Lecture 7.4: Divisibility and factorization

Matthew Macauley

Department of Mathematical Sciences
Clemson University
http://www.math.clemson.edu/~macaule/

Math 4120, Modern Algebra

Introduction

A ring is in some sense, a generalization of the familiar number systems like $\mathbb{Z}$, $\mathbb{R}$, and $\mathbb{C}$, where we are allowed to add, subtract, and multiply.

Two key properties about these structures are:

- multiplication is commutative,
- there are no (nonzero) zero divisors.

Blanket assumption

Throughout this lecture, unless explicitly mentioned otherwise, R is assumed to be an integral domain, and we will define $R^* := R \setminus \{0\}$.

The integers have several basic properties that we usually take for granted:

- every nonzero number can be factored uniquely into primes;
- any two numbers have a unique greatest common divisor and least common multiple;
- there is a Euclidean algorithm, which can find the gcd of two numbers.

Surprisingly, these need not always hold in integrals domains! We would like to understand this better.

Divisibility

Definition

If $a, b \in R$, say that a divides b, or b is a multiple of a if $b = ac$ for some $c \in R$. We write $a \mid b$.

If $a \mid b$ and $b \mid a$, then a and b are associates, written $a \sim b$.

Examples

- In $\mathbb{Z}$: n and $-n$ are associates.
- In $\mathbb{R}[x]$: $f(x)$ and $c \cdot f(x)$ are associates for any $c \neq 0$.
- The only associate of 0 is itself.
- The associates of 1 are the units of R.

Proposition (HW)

Two elements $a, b \in R$ are associates if and only if $a = bu$ for some unit $u \in U(R)$.

This defines an equivalence relation on R, and partitions R into equivalence classes.

Irreducibles and primes

Note that units divide everything: if $b \in R$ and $u \in U(R)$, then $u \mid b$.

Definition

If $b \in R$ is not a unit, and the only divisors of b are units and associates of b, then b is irreducible.

An element $p \in R$ is prime if p is not a unit, and $p \mid ab$ implies $p \mid a$ or $p \mid b$.

Proposition

If $0 \neq p \in R$ is prime, then p is irreducible.

Proof

Suppose p is prime but not irreducible. Then $p = ab$ with $a, b \notin U(R)$.

Then (wlog) $p \mid a$, so $a = pc$ for some $c \in R$. Now,

$$p = ab = (pc)b = p(cb)\,.$$

This means that $cb = 1$, and thus $b \in U(R)$, a contradiction. $\square$

Irreducibles and primes

Caveat: Irreducible $\not\Rightarrow$ prime

Consider the ring $R_{-5} := \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$.

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

but $3 \nmid 2 + \sqrt{-5}$ and $3 \nmid 2 - \sqrt{-5}$.

Thus, 3 is irreducible in R_{-5} but *not* prime.

When irreducibles fail to be prime, we can lose nice properties like unique factorization.

Things can get really bad: not even the *lengths* of factorizations into irreducibles need be the same!

For example, consider the ring $R = \mathbb{Z}[x^2, x^3]$. Then

$$x^6 = x^2 \cdot x^2 \cdot x^2 = x^3 \cdot x^3.$$

The element $x^2 \in R$ is not prime because $x^2 \mid x^3 \cdot x^3$ yet $x^2 \nmid x^3$ in R (note: $x \notin R$).

Principal ideal domains

Fortunately, there is a type of ring where such "bad things" don't happen.

Definition

An ideal I generated by a single element $a \in R$ is called a principal ideal. We denote this by $I = (a)$.

If every ideal of R is principal, then R is a principal ideal domain (PID).

Examples

The following are all PIDs (stated without proof):

- The ring of integers, $\mathbb{Z}$.
- Any field F.
- The polynomial ring $F[x]$ over a field.

As we will see shortly, PIDs are "nice" rings. Here are some properties they enjoy:

- pairs of elements have a "greatest common divisor" & "least common multiple";
- irreducible $\Rightarrow$ prime;
- Every element factors uniquely into primes.

Greatest common divisors & least common multiples

Proposition

If $I \subseteq \mathbb{Z}$ is an ideal, and $a \in I$ is its smallest positive element, then $I = (a)$.

Proof

Pick any positive $b \in I$. Write $b = aq + r$, for $q, r \in \mathbb{Z}$ and $0 \leq r < a$.

Then $r = b - aq \in I$, so $r = 0$. Therefore, $b = qa \in (a)$. $\square$

Definition

A common divisor of $a, b \in R$ is an element $d \in R$ such that $d \mid a$ and $d \mid b$.

Moreover, d is a greatest common divisor (GCD) if $c \mid d$ for all other common divisors c of a and b.

A common multiple of $a, b \in R$ is an element $m \in R$ such that $a \mid m$ and $b \mid m$.

Moreover, m is a least common multiple (LCM) if $m \mid n$ for all other common multiples n of a and b.

Nice properties of PIDs

Proposition

If R is a PID, then any $a, b \in R^*$ have a GCD, $d = \gcd(a, b)$.

It is *unique up to associates*, and can be written as $d = xa + yb$ for some $x, y \in R$.

Proof

Existence. The ideal generated by a and b is

$$I = (a, b) = \{ua + vb : u, v \in R\} .$$

Since R is a PID, we can write $I = (d)$ for some $d \in I$, and so $d = xa + yb$.

Since $a, b \in (d)$, both $d \mid a$ and $d \mid b$ hold.

If c is a divisor of a & b, then $c \mid xa + yb = d$, so d is a GCD for a and b. ✓

Uniqueness. If d' is another GCD, then $d \mid d'$ and $d' \mid d$, so $d \sim d'$. ✓ □

Nice properties of PIDs

Corollary

If R is a PID, then every irreducible element is prime.

Proof

Let $p \in R$ be irreducible and suppose $p \mid ab$ for some $a, b \in R$.

If $p \nmid a$, then $\gcd(p, a) = 1$, so we may write $1 = xa + yp$ for some $x, y \in R$. Thus

$$b = (xa + yp)b = x(ab) + (yb)p\,.$$

Since $p \mid x(ab)$ and $p \mid (yb)p$, then $p \mid x(ab) + (yb)p = b$. $\square$

Not surprisingly, least common multiples also have a nice characterization in PIDs.

Proposition (HW)

If R is a PID, then any $a, b \in R^*$ have an LCM, $m = \operatorname{lcm}(a, b)$.

It is *unique up to associates*, and can be characterized as a generator of the ideal $I := (a) \cap (b)$.

Unique factorization domains

Definition

An integral domain is a unique factorization domain (UFD) if:

(i) Every nonzero element is a product of irreducible elements;

(ii) Every irreducible element is prime.

Examples

1. $\mathbb{Z}$ is a UFD: Every integer $n \in \mathbb{Z}$ can be uniquely factored as a product of irreducibles (primes):
$$n = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}.$$
This is the *fundamental theorem of arithmetic*.

2. The ring $\mathbb{Z}[x]$ is a UFD, because every polynomial can be factored into irreducibles. But it is not a PID because the following ideal is not principal:
$$(2, x) = \{f(x) : \text{ the constant term is even}\}.$$

3. The ring R_{-5} is not a UFD because $9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$.

4. We've shown that (ii) holds for PIDs. Next, we will see that (i) holds as well.

Unique factorization domains

Theorem

If R is a PID, then R is a UFD.

Proof

We need to show Condition (i) holds: every element is a product of irreducibles. A ring is Noetherian if every ascending chain of ideals

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

stabilizes, meaning that $I_k = I_{k+1} = I_{k+2} = \cdots$ holds for some k.

Suppose R is a PID. It is not hard to show that R is Noetherian (HW). Define

$$X = \{a \in R^* \setminus U(R) : a \text{ can't be written as a product of irreducibles}\}.$$

If $X \neq \emptyset$, then pick $a_1 \in X$. Factor this as $a_1 = a_2 b$, where $a_2 \in X$ and $b \notin U(R)$. Then $(a_1) \subsetneq (a_2) \subsetneq R$, and repeat this process. We get an ascending chain

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

that does not stabilize. This is impossible in a PID, so $X = \emptyset$. □

Summary of ring types