DEDEKIND DOMAINS AND IDEAL CLASS GROUPS

Darren Yao

ABSTRACT

In this paper, we explore the different types of domains, which are special subclasses of rings that have many interesting properties about divisibility, factorization, and generation of ideals. This leads to the study of Dedekind domains, where we prove several important results. In the third section, we investigate the ideal class group and the finiteness of the class number of an algebraic number field. Finally, we conclude with an application to elliptic curve cryptography.

In this paper, unless stated otherwise, all rings are assumed to be commutative and contain an identity.

1 Types of Domains

We start by connecting commutative rings to fields with the following chain of subclass inclusions:

> commutative rings $\subset$ integral domains $\subset$ integrally closed domains $\subset$ GCD domains $\subset$ unique factorization domains $\subset$ principal ideal domains $\subset$ Euclidean domains $\subset$ fields.

In this first section, we look at each of the types of domains and provide some examples of each.

Integral domains are essentially a general form of ring that holds an important property of the integers.

Definition 1.1. An **integral domain** A is a ring with no nontrivial zero divisors. Equivalently, $ab = 0$ implies either $a = 0$ or $b = 0$, and if $a \neq 0$ then $ab = ac$ implies $b = c$.

In an integral domain, divisibility makes some sort of sense, although not in the way that one might expect. For two elements a, b in ring R, we say that a divides b if there exists another element c such that $ac = b$. Two elements divide each other if and only if there exists an invertible element u such that $a = ub$. In this case, we say that a and b are **associated**.

Proposition 1.2. *Two associated elements generate the same principal ideal.*

Proof. By the definition of associated elements, we have $a = ub$ and $b = va$ for elements u and v. This means that $a \in (b)$ and $b \in (a)$. Thus, $(a) \subset (b)$ and $(b) \subset (a)$, so $(a) = (b)$. ■

Related to (and a specific type of) integral domains are the integrally closed domains.

Definition 1.3. Given a ring R its **field of fractions** K is the localization such that all nonzero elements of R are invertible. Specifically, every element of K can be written as $\frac{a}{b}$ where $a, b \in R$ and $b \neq 0$.

Example. The field of fractions of the integers $\mathbb{Z}$ is the rationals $\mathbb{Q}$.

Example. The field of fractions of any field is the field itself.

Definition 1.4. An **integrally closed domain** A is a ring which is integrally closed in its field of fractions. In other words, every integral element in the field of fractions of A, belongs to A.

Example. The quadratic integers $\mathbb{Q}[\sqrt{-5}]$ are integrally closed, because every root of a monic polynomial with coefficients in $\mathbb{Q}[\sqrt{-5}]$ is contained in $\mathbb{Q}[\sqrt{-5}]$. More generally, this property holds for $\mathbb{Q}[\sqrt{d}]$ for $n = 2, 3 \pmod 4$.

Now we move on to the GCD domain, which is essentially what it seems like: the GCD of any two elements is well-defined.

Definition 1.5. A **GCD domain** is an integral domain such that there is a unique principal ideal containing the ideal generated by any two elements.

The element generating the unique principal ideal is considered the GCD of the two original elements.

Definition 1.6. An **algebraic integer** is a complex number that is the root of a monic polynomial with integer coefficients.

Example. The set of algebraic integers $\overline{\mathbb{Z}}$ is a GCD domain.

One important property of the GCD domain is that every irreducible element is prime.

Definition 1.7. A **unique factorization domain (UFD)** is a ring where every element can be written as a product of prime elements in exactly one way, up to units.

Example. The integers $\mathbb{Z}$ are a UFD because of the Fundamental Theorem of Algebra.

Example. The polynomial ring of a field $F[x_1, x_2, \cdots x_n]$ is a UFD

Nonexample. $\mathbb{Z}[\sqrt{5}]$ is not a UFD because $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

Nonexample. This also fails for the algebraic integers in general $\overline{\mathbb{Z}}$. Since for any $a \in \overline{\mathbb{Z}}$, we can factor a as $\sqrt{a} \cdot \sqrt{a}$, factorizations are not unique, so $\overline{\mathbb{Z}}$ is not a UFD.

Definition 1.8. A **principal ideal domain** is an integral domain where every ideal is principal (generated by a single element).

Example. $\mathbb{Q}[x]$, the polynomials in x with rational coefficients

Nonexample. The multivariable polynomials $K[x_1, x_2, \cdots x_n]$ are not a PID because $\langle x_1, x_2 \rangle$ is not principal.

Theorem 1.9. *All principal ideal domains are unique factorization domains.*

Proof. Suppose an element in a PID can be factored two different ways into irreducibles, $p_1 \cdots p_m$ and $q_1 \cdots q_n$, where WLOG $n \geq m$.

Since p_1 is irreducible, it is prime. Since p_1 divides the product on the right, it must also divide one of the factors q_i (easily shown by induction). Without loss of generality, suppose it divides q_1. We can write $q_1 = p_1 a_1$ and divide both sides by p_1 (which we are allowed to do because PIDs are integral domains). This leaves us with

$$p_2 \cdots p_m = a_1 q_2 \cdots q_m$$

If we continue until we run out of p_i's, we end up with

$$1 = a_1 \cdots a_m \cdot q_{m+1} \cdots q_n$$

This means that the $q_{m+1} \cdots q_n$, if they exist, must be units. However, since irreducible elements can't be units, we have $m = n$. Hence, the factorization must be unique, because all p_i and q_i are irreducible. ■

The converse is not true. The multivariable polynomials $K[x_1, x_2, \cdots x_n]$ are a UFD but not a PID, as shown above.

Definition 1.10. A **Euclidean domain** is an integral domain R with a function f from the nonzero elements of R to the nonnegative integers satisfying the following properties:

- $f(a) \leq f(ab)$ for all nonzero $a, b \in R$
- for all $a, b \in R$ such that $b \neq 0$ there exist $q, r \in R$ such that $a = bq + r$ and $r = 0$ or $f(r) < f(b)$.

The Euclidean function f is not part of the definition of the Euclidean domain, because in general, a Euclidean domain can have many different Euclidean functions. It is only necessary for a suitable Euclidean function to exist.

Example. The Gaussian integers $\mathbb{Z}[i]$ are a Euclidean domain, where the function f is simply the norm of the Gaussian integer: $f(a + bi) = a^2 + b^2$

Nonexample. $\mathbb{Q}[\sqrt{-19}]$ is a PID but not a Euclidean domain.

Remark 1.11. An important problem in algebraic number theory asks when the quadratic integers $a + b\sqrt{d}$ are a Euclidean domain for the function of the algebraic norm. It turns out that this is the case only when $d \in \{-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}$

2 Dedekind Domains

Now, we get to the main topic of the paper, Dedekind domains, which are one of the most important topics in algebraic number theory. The applications of Dedekind domains include analyzing quadratic forms, localizations of Noetherian rings, and even elliptic curves. First, we need to start by defining it:

Definition 2.1. A **Dedekind domain** is an integrally closed domain A satisfying the following properties:

- A is Noetherian
- every nonzero prime ideal in A is maximal

Example. The most trivial example of a Dedekind domain is the integers.

Example. The integral closure of a ring over any finite degree extension of its fraction field is a Dedekind domain.

Definition 2.2. The **Krull dimension** of a ring is the maximum length of an increasing chain of prime ideals.

Corollary 2.3. *Dedekind domains have Krull dimension 1.*

Now, we introduce the concept of fractional ideals, which essentially act as inverses to integral ideals (what we think of as normal ideals).

Definition 2.4. In a ring A, a **fractional ideal** $\mathfrak{a}$ is a set of elements in A such that for some $d \in A$, $d\mathfrak{a}$ is an integral ideal.

Example. An example of a fractional ideal is $\frac{p}{q} \cdot \mathbb{Z}$ for relatively prime $p, q \in \mathbb{Z}$.

Definition 2.5. A **principal fractional ideal** is a fractional ideal with a single generator.

The above example is also an example of a principal fractional ideal, because it is generated by $(\frac{p}{q})$.

One of the most important theorems about Dedekind domains is the existence and uniqueness of ideal factorization. First, we prove some preliminary results:

Theorem 2.6. *In a Dedekind domain A, the set of prime ideals containing an element $a \in A$ is finite.*

Proof. Let I_A be the group of ideals of A, then we look at the following subsets:

- $S := I \in I_A : (a) \subseteq I \subseteq A$
- $T := I \in I_A : A \subseteq I \subseteq (a)^{-1}$

We can look at the following bijections:

- $\phi_1 : S \to T : I \to I^{-1}$
- $\phi_2 : T \to S : I \to aI$

Since S and T are nonempty and partially ordered, ϕ_1 is order-reversing and ϕ_2 is order-preserving. Thus the composition $\phi = \phi_2 \cdot \phi_1$ is also order-reversing. Before and after applying ϕ, S satisfies the ascending and descending chain conditions, respectively.

Now we can proceed by contradiction. Suppose there are infinitely many distinct prime ideals that contain a, which we call $\mathfrak{p}_1, \mathfrak{p}_2, \ldots$.

Then, we have

$$\mathfrak{p}_1 \supseteq \mathfrak{p}_1 \cap \mathfrak{p}_2 \supseteq \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{p}_3 \supseteq \cdots$$

which is a descending chain of ideals. By DCC, this must stabilize at some n, meaning

$$\mathfrak{p}_1 \cdots \mathfrak{p}_{n-1} \subseteq \mathfrak{p}_1 \cap \cdots \cap p_{n-1} = \mathfrak{p}_1 \cap \cdots \cap p_n \subseteq \mathfrak{p}_n$$

Since $\mathfrak{p}_n$ contains $\mathfrak{p}_1 \cdots \mathfrak{p}_n$, it must contain at least one of the $\mathfrak{p}_i$'s for some i, by definition of prime ideal. This implies the existence of a chain $(0) \subsetneq p_i \subsetneq p_n$ of length 2, violating $dim(A) \leq 1$, a contradiction. ■

Corollary 2.7. *The number of prime ideals of a Dedekind domain A that contain any given nonzero ideal I is finite.*

Proof. The proof follows trivially from the previous lemma by taking some element $a \in I$. ■

Definition 2.8. A **discrete valuation** is a function v from a field K to the integers satisfying the following conditions:

- $v(x \cdot y) = v(x) + v(y)$
- $v(x + y) \geq min(v(x), v(y))$

- $v(x) = \infty$ if and only if $x = 0$

We define the discrete valuation on a prime ideal $\mathfrak{p}$ as a subset of the image of the discrete valuation function from the minimal field.

Lemma 2.9. *Let $\mathfrak{p}$ be a nonzero prime ideal in a Dedekind domain A. If I is an ideal of A then $v_p(I) = 0$ if and only if $\mathfrak{p}$ does not contain I. If $\mathfrak{q}$ is a nonzero prime ideal different from $\mathfrak{p}$, then $v_\mathfrak{q}(\mathfrak{p}) = v_\mathfrak{p}(\mathfrak{q}) = 0$*

Proof. If $I \subseteq \mathfrak{p}$ then $v_\mathfrak{p}(I) \geq v_\mathfrak{p}(\mathfrak{p}) = 1$ is nonzero. If $I \subsetneq \mathfrak{p}$ then pick $a \in I - \mathfrak{p}$. Then, $0 = v_\mathfrak{p}(a) \geq v_\mathfrak{p}(I) \geq v_\mathfrak{p}(A) = 0$ because $(a) \subseteq I \subseteq A$. The prime ideals $\mathfrak{p}$ and $\mathfrak{q}$ are nonzero and maximal by definition of a Dedekind domain, so neither contains the other and $v_\mathfrak{q}(\mathfrak{p}) = v_\mathfrak{p}(\mathfrak{q}) = 0$. ■

Corollary 2.10. *Let A be a Dedekind domain with fraction field K. For each nonzero fractional ideal I we have $v_\mathfrak{p}(I) = 0$ for all but finitely many prime ideals $\mathfrak{p}$. In particular, if $x \in K^\times$ then $v_\mathfrak{p}(x) = 0$ for all but finitely many $\mathfrak{p}$.*

With these two lemmas, we can finally prove our main result.

Theorem 2.11. *Let A be a Dedekind domain. The ideal group I_A of A is the free abelian group generated by its nonzero prime ideals $\mathfrak{p}$. The isomorphism*

$$I_A \simeq \bigoplus_\mathfrak{p} \mathbb{Z}$$

is given by the inverse maps

$$I \to (\cdots, v_p(I), \cdots$$

$$\prod_\mathfrak{p} \mathfrak{p}^{e_\mathfrak{p}} \leftarrow (\cdots e_p \cdots)$$

Proof. By Corollary 2.10, the first map is well defined because there are only finitely many nonzero $v_\mathfrak{p}(I)$ terms. Since $I \to v_\mathfrak{p}(I)$ and $e_\mathfrak{p} \to \mathfrak{p}^{e_\mathfrak{p}}$ are group homomorphisms for nonzero prime ideals $\mathfrak{p}$, the maps in the theorem are also group homomorphisms. It remains to prove that the homomorphisms are injective and surjective.

For injectivity, if $v_\mathfrak{p}(I) = v_\mathfrak{p}(J)$ then $I_\mathfrak{p} = J_\mathfrak{p}$, and if this holds for every $\mathfrak{p}$ then $I = \bigcap_\mathfrak{p} I_\mathfrak{p} = \bigcap_\mathfrak{p} J_\mathfrak{p} = J$.

For surjectivity, by Lemma 2.9, for any vector $(\cdots e_\mathfrak{p} \cdots)$ in the image, we have

$$v_\mathfrak{q}(\prod_\mathfrak{p} \mathfrak{p}^{e_\mathfrak{p}}) = \sum_\mathfrak{p} e_\mathfrak{p} v_\mathfrak{q}(\mathfrak{p}) = e_\mathfrak{q}$$

This means that $\prod_\mathfrak{p} \mathfrak{p}^{e_\mathfrak{p}}$ is the preimage of $(\cdots e_\mathfrak{p} \cdots)$. Furthermore, the two maps are inverses of each other. ■

Corollary 2.12 (Unique factorization of ideals)**.** *Every proper nonzero ideal of a Dedekind domain can be written in the form $\prod_{i=1}^k \mathfrak{p}_1^{n_i}$ where the $\mathfrak{p}_i$ are distinct prime ideals and the n_i are positive integers, in exactly one way.*

Theorem 2.13. *In a Dedekind domain A, any integral ideal I can be generated by at most two elements.*

Proof. Take a nonzero element $r \in I$. Then, $I/(r)$ is an ideal of $A/(r)$ and therefore principal. Now, if $I + (s) \in (r)$, then $I = (r, s)$. ■

Theorem 2.14. *A Dedekind domain R is a principal ideal domain if and only if it is a unique factorization domain.*

Proof. Any PID is a UFD, as we showed in Theorem 1.9. Now, let R be a UFD, and let P be a prime ideal in R. Let a be a nonzero element of P. Then, there exists an irreducible factor t of a in P, so $(t) \subset P$. However, since $dim(R) = 1$, $(t) = P$. Thus every prime ideal is principal. Since every ideal is a product of prime ideals, every ideal is principal. ■

3 The Ideal Class Group

The ideal class group tells us a lot about algebraic integers. It also develops the subject of class field theory, which deals with Galois extensions of fields. One of the most important results is the Kronecker-Weber theorem, which states for any abelian extension $K/\mathbb{Q}$, there is a cyclotomic field containing K. In this section, we introduce properties of the class group and prove that the class group of an algebraic number field is finite.

Proposition 3.1. *The set of fractional ideals of a Dedekind domain A is an abelian group under ideal multiplication. The set of principal fractional ideals forms a subgroup of this group.*

Proof. Multiplication of fractional ideals is associative and commutative, inverses exist by definition, and (1) is the identity. Every principal fractional ideal (a) has an inverse $(1/a)$, and a product of principal ideals is principal, so they form a subgroup. ■

Definition 3.2. The **ideal class group** is the quotient of the group of fractional ideals $I(A)$ by the group of principal fractional ideals $P(A)$. $Cl(A) = I(A)/P(A)$. We will see soon that the order of this group is finite over algebraic number fields.

Definition 3.3. The **class number** is the order of the class group.

Definition 3.4. An **algebraic number field** F is a finite degree (equivalently, algebraic) field extension of the field of rational numbers $\mathbb{Q}$.

Definition 3.5. The norm $||I||$ of an ideal I in a ring R is the size of the quotient ring R/I.

Theorem 3.6. *Let K be a number field such that the ring R satisfies $R = \overline{\mathbb{Z}} \cap K$. Then, there exists a positive real number λ (depending on K) such that every nonzero ideal I of R contains a nonzero element α satisfying*

$$|N_{\mathbb{Q}}^{K}(\alpha)| \leq \lambda ||I||$$

Remark 3.7. Note that the value λ is independent of the ideal I, because otherwise this theorem is not very meaningful.

Proof. Fix an integral basis $\alpha_1, \cdots, \alpha_n$ for R and let $\sigma_1, \cdots, \sigma_n$ denote the embeddings of K in $\mathbb{C}$. (An embedding of a field F_1 in a larger field F_2 is a ring homomorphism such that $\sigma(F_1)$ is isomorphic to F_2). We claim that we can always take

$$\lambda = \prod_{i=1}^{n} \sum_{j=1}^{n} |\sigma_i \alpha_j|$$

For any ideal I, we let m be the unique positive integer such that

$$m^n \leq ||I|| \leq (m+1)^n$$

Now, consider the $(m+1)^n$ members of R

$$\sum_{j=1}^{n} m_j \alpha_j; m_j \in \mathbb{Z}; 0 \leq m_j \leq m$$

Since there are more than $||I||$ of these, two of them must be congruent modulo I. This means we can subtract them to get

$$\alpha = \sum_{j=1}^{n} m_j \alpha_j; m_j \in \mathbb{Z}; |m_j| \leq m$$

Finally, we have

$$|N_{\mathbb{Q}}^{K}(\alpha) = \prod_{i=1}^{n} |\sigma_i \alpha| \leq \prod_{i=1}^{n} \sum_{j=1}^{n} m_j |\sigma_i \alpha_j \leq m^n \lambda \leq ||I|| \lambda$$

■

Corollary 3.8. *There are only finitely many ideal classes in R. Thus, the class number of an algebraic number field is finite.*

Proof. Only finitely many ideals J can satisfy $||J|| \leq \lambda$ since this inequality restricts the possible prime divisors of J to a finite set, and bounds the powers of the ideals in the factorization. This is because

$$J = \prod P_i^{n_i} \rightarrow ||J|| = \prod ||P_i||^{n_i}$$

■

4 Applications to Elliptic Curve Cryptography

In this section we discuss applications of ideal class groups to cryptography.

Definition 4.1. An **isogeny** $\phi : E_1 \to E_2$ of elliptic curves is a non-constant morphism and group homomorphism with finite kernel.

Definition 4.2. An **endomorphism** of an elliptic curve E is an isogeny from E to itself. The endomorphisms form a ring.

Definition 4.3. Let E be an elliptic curve defined over a finite field F_q. Let $\mathcal{O}$ be the endomorphism ring of E, and let $\mathfrak{a} \in \mathcal{O}$ be an integral invertible ideal of norm coprime to q. We define the $\mathfrak{a}-$ **torsion subgroup** of E as

$$E[\mathfrak{a}] = \{P \in E | \alpha(P) = 0 \text{for all} \alpha \in \mathfrak{a}\}$$

We can now define the isogeny $\phi_{\mathfrak{a}} : E \to E_{\mathfrak{a}}$, where $E_{\mathfrak{a}} = E/E[\mathfrak{a}]$. Since $\mathfrak{a}$ is invertible, we can show that the endomorphism groups of E, $E_{\mathfrak{a}}$, and $\mathcal{O}$ are isomorphic. It can be further shown that the map $(\mathfrak{a}, E) \to E_{\mathfrak{a}}$ defines a group action of $Cl(\mathcal{O})$ on the set of elliptic curves.

Definition 4.4. An order $\mathcal{O}$ is a subring of a ring A such that:

- A is a finite dimensional algebra over $\mathbb{Q}$
- $\mathcal{O}$ is a free abelian group generated by a basis for A over $\mathbb{Q}$

Definition 4.5. An elliptic curve is said to have **complex multiplication** if there are nontrivial endomorphisms (i.e. endomorphisms generated by multiplying by complex numbers rather than just integers).

This leads to the main theorem of this section, which in turn allows us to define a cryptographic system.

Theorem 4.6. *Let F_q be a finite field, and let $\mathcal{O} \in Q[\sqrt{-d}]$ be an order in a quadratic imaginary field. Denote by $Ell_q(\mathcal{O})$ the set of elliptic curves defined over F_q with complex multiplication. Then, if $Ell_q(\mathcal{O})$ is nonempty, the class group acts freely and transitively over it. In other words, there is a map*

$$Cl(\mathcal{O}) \times Ell_q(\mathcal{O}) \to Ell_q(\mathcal{O})$$

$$(\mathfrak{a}, E) \to \mathfrak{a} \cdot E$$

such that $\mathfrak{a} \cdot (\mathfrak{b} \cdot E) = (\mathfrak{a}\mathfrak{b}) \cdot E$ for all $\mathfrak{a}, \mathfrak{b} \in Cl(\mathcal{O})$ and $E \in Ell_q(\mathcal{O})$ and such that for any $E, E' \in Ell_q(\mathcal{O})$ there is a unique $\mathfrak{a} \in Cl(\mathcal{O})$ such that $E' = \mathfrak{a} \cdot E$.

These properties form the basis for the isogeny based cryptosystem. While it is still vulnerable to attacks from quantum computers, it is still an improvement over other existing cryptosystems because it can use smaller keys to accomplish the same level of security. Therefore, the isogeny based cryptosystem is likely a good option for cryptography, at least for now.

References

[1] Milne, J. S.: Algebraic Number Theory. `https://www.jmilne.org/math/CourseNotes/ANT.pdf`

[2] Quinlan, Rachel: Ring Theory, NUI Galway `http://www.maths.nuigalway.ie/MA416/section4-2.pdf`

[3] Sutherland, Andrew: Number Theory I. Massachusetts Institute of Technology `https://math.mit.edu/classes/18.785/2018fa/LectureNotes2.pdf` `https://math.mit.edu/classes/18.785/2018fa/LectureNotes3.pdf`

[4] Goodman, Frederick M.: Algebra, Abstract and Concrete. `http://homepage.divms.uiowa.edu/~goodman/algebrabook.dir/book.2.6.pdf`

[5] Conrad, Keith: Remarks about Euclidean Domains. `https://kconrad.math.uconn.edu/blurbs/ringtheory/euclideanrk.pdf`

[6] Ikenaga, Bruce: Principal Ideal Domains and Unique Factorization Domains `http://sites.millersville.edu/bikenaga/abstract-algebra-2/pid-ufd/pid-ufd.pdf`

[7] May, J. P.: Notes on Dedekind Rings, University of Chicago `https://www.math.uchicago.edu/~may/MISC/Dedekind.pdf`

[8] Hegde, Milind: Algebraic Number Theory, TIFR VSRP `https://math.berkeley.edu/~mhegde/pdfs/algebraic_number_theory.pdf`

[9] Conrad, Brian: Finitely Generated Modules over a PID, I. Stanford University http://math.stanford.edu/~conrad/210APage/handouts/PIDGreg.pdf

[10] Marcus, Daniel: Number Fields

[11] De Feo, Luca; Mathematics of Isogeny Based Cryptography. Université de Versailles https://arxiv.org/pdf/1711.04062.pdf

[12] Galbraith, Steven: Isogeny Cryptography: Strengths, Weaknesses, and Challenges. University of Auckland, New Zealand https://www.math.auckland.ac.nz/~sgal018/adelaide.pdf

[13] Galbraith, Steven: Mathematics of Public Key Cryptography https://www.math.auckland.ac.nz/~sgal018/crypto-book/ch25.pdf

[14] Li, Chao: Endomorphism rings of elliptic curves. Columbia University http://www.math.columbia.edu/~chaoli/docs/MinorThesis1.html