DEDEKIND DOMAINS AND THE IDEAL CLASS GROUP

BENJAMIN BOYAJIAN

Abstract. In this paper, we will define a discrete valuation ring and Dedekind domain, and will develop a notion of the ideal group and ideal class group of a Dedekind domain. We will also prove that the ring of algebraic integers in an imaginary quadratic number field is a Dedekind domain, and will prove some additional theorems about the ideal class group for this special case.

Contents

1. Factorization in Commutative Rings

First, we will provide some background material on factorization, which will be important for the rest of the paper. We assume that the reader is acquainted with basic ring theory, and proceed with a few important definitions. Throughout this paper, R will denote a commutative ring, 0 will denote the additive identity of R, and 1 will denote the multiplicative identity of R.

Definition 1.1. An element $u \in R$ is a unit if it has a multiplicative inverse.

Definition 1.2. For two elements $a, b \in R$, we say that a divides b if there exists an element $c \in R$ such that $ac = b$. We write $a \mid b$ if a divides b and $a \nmid b$ if a does not divide b.

Definition 1.3. Two elements $a, b \in R$ are associates if there exists a unit $u \in R$ such that $au = b$.

Remark 1.4. If $a, b \in R$ are associates, then $a \mid b$ and $b \mid a$.

Definition 1.5. If $a, b \in R$, we say that a is a proper divisor of b if a is not a unit, and there exists $c \in R$ such that $ac = b$, where c is not a unit.

Definition 1.6. An element $a \in R$ that is nonzero and not a unit is irreducible if there do not exist elements $b, c \in R$ that are not units such that $a = bc$.

Date: August 26, 2011.

Definition 1.7. An element $p \in R$ that is nonzero and not a unit is prime if for any elements $a, b \in R$ such that $p \mid ab$, either $p \mid a$ or $p \mid b$.

Example 1.8. In $\mathbb{Z}[\sqrt{-5}]$, the element 2 is irreducible, but not prime. To prove that it is irreducible, note that for all $a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$, we have $|a + b\sqrt{-5}|^2 = a^2 + 5b^2 \in \mathbb{Z}$. Suppose the only elements of $\mathbb{Z}[\sqrt{-5}]$ that have absolute value 1 are ± 1, which are units. Suppose there is an element $a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ that is a proper divisor of 2. Then $|a+b\sqrt{-5}|^2 = a^2+5b^2$ divides $|2|^2 = 4$, thus $a^2+5b^2 = 2$, which is impossible. Also, 2 is not prime because $2 \mid (1+\sqrt{-5})(1-\sqrt{-5}) = 6$, but $2 \nmid 1 + \sqrt{-5}$ and $2 \nmid 1 - \sqrt{-5}$.

Definition 1.9. An ideal $I \subseteq R$ is principal if $I = \{ar \mid r \in R\}$ for some $a \in R$. We say that I is the principal ideal generated by a, and we write $I = (a)$.

Remark 1.10. If $a, b \in R$ are associates, then $(a) = (b)$. Similarly, $u \in R$ is a unit if and only if $(u) = (1) = R$.

Definition 1.11. A commutative ring R is an integral domain if for any elements $a, b \in R$ such that $ab = 0$, either $a = 0$ or $b = 0$.

Definition 1.12. An ideal $P \subseteq R$ is prime if for any elements $a, b \in R$ such that $ab \in P$, either $a \in P$ or $b \in P$.

Remark 1.13. A principal ideal $(p) \subseteq R$ is prime if and only if $p \in R$ is prime. This follows because saying that $p \mid a$ is equivalent to saying that $a \in (p)$.

Proposition 1.14. *An ideal $P \subseteq R$ is prime if and only if the quotient ring R/P is an integral domain.*

Proof. This follows because $a \in P$ if and only if $\overline{a} = 0$, where $\overline{a}$ is the equivalence class of a in R/P. □

Definition 1.15. An ideal $M \subseteq R$ is maximal if the only ideals that contain M are M and R.

Proposition 1.16. *An ideal $M \subseteq R$ is maximal if and only if the quotient ring R/M is a field.*

Proof. By the Correspondence Theorem (see Artin Chapter 10, Proposition 4.3), the ideals of R that contain M are in bijective correspondence with the ideals of R/M. If M is a maximal ideal, then there only two ideals of R/M, thus R/M is a field. Conversely, if R/M is a field, then there are only two ideals of R that contain M, thus M is a maximal ideal. □

Corollary 1.17. *A maximal ideal is a prime ideal.*

Proof. Let $M \subset R$ be a maximal ideal. Then the quotient ring R/M is a field, thus it is an integral domain. By (1.12), M is a prime ideal. □

Proposition 1.18. *If an element $p \in R$ is prime and R is an integral domain, then p is irreducible.*

Proof. Suppose there exist elements $a, b \in R$ that are not units such that $ab = p$. Then $p \mid ab$, but $p \nmid a$. This is because $a = cp$ implies $p = ab = bcp$, which implies $bc = 1$ by the Cancellation Law. Similarly, $p \nmid b$, which contradicts the definition of prime. □

Definition 1.19. An integral domain R is an principal ideal domain if every ideal of R is principal.

Definition 1.20. n ring R is Noetherian if it does not contain an infinite increasing chain of ideals $I_1 \subset I_2 \subset \ldots$.

Definition 1.21. A ring R has the ascending chain property if it does not contain an infinite increasing chain of principal ideals $(a_1) \subset (a_2) \subset \ldots$.

Proposition 1.22. *An integral domain R has the ascending chain property if and only if the process of factoring any element into irreducible elements terminates after a finite number of steps.*

Proof. Suppose that R contains an infinite increasing chain of principal ideals $(a_1) \subset (a_2) \subset \ldots$. Then $(a_n) \neq R$ for all $n \in \mathbb{N}$, thus each a_n is not a unit. Also, $(a_{n-1}) \subset (a_n)$, so a_n is a proper divisor of a_{n-1}. So then we can write $a_1 = b_1 a_2 = b_1 b_2 a_3 = \ldots$, where the b_i are not units, and the factoring process does not terminate. Conversely, if the process of factoring does not terminate, then we have $a_1 = b_1 a_2 = b_1 b_2 a_3 = \ldots$ where the b_i are not units, thus $(a_1) \subset (a_2) \subset \ldots$ is a strictly increasing chain of principal ideals. □

Definition 1.23. An integral domain R is a unique factorization domain if every element $a \in R$ can be factored $a = a_1 \ldots a_n$ into irreducible elements, and this factorization is unique up to associates.

Example 1.24. The ring $\mathbb{Z}[\sqrt{-5}]$ is not a unique factorization domain. To see this, observe that $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ has two distinct factorizations into irreducible elements. The proofs that $2, 3, (1+\sqrt{-5}), (1-\sqrt{-5})$ are irreducible follow in the same way as Example 1.8.

Proposition 1.25. *Let R be an integral domain with the ascending chain property. Then R is a unique factorization domain if and only if every irreducible element is prime.*

Proof. Suppose that R is a unique factorization domain, and let $a \in R$ be an irreducible element. If that $a \mid bc$ for some $b, c \in R$, then bc can be factored $bc = a_1 \ldots a_n$. This factorization is unique, so a_i is an associate of a for some $1 \leq i \leq n$. Then either b or c must contain an associate of a in its unique factorization. Conversely, suppose that R is not a unique factorization domain, and then there exists $a \in R$ that has two distinct factorizations $a = b_1 \ldots b_n = c_1 \ldots c_m$. Then there exists $1 \leq i \leq n$ such that b_i is not an associate of c_j for any $1 \leq j \leq m$. Then $b \mid a$, but $b \nmid c_1 \ldots c_{m-1}$ and $b \nmid c_m$. □

Proposition 1.26. *In a principal ideal domain, every irreducible element is prime.*

Proof. Let R be a principal ideal domain, and let $a \in R$ be an irreducible element. Then the principal ideal $(a) \subset R$ is a maximal ideal. To prove this, suppose that there exists an intermediate principal ideal $(a) \subset (b) \subset R$. Then b is a proper divisor of a, but b is not a unit, which contradicts the assumption that a is irreducible. Then the quotient ring $R/(a)$ is a field, thus it is an integral domain. Then (a) is a prime ideal, thus a is prime. □

Theorem 1.27. *A principal ideal domain is a unique factorization domain.*

Proof. Let R be a principal ideal domain, and then every irreducible element is prime. So we only need to prove the existence of factorizations for elements in R, which is equivalent to showing that R contains no infinite increasing chain of principal ideals. Suppose that $(a_1) \subset (a_2) \subset \ldots$ is such a chain, and then the union $\cup_{n\in\mathbb{N}}(a_n)$ is an ideal, thus is it generated by some $b \in R$. Then b is contained in one of the ideals (a_n), thus $(b) \subseteq (a_n)$. However, by definition $(a_{n+1}) \subseteq (b)$, which contradicts the assumption that the chain of ideals is increasing. □

2. Localization and Integrality

Definition 2.1. Let R be an integral domain. Then the field of fractions of R is the set of equivalence classes of $\{(a, b)|a \in R, b \in R\backslash\{0\}\}$, where $(a, b) \sim (c, d)$ if $ad = bc$. We write a/b for the equivalence class of (a, b).

We define $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ and $(\frac{a}{b})(\frac{c}{d}) = \frac{ac}{bd}$. The proofs that addition and multiplication are well-defined and that the field of fractions is in fact a field are straightforward, so we omit them.

Definition 2.2. Let R be a ring. A set $S \subseteq R$ is multiplicatively closed if $1 \in S$, and for any elements $a, b \in S$, we have $ab \in S$.

Example 2.3. Let P be a prime ideal of R, and then $R\backslash P$ is a multiplicatively closed subset. This follows from the definition of prime ideal.

Now we can extend the notion of a field of fractions to an arbitrary ring. Let $S^{-1}R$ be the set of equivalence classes of $\{(a, b)|a \in R, b \in S\}$, where $(a, s) \equiv (b, t)$ if $(at-bs)u = 0$ for some element $u \in S$. We define $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ and $(\frac{a}{b})(\frac{c}{d}) = \frac{ac}{bd}$, and then one can prove that $S^{-1}R$ is a commutative ring, using the same techniques as before. We write $S^{-1}R = R_P$ if $S = R\backslash P$, where P is a prime ideal of R. Also, for any $x \in R$, we write $S^{-1}R = R_x$ if $S = \{1, x, \ldots\}$.

Definition 2.4. Let A, B be rings such that $A \subseteq B$. Then an element $x \in B$ is integral over A if there exist $a_0, \ldots, a_{n-1} \in A$ such that $x^n + a_{n-1}x^{n_1} + \ldots + a_0 = 0$.

Definition 2.5. Let R, R' be rings such that $R \subseteq R'$. We say that R is integrally closed in R' if the only elements of R' that are integral over R are elements of R.

Example 2.6. The ring $\mathbb{Z}$ is not integrally closed in $\mathbb{Z}[\sqrt{2}]$ because $\sqrt{2}$ is integral over $\mathbb{Z}$. However, $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$. This is because for any element $\frac{a}{b} \in \mathbb{Q}$, with $b \neq 1$, the irreducible polynomial of $\frac{a}{b}$ over $\mathbb{Z}$ is not monic, thus $\frac{a}{b}$ is not integral over $\mathbb{Z}$ (see Artin, Chapter 11, Proposition 6.7).

We say that a ring R is integrally closed if it is integrally closed in its field of fractions. For example, $\mathbb{Z}$ is integrally closed, because its field of fractions is $\mathbb{Q}$.

3. Discrete Valuation Rings

Definition 3.1. A commutative ring R is a discrete valuation ring if it is a principal ideal domain and has a unique nonzero prime ideal.

Definition 3.2. A commutative ring R is a local ring if it contains exactly one maximal ideal.

Proposition 3.3. *Let M be the unique nonzero prime ideal of R. Then M is maximal.*

Proof. Suppose there exists an intermediate ideal $M \subset M' \subset R$. Let π be a generator for M, let π' be a generator for M', and then $\pi = \pi' a$ for some $a \in R$. Also, a cannot be a unit, because otherwise we would have $M = M'$. Then π is not irreducible, thus it is not prime, and neither is M. □

Definition 3.4. The field R/M is the residue field of R.

Proposition 3.5. *Let π be a generator for the prime ideal of a discrete valuation ring R. Then every nonzero element of R can be written uniquely in the form $\pi^n u$, where $n \in \mathbb{N} \cup \{0\}$ and u is a unit.*

Proof. Because R is a unique factorization domain, any element $a \in R$ can be written uniquely in the form $\pi^n a'$, where $n \in \mathbb{N} \cup \{0\}$ and $\pi \nmid a'$. Then $a' \notin M$, thus the equivalence class of a' is a nonzero element of R/M. Then the equivalence class of a' is a unit in R/M, thus a' is a unit in R. □

We define the valuation of $x \in R$ to be $\nu(x) = n$, where $x = \pi^n u$ and u is a unit.

Corollary 3.6. *Let K be the field of fractions of R. Then every nonzero element of K can be written $\pi^n u$, where $n \in \mathbb{Z}$ and u is a unit.*

Example 3.7. The ring $\mathbb{Z}_{(p)} = \{\frac{a}{b} | p \nmid b\}$ is a discrete valuation ring. This is true because (p) is a prime ideal for any prime p.

Theorem 3.8. *A ring R is a discrete valuation ring if and only if it is a Noetherian local ring and has a maximal ideal generated by a non-nilpotent element. (An element $x \in R$ is nilpotent if there exists $n \in \mathbb{N}$ such that $x^n = 0$.)*

Proof. A discrete valuation ring clearly satisfies the above properties. Now suppose that these conditions hold in any ring R, and let π be a non-nilpoent generator for the maximal ideal $M \subseteq R$. Let $U \subseteq R$ be the ideal of elements $x \in R$ such that $x\pi^n = 0$ for some $n \in \mathbb{N}$. Then U is finitely generated, thus there exists $N \in \mathbb{N}$ such that $x\pi^N = 0$ for all $x \in U$. Now we prove that $\cap_{n\in\mathbb{N}} M^n = 0$. Let $y \in \cap_{n\in\mathbb{N}} M^n$, and then we can write $y = \pi^n x_n$ for all $n \in \mathbb{N}$. Then $\pi^n(x_n - \pi x_{n+1}) = 0$, thus $x_n - \pi x_{n+1} \in U$. Also, the sequence $U + (x_1) \subseteq U + (x_2) \subseteq \ldots$ is an ascending chain of ideals, so we must have $U + (x_n) = U + (x_{n+1})$ for sufficiently large n. Then $x_{n+1} = z + tx_n$ where $z \in U$ and $t \in R$, and $x_n = \pi x_{n+1} + z'$ where $z \in U$. By substituting, we get $(1 - \pi t)x_{n+1} \in U$. But $1 - \pi t \notin M$, therefore it is a unit, so $x_{n+1} \in U$. Therefore if $n + 1 \geq N$, then $y = \pi^{n+1} x_{n+1} = 0$.

Now for every element $x \in R$, there exists $n \in \mathbb{N}$ such that $x \in M^n$ but $x \notin M^{n+1}$. Then we can write $x = \pi^n u$, where $u \notin M$, which implies that u is a unique. This representation $x = \pi^n u$ is clearly unique, which shows that R is a discrete valuation ring. □

For the next theorem, we will first introduce some notation. If R is a commutative ring and I, J are ideals of R, we define the sum of ideals $I + J$ to be $\{a + b | a \in I, b \in J\}$ and the product of ideals IJ to be $\{\sum_{i\in I} x_i y_i | x_i \in I, y_i \in J\}$.

Theorem 3.9. *If R is a Noetherian integral domain, then R is a discrete valuation ring if and only if R is integrally closed and has a unique nonzero prime ideal.*

Proof. By definition, a discrete valuation ring has a unique nonzero prime ideal. Now let R be a discrete valuation ring with maximal ideal M and field of fractions K, and let $x \in K \backslash R$. Then $x = \pi^{-m} u$ for some $m > 0$, where π is a generator of M

and u is a unit. Suppose that $x^n+a_{n-1}x^{n-1}+\ldots+a_0 = 0$ for some $a_0, \ldots, a_{n-1} \in R$, and then $\pi^{mn}x^n + \pi^{mn}a_{n-1}x^{n-1} + \ldots + \pi^{mn}a_0 = 0$. Then $\nu(\pi^{mn}a_ix^i) > 0$ for all $1 \leq i \leq n-1$, but $\nu(\pi^{mn}x^n) = 0$. Then $\pi^{mn}a_ix^i \in M$ for all $1 \leq i \leq n-1$, but $\pi^{mn}x^n \notin M$, which is a contradiction.

Conversely, suppose that R is a Noetherian integral domain that is integrally closed and has a unique nonzero prime ideal. Let M be the unique nonzero prime ideal, and let K be the field of fractions of R. Let $M' = \{x \in K | xM \subseteq R\}$, and then M' is an R-module. Then the product $MM' = \{\sum x_iy_i | x_i \in M, y_i \in M'\}$ is contained in R by the definition of M', thus it is an ideal. Also, $M \subseteq MM'$, thus either $MM' = M$ or $MM' = R$.

Lemma 3.10. *If $MM' = R$, then M is a principal ideal.*

Proof. If $MM' = R$, then $\sum x_iy_i = 1$ for some $x_i \in M, y_i \in M'$. By the definition of M', all the products x_iy_i are contained in R, and at least one of them, let us say x_jy_j, is not contained in M, and is therefore invertible in R. If $z \in M$, then $z = x_j(x_jy_j)^{-1}y_jz$, and $y_jz \in R$ because $y_j \in M'$, thus $z \in (x_j)$. However, $x_j \in M$, thus $M = (x_j)$. □

Lemma 3.11. *If $MM' = M$ and R is integrally closed, then $M' = R$.*

Proof. Suppose that $MM' = M$, and let $x \in M'$. Then $xM \subseteq M$, and by induction, $x^nM \subseteq M$ for all $n \in \mathbb{N}$. Also, fixing $y \in M$, we have $xy \in R$ for all $x \in M'$, thus $M' \subseteq y^{-1}R$, so M' is finitely generated. Let R_n be the R-module generated by $\{1, x, \ldots, x^n\}$, and then because R is Noetherian, there exists $N \in \mathbb{N}$ such that $R_N = R_{N-1}$. Then $x^N \in R_{N-1}$, thus we can write $x^N + a_{N-1}x^{N-1} + \ldots + a_0 = 0$, where $a_0, \ldots, a_{N-1} \in R$. Then $x \in R$ because R is integrally closed, and it follows that $M' = R$. □

Lemma 3.12. *If R has a unique nonzero prime ideal M, then $M' \neq R$.*

Proof. Let x be an nonzero element of M. Then we must have $R_x = K$, because R_x has no nonzero prime ideals, and is thus a field. Then every element $z \in K$ can be written in the form y/x^n, where $y \in R$. Then $1/z = y/x^n$, thus $x^n = yz \in zR$. Let $x_1, \ldots, x_k$ generate M and let $n \in \mathbb{N}$ be such that $x_i^n \in zR$ for all $1 \leq i \leq k$. If $N > k(n-1)$, then the monomials in the x_i of total degree N contain an x_i^n as a factor, and therefore belong to zR. The ideal M^N is generated by these monomials, so $M^N \subseteq zR$. Then there is a smallest integer $N \geq 1$ such that $M^N \subseteq zA$. Let $y \in M^{N-1}, y \notin zR$. Then $yM \subseteq zR$, thus $y/z \in M'$ and $y/z \notin R$, which proves that $M' \neq R$. □

Now we can complete the proof of Theorem 3.9. From the above three lemmas, it follows that we cannot have $MM' = M$. Therefore M is a principal ideal, thus R is a discrete valuation ring. □

4. Dedekind Domains

Theorem 4.1. *If R is a Noetherian integral domain, then R_P is a discrete valuation ring for every prime ideal $P \subseteq R$ if and only if R is integrally closed and every nonzero prime ideal of R is maximal.*

Proof. Suppose that R_P is a discrete valuation ring for every prime ideal $P \subseteq R$, and suppose that $P \subseteq P'$ are prime ideals in R. Then $R_{P'}$ contains the prime ideal

$PR_{P'}$, which means that either $P = 0$ or $P = P'$. Also, if $a \in K$ is integral over R, then it is integral over R_P for all prime ideals $P \subseteq R$. Then by Theorem 3.9, R_P is integrally closed, thus $a \in R_P$. Write $a = b/c$, where $b, c \in A$ and $c \neq 0$, and let I be the ideal of all $x \in A$ such that $xb \in (c)$. Then I is not contained in any prime ideal, thus $I = R$. Then $b \in (c)$, thus $a = b/c \in R$.

Conversely, supose that R is integrally closed and every nonzero prime ideal of R is maximal. We prove that R_P is integrally closed for all prime ideals $P \subset R$, and it follows by Theorem (3.8) that R_P is a discrete valuation ring. Let x be integral over R_P, and then we have $sx^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$, where $a_i \in R$ and $s \in R\backslash P$. Multiplying by s^{n-1}, we get $(sx)^n + a_{n-1}(sx)^{n-1} + \ldots + a_0 s^{n-1} = 0$, thus sx is integral over R. Then $sx \in R$, thus $x \in R_P$. □

Definition 4.2. A Noetherian integral domain that satisfies the above conditions is a Dedekind domain.

5. The Ideal Class Group

Definition 5.1. Let R be an integral domain, and let K be the field of fractions of R. Then a fractional ideal of R is a sub-R-module of K that is finitely generated.

We say that a fractional ideal I of R is invertible if there exists another fractional ideal $I' \subseteq K$ such that $II' = R$. We define $(I : J)$ to be the ideal of all $x \in K$ such that $xJ \subseteq I$. Note that $I(R : I) \subseteq R$, and a fractional ideal I is invertible if and only if its inverse is $(R : I)$.

Theorem 5.2. *In a Dedekind domain, every nonzero fractional ideal is invertible.*

Proof. Let R be a Dedekind domain. Then R_P is a discrete valuation ring for every prime ideal $P \subset R$. Then any fractional ideal of R_P has the form $I_P = \pi^n R_P$, where $n \in \mathbb{Z}$, and is thus invertible, where $(R_P : I_P) = \pi^{-n} R_P$. To prove that a fractional ideal I of R is invertible, we use localization to prove that $(IJ)_P = I_P J_P$ and $(I : J)_P = (I_P : J_P)$. For the first part, note that every element of $(IJ)_P$ can be written a/s, where $a \in IJ$ and $s \in R\backslash P$. Then $a = \sum_{i=1}^n x_i y_i$ where $x_i \in I$ and $y_i \in J$, thus $a/s = \sum_{i=1}^n (x_i/s) y_i \in I_P J_P$. Conversely, every element of $I_P J_P$ can be written $\sum_{i=1}^n (x_i/s_i)(y_i/t_i) = \sum_{i=1}^n (x_i y_i / s_i t_i)$. This can be rewritten $a/\prod_{i=1}^n s_i t_i$ where $a = \sum_{i=1}^n (x_i y_i \prod_{j \neq i} s_j t_j)$ and $\prod_{i=1}^n s_i t_i \in R\backslash P$, so it is an element of $(IJ)_P$. For the second part, note that every element of $(I : J)_P$ can be written x/s where $xJ \in I$ and $s \in R\backslash P$. Then $(x/s)J_P \subseteq xJ_P \subseteq I_P$, whus $x/s \in (I_P : J_P)$. Conversely, let $x \in (I_P : J_P)$, and then $xJ_P \subseteq I_P$, thus every element xy/s, where $y \in J$ and $s \in R\backslash P$, is contained in I_P. Then $(tx)y \in I$ for some $t \in R\backslash P$, thus $x \in (I : J)_P$.

Because we have $(I(R : I))_P = I_P(R_P : I_P) = R_P$, we have $I(R : I) = R$, thus I is invertible. □

Corollary 5.3. *The set of fractional ideals of a Dedekind domain R forms a group under multiplication of ideals, with R as the identity.*

We call this group the ideal group. Note that the ideal group is abelian, because ideal multiplication is commutative in a commutative ring.

Theorem 5.4. *If $x \in R\backslash\{0\}$, then only finitely many prime ideals contain x.*

Proof. Note that R is Noetherian, so for any sequence of ideals $I_1 \supseteq I_2 \supseteq \ldots \supseteq xR$, we can take inverses, so the sequence $I_1^{-1} \subseteq I_2^{-1} \subseteq \ldots \subseteq x^{-1}R$ is stationary. Then $I_n^{-1} = I_{n+1}^{-1}$ for some $n \in \mathbb{N}$, thus $I_n = I_{n+1}$. Suppose that $P_1, P_2, \ldots$ are prime ideals that contain x, and then the sequence $P_1 \supseteq P_1 \cap P_2 \supseteq \ldots \supseteq xR$ is stationary, so at some point we have $P_i \supseteq P_1 \cap \ldots \cap P_k \supseteq P_1 \ldots P_k$. Because the P_j are prime, it follows that P_i is one of the $P_1, \ldots, P_k$. □

Let I be an arbitrary fractional ideal of R. Then I is contained in only finitely many prime ideals P. Then the image I_P of I in R_P has the form $A_P = (PR_P)^{\nu_P(I)}$, where $\nu_P(I)$ is an integer. This is true because R_P is a discrete valuation ring, and PR_P is the nonzero prime ideal of R_P.

Proposition 5.5. *Let R be an integral domain with field of fractions K. Then every fractional ideal $I \subseteq K$ can be written uniquely in the form $I = \prod_P P^{\nu_P(I)}$.*

Proof. Let $I \subseteq K$ be a fractional ideal of R, and then I_P is a fractional ideal of R_P, and $I_P = (PA_P)^{\nu_P(I)}$. By Theorem (5.6), $\nu_P(I) = 0$ for all but finitely many prime ideals P. Let $I' = \prod_P P^{\nu_P(I)}$, and then for any prime ideal $Q \subseteq R$, we have $I'_Q = \prod_P P_Q^{\nu_P(I)}$. Now either $P = Q$, or $P \neq Q$, in which case $P_Q = R_Q$. Then $I'_Q = Q_Q^{\nu_Q(I)} \prod_{P \neq Q} R_Q^{\nu_P(I)} = Q_Q^{\nu_Q(I)} = I_Q$. Because this is true for all prime ideal $Q \subseteq R$, it follows that $I' = I$.

To prove that the factorization $I = \prod_{P_i} P_i^{\nu_{P_i}(I)}$ into prime ideals is unique, note that $\nu_P(\prod_{P_i} P_i^{\nu_{P_i}(I)}) = \nu_P(I)$. Suppose that there were another factorization $I = \prod_{P_i} P_i^{a_i}$, where $a_j \neq \nu_{P_j}(I)$ for some P_j. Then $I_{P_j} = (P_j R_{P_j})^{\nu_{R_j}(I)} \neq (P_j R_{P_j})^{a_j} = (\prod_{P_i} P_i^{a_i})_{P_j}$, thus $I \neq \prod_{P_i} P_i^{a_i}$. □

Now let R be an integral domain, and let K be its field of fractions. Let L be a finite extension of K, and then we define the integral closure of R in L to be the set of elements $x \in L$ such that x is integral over R.

Proposition 5.6. *If $R \subseteq R'$ and $\alpha, \beta \in R'$ are integral over R, then $\alpha + \beta$ and $\alpha\beta$ are integral over R.*

If $\alpha, \beta \in R'$ are integral over R, then $R[\alpha]$ is a finitely generated R-module and $R[\alpha, \beta]$ is a finitely generated $R[\alpha]$-module, thus $R[\alpha, \beta]$ is a finitely generated R-module. Because $\alpha + \beta, \alpha\beta \in R[\alpha, \beta]$, it follows that $\alpha + \beta$ and $\alpha\beta$ are integral over R.

Theorem 5.7. *Let R be an Noetherian integrally closed domain with field of fractions K, let L be a separable extension of K of degree n, and let B be the integral closure of R in L. Then B is a finitely generated R-module.*

Proof. One can think of L as a vector space over K, and multiplication by $x \in L$ as a linear transformation on K. Let $\phi : L \mapsto K$ be the trace map for this transformation, and then $\phi(xy)$ is a symmetric non-degenenerate bilinear form on L (see Bourbaki, Commutative Algebra, Chapter 6, Proposition 10.12). If $x \in B$, then the conjugates of x with respect to the Galois group of L/K are integral over R, and their sum is $\phi(x)$. So $\phi(x) \in B$, and because $\phi(x) \in K$, it follows that $\phi(x) \in R$.

Now let $(e_1, \ldots, e_n)$ be a basis for L over K, with $e_i \in B$ for $1 \leq i \leq n$, and let V be the R-module generated by $(e_1, \ldots, e_n)$. To prove that we can have $e_i \in B$, let

$x \in L$, and then x satisfies some polynomial equation $x^n + \frac{a_{n-1}}{b_{n-1}}x^{n-1} + \ldots + \frac{a_0}{b_0} = 0$, where $a_i, b_i \in R$. Let $b = b_0 \ldots b_{n-1}$, and then $(bx)^n + \frac{a_{n-1}b}{b_{n-1}}(bx)^{n-1} + \ldots + \frac{a_0 b^n}{b_0} = b^n(x^n + \frac{a_{n-1}}{b_{n-1}}x^{n-1} + \ldots + \frac{a_0}{b_0}) = 0$, and the coefficients are in R, so $bx \in B$.

Let B^* be the R-module of the $x \in L$ such that $\phi(xy) \in R$ for all $y \in B$, and define V^* similarly. Then clearly $V \subseteq B$, and $B \subseteq B^*$ because $\phi(x) \in R$ for all $x \in B$. Also, $B^* \subseteq V^*$, because $\phi(xy) \in R$ for all $y \in B$ implies $\phi(xy) \in R$ for all $y \in V$. However, the dimension of V^* over R is finite, thus B is finitely generated. □

Theorem 5.8. *If R is Dedekind, then B is Dedekind.*

Proof. Because B is finitely generated as an R-module, it is Noetherian, and B is also integrally closed by transitivity of integrality. Now all we need is to show that all prime ideals of B are maximal, and then by Theorem (4.1) it follows that B is Dedekind. Observe that if $P \cap R = Q \cap R$ for prime ideals $P, Q \subseteq B$, then $P = Q$. To prove this, we can look at the quotient B/P instead, so we can assume that $P = 0$, and that Q contains a nonzero element x. Let $x^n + \ldots + a_0 = 0$ be the minimal equation for x, and then $a_0 \neq 0$, and $a_0 \in xB \subseteq Q \cap R = P \cap R$, which is a contradiction. So $Q \subseteq P$, and by repeating the same proof but switching P and Q, we obtain $P \subseteq Q$, so $P = Q$.

Then if $P_0 \subset P_1 \subset P_2$ is a chain of increasing prime ideals, it follows that $P_0 \cap R \subset P_1 \cap R \subset P_2 \cap R$ is an increasing chain of prime ideals, which is a contradiction. □

Corollary 5.9. *The integral closure of $\mathbb{Z}$ in any algebraic extension of $\mathbb{Q}$ is Dedekind. In particular, the integral closure of any quadratic number field, as described in Example 5.8, is Dedekind.*

Definition 5.10. A fractional ideal $I \subseteq K$ is principal if $I = xR$ for some $x \in K$.

Proposition 5.11. *The set of principal fractional ideals form a normal subgroup of the ideal group.*

Proof. Let G be the ideal group, and let N be the subset of principal fractional ideals. Then N is a subgroup of G, because $(xR)(yR) = xyR$ and $(R : xR) = x^{-1}R$. □

The quotient group G/N is called the ideal class group. For the rest of the paper, we will look at the ideal class group pf the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$, where d is a squarefree integer and $d < 0$. Note that $\mathbb{Q}(\sqrt{d})$ is called an imaginary quadratic number field. We will prove that the ideal class group is finite, but to accomplish this, we must first prove some additional theorems.

Proposition 5.12. *Let $R = \mathbb{Z}$ so that $K = \mathbb{Q}$, and let $L = \mathbb{Q}(\sqrt{d})$ for some square-free integer d. Then the integral closure of R in L is $\{a + b\sqrt{d} | a, b \in \mathbb{Z}\}$ if $d \equiv 2, 3 \pmod 4$ and $\{a + b(\frac{1+\sqrt{d}}{2}) | a, b \in \mathbb{Z}\}$ if $d \equiv 1 \pmod 4$.*

Proof. If $\alpha = a + b\sqrt{d}$ where $a, b \in \mathbb{Z}$, then $(\alpha - a)^2 - b^2 d = (b\sqrt{d})^2 - bd^2 = 0$, thus α satisfies the monic polynomial $(x - a)^2 - b^2 d$. If $d \equiv 1 \pmod 4$ and $\alpha = \frac{a+b\sqrt{d}}{2}$ where a and b are odd, then $a^2, b^2 d \equiv 1 \pmod 4$, thus there exists $n \in \mathbb{Z}$ such that $4n = a^2 - b^2 d$. Then the solutions to the equation $x^2 - ax + n = 0$ are $x = \frac{a \pm \sqrt{a^2 - 4n}}{2} = \frac{a \pm b\sqrt{d}}{2}$.

Conversely, suppose that $\alpha = a + b\sqrt{d}$ is integral over $\mathbb{Z}$, where $a, b \in \mathbb{Q}$. Then the irreducible polynomial for α in $\mathbb{Q}[x]$ is $x^2 - 2ax + a^2 - b^2 d$. Then the coefficients $2a$ and $a^2 - b^2 d$ must be in $\mathbb{Z}$, so there are two cases: either $a \in \mathbb{Z}$ or $a \in \mathbb{Z} + \frac{1}{2}$. In the first case, d is squarefree, so we must have $b \in \mathbb{Z}$. In the second case, we have $4a^2 \equiv 1 \pmod 4$, and $4a^2 - 4b^2 d \equiv 0 \pmod 4$, so $4b^2 d \equiv 1 \pmod 4$. Because d is squarefree, $2b$ must be an odd integer, and $d \equiv 1 \pmod 4$. □

Theorem 5.13. *Let R be the integral closure of $\mathbb{Z}$ in an imaginary quadratic field $\mathbb{Q}(\sqrt{d})$, and then for every ideal $I \subseteq R$, the product $I\bar{I}$ is a principal ideal generated by an integer, where $\bar{I}$ is the ideal of complex conjugates of elements of I.*

Proof. Let $\alpha, \beta \in I$ be generators for I, and then $\bar{\alpha}, \bar{\beta}$ generate $\bar{I}$. Then the elements $\alpha\bar{\alpha}, \alpha\bar{\beta}, \beta\bar{\alpha}, \beta\bar{\beta}$ generate $I\bar{I}$. Note that $\alpha\bar{\alpha}, \beta\bar{\beta}, \alpha\bar{\beta} + \beta\bar{\beta}$ are elements of $\mathbb{Z}$. Let n be their greatest common divisor in $\mathbb{Z}$, and then n is a linear combination of $\alpha\bar{\alpha}, \beta\bar{\beta}, \alpha\bar{\beta} + \beta\bar{\beta}$, thus $n \in I\bar{I}$ and $(n) \subseteq I\bar{I}$. Also, n divides $\alpha\bar{\alpha}, \beta\bar{\beta}$, thus $\alpha\bar{\alpha}, \beta\bar{\beta} \in (n)$. Also, $(\alpha\bar{\beta})/n, (\beta\bar{\alpha})/n$ are the roots of $x^2 + \frac{\alpha\bar{\beta}+\beta\bar{\alpha}}{n}x + \frac{\alpha\bar{\alpha}\beta\bar{\beta}}{n^2} = 0$, and thus are algebraic integers, so $\alpha\bar{\beta}, \beta\bar{\alpha} \in (n)$. It follows that $I\bar{I} = (n)$. □

Note that the integral closure R of $\mathbb{Z}$ in an imaginary quadratic number field can be thought of as a lattice in $\mathbb{R}^2$, and the ideals of R can be thought of as sublattices.

Definition 5.14. For any lattice $L \subseteq \mathbb{R}^2$, we define $\Delta(L)$ be the area of the parallelogram spanned by a lattice basis for L. It is easy to verify that the area is the same no matter what lattice basis is used.

Proposition 5.15. *If L is the integral closure of $\mathbb{Z}$ in an imaginary quadratic number field $\mathbb{Q}(\sqrt{d})$, then $\Delta(L) = \sqrt{|d|}$ if $d \equiv 2, 3 \pmod 4$ and $\Delta(L) = \frac{\sqrt{|d|}}{2}$ if $d \equiv 1 \pmod 4$.*

Proof. Recall from Proposition (5.6) that $L = \{a + b\sqrt{d} | a, b \in \mathbb{Z}\}$ if $d \equiv 2, 3 \pmod 4$ and $L = \{a + b(\frac{1+\sqrt{d}}{2}) | a, b \in \mathbb{Z}\}$ if $d \equiv 1 \pmod 4$. In the first case, $(1, \sqrt{d})$ is a lattice basis for L, and the parallelogram spanning the lattice basis has area $\sqrt{|d|}$. In the second case, $(1, \frac{1+\sqrt{d}}{2})$ is a lattice basis for L, and the parallelogram spanning the lattice basis has area $\frac{\sqrt{|d|}}{2}$. □

The next theorem is important to our proof that the ideal class group is finite. First we introduce two definitions: a set $S \subseteq \mathbb{R}^2$ is centrally symmetric if $p \in S$ implies $-p \in S$, and S is convex if $p, q \in S$ implies $pt + q(1-t) \in S$ for all $0 < t < 1$.

Theorem 5.16. *(Minkowski's Lemma): Let L be a lattice in $\mathbb{R}^2$, and let S be a bounded, convex, centrally symmetric subset of $\mathbb{R}$ that contains no lattice points other than 0. Then the area of S is at most $4\Delta(L)$.*

Proof. Define $U = \{\frac{1}{2}p | p \in S\}$, and then we prove that the area of U is at most $\Delta(L)$. Assume for the sake of contradiction that the area of U is greater than $\Delta(L)$.

Lemma 5.17. *There exists an element $\alpha \in L$ such that U and $U + \alpha$ are not disjoint.*

Proof. Let P be the parallelogram spanned by the lattice basis for L. Then because U is bounded, there are only finitely many $a_i \in L$ such that U and $P + \alpha_i$ are not disjoint. Let $U_i = (P + \alpha_i) \cap U$, and then the U_i are disjoint and $U = \cup U_i$, so $\text{Area}(U) = \sum \text{Area}(U_i)$. Also, if $V_i = U_i - \alpha_i$, then $V_i \in P$. However, $\sum \text{Area}(V_i) =$

$\sum \text{Area}(U_i) = \text{Area}U > \Delta(L)$, so there must exist $i \neq j$ such that V_i and V_j are not disjoint. Then $U - \alpha_i$ and $U - \alpha_j$ are not disjoint, thus U and $U + \alpha_i - \alpha_j$ are not disjoint. □

Continuing with the proof of the theorem, choose $\alpha \in L$ such that U and $U + \alpha$ are not disjoint, and let $p \in U \cap (U + \alpha)$. Then $p - \alpha \in U$, thus $\alpha - p \in U$ by central symmetry. By convexity, $\frac{1}{2}\alpha = \frac{1}{2}p + \frac{1}{2}(\alpha - p) \in U$, thus $\alpha \in S$, which is a contradiction. □

Theorem 5.18. *Let L be a lattice in $\mathbb{R}^2$, and then there exists $\alpha \in L$ such that $|\alpha|^2 \leq \frac{4\Delta(L)}{\pi}$.*

Proof. Let $S(r)$ be the circle of radius r around the origin. If $\pi r^2 > 4\Delta(L)$, then S contains a nonzero lattice point $\alpha \in L$. Then for all $\epsilon > 0$, there exists $\alpha \in L$ such that $|\alpha|^2 < \frac{4\Delta(L)}{\pi} + \epsilon$. Because this is true for all $\epsilon > 0$ and $S(r)$ only contains finitely many lattice points, it follows that there exists $\alpha \in L$ such that $|\alpha|^2 \leq \frac{4\Delta(L)}{\pi}$. □

Now let R be the integral closure of $\mathbb{Z}$ in an imaginary quadratic number field $\mathbb{Q}(\sqrt{d})$. Then for ideals $I \subseteq J \subseteq R$, we define $[J : I]$ to be the number of additive cosets of I in J. It is clear that $[J : I] = \frac{\Delta(I)}{\Delta(J)}$, and it follows that $[R : I] = [R : J][J : I]$.

For any ideal $I \subseteq R$, we can also define $N(I) = n$, where $I\bar{I} = (n)$. Note that $N(IJ) = N(I)N(J)$, because $(N(IJ)) = IJ\bar{I}\bar{J} = I\bar{I}J\bar{J} = (N(I))(N(J)) = (N(I)N(J))$.

Theorem 5.19. *For any ideal $I \subseteq R$, we have $[R : I] = N(I)$.*

Proof. We first prove the theorem for prime ideals $P \subset R$, and we also prove that for any nonzero ideal $I \subseteq R$, we have $[R : IP] = [R : I][R : P]$. There are two cases (see Artin, Chapter 11, Proposition 9.1): either there is a prime integer $p \in \mathbb{Z}$ such that $P = (p)$, or there is a prime integer $p \in \mathbb{Z}$ such that $P\bar{P} = (p)$.

Lemma 5.20. *Let $I \subseteq R$ be any ideal, and then for all $n \in \mathbb{Z}$, we have $[R : nI] = n^2[R : I]$.*

Proof. Note that $\Delta(nI) = n^2\Delta I$, so $[I : nI] = \frac{\Delta(nI)}{\Delta(I)} = n^2$. Then $[R : nI] = [R : I][I : nI] = n^2[R : I]$. □

Returning to the original theorem, in the first case, we have $N(P) = p^2$ and $IP = pI$. Then by the previous lemma, $[R : P] = p^2[R : pR] = p^2 = N(P)$ and $[R : IP] = p^2[R : I] = [R : I][R : P]$. In the second case, $N(P) = p$. Also, the chain of ideals $A \subset IP \subset IP\bar{P} = pI$ is increasing, thus $[R : I] < [R : IP] < [R : pI] = p^2[R : I]$. Also, $[R : IP] = [R : I][I : IP]$, thus $[R : I]$ is a proper divisor of $[R : IP]$, so we must have $[R : IP] = p[R : I]$. If we let $I = R$, then $[R : P] = p[R : R] = p = N(P)$. Then $[R : IP] = p[R : I] = [R : I][R : P]$.

For the general case, recall that every nonzero ideal $I \subseteq R$ can be uniquely factored in prime ideals, so $I = P_1 \dots P_n$, so we induct on n. For the base case $n = 1$, we already proved that $[R : P] = N(P)$. Now assume that $[R : P_1 \dots P_n] = N(P_1 \dots P_n)$, and then $[R : P_1 \dots P_n P_{n+1}] = [R : P_1 \dots P_n][R : P_{n+1}] = N(P_1 \dots P_n)N(P_{n+1}) = N(P_1 \dots P_n P_{n+1})$. □

Theorem 5.21. *Let $\mu = 2\sqrt{|D|}\pi$, where $D = 4d$ if $d \equiv 2, 3 \pmod 4$ and $D = d$ if $d \equiv 1 \pmod 4$, and then every ideal class contains an ideal I such that $N(I) \leq \mu$.*

Proof. Let $I \subseteq R$ be an ideal. Then there exists $\alpha \in I$ such that $N(\alpha) \leq \frac{4\Delta(I)}{\pi}$. Then $(\alpha) \subseteq I$, which implies that $IJ = (\alpha)$ for some ideal $J \subseteq R$. Then $N(I)N(J) = N(\alpha) \leq \frac{4\Delta(I)}{\pi}$. Also, $\Delta(I) = [R : I]\Delta(R) = \frac{1}{2}N(I)\sqrt{|D|}$, thus substituing we have $N(I)N(J) \leq 2I\sqrt{|D|}\pi$, thus $N(J) \leq 2\sqrt{|D|}\pi = \mu$. Also, IJ is a principal ideal, thus the classes of I and J are inverses in their ideal class group. By pairing elements of the ideal class group with their inverses, it follows that every ideal class contains an ideal I such that $N(I) \leq \mu$. □

Theorem 5.22. *If R is the integral closure of $\mathbb{Z}$ in an imaginary quadratic number field $\mathbb{Q}(\sqrt{d})$, then the ideal class group of R is finite.*

Proof. Because of Theorems (5.19) and (5.21), it is enough to show that there are finitely many ideals $I \subseteq R$ with index $[R : I] \leq \mu$. Let $I \subseteq R$ be an ideal such that $[R : I] = n$, where $n \leq \mu$, and then R/I is an abelian group of order n, so $nR \subseteq I$. Then by translation, if $\alpha \in I$ then $\alpha + n\beta \in I$ for all $\beta \in R$. Then for any equivalence classes $\bar{\alpha} \in R/nR$, either all the elements of $\bar{\alpha}$ or none of its elements are in I. Since there are only n^2 equivalence classes in R/nR, there are only a finite number of choices for I, and since there are also a finite number of choices for n, this completes the proof. □

Acknowledgments. It is a pleasure to thank my mentor, Robin Walters, for providing me with assistance in writing my paper.

References

[1] Artin, Michael. Algebra. Upper Saddle River, New Jersey: Prentice-Hall, Inc., 1991.
[2] Atiyah, M. F. Introduction to Commutative Algebra. Great Britain: Addison-Wesley Publishing Company, Inc., 1969.
[3] Bourbaki, Nicolas. Commutative Algebra. New York, New York: Springer-Verlag. 1989.
[4] Jean-Pierre Serre. Local Fields. Trans. Greenberg, Martin. New York, New York: Springer-Verlag. 1979.