Factorization in Domains

Ryan C. Daileda

Trinity University

Modern Algebra II

Last Time

Motivated by the Fundamental Theorem of Arithmetic (FTA), given a domain D and $a \in D \setminus (D^\times \cup \{0\})$ we decided:

- a is *irreducible* if $a = bc$ with in D implies $b \in D^\times$ or $c \in D^\times$;
- a is prime if $a|bc$ in D implies $a|b$ or $a|c$ (in D).

We also proved a few fundamental results.

Lemma

Let D be a domain and $a \in D \setminus (D^\times \cup \{0\})$. Then:

- *a is prime iff (a) is a prime ideal.*
- *a is irreducible iff (a) is maximal among principal ideals.*

Lemma

In a domain, prime implies irreducible.

Theorem

If D is a PID, then prime and irreducible are equivalent notions. In particular, prime elements generate maximal ideals.

Corollary

If $f \in F[x]$ is irreducible, then $K = F[x]/(f)$ is a field extension of F containing a root of f, namely $\alpha = x + (f)$.

Example. $x^2 + 1 \in \mathbb{F}_3[x]$ is irreducible since it has no root in $\mathbb{F}_3$. By the division algorithm, the distinct elements of

$$K = \mathbb{F}_3[x]/(x^2 + 1)$$

have the form $a + bx + (f)$ $(a, b \in \mathbb{F}_3)$.Write $a + bi$ for such a coset.
Since $i = x + (f)$ is a root of f, it satisfies $i^2 + 1 = 0$ or $i^2 = -1$.Thus

$$K = \{a + bi \,|\, a, b \in \mathbb{F}_3 \text{ and } i^2 = -1\}$$

is a field extension of $\mathbb{F}_3$ with 9 elements containing a root of $x^2 + 1$.

The ACC

A sequence

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \tag{1}$$

of ideals in a ring R is called an *ascending chain of ideals*.

We say the chain (1) *stabilizes* if there is an $n \in \mathbb{N}$ so that $I_n = I_k$ for all $k \geq n$.

Finally, R is said to satisfy the *ascending chain condition* (ACC) if every ascending chain of ideals in R stabilizes. In this case we call R *Noetherian*.

We will connect ascending chains of ideals to factorizations of ring elements. First we present an alternate formulation of the Noetherian property.

Noetherian iff Ideals are Finitely Generated

Theorem

Let R be a commutative ring with unity. Then R is Noetherian if and only if every ideal in R has the form

$$Ra_1 + Ra_2 + \cdots + Ra_n = (a_1, a_2, \ldots, a_n)$$

for some $n \in \mathbb{N}$ and $a_i \in R$, i.e. every ideal is finitely generated.

Proof. ($\Leftarrow$) Consider a chain (1) of ideals in R and let $I = \bigcup_{k \in \mathbb{N}} I_k$, also an ideal in R (HW).

Write $I = (a_1, a_2, \ldots, a_m)$.

Since each a_i must belong to some ideal in the chain, the right-most of these, I_n, contains all of the a_i, and hence I.

That is

$$I \subseteq I_n \subseteq I_{n+1} \subseteq I_{n+2} \subseteq \cdots \subseteq I,$$

proving that each of these inclusions is an equality, and that the chain stabilizes.

Hence R is Noetherian.

($\Rightarrow$) We prove the contrapositive. Suppose R contains an ideal I that is not finitely generated.

Since I is not finitely generated we may successively choose $a_1 \in I$, $a_2 \in I \setminus (a_1)$, $a_3 \in I \setminus (a_1, a_2)$, $a_4 \in I \setminus (a_1, a_2, a_3), \ldots$

This produces a chain of proper containments

$$(a_1) \subset (a_1, a_2) \subset (a_1, a_2, a_3) \subset (a_1, a_2, a_3, a_4) \subset \cdots$$

i.e. a chain of ideals that doesn't stabilize.

Therefore R is not Noetherian. □

Corollary

Every PID is Noetherian.

Remark. We will primarily be interested in chains of principal ideals in a domain D. It is therefore worth noting that for $a, b \in D \setminus \{0\}$:

- $(a) \subseteq (b) \iff b|a$;
  "To contain is to divide."
- $(a) = (b) \iff a = bc$ for some $c \in D^\times$
  a and b are *associates* ;
- $(a) \subset (b) \iff a = bc$ for some $c \in D \setminus (D^\times \cup \{0\})$.

Lemma

Let D be a domain. If $a \in D \setminus (D^\times \cup \{0\})$ is not a product of irreducibles, then there exists $b \in D \setminus (D^\times \cup \{0\})$ that is not a product of irreducibles so that $(a) \subset (b)$.

Proof. If $a \in D \setminus (D^\times \cup \{0\})$ is not a product of irreducibles, then in particular it is not irreducible.

So we can write $a = bc$ with $b, c \in D \setminus (D^\times \cup \{0\})$.

If both b and c were products of irreducibles, then so would be $bc = a$.

Therefore, without loss of generality, b is not a product of irreducibles, and since $c \notin D^\times$, $(a) \subset (b)$. □

ACC and Irreducible Factorizations

Theorem

Let D be a domain. If D satisfies the ACC on principal ideals, then every $a \in D \setminus (D^\times \cup \{0\})$ is equal to a product of irreducibles.

Proof. Any ascending chain

$$(a_1) \subset (a_2) \subset (a_3) \subset \cdots \subset (a_n), \quad n \geq 1,$$

of principal ideals generated by elements that are not products of irreducibles can always be lenghtened, according to the preceding lemma.

So if there is $a_1 \in D \setminus (D^\times \cup \{0\})$ that is not a product of irreducibles (to start the chain), we can construct an ascending chain of principal ideals that does not stabilize.

D will therefore not satisfy the ACC on principal ideals.

This establishes the contrapositive of the theorem, thereby proving it. □

Corollary

Elements of a Noetherian domain can be factored into products of irreducibles.

Corollary

Elements of a PID can be factored into products of irreducibles.

Unique Factorizations

We have seen that a certain chain condition on ideals yields factorizations of elements into irreducibles. What, if anything, guarantees that such factorizations are unique?

Uniqueness Requirement 1. First of all, since we are dealing with commutative rings that may not possess any natural ordering, we should allow for rearrangement of the factors.

Some additional conditions are still needed, however, as the next examples demonstrate.

Example. According to the definition,

$$6 = 2 \cdot 3 = (-2)(-3)$$

are both factorizations of 6 into irreducibles in $\mathbb{Z}$. Clearly they are not the same, even if we allow rearrangement.

The problem is the signs, which are the units of $\mathbb{Z}$.

These are easy to dispense with in the FTA by dealing only with positive primes.

But in general we cannot simply avoid elements that are associate.

Uniqueness Requirement 2. Associate factors should be considered equivalent.

There's still one more issue to consider.

Example. Consider the factorizations

$$4 = 2 \cdot 2 = \underbrace{(1+\sqrt{-3})}_{\alpha}\underbrace{(1-\sqrt{-3})}_{\beta} \quad \text{in } D = \mathbb{Z}[\sqrt{-3}].$$

We know α, likewise β, is irreducible in D.

So is 2, for if $2 = xy$ in D then

$$4 = N(2) = N(xy) = N(x)N(y).$$

We have already seen this equation implies x or y is a unit.

We have also seen that $\alpha \nmid 2$ in D, so that α and 2 are not associates.

4 therefore has two distinct (even allowing for reordering and associates) factorizations into irreducibles in D.

The Problem. In the proof of the FTA it is the irreducibility of prime numbers that provides prime factorizations, but it is the fact that prime numbers are actually ring-theoretically prime that proves the uniqueness of those factorizations.

The latter is true in general. To prove it we first require a lemma.

Lemma

Let D be a domain and $p, q \in D$ be prime. Then $p|q$ if and only if p and q are associates.

Proof. $p|q$ iff $(q) \subseteq (p)$ iff $(q) = (p)$ iff p and q are associates.

Here we have used the facts that:

- primes are irreducible and;
- irreducibles generate ideals that are maximal among principal ideals.

□

Theorem (Uniqueness of Prime Factorizations)

Let D be a domain and let $p_1, p_2, \ldots, p_k, q_1, q_2, \ldots, q_\ell \in D \setminus (D^\times \cup \{0\})$ be prime. If

$$p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell \tag{2}$$

then $k = \ell$ and, after possibly reordering, p_i is associate to q_i for all i.

Proof (sketch). Since p_1 is prime, after possibly reordering, $p_1 | q_1$, and hence the two are associates by the previous result.

Absorbing the unit difference into p_2, we can cancel to obtain

$$p_2 \cdots p_k = q_2 \cdots q_\ell.$$

Now repeat with p_2 and q_2, p_3 and q_3, etc. until one side runs out of primes and is simply a unit.

This makes any factors on the other side units as well. Since primes are not units, there can be no primes on the other side, so $k = \ell$. □

A cleaner, more precise, proof is given by inducting on k.

FTA domains

Finally we have

Uniqueness Requirement 3. Irreducibles must be prime.

Because the analogue of the FTA as we have formulated it would hold in a domain D in which irreducibles are prime and all nonzero, nonunit elements possess factorizations into irreducibles, we call such a ring an *FTA domain*.

Remarks.

- The terminology FTA domain is non-standard, but is equivalent to the following more traditional definition.
- The equivalence of irreducible with prime and the existence of irreducible factorizations are independent: a ring may have one property and not the other.

UFDs

Definition

Let D be a domain and suppose that every $a \in D \setminus (D^\times \cup \{0\})$ has a unique factorization into irreducibles, i.e. there exist irreducibles $r_1, r_2, \ldots, r_k \in D$ so that $a = r_1 r_2 \cdots r_k$ and if $s_1, s_2, \ldots, s_\ell \in D$ are irreducible and satisfy $a = s_1 s_2 \cdots s_\ell$, then $k = \ell$ and, after possibly reordering, r_i is associate to s_i for all i. Then D is called a unique factorization domain *(UFD).*

According to the results we have established, every FTA domain is a UFD. The converse follows from the following fact.

Theorem

Let D be a UFD. If $a \in D$ is irreducible, then a is prime.

Proof. Let $a \in D$ be irreducible and suppose $a|bc$ in D.

Write $ad = bc$ and factor each of b, c, d into irreducibles.

Since a occurs in the irreducible factorization of ad, uniqueness of factorizations implies, without loss of generality, it is associate to one of the irreducibles occurring in b.

That is, $a|b$ and hence a is prime. □

Because they are FTA domains according to earlier results,

Theorem

Every Noetherian domain in which irreducibles are prime is a UFD.

We immediately point out that Noetherian may be weakened to satisfying the ACC on principal ideals.

Corollary

Every PID is a UFD.

Corollary

$\mathbb{Z}$ *and* $F[x]$ *are UFDs.*

If D is a UFD, then content of polynomials in $D[x]$ is well-defined, and Gauss' Lemma and its consequences can be proven to hold. In particular, one can use these results to prove that

Theorem

If D *is a UFD, then so is* $D[x]$.

$\mathbb{Z}[x]$ and $F[x, y]$ therefore provide examples of UFDs that are not PIDs.

Regarding PIDs, we have thus far seen two: $\mathbb{Z}$ and $F[x]$.

Both were shown to be PIDs using an appropriate division algorithm.

This puts them into a narrower class of domains, namely the *Euclidean domains.*

Euclidean domains

Definition

Let D be a domain. D is called a Euclidean domain *(ED) if there exists a function $d : D \setminus \{0\} \to \mathbb{N}_0$ so that:*

a. *$d(a) \leq d(ab)$ for all $a, b \in D \setminus \{0\}$;*

b. *if $a, b \in D$ and $b \neq 0$, then there exist $q, r \in D$ so that $a = bq + r$ with $r = 0$ or $d(r) < d(b)$.*

$\mathbb{Z}$ is an ED with $d(n) = |n|$ and $F[x]$ is an ED with $d(f) = \deg(f)$.

Although they enjoy a host of properties similar to those of $\mathbb{Z}$ and $F[x]$, for now we will only be concerned with one.

Theorem

Every ED is a PID.

We give the "usual" proof.

Proof. Let D be an ED and I a nonzero ideal in D.

By the Well Ordering Principle, $d(I \setminus \{0\})$ has a least element $d(a)$.

Let $b \in I$ and write $b = aq + r$ with $r = 0$ or $d(r) < d(a)$.

Since $r = b - aq \in I$, we cannot have $d(r) < d(a)$.

Therefore $r = 0$ and $b = aq \in (a)$.

Hence $I \subseteq (a) \subseteq I$, and so $I = (a)$ is principal. □

Final Remarks

- One can show that $\mathbb{Z}[i]$ with

$$d(x+iy) = N(x+iy) = (x+iy)(x-iy) = x^2 + y^2$$

  is an ED. See the textbook.
- We have proven that

$$\text{ED} \quad \Rightarrow \quad \text{PID} \quad \Rightarrow \quad \text{UFD}.$$

  Neither implication is reversible.
- An example of a non-Euclidean PID is the ring

$$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] = \left\{ \frac{a+b\sqrt{-19}}{2} \;\middle|\; a \equiv b \pmod 2 \right\}.$$

  See *A Principal Ideal Ring That Is Not A Euclidean Ring*.