ON DEDEKIND DOMAINS & THE IDEAL CLASS GROUP

AKASH DHIRAJ

ABSTRACT. Through the course of this paper, we introduce *Dedekind Domains* and present some important of properties of these structures. Of particular importance is the property that all ideals factor uniquely into the product of prime ideals (Theorem 3.3). We then return back to our original source of motivation and discuss the *Ideal Class Group* and its application in solving Diophantine equations.

1. SOME MOTIVATION

Suppose we hope to solve the Diophantine equation $x^2 - dy^2 = n$. The approach would be to factor n in $\mathbb{Z}[\sqrt{-d}]$, but $\mathbb{Z}[\sqrt{-d}]$ isn't necessarily a UFD (consider $d = -17$). It's close though. It's what we call a *Dedekind Domain*. Dedekind domains have the special property that ideals factor uniquely into the product of prime ideals. Using the factorization of (n) as an ideal, we can bypass the issue we had with $\mathbb{Z}[\sqrt{-d}]$ and recover all factorizations of n in $\mathbb{Z}[-d]$, allowing us to solve our Diophantine equation as usual. After some discussion of the *Ideal Class Group*, we further expand our repertoire of skills for solving Diphantine equations (See Section 6).

2. INTRODUCTION

As expected from an expository paper, we begin with a sequence of preliminary definitions, culminating in that of a *Dedekind Domain*.

Definition 2.1 (Noetherian)**.** We call a ring[1] R *Noetherian* if it satisifies one (and hence all) of the equivalent conditions:

(1) Every ideal of R is finitely generated;
(2) The ideals of R satisfy the *Ascending Chain Condition*: if $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ is an ascending chain of ideals of R, then there is some $N > 0$ such that if $m, n > N$, then $I_m = I_n$;
(3) If S is any nonempty collection of ideals of R, then S has a maximal element, i.e. there is some $I \in S$ such that if there exists $J \in S$ with $J \supseteq I$, then $I = J$;

Definition 2.2. Consider the subring S of R. An element $r \in R$ is said to be *integral* over S if r is the root of some monic $f(x) \in S[x]$. The set of integral elements over S, denoted $\overline{S}$, is the integral closure of S. We say a ring R is integrally closed if its integral closure in $\text{Frac}(R)$ is itself.

Proposition 2.1. *Let F be a field containing R. An element $x \in F$ is integral over R if and only if there exists a finitely generated R-submodule M of F such that $\alpha M \subseteq M$.*[2]

Date: July 10, 2020.

[1] Note that we use *'Ring'* to mean *'Commutative, Unitary Ring'*

[2] A proof of this can be found in any algebra textbook

Finally,

Definition 2.3 (Dedekind Domain)**.** An integral domain R (that is not a field) is said to be a *Dedekind Domain* if

(1) R is Noetherian,
(2) R is integrally closed,
(3) and every non-zero prime ideal is maximal.

Perhaps the most obvious example of a Dedekind domain is $\mathbb{Z}$. As $\mathbb{Z}$ is a PID, we note that every ideal is finitely generated (i.e. it's Noetherian), and all non-zero prime ideals are maximal. By application of the *Rational Root Theorem*, the integral closure of $\mathbb{Z}$ in $\mathbb{Q}$ is $\mathbb{Z}$.

Example 2.1. One can apply a similar argument to show a PID R is a Dedekind domain. Conditions (1) and (3) of Definition 2.3 follow directly from the definition of a PID. Condition (2) requires use of the fact that PIDs are UFDs and, hence, GCD Domains. Then, we employ what is essentially the Rational Root Theorem to note if $\frac{a}{b} \in \operatorname{Frac}(R)$ where $\gcd(a, b) \in R^{\times}$, then

$$\left(\frac{a}{b}\right)^n + a_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + a_0 = 0 \quad (a_i \in R \text{ for all } i = 0, \ldots, n-1)$$

implies $b \mid a^n$. b must then be a unit, and, hence, $\frac{a}{b} = ab^{-1} \in R$.

Example 2.1 lets us quickly conclude many rings are Dedekind domains: $R[x], \mathbb{Z}[i], \mathbb{Z}_{(2)}, \mathbb{Q}[[x]]$ to name a few.

Non-example 2.2. Consider a Dedekind domain R, with some prime element p. $R[x]$ satisfies Condition (1) of Definition 2.3 by *Hilbert's Basis Theorem*. Condition (2) may or may not be satisfied, but we can definitely say Condition (3) breaks as $(p) \subset (p, x)$. For a concrete non-example, consider $R = \mathbb{Z}$.

Dedekind domains are found in many places. We point out specific Dedekind domains in Geometry and Number Theory.

Example 2.3. From Geometry, consider the coordinate ring of the elliptic curve $y^2 - x^3 - x - 1$:

$$\mathcal{O}(V(y^2 - x^3 - x - 1)) = \frac{\mathbb{C}[x, y]}{(y^2 - x^3 - x - 1)}.$$

This ring is a Dedekind domain. As $y^2 - x^3 - x - 1$ is prime/irreducible[3], $\mathcal{O}(V(y^2 - x^3 - x - 1))$ is an integral domain. From Hilbert's Basis Theorem, $\mathcal{O}(V(y^2 - x^3 - x - 1))$ is Noetherian. Recall from Algebraic Geometry that $y^2 - x^3 - x - 1$ is smooth and, hence, normal, i.e. $\mathcal{O}(V(y^2 - x^3 - x - 1))$ is integrally closed. Lastly, we once again recall that, as a consequence of *Hilbert's Nullstellensatz*, subvarieties correspond to the prime ideals of $\mathcal{O}(V(y^2 - x^3 - x - 1))$. Since these subvarieties must be finite (the only infinite subvariety is the entire curve) and all finite subvarieties are single points, we conclude that all prime ideals are maximal.

Definition 2.4. $\alpha \in \mathbb{C}$ is said to be an *algebraic integer* if there exists monic $f \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$.

Example 2.4. Let K be a number field. An important example of a Dedekind domain in algebraic number theory is $\mathcal{O}_K$, the subring of algebraic integers in K. We omit the details, but instead provide a sketch. The result follows from noting

[3] Feel free to check this by writing $y^2 - x^3 - x - 1$ as the product of polynomials and making a degree argument

(1) For an ideal $\mathfrak{p} \subset \mathcal{O}_K$, $\mathcal{O}_K/\mathfrak{p}$ is finite;
(2) For a ring R, the integral closure $\overline{R}$ in $\text{Frac}(R)$ is integrally closed.

(1) implies $\mathcal{O}_K$ satisfies the Ascending Chain Condition. Choosing $\mathfrak{p}$ to be prime, we note $\mathcal{O}_K/\mathfrak{p}$ is a finite integral domain, i.e. a field. (2) allows use to conclude $\mathcal{O}_K$ is integrally closed as it's the integral closure of $\mathbb{Z}$ in K. See [Jac89, pp. 631 - 634] for a more rigorous treatment.

3. Properties of Dedekind Domains

One might wonder the extent to which the converse of Example 2.1 holds. Curiously, it turns out it does if we restrict to local rings.

Proposition 3.1. *Let R be a local Dedekind domains. Then, R is a principal ideals domain.*

Proof. For our proof, we require the notion of an *Annihilator*. For an R-module M, we define the annihilator of $m \in M$ as $\text{Ann}(m) := \{r \in R |\ rm = 0\}$. When m is non-zero, $\text{Ann}(m)$ is a proper ideal of R. For our purposes, we choose arbitrary non-zero, non-unit $c \in R$ and let $M = R/(c)$. Consider the set of ideals $S = \{\text{Ann}(m) |\ m \in M,\ m \neq 0\}$. As R is Noetherian, we may choose $m = b + (a)$ such that $\text{Ann}(m)$ is maximal in S. We hope to show $\text{Ann}(m)$ is prime. Striving for a contradiction, assume the opposite, i.e. there exists $x, y \in R$ such that $xy \in \text{Ann}(m)$ but $x, y \notin \text{Ann}(m)$. Then, let $m' = by + (a)$. As $\text{Ann}(m)$ is contained in $\text{Ann}(m')$ and $x \in \text{Ann}(m')$, we contradict the maximality of $\text{Ann}(m)$. Moving forward, we denote $\mathfrak{p} = \text{Ann}(m)$. Now, we start by showing $\mathfrak{p}$ is principal, using which we conclude that all other ideals are as well. We now work over $\text{Frac}(R)$.

(1) We first show $\frac{b}{a} \notin R$. If this wasn't the case, then $b = a \times \frac{b}{a} \in (a) \implies m = 0$ in $R/(c)$. This a violation of our definition of S.
(2) Next, we show $\frac{a}{b} \in R$, and, in fact, $\mathfrak{p} = \left(\frac{a}{b}\right)$. Using our definition of $\mathfrak{p}$, we note that $b\mathfrak{p} \subseteq (a)$. Then, the ideal $\frac{b}{a}\mathfrak{p} \subseteq R$. Assuming $\frac{b}{a}\mathfrak{p}$ is not the entire ring, we use that R is local to conclude that $\frac{b}{a}\mathfrak{p} \subseteq \mathfrak{p}$. As R is Noetherian, $\mathfrak{p}$ is finitely generated so we may employ Proposition 2.1 to conclude that $\frac{b}{a}$ is integral over R and, hence, $\frac{b}{a} \in R$ since R is integrally closed. Having contradicted (1), we conclude $\frac{b}{a}\mathfrak{p} = R$, i.e. $\mathfrak{p} = (\frac{a}{b})$.

Now, consider an arbitrary ideal $\mathfrak{q} \subset R$ and the chain

$$\mathfrak{q} \subseteq \mathfrak{q}\frac{b}{a} \subseteq \mathfrak{q}\left(\frac{b}{a}\right)^2 \cdots .$$

Suppose the chain stabilizes. Then, there exists n such that

$$\mathfrak{q}\left(\frac{b}{a}\right)^n = \mathfrak{q}\left(\frac{b}{a}\right)^{n+1} \implies \mathfrak{q}\left(\frac{b}{a}\right)^n = \mathfrak{q}\left(\frac{b}{a}\right)^n \frac{b}{a}.$$

Since $\mathfrak{q}$ is finitely generated, we use Proposition 2.1 to note $\frac{b}{a}$ is integral over R and, hence, belongs in R. From our contradiction, we note our chain is strictly increasing. As R is Noetherian, our chain isn't contained in R. Choose n such that $\mathfrak{q}\left(\frac{b}{a}\right)^n \subseteq R$, but $\mathfrak{q}\left(\frac{b}{a}\right)^{n+1} \not\subseteq R$. Then, we note $\mathfrak{q}\left(\frac{b}{a}\right)^n \not\subseteq \mathfrak{p}$ since $\mathfrak{p}\frac{b}{a} = R$. Thus, $\mathfrak{q}\left(\frac{b}{a}\right)^n = R$, and, hence, $\mathfrak{q} = \left(\frac{a}{b}\right)^n$. ■

These local Dedekind domains (often called *Discrete Valuation Rings*) have the property that all elements are of the form up^m, where u is a unit and p is the unique (up to associates) prime element that generates the maximal ideal $\mathfrak{p}$ of R. It follows that all ideals are then of the form $\mathfrak{p}^m$ for $m \in \mathbb{N}$.

Dedekind domains play nicely with localization.

Proposition 3.2. *If R is a Dedekind and S is a multiplicatively closed subset of R, $S^{-1}R$ is a Dedekind domain.*

Proof. Consider an ideal $\mathfrak{a} \subset S^{-1}R$ and recall $\mathfrak{b} := R \cap \mathfrak{a}$ is an ideal of R, who's generating set generates $\mathfrak{a}$. As R is Noetherian, both $\mathfrak{a}$ and $\mathfrak{b}$ are finitely generated, i.e. $S^{-1}R$ is Noetherian. Note that the prime ideals of $S^{-1}R$ are of the form $S^{-1}\mathfrak{p}$ for prime ideal $\mathfrak{p} \subset R$. As $S^{-1}\mathfrak{p} \subseteq S^{-1}\mathfrak{q} \iff \mathfrak{p} \subseteq \mathfrak{q}$ for prime ideal $\mathfrak{q} \subset R$, we conclude the prime ideals of $S^{-1}R$ are maximal. Consider $\alpha \in \operatorname{Frac}(R)$ (which is the same as $\operatorname{Frac}(S^{-1}R)$) for which there exists monic $f \in S^{-1}R[x]$ such that

$$f(\alpha) = \alpha^n + \frac{r_{n-1}}{s_{n-1}}\alpha^{n-1} + \cdots + \frac{r_0}{s_0} = 0.$$

Since $\alpha s_{n-1} \cdots s_0$ is a root of the monic polynomial

$$(s_{n-1} \cdots s_0)^n f\left(\frac{x}{s_{n-1} \cdots s_0}\right)$$

in $R[x]$, we use that R is integrally closed to conclude

$$\alpha s_{n-1} \cdots s_0 \in R \implies \alpha = \frac{\alpha s_{n-1} \cdots s_0}{s_{n-1} \cdots s_0} \in S^{-1}R.$$

■

An important result of Dedekind domains is the unique factorization of ideals. Specifically,

Theorem 3.3 (Unique Factorization of Ideals)**.** *In a Dedekind domain, every non-zero proper ideal can be written uniquely as the product of prime ideals.*

Lemma 3.4. *Let R be a Noetherian ring. Then every ideal $\mathfrak{n}$ in R contains a product of nonzero prime ideals.*

Proof. As R is Noetherian, we assume the result is false and let $\mathfrak{n}$ be a maximal counterexample. As $\mathfrak{n}$ is not prime, consider $ab \in \mathfrak{n}$. As $(a) + \mathfrak{n}, (b) + \mathfrak{n} \supset \mathfrak{n}$, a product of prime ideals $\mathfrak{p}$ and $\mathfrak{q}$ are contained in $(a) + \mathfrak{n}$ and $(b) + \mathfrak{n}$ respectively. Then,

$$\mathfrak{n} \supseteq ((a) + \mathfrak{n})((b) + \mathfrak{n}) \supseteq \mathfrak{p}\mathfrak{q}.$$

■

Lemma 3.5. *Let R be a ring and let $\mathfrak{m}$ and $\mathfrak{n}$ be relatively prime ideals*[4] *in R. For all $m, n \in \mathbb{N}$, $\mathfrak{m}^m$ and $\mathfrak{n}^n$ are relatively prime.*

Proof. We prove the contrapositive. Suppose $\mathfrak{m}^m$ and $\mathfrak{n}^n$ are not relatively prime, i.e. there exists some prime ideal $\mathfrak{p}$ such that $\mathfrak{p} \supseteq \mathfrak{m}^m + \mathfrak{n}^n$. By the primality of $\mathfrak{p}$, $\mathfrak{m}, \mathfrak{n} \subseteq \mathfrak{p} \implies \mathfrak{m} + \mathfrak{n} \neq R$. ■

Lemma 3.6. *Let $\mathfrak{p}$ be a maximal ideal in the integral domain R and let $\mathfrak{q} := \mathfrak{p}R_{\mathfrak{p}}$. Then, the map $\phi : R/\mathfrak{p}^m \to R_{\mathfrak{p}}/\mathfrak{q}^m$, where $\phi(x + \mathfrak{p}^m) = x + \mathfrak{q}^m$, is an isomorphism.*

[4] Recall that ideals I and J in R are relatively prime when $I + J = R$

Proof. The homomorphism property of ϕ follows easily. Consider $x, y \in R$.

$$\phi\left((x+y)+\mathfrak{p}^m\right) = (x+y)+\mathfrak{q}^m = (x+\mathfrak{q}^m)+(y+\mathfrak{q}^m) = \phi\left(x+\mathfrak{p}^m\right)+\phi\left(y+\mathfrak{p}^m\right), \tag{1}$$

$$\phi\left((x\times y)+\mathfrak{p}^m\right) = (x\times y)+\mathfrak{q}^m = (x+\mathfrak{q}^m)\times(y+\mathfrak{q}^m) = \phi\left(x+\mathfrak{p}^m\right)\times\phi\left(y+\mathfrak{p}^m\right), \tag{2}$$

$$\phi(1+\mathfrak{p}^m) = 1+\mathfrak{q}^m. \tag{3}$$

To prove $\ker(\phi)$ is trivial, we hope to show $R\cap\mathfrak{q}^m = \mathfrak{p}^m$. We obtain one inclusion for free: $\mathfrak{p}^m \subseteq R\cap\mathfrak{q}^m$. For the other inclusion, we note $\mathfrak{q}^m = \mathfrak{p}^m R_{\mathfrak{p}}$. Then, the elements of $R\cap\mathfrak{q}^m$ are of the form $\frac{a}{b}$, where $a\in\mathfrak{p}^m$ and $b\notin\mathfrak{p}$. Since $\mathfrak{p}$ is the only maximal ideal $\mathfrak{p}^m$ is contained in[5], $R/\mathfrak{p}^m$ is local and $R/\mathfrak{p}^m\setminus\mathfrak{p}/\mathfrak{p}^m$ is the set of units. We conclude that b is a unit in $R/\mathfrak{p}^m$ and $\frac{a}{b}\cdot b = 0 \implies \frac{a}{b} = 0$ in $R/\mathfrak{p}^m$. To note $\mathrm{im}(\phi) = R_{\mathfrak{p}}/\mathfrak{q}^m$, we make use of Lemma 3.5. Consider an element $\frac{x}{y}\in R_{\mathfrak{p}}$. Since $y\notin\mathfrak{p}$ and $\mathfrak{p}$ is maximal, $(y)+\mathfrak{p} = R \implies (y)+\mathfrak{p}^m = R$, i.e. there exists $k\in R$ and $q\in\mathfrak{p}^m$ such that

$$ky+q = 1 \implies \phi(kx+\mathfrak{p}^m) = \frac{x}{y}+\mathfrak{q}^m.$$

■

Barring the final parts of Lemma 3.6, much of these proofs have no real content. They're mostly simple checks. However, with them, we can prove our first important result: Theorem 3.3.

Proof. In a Dedekind domain R, consider an ideal I. By Lemma 3.4, there exists prime ideals $\mathfrak{p}_1,\dots,\mathfrak{p}_m$ such that $\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_m^{e_m}\subseteq I$. We note $\mathfrak{p}_i$ and $\mathfrak{p}_j$ are relatively prime for all $i\neq j$ as they're maximal. Applying Lemma 3.5, we have that $\mathfrak{p}_i^{e_i}$ and $\mathfrak{p}_j^{e_j}$ are relatively prime. By the *Chinese Remainder Theorem* and Lemma 3.6,

$$\frac{R}{\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_m^{e_m}} \cong \frac{R}{\mathfrak{p}_1^{e_1}}\times\cdots\times\frac{R}{\mathfrak{p}_m^{e_m}} \cong \frac{R_{\mathfrak{p}_1}}{\mathfrak{q}_1^{e_1}}\times\cdots\times\frac{R_{\mathfrak{p}_m}}{\mathfrak{q}_m^{e_m}},$$

where $\mathfrak{q}_i := \mathfrak{p}_i R_{\mathfrak{p}_i}$. Now, note that $R_{\mathfrak{p}_i}$ is a local PID from Propositions 3.1 and 3.2. Recall the ideals of $R_{\mathfrak{p}_i}$ are of the form $\mathfrak{q}_i^n$ for $n\in\mathbb{N}$. We conclude there exists $\mathfrak{q}_i\subseteq R_{\mathfrak{p}_i}$ such that

$$\frac{I}{\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_m^{e_m}} \cong \frac{\mathfrak{q}_1^{s_1}}{\mathfrak{q}_1^{e_1}}\times\cdots\times\frac{\mathfrak{q}_m^{s_m}}{\mathfrak{q}_m^{e_m}},$$

where $s_i\leq e_i$ for all i. Since

$$\mathfrak{p}_1^{s_1}\cdots\mathfrak{p}_m^{s_m}R_{\mathfrak{p}_i} = \mathfrak{p}_i^{s_i}R_{\mathfrak{p}_i} = \mathfrak{q}_i^{s_i},$$

we have that $I = \mathfrak{p}_1^{s_1}\cdots\mathfrak{p}_m^{s_m}$ because both ideals contain $\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_m^{e_m}$ and have the same image in $R_{\mathfrak{p}_1}/\mathfrak{q}_1^{e_1}\times\cdots\times R_{\mathfrak{p}_m}/\mathfrak{q}_m^{e_m}$. Now, for the uniqueness part of our proof, suppose $\mathfrak{p}_1^{s_1}\cdots\mathfrak{p}_m^{s_m} = I = \mathfrak{p}_1^{t_1}\cdots\mathfrak{p}_m^{t_m}$. We may assume the same primes occur in both factorization by adding sufficiently many prime ideals with zero exponent. Then, it follows

$$\mathfrak{q}_i^{s_i} = IR_{\mathfrak{p}_i} = \mathfrak{q}_i^{t_i} \implies s_i = t_i$$

for all i. ■

A useful result that follows from Theorem 3.3 is that every ideal of a Dedekind domain is generated by at most two elements. More generally,

Corollary 3.7. *Let R be a Dedekind Domain and I an ideal of R. For $i\in I$, there exists $j\in I$ such that $(i,j) = I$.*

[5] For any prime ideal $\mathfrak{m}$, $\mathfrak{p}^m\subseteq\mathfrak{m} \iff \mathfrak{p}\subseteq\mathfrak{m}$

Proof. Let $(i) = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_m^{e_m}$ and $I = \mathfrak{p}_1^{s_1}\mathfrak{p}_2^{s_2}\cdots\mathfrak{p}_m^{s_m}$, where $s_i \leq e_i$ for all i. Then, choose j_i such that

$$j_i \in \mathfrak{p}_1^{s_1+1}\mathfrak{p}_2^{s_2+1}\cdots\mathfrak{p}_i^{s_i}\cdots\mathfrak{p}_m^{s_m+1} \tag{4}$$

$$j_i \notin \mathfrak{p}_1^{s_1+1}\mathfrak{p}_2^{s_2+1}\cdots\mathfrak{p}_i^{s_i+1}\cdots\mathfrak{p}_m^{s_m+1} \tag{5}$$

Then, define $j \coloneqq j_1+\cdots+j_m$. We hope to show $(i,j) = I$. The first inclusion follows for free: $(i,j) \subseteq I$. For the second, write the prime factorization of $(i,j) = \mathfrak{p}_1^{t_1}\mathfrak{p}_2^{t_2}\cdots\mathfrak{p}_m^{t_m}$ and note that $t_i \leq s_i$ for all i since our construction guarantees $j \notin \mathfrak{p}_i^{s_i+1}$ for all i: i.e. $I \subseteq (i,j)$. ■

Corollary 3.8. *Let R be a Dedekind Domain and I an ideal of R. Then, there exists an ideal $I' \subseteq R$ such that II' is principal. In particular, we can choose I' such that $II' = (a)$ for any $a \in I$.*

Proof. Let $(a) = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_m^{e_m}$ and $I = \mathfrak{p}_1^{s_1}\mathfrak{p}_2^{s_2}\cdots\mathfrak{p}_m^{s_m}$, where $s_i \leq e_i$ for all i. Then, $I' = \mathfrak{p}_1^{e_1-s_1}\mathfrak{p}_2^{e_2-s_2}\cdots\mathfrak{p}_m^{e_m-s_m}$. ■

Corollary 3.9. *A Dedekind domain R, that is a principal ideal domain, is a unique factorization domain.*

Proof. Pick an arbitrary element $a \in R$ and factor $(a) = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_m^{e_m}$. Since $\mathfrak{p}_i^{e_i} = (p_i^{e_i})$ for some prime p_i,

$$(a) = (p_1^{e_1}\cdots p_m^{e_m}) \implies a = up_1^{e_1}\cdots p_m^{e_m},$$

for some unit u. The uniqness of this factorization follows from the uniqness of the prime factorization of (a). ■

4. Prime Factorizing Ideals in $\mathcal{O}_K$

Having proven Theorem 3.3, the natural next question to ask is how might one factor these ideals. In particular, we hope to answer this question when $K = \mathbb{Q}(\alpha)$, for algebraic α. Let's begin by considering a few examples.

Example 4.1. Let $K = \mathbb{Q}(\sqrt{-5})$. Then, $\mathcal{O}_K = \mathbb{Z}(\sqrt{-5})$[6]. Here (6) factorizes as

$$(6) = (2, 1+\sqrt{-5})^2(3, 1+\sqrt{-5})(3, 1-\sqrt{-5}).$$

Seeing this amounts to some ideal arithmetic and a helpful isomorphism.

$$\begin{aligned} &= (2, 1+\sqrt{-5})^2(3, 1+\sqrt{-5})(3, 1-\sqrt{-5}) \\ &= (4, -4+2\sqrt{-5}, 4+4\sqrt{-5})(9, 3-3\sqrt{-5}, 3+3\sqrt{-5}, 6) \\ &= (4, 12, -4+2\sqrt{-5})(3, 3-3\sqrt{-5}, 3+3\sqrt{-5}, 6) \\ &= (2)(3) = (6) \end{aligned}$$

To note $(2, 1+\sqrt{-5})$ is prime, we require the isomorphism $\mathbb{Z}[\sqrt{-5}] \cong \mathbb{Z}[x]/(x^2+5)$, given by $a + b\sqrt{-5} \mapsto a + bx$. Hence[7],

$$\frac{\mathcal{O}_K}{(2, 1+\sqrt{-5})} \cong \frac{\mathbb{Z}[x]/(x^2+5)}{(2, 1+x)} \cong \frac{\mathbb{Z}[x]}{(x^2+5, 2, 1+x)} \cong \frac{\mathbb{F}_2[x]}{(x^2+5, 1+x)} \cong \frac{\mathbb{F}_2}{(0)} = \mathbb{F}_2.$$

To note the primality of the other factors, apply a similar argument. We leave this to the reader.

[6] The integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$ (for square free d) is $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ for $d \equiv 1 \pmod 4$ and $\mathbb{Z}[\sqrt{d}]$ otherwise

[7] We use implicitly that the order of quotients doesn't matter

Example 4.2. Along the same lines as the previous example, we consider $K = \mathbb{Q}(\sqrt{-13})$ and $\mathcal{O}_K = \mathbb{Z}[\sqrt{-13}]$. The ideal (14) factors as

$$(14) = (7, \sqrt{-13}+1)(7, \sqrt{-13}+6)(2, \sqrt{-13}+1)(2, \sqrt{-13}-1).$$

The justification of these claims follows by use of similar arguments made in Example 4.1.

Generalizing these two examples leads us to the *Dedekind-Kummer Theorem.*

Theorem 4.1 (Dedekind-Kummer). *Let $K = \mathbb{Q}(\alpha)$ be a number field such that $\alpha \in \mathcal{O}_K$. Let p be any integer prime, where $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$. Then, call $f(x)$ the minimal polynomial of α over $\mathbb{Z}$. Then, we factor (p) as $(p) = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_m^{e_m}$, where*

$$f(x) \equiv \prod_{i=1}^{m} (f_i(x))^{e_i} \pmod{p},$$

the f_i's are irreducible modulo p, and $\mathfrak{p}_i = (f_i(\alpha), p)$.

p	$f(x) = x^2 + 17 \pmod{p}$	(p)
2	$(x+1)^2$	$(2, \sqrt{-17}+1)^2$
3	$(x+1)(x+2)$	$(3, \sqrt{-17}+1)(3, \sqrt{-17}+2)$
5	x^2+2	(5)

Figure 1. Factorizing Prime Ideals in $\mathbb{Z}[\sqrt{-17}]$ using Theorem 4.1

Over number fields where $\mathcal{O}_K = \mathbb{Z}[\alpha]$, Theorem 4.1 provides a simple algorithm to prime factorize ideals of the form (n) for $n \in \mathbb{Z}$.

- Prime factorize n in $\mathbb{Z}$: $n = p_1^{e_1}p_2^{e_2}\cdots p_m^{e_m}$.
- Compute the minimal polynomial f of α over $\mathbb{Z}$.
- Prime factorize f in $\mathbb{F}_{p_i}[x]$ for all i:
$$f(x) \equiv (f_1(x))^{e_{i,1}}(f_2(x))^{e_{i,2}}\cdots(f_{j_i}(x))^{e_{i,j_i}} \pmod{p_i}.$$
- Conclude
$$(n) = \Big((p_1, f_1(\alpha))^{e_{1,1}}\cdots(p_1, f_{j_1}(\alpha))^{e_{1,j_1}}\Big)^{e_1}\cdots\Big((p_m, f_1(\alpha))^{e_{m,1}}\cdots(p_m, f_{j_m}(\alpha))^{e_{m,j_m}}\Big)^{e_m}.$$

Example 4.3. As discussed in Section 1, let's solve a Diophantine equation with our new Theorem. Consider $x^2 + 5y^2 = 6$. Factoring in $\mathbb{Z}[\sqrt{-5}]$, we obtain

$$x^2 + 5y^2 = 6 \implies (x + \sqrt{-5}y)(x - \sqrt{-5}y) = 6.$$

From Example 4.1 or Theorem 4.1, we note $(6) = (2, 1+\sqrt{-5})^2(3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$. From checking the ideal divisors of (6), we conclude 6 can be written as $6 = 2 \times 3$ or $6 = (1+\sqrt{-5})(1-\sqrt{-5})$. This allows us to conclude our only solutions are

$$x = 1,\ y = 1$$
$$x = 1,\ y = -1$$

Note that we omit the proof of Theorem 4.1, not because it's particularly difficult or requires background the reader lacks, but simply because the proof is long and only tangentially related to our further points of discussion. That being said, if interested, the reader should see [Con, pp. 3 - 4].

5. Fractional Ideals & The Ideal Class Group

For the remainder of this section, we restrict our attention to a special class of Dedekind domains: $\mathcal{O}_K$ for number fields K. Let's now take a moment to extend our notion of the ideal in Dedekind domains.

Definition 5.1 (Fractional Ideal)**.** Let R be a Dedekind domain. Let $\mathfrak{a}$ be an R-submodule of $\mathrm{Frac}(R)$. Then, we say $\mathfrak{a}$ is a *Fractional Ideal* if there exist $b \in R$ such that $b\mathfrak{a}$ is an ideal of R. The fractional ideals that are also ideals of R are often called *Integral Ideals* for emphasis.

Intuitively, think of this as meaning the elements $\mathfrak{a}$ have a common denominator b. With this in mind, it's easy to see why it's equivalent to say $\mathfrak{a}$ is a fractional ideal when $\mathfrak{a} = \frac{1}{x}\mathfrak{y}$ for an ideal $\mathfrak{y} \subseteq R$ and $x \in R$.

Example 5.1. Let R be a Dedekind domain. Every non-zero element $x \in R$ defines a fractional ideal

$$(x) \coloneqq xR = \{xr \in R \mid r \in R\}.$$

Naturally, we say fractional ideals of this type are *principal.*

Theorem 5.1. *Let R be a Dedekind domain. The set of fractional ideals* $\mathrm{Id}(R)$ *has a group structure. In fact,* $\mathrm{Id}(R)$ *is a free abelian group.*

Proof. We define the composition of fractional ideals much like the product of ideals: for fractional ideals $\mathfrak{a}, \mathfrak{b}$,

$$\mathfrak{a}\mathfrak{b} = \left\{ \sum a_i b_j \mid a_i \in \mathfrak{a},\ b_j \in \mathfrak{b} \right\}.$$

Closure, Identity ($R = (1)$), and Associativity follow immediately. To show the existence of inverses, consider a fractional ideal $\frac{1}{x}\mathfrak{y}$, where $\mathfrak{y}$ is an integral ideal. Then, by Corollary 3.8, there exists $\mathfrak{y}'$ such that $\mathfrak{y}\mathfrak{y}' = (y)$ for some $y \in \mathfrak{y}$. Then, notice $\frac{x}{y}\mathfrak{y}'$ is our desired inverse. Now, to conclude $\mathrm{Id}(R)$ is free abelian, we show that it's generated by the prime ideals. We note

$$x \cdot \frac{1}{x}\mathfrak{y} = (x)\frac{1}{x}\mathfrak{y} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_m^{e_m} \implies \frac{1}{x}\mathfrak{y} = \mathfrak{p}_1^{e_1 - s_1} \cdots \mathfrak{p}_m^{e_m - s_m},$$

where $(x) = \mathfrak{p}_1^{s_1} \cdots \mathfrak{p}_m^{s_m}$ for prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$. This factorization is unique. ■

Consider the subgroup of principal fractional ideals[8] $\mathrm{P}(R)$ of $\mathrm{Id}(R)$.

Definition 5.2 (Ideal Class Group & Class Number)**.** Let R be a Dedekind domain. We define the *Ideal Class Group*, $\mathrm{Cl}(R)$, as the quotient $\mathrm{Cl}(R) \coloneqq \mathrm{Id}(R)/\mathrm{P}(R)$ and the *Ideal Class Number* as $|\mathrm{Cl}(R)|$.

It turns out that the class number of $\mathcal{O}_K$ is always finite. But, before we get there, we require some definitions.

Definition 5.3 (Ideal Norm v1)**.** Let K be a number field and $\mathfrak{a}$ be an integral ideal of $\mathcal{O}_K$. We define the ideal norm of $\mathfrak{a}$, $N(\mathfrak{a})$, as

$$N(\mathfrak{a}) \coloneqq |\mathcal{O}_K/\mathfrak{a}|.$$

Proposition 5.2. *Let K be a number field. Let $\mathfrak{a}, \mathfrak{b}$ be integral ideals of $\mathcal{O}_K$ and $x \in \mathcal{O}_K$.*

(1) $N(\mathfrak{a})$ is finite

[8] Can you name $(x)(y)$ and $(x)^{-1}$?

(2) $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$
(3) $N((x)) = N_{K/\mathbb{Q}}(x)$[9].

We omit the proof. Using (3), we can naturally extend our notion of the ideal norm to fractional ideals.

Definition 5.4 (Ideal Norm v2)**.** Let K be a number field and $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}_K$. Factorize $\mathfrak{a}$ as $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_m^{e_m} \mathfrak{q}_1^{-s_1} \cdots \mathfrak{q}_n^{-s_n}$, where the $\mathfrak{p}_i$'s and $\mathfrak{q}_j$'s are prime and $e_1, \ldots, e_m, s_1, \ldots, s_n \geq 0$. Then,

$$N(\mathfrak{a}) \coloneqq \frac{\prod_{i=1}^m \mathfrak{p}_i^{e_i}}{\prod_{j=1}^n \mathfrak{q}_j^{s_j}}.$$

Definition 5.5. Let K be a number field and $b_1, \ldots, b_n$ be the basis of $\mathcal{O}_K$ as a Z-module. Let $\sigma_1, \ldots, \sigma_n$ be the n embeddings of K in $\mathbb{C}$ Then, the discriminant of K, Δ_K, is defined as

$$\Delta_K \coloneqq \det \begin{pmatrix} \sigma_1(b_1) & \sigma_1(b_2) & \cdots & \sigma_1(b_n) \\ \sigma_2(b_1) & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ \sigma_n(b_1) & \cdots & \cdots & \sigma_n(b_n) \end{pmatrix}^2 .$$

At last,

Theorem 5.3 (Minkowski's bound)**.** *Let K be a number field, where $[K : \mathbb{Q}] = n$, and $2s$ the number of non-real complex embeddings of K. Then, there exists a set of representatives of $\mathrm{Cl}(\mathcal{O}_K)$ consisting of integral ideals $\mathfrak{a}$, with*

$$N(\mathfrak{a}) \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|\Delta_K|}.$$

With this we can show $\mathrm{Cl}(\mathcal{O}_K)$ is finite. It suffices to show there are only finitely many integral ideals $\mathfrak{a}$ with $N(\mathfrak{a}) \leq M$ for any integer M. Suppose we wanted to construct such $\mathfrak{a}$. We begin by showing that every prime ideal is a divisor of precisely one (p) for some prime $p \in \mathbb{Z}$.

- We use (3) of Proposition 5.2. Consider arbitrary $\alpha \in \mathfrak{p}$. Note $N((\alpha)) = N_{K/\mathbb{Q}}(\alpha)$ is an integer. Since the galois conjugates of α are algebraic integers, $N_{K/\mathbb{Q}}(\alpha)/\alpha \in \mathcal{O}_K$ and $N_{K/\mathbb{Q}}(\alpha) \in \mathfrak{p}$. As $\mathfrak{p} \cap \mathbb{Z} \setminus \{0\}$ is non-empty, choose p to be the smallest positive integer in $\mathfrak{p}$. If p is composite, there exists integer $xy = p \in \mathfrak{p} \implies x, y \in \mathfrak{p}$, contradicting the minimality of p.
- This next part is easier. If $\mathfrak{p} \mid (p)$, then $\mathfrak{p} \nmid (q)$ for distinct prime q since $\gcd(p, q) = 1$.

Now, group the prime ideals based on which prime p it contains. If a prime ideal $\mathfrak{p}$ lies in the group of p, we say it's associated to p. See Figure 2. Note that if $\mathfrak{p} \supset (p)$, then $N(\mathfrak{p}) \mid N(p)$. Hence, for sufficiently large n, the prime ideals $\mathfrak{p}$ assigned to $p > n$ no longer satisfy $N(\mathfrak{p}) \leq M$. Since we can only construct $\mathfrak{a}$ using the prime ideals associated to $p \leq n$ and there can only be finitely many prime ideals associated with any given p, we conclude that only finitely many $\mathfrak{a}$ can be constructed.

[9] You may recall the *norm* (product of Galois conjugates) from Galois Theory. Our new definition for ideals is actually an extension of this idea

2	$\mathfrak{p}_1, \mathfrak{p}_2, \cdots$
3	$\mathfrak{q}_1, \mathfrak{q}_2, \cdots$
5	$\mathfrak{r}_1, \mathfrak{r}_2, \cdots$
7	$\mathfrak{s}_1, \mathfrak{s}_2, \cdots$
$\vdots$	$\cdots$

FIGURE 2. Visual aid; the $\mathfrak{p}_i$'s, $\mathfrak{q}_i$'s, and $\mathfrak{s}_i$'s are prime ideals that contain (2), (3), and (5) respectively

Now, let's actually use Theorem 5.3.

Example 5.2. We hope to show $\mathbb{Z}[i]$ is a PID. As $\mathbb{Q}(i)$ has 2 non-real complex embeddings, we know that the representative $\mathfrak{a}$ of any class in $\text{Id}(\mathcal{O}_K)$ is such that

$$N(\mathfrak{a}) \leq \frac{2!}{2^2}\frac{4}{\pi}\sqrt{4} = \frac{4}{\pi} < 2 \implies \mathfrak{a} = (1).$$

The desired result follows.

We omit the proof of Theorem 5.3 and instead turn to an interesting application. See [Mil08, pp. 125 - 139] for a proof.

6. The Mordell Equation

The *Mordell equation* is the Diophantine equation $y^2 + k = x^3$. Let's solve it in some special cases.

Definition 6.1 (Comaximal Powers Trick)**.** We say an integral domain R has the property $CM(n)$ when $xy = z^n$ implies there exists units $u, v \in R$ and elements $a, b \in R$ such that $x = ua^n$ and $y = vb^n$.

Theorem 6.1. *Let $k \in \mathbb{Z}^+$ ($k > 1$) be square free with $k \equiv 1, 2 \pmod 4$. Then, if $\mathbb{Z}[\sqrt{-k}]$ has the property $CM(n)$,*

(1) the only integer solutions to the Mordell equation are $x = a^2 + k$ and $y = \pm a(a^2 - 3k)$ if there exists $a \in \mathbb{Z}$ such that $k = 3a^2 \pm 1$;

(2) the Mordell equation has no solutions if we cant find a such that $k = 3a^2 \pm 1$.

Proof. Suppose (x, y) is a solution of $y^2 + k = x^3$. Suppose x is even. Reducing modulo 4, we find

$$y^2 + k \equiv 0 \pmod 4 \implies y^2 \equiv 3, 2 \pmod 4,$$

resulting in a contradiction. x must then be odd. Next, we hope to show $\gcd(x, k) = 1$. If not, there exists a prime p such that $p \mid x, k$. Then,

$$p \mid y^2 = x^3 - k \implies p \mid y.$$

Then, we contradict that k is square free by noting $p^2 \mid x^3 - y^2 = k$. Factoring in $\mathbb{Z}[\sqrt{-k}]$, we obtain

$$(y - \sqrt{-k})(y + \sqrt{-k}) = x^3.$$

To use the $CM(3)$ property, we hope to show $(y - \sqrt{-k}, y + \sqrt{-k}) = \mathbb{Z}[\sqrt{-k}]$. Assuming the contrary, we note the existence of a prime ideal $\mathfrak{p} \supseteq (y - \sqrt{-k}, y + \sqrt{-k})$. Then,

$\mathbb{Q}(\sqrt{-n})$	$\lvert\mathrm{Cl}(\mathcal{O}_K)\rvert$
$\mathbb{Q}(\sqrt{-6})$	2
$\mathbb{Q}(\sqrt{-10})$	2
$\mathbb{Q}(\sqrt{-13})$	2
$\mathbb{Q}(\sqrt{-30})$	4
$\mathbb{Q}(\sqrt{-57})$	4
$\mathbb{Q}(\sqrt{-73})$	4
$\mathbb{Q}(\sqrt{-93})$	4

FIGURE 3. Number Fields with Class Numbers 2 & 4; from [Ide]

$-((y+\sqrt{-k})-(y-\sqrt{-k}))^2 = 4k \in \mathfrak{p}$ and $y^2+k = x^3 \in \mathfrak{p} \implies x \in \mathfrak{p}$. Since x is odd, $\gcd(x, 4k) = 1$ and we obtain a contradiction. Using $CM(3)$, we note

$$y+\sqrt{-k} = (a+b\sqrt{-k})^3 = a(a^2-3kb^2) + b(3a^2-b^2k)\sqrt{-k}.$$

Since ± 1 are the only units in $\mathbb{Z}[\sqrt{-k}]$, we note $b = \pm 1$. After some computation, we conclude $k = 3a^2 \pm 1$, $x = a^2+k$ and $y = \pm a(a^2-3k)$. Verifying that these are always solutions is left to the reader. ■

So, what does this have to do with Dedekind domains and the ideal class group? It turns out

Theorem 6.2. *For $n \in \mathbb{Z}^+$ and a number field K, if $\gcd(n, |\mathrm{Cl}(\mathcal{O}_K)|) = 1$, then $\mathcal{O}_K$ has the property $CM(n)$.*

Proof. Suppose $xy = z^n$ and $px+qy = 1$. Then, we hope to show $(x,z)^n = (x)$. We begin by noting the elements of $(x,z)^n$ are of the form

$$\sum_{i=1}^{n} a_i x^{n-i} z^i = \sum_{i=1}^{n-1} a_i x^{n-i} z^i + a_n xy \in (x).$$

For the opposite inclusion, we proceed by induction on j to show $x^{n-j} \in (x,z)^n$. For $j = 0$, the result is apparent. Assume the result to be true for j. Then,

$$\begin{aligned} &\implies qz^n = qxy = x(1-px) \in (x,z)^n \\ &\implies x^{n-j-2}x(1-px) = x^{n-j-1} + px^{n-j} \in (x,z)^n \\ &\implies x^{n-(j+1)} \in (x,z)^n. \end{aligned}$$

The desired result follows. Using which, we note the order (x,z) is 1 in $\mathrm{Cl}(\mathcal{O}_K)$, i.e. $(x,z) = (a)$ and $(x,z)^n = (x) = (a)^n$. Then, there exists unit u such that $x = ua^n$. We may apply an equivalent argument to show the desired result for y. ■

This makes determining the solutions of the Mordell equation doable using Theorems 5.3 and 6.2.

Example 6.1. From Figure 3, we can conclude the solutions of the Mordell equation $y^2+k = x^3$ for $k = 6, 10, 13, 30, 57, 73, 93$ using Theorems 6.1 and 6.2. Note that this exact argument should work for far more such k as well.

7. Conclusion & Remarks

We hope this paper offered a helpful glimpse into Dedekind domains. However, we must note that Dedekind domains and ideal class groups have properties and applications beyond what we've discussed: some notable examples being Kummer's proof of *Fermat's Last Theorem* for regular primes and Dirichlet's proof that if a and b are coprime natural numbers, then there are infinitely many primes p such that p is congruent to a modulo b.

As much of the material in this paper comes from [Mil08] and [MS77], the reader is advised to consult these books for more information if interested.

References

[Cla] Pete L Clark. The mordell equation.

[Con] Keith Conrad. Factoring after dedekind.

[Ide] Tables of imaginary quadratic fields with small class numbers. http://www.numbertheory.org/classnos/.

[Jac89] Nathan Jacobsen. *Basic Algebra II.* WH Freeman and Company, New York, 1989.

[Mil08] James S Milne. *Algebraic number theory.* JS Milne, 2008.

[MS77] Daniel A Marcus and Emanuele Sacco. *Number fields*, volume 2. Springer, 1977.

[RS] Simon Rubinstein-Salzedo. *Abstract Algebra.*

Email address: akashdhiraj2019@gmail.com