Artin: Factoring

James Pagan

February 2024

Contents

1 Unique Factorization Domains

1.1 Terminology

Let R be an integral domain. Before we introduce unique factorization domains, we must define several terms for $a, b \in R$:

1. a **divides** b if $(b) \subseteq (a)$.
2. a is a **proper divisor** if b if $(b) \subset (a) \subset R$.
3. a and b are **associates** if $(a) = (b)$.
4. a is **irreducible** if $(a) \subset R$ and there is no principal ideal (c) such that $(a) \subset (c) \subset R$.
5. p is a **prime element** if $p \neq 0$ and (p) is prime.

These may be equivalently expressed ideal-free (AbstractAlgebra/homework3.tex):

1. a **divides** b if $b = aq$ for some $q \in R$.
2. a is a **proper divisor** of b if $b = aq$ and neither a nor q is a unit.
3. a and b are **associates** if each divides the other — that is, $b = ua$ for some unit u.
4. a is **irreducible** if it has no proper divisors — its only divisors are units and associates.
5. p is a **prime element** if $p \neq 0$ and p divides ab implies p divides a or p divides b.

A **size function** is a mapping $\sigma : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$.

Theorem 1. *Let R be an integral domain. Then all prime elements of R are irreducible.*

Proof. Suppose that p is prime and that $(p) \subseteq (c) \subset R$. Hence there exists x such that $p = cx$, so $cx \in (p)$. We have two possibilities: $c \in (p)$ or $x \in (p)$.

Suppose for contradiction that $x \in (p)$. Then $x = py$ for some y — substituting into the above equality yields

$$p = c(py) \implies p(1 - cy) = 0.$$

Since $p \neq 0$, we have $1 = cy$ — hence c is a unit and $(c) = R$, a contradiction. We must have $c \in (p)$, so $(c) = (p)$. We conclude that (p) is irreducible. $\square$

1.2 Definition

A **unique factorization domain** R is an integral domain if for every nonzero $x \in R$, there exists a unit u and irreducible elements $p_1, \ldots, p_n$ such that

$$x = up_1 \cdots p_n,$$

and this factorization is unique in the following sense: if there exists a second factorization

$$x = wq_1 \cdots q_m,$$

then $n = m$ and there exists a bijection such that $(p_i) = (q_j)$ for each paired i, j (that is, p_i and q_j associate).

Theorem 2. *Every irreducible element in a unique factorization domain is prime.*

Proof. Suppose that (p) is not prime — then there exist $a, b \notin (p)$ such that $ab \in (p)$. Thus we have $(p) \subset (a)$. Since a is a nonunit, $(a) \subset R$, so

$$(p) \subset (a) \subset R.$$

Hence (p) is not irreducible. Taking the contrapositive yields the desired result. $\square$

Hence, we could equivalently define unique factorization as decomposition to *prime* elements. In this sense, factoriation in R "terminates" if and only if R satisfies the ascending chain condition for principal ideals; namely, the chain

$$x \quad \subseteq \quad \bigcap_{i=1}^{\infty}(p_i) \quad \subseteq \quad \bigcap_{i=2}^{\infty}(p_i) \quad \subseteq \quad \bigcap_{i=3}^{\infty}(p_i) \quad \subseteq \quad \cdots$$

is stationary.

2 Principal Ideal Domains

2.1 Definition

A **principal ideal domain** is an integral domain in which all ideals are principal. It is clear that all such domains are Noetherian.

Theorem 3. *Let R be a principal ideal domain. Then all nonzero prime ideals of R are maximal.*

Proof. Let (p) be a prime ideal contained in the maximal ideal (m). Supposing for contradiction that

$$(p) \subset (m) \subset R,$$

we obtain that (p) is not irreducible, which contradicts Theorem 1. Hence $(p) = (m)$, so (p) is maximal. $\square$

Three helpful facts about principal ideal domains are as follows:

1. If $\mathfrak{a}_1 = (a_1)$ and $\mathfrak{a}_2 = (a_2)$ are principal ideals, then $\mathfrak{a}_1\mathfrak{a}_2 = (a_1a_2)$. This holds in any commutative ring.

2. Prime ideals cannot contain other prime ideals: if $(p_1) \subset (p_2)$ are prime, then the fact

$$(p_1) \ \subset \ (p_2) \ \subset \ R$$

implies that (p_1) is not irreducible — a contradiction.

3. All prime ideals are relatively prime. This is because if (p_1) and (p_2) are prime, we have

$$(p_1) \ \subseteq \ (p_1) + (p_2) \ \subseteq \ R$$

We cannot have $(p_1) = (p_1) + (p_2)$ by Fact 2; thus since (p_1) to be irreducible, we conclude that $(p_1) + (p_2) = R$.

4. If $(p_1), \ldots, (p_n)$ are prime ideals, then

$$(p_1) \cap \cdots \cap (p_n) \ = \ (p_1) \times \cdots \times (p_n) \ = \ (p_1 \cdots p_n).$$

2.2 Relation with Unique Factorization Domains

Theorem 4. *All principal ideal domains are unique factorization domains.*

Proof. Let R be a principal ideal domain and select $x \in R$. Then since R is Noetherian, factoring terminates: each ascending chain of principal ideals is stationary.

Let $(p_1), \ldots, (p_n)$ be the prime ideals which contain x. By Fact 4, we deduce that $x \in (p_1p_2 \cdots p_n)$. Thus we can write x in the form

$$x \ = \ u_1p_1 \cdots p_n.$$

If u_1 is contained in prime ideals, then they must be among $(p_1), \ldots, (p_n)$. Hence we can express u_1 as a product of some $p_1, \ldots, p_n$ times u_2. Repeating at nauseum, we obtain a sequence $u_1, u_2, \ldots$ which yields the stationary chain

$$(x) \subseteq (u_1) \subseteq (u_2) \subseteq \cdots .$$

Hence there must exist $n \in \mathbb{Z}_{>0}$ such that $(u_n) = (u_{n+1}) = \cdots$. Thus we have $u_n = u \cdot u_{n+1}$ for some unit u. Recursive substitution into our expression for x yields

$$x = up_1^{e_1} \cdots p_n^{e_n},$$

which completes the existence portion of the proof. As per uniqueness, suppose that

$$up_1 \cdots p_n \; = \; x \; = \; wq_1 \cdots q_m$$

A quick induction on $\max\{m, n\}$ yields that since two primes on either side must be adjoints, we can divide and yield a number which factors uniquely. This completes the proof. □

3 Euclidean Domain

3.1 Definition

An integral domain R is a **Euclidean domain** if there exists a size function σ such that $a \in R$ and *nonzero* $b \in R$ implies the existence of $q, r \in R$ such that $a = bq + r$, where $\sigma(r) < \sigma(b)$. It is clear that $\mathbb{Z}$ is a Euclidean domain.

3.2 Examples

Theorem 5. $\mathbb{Z}[i]$ *is a Euclidean domain.*

Proof. Using the norm $\|a + bi\| = a^2 + b^2$, we will divide $a + bi$ by $c + di$. It is easy to deduce that there exist rationals r, s such that

$$\frac{a + bi}{c + di} \; = \; r + si.$$

Approximate r and s by integers: namely define $n, m \in \mathbb{Z}$ such that $|r - n| \leq \frac{1}{2}$ and $|s - m| \leq \frac{1}{2}$. Then we can express the above as

$$r + si = (n + mi) \; + \; (r - n) + i(s - m).$$

Expanding this out, we obtain a rather messy equation:

$$a + bi \quad = \quad (n + ni)(c + di) \quad + \quad \big((r - n) + i(s - m)\big)(c + di).$$

All that remains to be proven is that the right-most term has a norm less than $c + di$, which is equivalent to showing that $(r - n) + i(s - m)$ has a norm less than one:

$$\|(r - n) + i(s - m)\| = (r - n)^2 + (s - m)^2 \leq \frac{1}{4} + \frac{1}{4} < 1.$$

This completes the proof. □

For a field F, the ring $F[x]$ is a field. I proved this in my contest algebra notes.

Theorem 6. *All fields are Euclidean domains.*

Proof. Let R be a field, and select $a, b \in F$. Then

$$a = b\left(\tfrac{a}{b}\right) + 0.$$

If σ is an arbitrary size function on R, then the caveat of remainder zero ensures that the above equations dictate a valid Euclidean division. □

3.3 Relation with Principal Ideal Domains

Theorem 7. *All Euclidean domains are principal ideal domains.*

Proof. Let R be a Euclidean domain with size function σ and let $\mathfrak{a} \subseteq R$ be an ideal. If $\mathfrak{a} = 0$, then $\mathfrak{a}$ is principal; otherwise, the Well-Ordering Theorem guarantees that there exists a nonzero element $a \in \mathfrak{a}$ of minimal size.

Let $b \in \mathfrak{a}$. Then there exist $q, r \in R$ such that

$$b = aq + r,$$

where $\sigma(r) < \sigma(a)$. Since a is minimal, we must have $r = 0$, in which case $b \in (a)$. We conclude that $\mathfrak{a} = (a)$, so all ideals of R are principal. □

We have thus attained a sequence of types of rings:

rings $\subseteq$ commutative rings $\subseteq$ integral domains $\subseteq$ UFDs $\subseteq$ PIDs $\subseteq$ GDs $\subseteq$ fields.

4 Greatest Common Divisor

Let R be an integral domain, and select $a, b \in R$. A **greatest common divisor** of a and b is an element $d \in R$ such that:

1. $d \mid a$ and $d \mid b$.
2. $c \mid a$ and $c \mid b$ implies $c \mid d$.

It is clear that GCDs are unique up to association by Condition 2 — thus we can speak of *the* GCD. If the only greatest common divisors of a and b are units, we set $\gcd(a, b) = 1$ and call a, b **relatively prime**.

Theorem 8. *Suppose R is a principal ideal domain. Then the generator of the ideal (a, b) is the greatest common divisor of a, b.*

Proof. It is clear that $a, b \in (d)$ implies $d \mid a$ and $d \mid b$. $\square$