PRINCIPAL IDEAL DOMAINS, UNIQUE FACTORIZATION DOMAINS AND EUCLIDEAN DOMAINS

JOSH ZEITLIN

Abstract

In this paper, we will touch on some interesting types of rings and domains. We are going to study principal ideal domains where we will use special properties of principal ideals and will generalize that to study euclidean domains and almost euclidean domains. Furthermore, we will study Unique Factorization Domains which are essentially just domains that satisfy unique factorization. Building off of these ideas we will see how these generalizations can be used to describe certain rings and why we can prove that certain rings have unique factorization once it can be shown that there is some sort of division algorithm.

1. Preliminary Definitions

In the tradition of writing a good expository paper, we will start off with a list of extensive definitions. First, let's define an integral domain.

Definition 1.1. An *Integral Domain* is a commutative ring that as unity and no 0 divisors.

Definition 1.2. A *Divisor* is an element b of an integral domain D so that if there is some $a \in D$ then $b|a$, or in other words $\exists c \in D$ such that $a = b \cdot c$.

Building off of this definition we see that divisors have some interesting properties in integral domains. If D is an integral domain, then the divisors have the reflexive and transitive properties. In addition, $a|b \iff ac|bc$ for some nonzero $c \in D$. Similarly, every element of D divides 0, 1 divides every element of D and lastly if 0 divides an element of D, then that element must also be 0.

Another special type of element of an integral domain is a unit, which we will define next.

Definition 1.3. A *unit* of an integral domain D is any element that is a divisor of the multiplicative identity.

The set of all units of D can be written as $D^\times$ or occasionally some mathematicians or textbooks will write $U(D)$.

Next, we will discuss prime and irreducible elements which are two ways of describing elements that cannot be split apart.

Definition 1.4. A *prime* element of an integral domain is an element $p \in D$ such that if $p|ab$ then $p|a$ or $p|b$.

On the other hand, an irreducible element can be described in the following manner.

Definition 1.5. An *irreducible* element of an integral domain is one such that if $a = bc$ then either b or c is a unit where a is the irreducible element.

It is easy to see from every that any prime element of an integral domain is irreducible; however, it is not necessarily the case that every irreducible element is prime.

Now that we have these definitions related to elements of integral domains down we'll move on to definitions related to ideals.

First we'll define a proper ideal.

Definition 1.6. An ideal I of an integral domain D is called a proper ideal of D if $I \neq \langle 0 \rangle, \langle 1 \rangle$

Moving on, we'll reiterate the concepts of principal, prime and maximal ideals.

Definition 1.7. An ideal I of an integral domain D is a *Principal Ideal* is there exists $a \in I$ such that $I = \langle a \rangle$.

In this case, we get that the element a generates the ideal I.

Definition 1.8. A *prime ideal* is an ideal I such that if $ab \in I$, then $a \in I$ or $b \in I$.

Next we'll define a very similar ideal, a maximal ideal.

Definition 1.9. A maximal ideal of a ring R is a proper ideal I such that if J such that $I \subseteq J$ then either $J = I$ or $J = R$.

Finally, we'll define one more term which is the Legendre symbol.

Definition 1.10. The *Legendre Symbol* is denoted $\left(\frac{a}{p}\right)$ where p is a prime, then $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$ where this essentially means that the Legendre symbol is 0 if $a \equiv 0 \mod p$, 1 if a is a quadratic residue modulo p and -1 if a is a non-residue modulo p.

2. Principal Ideal Domains

In this section we'll go over the basics of principal ideal domains.

Definition 2.1. A *Principal Ideal Domain* is an integral domain in which every ideal is principal.

One example of this is the integers, $\mathbb{Z}$, where every ideal is principal. Now, let's look at a few properties of principal ideal domains.

Theorem 2.2. *In a Principal Ideal Domain, an irreducible element is prime.*

Now, let's prove this theorem.

Proof. Let p be an irreducible element and let it be an element of the principal ideal domain D. Now, suppose $p|ab$ given $a, b \in D$. Now, if $p \not| a$ call $I = \langle p, a \rangle \in D$. Because D is a principal ideal domain it most be so that our ideal I can be written in the form of $I = \langle c \rangle$ where c is an element of D and generates I. Because $a, p \in I$ it must be so that $c|a, p$. Now, assume that $c = up$ where u is a unit. This would mean that $p|a$ which is a contradiction so it cannot be possible that c is a unit multiple of p. Because p is irreducible then c has to be a unit. Hence, $\exists d \in D$ s.t, $cd = 1$. Next, $c \in \langle a, p \rangle$ so it must be so that $c = xa + yp$ for some $x, y \in D$. Thus, $1 = cd = dxa + dyp$ and thus $b = (dx) \cdot ab + (bdy) \cdot p$. Now, becomes $p|ab$ we can pull out a p proving that $p|b$ showing that p is prime in D. ■

Now, we know that in a PID an irreducible is prime. However, unlike in most rings we can see that all prime elements in a PID are also irreducible.

Theorem 2.3. *In a Principal Ideal Domain if an element is prime then it is also irreducible.*

When we introduced this idea we know that in all integral domains that all prime elements are irreducible proving that an element of a PID is irreducible if and only if it is prime which we can see more formally in this next theorem.

Theorem 2.4. *Given an element $a \in D$ where D is a principal ideal domain, we have that a is irreducible if and only if a is prime.*

Now that we understand principal ideal domains, let's learn about a new concept called the greatest common divisor.

Definition 2.5. If D is a principal ideal domain and $\{a_1, ..., a_n\}$

And for our final theorem in this section we'll learn about the relationship between maximal and prime ideals in principal ideal domains.

Theorem 2.6. *Let D be an integral domain. Let $a \in D$ be such that $a \neq 0$ and $a \notin U(D)$. Then, $\langle a \rangle$ is a maximal ideal of D if and only if a is irreducible in D.*

From this theorem, we get this final result.

Theorem 2.7. *If D is a Principal Ideal Domain and if I is a proper ideal of D, then, I is maximal if and only if I is prime.*

3. Euclidean Domains

Definition 3.1. A Euclidean function is a function $\phi : D \to \mathbb{Z}$ if D is an Integral domain if $\phi(ab) \geq \phi(a) \forall a, b$ that are non-zero, and if $a, b \in D$ not equal to 0 then $q, r \in D$ so that $a = b \cdot q + r$ and $\phi(b) > \phi(r)$.

Let's now look at a few examples of what a Euclidean Function looks like.

- $\phi(a) = |a|$ with $a \in \mathbb{Z}$
- $\phi(p(x)) = \deg(p(x))$ where $p(x)$ is some polynomial.

Let's now look at some properties of Euclidean functions on an integral domain that follow from our definition.

Proposition 3.2. *If a and b are unit multiples, then $\phi(a) = \phi(b)$.*

Proof. We know that there is some $u \in D^\times$ and $u^{-1} \in D^\times$ such that $a = ub$ and $b = u^{-1}a$ which means that $\phi(a) \geq \phi(b)$ and $\phi(b) \geq \phi(a)$ implying that $\phi(a) = \phi(b)$ ■

Rattling off a few other properties we get the following set of results.

Proposition 3.3. *If $\phi(a) = \phi(b)$ then a and b are unit multiples.*

Proposition 3.4. *$\phi(a) = \phi(1)$ if and only if $a \in D^\times$*

And for our final basic property we get that

Proposition 3.5. *$\forall x \in D/\{0\}$ it is true that $\phi(x) > 0$.*

Now that we understand the definition of a Euclidean Function we'll introduce a new type of ring that is equipped with a Euclidean Function called a Euclidean Domain.

Definition 3.6. If D is an integral domain with a Euclidean Function ϕ then D is called a Euclidean Domain (with respect to ϕ).

Going back to our other examples we can see that $\mathbb{Z}$ is a Euclidean domain as well as $\mathbb{Z}[x]$. The rationals could also be considered a Euclidean Domain along with the Gaussian Integers $\{a + bi : a, b \in \mathbb{Z}\}$, denoted $\mathbb{Z}[i]$.

If you rattle through a few more examples you'll come to see that the one thing that all Euclidean Domains have in common is that they are all Principal Ideal Domains. Let's look at this in a more formal sense now and try to prove this idea.

Theorem 3.7. *If D is a Euclidean Domain then D is also a principal ideal domain.*

Proof. Obviously if $I = \{0\}$ then $I = \langle 0 \rangle$ and is a principal ideal domain. On the other hand if I is a non-zero proper ideal then let $S = \{\phi(x) : x \in I\}$ where S is non-zero. By the well-ordering principle there is a lower bound to S call it $\phi(x_0)$ given $x_0 \in I$. Then, if $x_1 \in I$ there are some q, r such that $x_1 = qx_0 + r$ so $\phi(r) < \phi(x_1)$. Because $x_1 \in I$ and $x_0 \in I$ we get that $-qx_0 \in I$ and then $x_1 - qx_0 \in I$. However, $\phi(x_0)$ is the smallest element of S so it must be so that $r = 0$ showing that $x_1 = qx_0$ so every element of I is a multiple of x_0 showing that $I = \langle x_0 \rangle$ showing that because every non-zero ideal is principal and the 0-ideal is principal we get that D is a principal ideal domain. ■

In the proof we used the property that given a, b we can write $a = bq + r$ with $\phi(b) > \phi(r)$. This is a very interesting property that gives way to an algorithm called the Euclidean Algorithm. If there is a Euclidean Function in your domain then your domain has the Euclidean Algorithm and is a Euclidean Domain. In any Euclidean domain you can complete the Euclidean algorithm so given a, b we get that $a = bq + r$ and then we also see that because $\phi(b) > \phi(r)$ we can write $b = q_0 r + r_0$ and then because $\phi(r) > \phi(r_0)$ it is true that $r = q_1 r_0 + r_2$. Continuing down this rabbit hole we'll eventually get some $r_i = 0$. Then, r_{i-1} is the last non-zero remainder and r_{i-1} is the greatest common divisor of (a, b).

4. Unique Factorization Domains

In this section we are going to study unique factorization domains. Let's begin with the definition.

Definition 4.1. A unique factorization domain (UFD) is an integral domain D such that every element $r \in R$ we get that r can be written as a finite number of irreducibles in a unique manner up to units.

Let's look at a few examples of UFD's.

- $\mathbb{Z}$ is a unique factorization domain by the fundamental theorem of algebra.
- $\mathbb{Z}[x]$ is a unique factorization domain.
- Every field is a unique factorization domain as every element is a unit in a field.
- Given a field F, $F[x]$ is a UFD.
- The Gaussian Integers $\mathbb{Z}[i]$ is also a UFD.

Now that we understand some examples of UFDs let's look at some examples of domains which are not UFDs.

- The ring $\mathbb{Z}[\sqrt{-5}]$ is not a Unique Factorization Domain, for example, $6 = 2 \cdot 3$, however, 6 also equals $(1 + \sqrt{-5})(1 - \sqrt{-5})$. This becomes true as all of these numbers, $2, 3, 1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are all irreducible elements of $\mathbb{Z}[\sqrt{-5}]$ which can be shown through some inspection and analysis of the norm in $\mathbb{Z}[\sqrt{-5}]$.

Let's now look at some lemmas related to Unique Factorization Domains and see how their properties relate to other properties that we've looked at.

Lemma 4.2. *If D is a UFD, then every irreducible is prime.*

Proof. Let p be an arbitrary irreducible element of D. Because p is irreducible the factorization of p is just $p \cdot \prod e_i$ where the e_i's are just units. Now, say the factorization of ab includes p. Ignoring the trivial case where a or b is in $D^\times$ we get that if $\prod q_i \prod r_j$ is ab where a and b are factored into those irreducibles q_i and r_j respectively, it must be so that p one of those irreducibles (or a unit multiple of one of those irreducibles) which means that $p|a$ or $p|b$ but not both. ■

We know that if F is a field then $F[x]$ is a UFD. We also know that F is a UFD. So this begs the question what is the relationship between a UFD and the set of all polynomials adjoined to that ring? This next theorem answers that question.

Theorem 4.3. *If D is a UFD then given n-variables $x_1, ..., x_n$ we have that $D[x_1, ..., x_n]$ is also a UFD.*

Proof. To prove this theorem we will only prove that if D is a UFD then $D[x]$ is a UFD because if we can prove it just for one variable then by a simple induction proof we can see that the property of being a UFD will hold for any n-variables. I won't give you the whole proof just yet, but just to give an outline, the key step is to use the field of fractions of the UFD to compare factorizations between the field of fractions as a polynomial ring and the UFD itself as a polynomial ring. ■

From this result we can actually do some analysis and inspection to show that if you have a ring D and a field of fractions F_D that if an element of D has a factorization in F_D then it has one in D.

The final theorem in this section before we move on to our main theorem is to show a lemma called Gauss's lemma which extends the notion that we just described in the previous paragraph.

Lemma 4.4. *If R is a UFD with a field of fractions F and if $f(x) \in R[x]$ then $f(x)$ has factorization $f(x) = g(x)h(x)$ in $F[x]$ with $\deg f, h \geq 1$ if and only if f has that same factorization in $R[x]$.*

To prove this theorem we need a new definition of a term we have not yet come across.

Definition 4.5. Given a UFD R and it's associated polynomial ring, an element $f \in R[x]$ is to be called primitive if all of the coefficients are co-prime.

Now, let's prove our lemma.

Proof. Suppose f and g are primitive polynomials with coefficients terms $f_i x^i$ and $g_i x^i$, respectively. If p is irreducible in R then there is k such that $p \not| f_k$ and j such that $p \not| g_j$. Then when we multiply $f \cdot g$ we get that the coefficient of x^{k+j} is $t = a_k b_j + \sum_{i<k} a_i b_{k+j-i} + \sum_{r<j} b_r a_{k+j-r}$. Because of the $a_k b_j$ term we get that $p \not| t$ which shows us that fg is primitive by the definition of a primitive polynomial.

Suppose $f(x)$ can be factored to fit the form $f(x) = \phi(x)\psi(x) \in F[x]$ with $\deg(\phi), \deg(\psi) \geq 1$. Let $f(x) = ef_1(x), \phi(x) = \frac{a}{b}\phi_1(x)$ and $\psi(x) = \frac{c}{d}\psi(x)$, where $f_1(x), \phi_1(x)$, and $\psi_1(x)$ are primitive in $R[x]$. Then $f(x) = ef_1(x) = \frac{ac}{bd}\phi_1(x)\psi_1(x)$. The product $\phi_1(x)\psi_1(x)$ is primitive in $R[x]$ which we will prove next. Because our domain is a UDF, it follows that $\frac{ac}{bd} = eu$, where $u \in R^{\times}$. Hence, $f(x)$ factors into the form $ue\phi_1(x)\psi_1(x) \in R[x]$. ■

Now, we can prove our theorem on the relationship between Unique Factorization Domains and their associated polynomial rings.

Proof. Let $g(x) \in R[x]/R[x]^{\times}$ and be non-zero. First, $g(x)$ can be written as $d \cdot f(x)$, where f is primitive and $d \in R$. Because R is a UFD we get that there is uniqueness. The element d has a unique factorization in R, by assumption, so it remains to show that $f(x)$ has a unique factorization into irreducibles in $R[x]$. But using the factorization of $f(x) \in F[x]$ and Gauss's Lemma, we can write $f(x) = p_1(x)p_2(x)\cdots p_s(x)$, where the $p_i(x)$ are elements of $R[x]$ that are irreducible in $F[x]$. Since $f(x)$ is primitive, every $p_i(x)$ is primitive too, and thus is irreducible in $R[x]$. The uniqueness of this factorization follows from the uniqueness of irreducible factorization in $F[x]$ together with the uniqueness of the factorization in $\frac{d}{b}f(x)$. In fact, suppose that $f(x) = p_1(x)p_2(x)\cdots p_s(x) = q_1(x)q_2(x)\cdots q_r(x)$, where the $p_i(x)$ and $q_i(x)$ are irreducible in $R[x]$. Since $f(x)$ is primitive, each $p_i(x)$ and $q_i(x)$ is primitive, and in particular of degree greater than or equal to 1. Then we see that $p_i(x)$ and $q_i(x)$ is irreducible in $F[x]$ because it is true that there is irreducibility in $R[x]$ if and only if it is in $F[x]$. By the uniqueness of the irreducible factorization in $F[x]$, after possibly renumbering the $q_i(x)$, we have $p_i(x) = c_i q_i(x)$ for each i for some $c_i \in F$ which is a unit. But then, by the uniqueness of the decomposition of $\frac{d}{b}f(x)$, each c_i is actually a unit in R. ■

5. Bringing it all together

We proved in earlier chapters that if an integral domain is a euclidean domain than it is also a principal ideal domain. Now, we are going to prove that if a domain is a principal ideal domain then it is also a unique factorization domain. We will only prove the uniqueness of factorization aspect of this theorem as a complete proof proving the basic fact that there exists a factorization into irreducibles requires using Noetherian Domains which take up a lot of time to study.

Theorem 5.1. *If D is an integral domain equipped with a Euclidean function then D is a Unique Factorization Domain.*

Proof. First of all we know that if D has a euclidean function ϕ then D is a euclidean domain with respect to ϕ. This then implies from our theorem earlier that D is a principal ideal domain. Now we have to show that being a principal ideal domain implies that that domain is a unique factorization domain. Now, as I said earlier, we are going to have to assume that every element of a PID can be factored into irreducibles which would make it a factorization domain, now we have to prove that that factorization is unique.

Now, assume for the sake of contradiction that there are two factorizations that are different to say that $n \in D$ can be written as both $\prod^s p_i$ and $\prod^r q_j$ and assume that each p_i and q_j is irreducible. Because irreducibility implies primality in UFDs we get that p_1 divides some q_j (so just assume that it is q_1 without loss of generality) and thus $p_1 = u_1 q_1$, or in other words, they are unit multiples. Thus, $p_1 \cdots p_s = u_1 q_1 p_2 \cdots p_s$ and thus $p_2 \cdots p_s = u_1 q_2 \cdots q_j$ and continuing down this rabbit hole we get that $1 = \cdots u_1 \cdots u_s \cdots q_{s+1} \cdots q_r$ and thus $q_{s+1}, ..., q_r \in D^\times$ but they can't be because they are irreducible which gives us a contradiction proving $s = r$ and each pair is a unit multiple. ■

6. Bibliography

(1) Barile, Margherita. ”Unique Factorization Domain.” From MathWorld–A Wolfram Web Resource, created by Eric W. Weisstein. https://mathworld.wolfram.com/UniqueFactorizationDomain.html
(2) Weisstein, Eric W. ”Integral Domain.” From MathWorld–A Wolfram Web Resource. https://mathworld.wolfram.com/IntegralDomain.html
(3) Barile, Margherita; Renze, John; and Weisstein, Eric W. ”Principal Ideal Domain.” From MathWorld–A Wolfram Web Resource. https://mathworld.wolfram.com/PrincipalIdealDomain.html
(4) Weisstein, Eric W. ”Principal Ideal.” From MathWorld–A Wolfram Web Resource. https://mathworld.wolfram.com/PrincipalIdeal.html
(5) Barile, Margherita and Weisstein, Eric W. ”Principal Ring.” From MathWorld–A Wolfram Web Resource. https://mathworld.wolfram.com/PrincipalRing.html
(6) Bourbaki, N. ”Anneaux Principaux.” §7.1 in Eléments de Mathématiques, Livre II: Algèbre, 2ème ed. Paris, France: Hermann, 1964.
(7) Wilson, J. C. ”A Principal Ring that is Not a Euclidean Ring.” Math. Mag. 34-38, 1973.

Email address: jzeitlin36@gmail.com