Factorization in Domains

Ryan C. Daileda

Trinity University

Modern Algebra II

Divisibility and Factors

Recall: Given a domain D and $a, b \in D$,

$$a|b \;\Leftrightarrow\; (\exists c \in D)(b = ac),$$

and we say a *divides* b or a is a *factor* of b.

In terms of principal ideals:

- $a|b \;\Leftrightarrow\; (b) \subset (a)$
- $u \in D^\times \;\Leftrightarrow\; (u) = D \;\Leftrightarrow\; (\forall a \in D)(u|a)$
- $a|b$ and $b|a \;\Leftrightarrow\; (a) = (b) \;\Leftrightarrow\; \underbrace{(\exists u \in D^\times)(a = bu)}_{a,b \text{ are } associates}$

Examples

1. $7|35$ in $\mathbb{Z}$ since $35 = 7 \cdot 5$.
2. $2 + 3i$ divides 13 in $\mathbb{Z}[i]$ since $13 = (2 + 3i)(2 - 3i)$.
3. If F is a field, $a \in F$ and $f(X) \in F[X]$ then

$$f(a) = 0 \quad \Leftrightarrow \quad X - a \text{ divides } f(X) \text{ in } F[X].$$

4. In $\mathbb{Z}[\sqrt{-5}]$, $2 + \sqrt{-5}$ is a factor of 9:

$$9 = (2 + \sqrt{-5})(2 - \sqrt{-5}).$$

Prime and Irreducible Elements

Let D be a domain and $\dot{D} = D \setminus (D^\times \cup \{0\})$. Motivated by arithmetic in $\mathbb{Z}$, we make the following definitions.

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

We will prefer "irreducible," but "atomic" is also common in the literature.

Remarks

1. $p \in \mathbb{Z}$ is "prime" in the traditional sense if and only if it is *irreducible* in the ring-theoretic sense. Every irreducible in $\mathbb{Z}$ is indeed prime, but *this requires proof* (i.e. Bézout's Lemma).

2. $a \in \dot{D}$ is irreducible if and only if the only factors of a are units and associates.

3. The element 0 is "prime," but we exclude it to avoid the need to distinguish between zero and nonzero primes otherwise.

Examples

1. $5 + 2i$ is irreducible in $\mathbb{Z}[i]$ because $N(5 + 2i) = 29$ is prime in $\mathbb{Z}$ (exercise). It is also prime, as we will see.

2. For $a \in F$ (a field), $X - a$ is irreducible and prime in $F[X]$, since only divisors have degree 1 or 0. For a different proof, see below.

3. In $Z[\sqrt{-5}]$, 3 and $2 \pm \sqrt{-5}$ are irreducible, but are *not* prime because $3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$ (HW).

Primes are Irreducible

Example 3 shows that irreducibles are not always prime. However, primes *are* always irreducible.

Lemma 1 (Primes are Irreducible)

Let D be a domain and $a \in \dot{D}$. If a is prime, then a is irreducible.

Proof. If $a \in \dot{D}$ is prime and $b, c \in D$, then

$$a = bc \;\Rightarrow\; 1 \cdot a = bc \;\Rightarrow\; a \mid bc \overset{\text{WLOG}}{\Longrightarrow} a \mid b$$

$$\Rightarrow\; a = (ad)c = a(cd),\ d \in D \;\Rightarrow\; cd = 1 \;\Rightarrow\; c \in R^{\times}$$

Therefore a is irreducible. □

Irreducibles and Ideals

Lemma 2

Let D be a domain and $a \in \dot{D}$. Then:

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

Proof. Let $a \in \dot{D}$. Then

$$a \text{ is prime } \Leftrightarrow \forall (b, c \in D)(a|bc \Rightarrow a|b \text{ or } a|c)$$

$$\Leftrightarrow \forall (b, c \in D)(bc \in (a) \Rightarrow b \in (a) \text{ or } c \in (a))$$

$$\Leftrightarrow (a) \text{ is prime.}$$

And

$$a \text{ is irred.} \Leftrightarrow \forall(b, c \in D)(a = bc \Rightarrow b \in R^\times \text{ or } c \in R^\times)$$

$$\Leftrightarrow \forall(b \in D)((a) \subset (b) \Rightarrow (a) = (b) \text{ or } (b) = R)$$

$$\Leftrightarrow (a) \text{ is maximal among principals.}$$

□

Corollary 1

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

Proof. In a PID, "maximal among principals" is just "maximal." Since maximal ideals are prime, this means irreducible elements are prime elements. Now apply Lemma 1.

AP Domains

A domain D in which every irreducible element is prime is called an *AP domain* (for "atomic implies prime").

1. $\mathbb{Z}$ and $\mathbb{Z}[i]$ are AP domains by Corollary 1.
2. If F is a field, then $F[X]$ is an AP domain by Corollary 1.
3. If F is a field, then the monoid ring

$$F[X;\mathbb{Q}_0^+] = \left\{ \sum_{r\in\mathbb{Q}_0^+} a_r X^r \;\middle|\; a_r \in F, \text{ almost all zero} \right\}$$

is an AP domain. See handout.

Factorization

Recall: Let D be a domain. A *factorization* of $a \in \dot{D}$ is a product

$$a = a_1 a_2 \cdots a_n, \quad a_i \in D, \quad n \geq 1. \tag{1}$$

We say (1) is *nontrivial* if $a_i \in \dot{D}$ for all i. We call n the *length* of (1).

Primes and irreducibles each play specific roles in factorization theory:

- Irreducibles tell us "when to stop factoring."
- Factorizations into primes are (nearly) unique.

We'll look at factorization by irreducibles first.

Factorization by Irreducibles

Irreducibles in D only have nontrivial factorizations of length 1: they cannot be factored nontrivially. What about other elements?

Negating the definition of irreducible we find $a \in \dot{D}$ is *reducible* if there are $b, c \in \dot{D}$ so that $a = bc$.

So reducible elements have nontrivial factorizations of length at least 2. How long can they be?

In general, suppose $a = a_1 \cdots a_n$ in $\dot{D}$ is nontrivial.

- If some a_i is reducible, we can replace it with $a_i' a_i''$. This yields a nontrivial factorization of length $n + 1$.
- If every a_i is irreducible, we cannot increase n through additional factorization.

Moral: The nontrivial factorizations of maximal length are the factorizations into irreducibles.

Warning: Different factorizations of the same element by irreducibles can have different lengths! And factorizations of the same length can involve different irreducibles!

Example: Let $M = \mathbb{N}_0 \setminus \{1\}$ and $D = F[X, M]$, the ring of all polynomials over F with no linear term.

Because $1 \notin M$, X^2 and X^3 are irreducible in D. Yet

$$X^6 = X^2X^2X^2 = X^3X^3.$$

Example: Let $D = \mathbb{Z}[\sqrt{-5}]$. As noted above, $3, 2 \pm \sqrt{-5}$ are all nonassociate irreducibles in D. However,

$$9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5}).$$

Factorization by Primes

Prime factorizations are a subclass of the irreducible factorizations.

Nonuniqueness difficulties with factorizations can be handled by considering factorization into primes.

Lemma 3 (Uniqueness of Prime Factorizations)

Let D be a domain and suppose

$$p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$$

with $p_i, q_j \in \dot{D}$ primes. Then $m = n$ and, after possibly reindexing, p_i is associate to q_i for all i.

Proof. We induct on m. When $m = 1$, p_1 is prime, hence irreducible, so its only nontrivial factorizations are of length 1. Thus $n = 1$ and $p_1 = q_1$.

Let $m > 1$ and assume the result for fewer than m primes p_i.

The hypotheses imply

$$p_m | q_1 \cdots q_n \quad \Rightarrow \quad p_m | q_k \text{ some } k.$$

But q_k is irreducible and p_m is not a unit, so p_m, q_k are associates.

Reindex the q_j so that $q_k \to q_n$. Then there is an $\epsilon_n \in D^\times$ so that

$$\begin{aligned} p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_{n-1} \epsilon_n p_m \quad \Rightarrow \quad p_1 \cdots p_{m-1} &= \epsilon_n q_1 \cdots q_{n-1} \\ &= q_1' q_2 \cdots q_{n-1}, \end{aligned}$$

where q_1' is associate to q_1 and therefore also prime.

By the inductive hypothesis, $m-1=n-1$ (so that $m=n$), and after reindexing p_i is associate to q_i for all $i \leq m-1$, too $\square$

We can now interpret our earlier nonuniqueness examples.

Example. When $D=F[X;M]$ with $M=\mathbb{N}_0 \setminus \{1\}$, in the irreducible factorizations

$$X^6 = X^2X^2X^2 = X^3X^3,$$

X^2 and X^3 are *not prime*, by Lemma 3.

Example. When $D=\mathbb{Z}[\sqrt{-5}]$, in the irreducible factorizations

$$9 = 3 \cdot 3 = (2+\sqrt{-5})(2-\sqrt{-5}),$$

3 and $2 \pm \sqrt{-5}$ are *not prime*, by Lemma 3.

Existence and Uniqueness Questions

Let D be a domain. We are now faced with two *fundamental factorization questions*:

(E) **Existence:** under what hypotheses does every element of $\dot{D}$ factor into irreducibles?

(U) **Uniqueness:** under what hypotheses does every element of $\dot{D}$ factor into primes?

Since an irreducible cannot factor as more than one prime, if every element in $\dot{D}$ has a prime factorization, then D is an AP domain.

Conversely, if D is an AP domain and every element of $\dot{D}$ factors into irreducibles, then every element has a prime factorization.

Unique Factorization Domains

Therefore

(AP domain+irred. factorizations) = (domain+prime factorizations).

A ring satisfying either of these equivalent sets of conditions is called a *Unique Factorization Domain* (UFD).

In a UFD every element has a unique (up to associates and order) factorization into irreducibles.

In fact, it is not hard to argue that existence and uniqueness of irreducible factorizations in a domain D is equivalent to the statement that D is a UFD.

This is frequently given as the *definition* of a UFD in textbooks.

Back to Question (E)

Putting aside the question of which domains are AP domains, we are only left with question (E).

The typical way to approach factorization into irreducibles is recursively. We start with $a \in \dot{D}$.

If a is irreducible, there's nothing to do. Otherwise $a = bc$ with $b, c \in \dot{D}$. Now recursively apply these steps to b and c.

So we keep finding divisors of divisors of divisors until (hopefully) we can't any more. What might go wrong?

Factorization and Chains of Ideals

Notice that if $a = a_1 b_1$ with $a_1, b_1 \dot{D}$, then $(a) \subsetneq (a_1)$.

If a_1 is not irreducible, then $a_1 = a_2 b_2$ with $a_2, b_2 \in \dot{D}$, and $(a_1) \subsetneq (a_2)$.

And if a_2 fails to be irreducible we obtain $a_3 \in \dot{D}$ so that $(a_2) \subsetneq (a_3)$.

This yields a *chain* of principal ideals

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots,$$

which terminates if ever a_i is irreducible.

But this may never happen!

Example

Let $D = F[X; \mathbb{Q}_0^+]$, the "polynomials" over F with nonnegative rational exponents.

Then $\cdots X^{\frac{1}{4}} | X^{\frac{1}{3}} | X^{\frac{1}{2}} | X$, simply because $\frac{1}{n} - \frac{1}{n+1} \in \mathbb{Q}_0^+$.

So in D we have the infinite chain

$$(X) \subsetneq (X^{\frac{1}{2}}) \subsetneq (X^{\frac{1}{3}}) \subsetneq (X^{\frac{1}{4}}) \subsetneq \cdots .$$

Something similar happens no matter how we try to factor X.

Therefore, $X \in \dot{D}$ *cannot* be factored into irreducibles in D.

The ACC and ACCP

A sequence

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \tag{2}$$

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

We say (2) *stabilizes* if there is an $n \in \mathbb{N}$ so that $I_n = I_k$ for all $k \geq n$.

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*.

R is said to satisfy the *ascending chain condition on principal ideals* (ACCP) if every ascending chain of principal ideals in R stabilizes.

Note that ACC $\Rightarrow$ ACCP. The converse of this statement is *false*.

Lemma 4

Let D be a domain. If $a \in \dot{D}$ lacks an irreducible factorization, then there exists $b \in \dot{D}$, also lacking an irreducible factorization, so that $(a) \subsetneq (b)$.

Proof. If $a \in \dot{D}$ doesn't factor into irreducibles, then it is not itself irreducible.

Therefore $a = bc$ with $b, c \in \dot{D}$.

If both b and c had irreducible factorizations, then so would be a, their product.

Therefore (WLOG) b is not a product of irreducibles, and since $c \notin D^\times$, $(a) \subsetneq (b)$. □

ACCP and Irreducible Factorizations

Theorem 1

Let D be a domain. If D satisfies the ACCP, then every $a \in \dot{D}$ factors into irreducibles.

Proof. Any ascending chain

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

of principal ideals generated by elements that don't factor into irreducibles can always be lenghtened, according to Lemma 4.

So if there is at least one $a_1 \in \dot{D}$ that is not a product of irreducibles, we can construct an ascending chain in violation of ACCP. This proves the contrapositive of the theorem. □

Factorization in Noetherian Domains

Because ACC $\Rightarrow$ ACCP, we immediately have:

Corollary 2

Elements of a Noetherian domain can be factored into irreducibles. A Noetherian AP domain is a UFD.

A practical way to show that ACC holds is to apply the following important result.

Theorem 2

Let R be a commutative ring. Then R is Noetherian if and only if every ideal in R is finitely generated.

Proof. ($\Leftarrow$) Consider a chain (2) 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.

$(\Rightarrow)$[1] We prove the contrapositive.

Suppose R contains an ideal I that is not finitely generated. Then we can successively choose

$$a_1 \in I, a_2 \in I \setminus (a_1), a_3 \in I \setminus (a_1, a_2), a_4 \in I \setminus (a_1, a_2, a_3), \ldots$$

[1] This proof contains a subtle logical error. Correcting it requires appealing to the Axiom of Choice.

This produces a chain of proper containments

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

which violates ACC. Therefore R is not Noetherian. □

Corollary 3

Every PID is Noetherian.

Corollary 4

Every PID is a UFD.

Proof. Every PID is a Noetherian AP domain, by Corollaries 3 and 1. Now appeal to Corollary 2. □

Example. The rings $\mathbb{Z}$, $\mathbb{Z}[i]$ and $F[X]$ are all UFDs.

Every UFD is a *Bézout domain*: a domain in which every finitely generated ideal is principal.

Given $a_1, \cdots a_n \in D$, we say $a \in D$ is their *greatest common divisor* if $(a_1, a_2, \ldots, a_n) = (a)$. The GCD is only unique up to association.

After studying localization and quotient fields, we will be able to use GCDs to prove the following important result.

Theorem 3 (Gauss)

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

Example. $\mathbb{Z}[x]$ and $F[x, y] = F[x][y]$ are UFDs that are not PIDs.

Final Remarks

- We have proven that

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

None of these implications are 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*.