that $I > IP > IP\overline{P} \Rightarrow [R : I] < [R : IP] < [R : IP\overline{P}]$. Since $P\overline{P} = (p) \Rightarrow pA = AP\overline{P}$, by Lemma 18, $[R : pI] = p^2[R : I]$. Thus, $[R : IP] = p[R : I]$. Note that if $I = R$, $[R : P] = p$, so $N(P) = p = [R : P]$. Otherwise, $[R : IP] = [R : I][R : P]$, and again we have $N(P) = [R : P]$. In the former case, $N(P) = p^2$, and $IP = pI$, which by Lemma 18 means that $[R : IP] = p^2[R : I]$. Also, $[R : P] = p^2[R : R] = p^2$. Consequently, $[R : IP] = [R : I][R : P]$ and $N(P) = [R : P]$.

It follows by induction on the prime factorization of an arbitrary nonzero ideal I and the fact that $N(I)$ is multiplicative that $[R : I] = N(I)$.

Theorem 3 *Let $\mu = \frac{2}{\pi}\sqrt{|D|}$. In every ideal class $\langle C \rangle$ there exists $I \in \langle C \rangle$ such that $N(I) \leq \mu$.*

Proof. Let I be an ideal; this means $\overline{I}$ is an ideal also. By Lemma 11, there exists $\gamma \in \overline{I}$ such that $N(\gamma) = |\gamma|^2 \leq \frac{4}{\pi}\Delta(\overline{I})$, since $N(\gamma) = |\gamma|^2$ by definition. Thus,

$$(\gamma) \subset \overline{I} \implies \exists J \text{ such that } \overline{I}J = (\gamma).$$

Since norms are multiplicative, $N(\overline{I})N(J) = N(\gamma)$. Thus, by Lemma 12 and Lemma 19,

$$\Delta(\overline{I}) = [R : \overline{I}]\Delta(R) = \frac{N(\overline{I})\sqrt{|D|}}{2} \implies N(J) \leq \mu.$$

Note that because $\overline{I}J$ is a principal ideal, $\langle J \rangle = \langle \overline{\overline{I}} \rangle = \langle I \rangle \Rightarrow \langle J \rangle = \langle \overline{I} \rangle^{-1}$. Thus, $\langle I \rangle$ contains an appropriate ideal. □

We now go on to our main result.

Theorem 4 *The ideal class group $\mathcal{C}$ is finite.*

Proof. Because there exists an ideal $I \subset R$ such that $N(I) \leq \mu$ in any class of ideals, and because for any $I \subset R$ it is the case that $[R : I] = N(I)$, we need to show that

Lemma 20 *there are finitely many sublattices $K \subset R$ such that $[R : K] \leq \mu$.*

Proof. We choose any integer $i \leq \mu$, and we let K be a sublattice such that $[R : K] = i$. This means that R/K is an abelian group with $|R/K| = i$, so $iR \subset K$, because sublattices with index i contain iR. We know by Lemma 13 that there are finitely many such lattices K, and because i is clearly finite, there must be finitely many such sublattices. □

By Lemma 20, and by the fact that sublattices of R correspond to ideals in R, there are finitely many ideals with index less than or equal to μ in R. This means every ideal class contains only ideals I such that $N(I) \leq \mu$, and since we have an explicit formula for μ, $\mathcal{C}$ must be finite. □

3.4 Examples

Theorem 5 *The ideal class group $\mathcal{C}$ is generated by the classes of prime ideals P which divide the integer primes $p \leq \lfloor \mu \rfloor$.*

Proof. Since $\forall C \in \mathcal{C}$, $\exists I \in C$ such that $N(I) \leq \mu$, and $N(I) \in \mathbb{Z}$, $N(I) \leq \lfloor \mu \rfloor$. Let $I = P_1 \cdots P_n$ be the prime factorization of I into ideals. Then, $N(I) = N(P_1 \cdots P_n) = N(P_1) \cdots N(P_n)$, which means $\forall P_i$, $N(P_i) \leq \lfloor \mu \rfloor$. Thus, the classes of prime ideals P with norm less than or equal to $\lfloor \mu \rfloor$ form the set of generators of $\mathcal{C}$. □

We can use Theorem 5 to examine the ideal class group $\mathcal{C}$ for particular values of d. We can do this by looking at each prime integer $p \leq \lfloor \mu \rfloor$, and if p is prime in R, (p) is principal and the class is trivial. Otherwise, we can include the class of one of its prime ideal factors in the set of generators of $\mathcal{C}$ (the other factor is in the inverse class). If it is still principal, we can also ignore it, leaving only the primes which generate $\mathcal{C}$. We consider a few examples.

(i) We consider $d = -23$. Since $23 \equiv 1 \bmod 4$, $R = \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{-23}}{2}$. We have $\lfloor \mu \rfloor = 3$, so only the classes of the prime ideals dividing (2) and (3) could possibly generate $\mathcal{C}$. However, the polynomial $f(x) = x^2 - x + 6$ is not irreducible modulo 2 or modulo 3.

Let $P = (2, \frac{1+\sqrt{-23}}{2})$; we have $P\overline{P} = (2)$. Let $(3) = Q\overline{Q}$. Because $N(\frac{1+\sqrt{-23}}{2}) = 6 = 2 \cdot 3$, and $N(1 + \frac{1+\sqrt{-23}}{2}) = 8 = 2 \cdot 2 \cdot 2$, we have $(\frac{1+\sqrt{-23}}{2})(\overline{\frac{1+\sqrt{-23}}{2}}) = P\overline{P}Q\overline{Q}$. Also, we have $(1 + \frac{1+\sqrt{-23}}{2})\overline{(1 + \frac{1+\sqrt{-23}}{2})} = (8) = (2)^3 = P^3\overline{P}^3$. Thus, $(\frac{1+\sqrt{-23}}{2}) = PQ$ and $(1 + \frac{1+\sqrt{-23}}{2}) = P^3$, which means $\langle P \rangle = \langle 1 \rangle$ and $\langle Q \rangle = \langle P \rangle^{-1}$. Thus, $\mathcal{C}$ must be cyclic, with $|\mathcal{C}| = 3$.

(ii) We consider $d = -14$. We know that $\lfloor \mu \rfloor = 4$, so, once again, only the classes of the prime ideals dividing (2) and (3) could possibly generate $\mathcal{C}$. Since $f(x) = x^2 + 14$ is reducible modulo both primes, neither of them are prime in R. Assume $(2) = P\overline{P}$ and $(3) = Q\overline{Q}$. We find that $P = (2, \sqrt{-14})$, and clearly $P = \overline{P}$. Thus, for $\langle P \rangle \in \mathcal{C}$, $|\langle P \rangle| = 2$. We now consider $2 + \sqrt{-14} \in R$. $N(2 + \sqrt{-14}) = 18 = 2 \cdot 3 \cdot 3$, so $(2 + \sqrt{-14})(2 - \sqrt{-14}) = P\overline{P}Q^2\overline{Q}^2$. The two factors generate conjugate ideals, so $(2 + \sqrt{-14}) = PQ^2$. Thus, because this ideal is principal, $\langle P \rangle \langle Q \rangle^2 = 1$, which means $\langle Q \rangle^2 = \langle P \rangle^{-1} = \langle P \rangle$. Consequently, since $\langle Q \rangle^4 = 1$, $\mathcal{C}$ is cyclic, where $|\mathcal{C}| = 4$. Additionally, we see that $\mathcal{C}$ is generated by $\langle Q \rangle$.