Section 45 – Unique factorization domains

Instructor: Yifan Yang

Spring 2007

Overview

- In section 27 we have seen that if F is a field, then every nonconstant polynomial in $F[x]$ can be factored into a product of irreducible polynomials, and the factorization is unique except for order and for units.
- In the same section, we have also seen that every ideal in $F[x]$ is a principal ideal.
- In general, if an integral domain has the unique factorization property, we say it is a unique factorization domain (UFD).
- If an integral domain has the property that every ideal is principal, we say it is a principal ideal domain (PID).
- We will show that if an integral domain is a PID, then it is a UFD.
- We will also describe the result that if D is a UFD, then so is $D[x]$, although we will not go over the proof in the class.

Divisibility, associates, and irreducibles

Definition

Let R be a commutative ring with unity. Let $a, b \in R$.

- If there exists $c \in R$ such that $b = ac$, then a divides b (or a is a factor of b, denoted by $a|b$. The notation $a \nmid b$ means a does not divide b.
- An element u is a unit if u divides 1.
- a and b are associates if $a = ub$ for some unit $u \in R$.

Assume that D is an integral domain.

- A nonzero element p that is not a unit is an irreducible of D if any factorization $p = ab$ in D has the property that either a or b is a unit.

Examples

Example

- The units in $\mathbb{Z}$ are ± 1. Thus, the associates of any integer $n \neq 0$ are $-n$ and n. The irreducibles are just prime numbers and their associates.
- Every nonzero element of a field F is a unit. Thus, any two nonzero elements are associates to each other. None of the elements is an irreducible.
- Let F be a field. The units in $F[x]$ are nonzero constant polynomials.

Unique factorization domains

Definition

An integral domain D is a unique factorization domain (UFD) is

- Every nonzero non-unit element of D can be factored into a product of a finite number of irreducibles.
- If $a \in D$ has two factorizations $p_1 \dots p_r$ and $q_1 \dots q_s$ into products of irreducibles, then $r = s$ and q_j can be renumbered so that p_i and q_i are associates.

Example

- Let F be a field. Then $F[x]$ is a UFD, by Theorem 23.20.
- $\mathbb{Z}$ is a UFD. (Fundamental theorem of arithmetics.)
- The integral domain $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$ is not a UFD. (We have $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, where $2, 3, 1 \pm \sqrt{-5}$ are all irreducibles, but mutually non-associates.)

Remark

- The notion of a UFD was first raised in 1840's in connection of Fermat's Last Theorem.
- Lamé in 1847 announced a "proof" of FLT, in which he used the assumption that $\mathbb{Z}[e^{2\pi i/p}]$ is a UFD.
- However, 1n 1844, Kummer already showed that $\mathbb{Z}[e^{2\pi i/23}]$ is not a UFD.
- Still, Lamé's argument showed that if $\mathbb{Z}[e^{2\pi i/p}]$ is a UFD, then $x^p + y^p = z^p$ has no nontrivial solutions.
- Kummer found a way to measure how far $\mathbb{Z}[e^{2\pi i/p}]$ is from being a UFD, and proved the FLT for many cases where $\mathbb{Z}[e^{2\pi i/p}]$ is not a UFD.

Principal ideal domains

Definition

An integral domain D is a principal ideal domain (PID) if every ideal in D is principal.

Example

- $\mathbb{Z}$ is a PID since an ideal in $\mathbb{Z}$ takes the form $n\mathbb{Z}$ for some integer n.
- By Theorem 27.24, if F is a field, then $F[x]$ is a PID.

PID $\Rightarrow$ UFD, first part

Theorem (45.11)

Let D be a PID. Then every nonzero non-unit element of D is a product of irreducibles.

Lemma (45.9)

Let R be a commutative ring. Suppose that $I_1 \subseteq I_2 \subseteq \cdots$ is an ascending chain of ideals in R. Then $I = \cup_i I_i$ is an ideal of R.

Proof of Lemma 45.9

- We need to show that
  - If $a, b \in I$, then $a + b \in I$.
  - If $a \in I$ and $r \in R$, then $ra \in I$.
- Assume $a, b \in I$. Then $a \in I_k$ and $b \in I_m$ for some k, m. Let $n = \max(k, m)$. Then $I_k, I_m \subseteq I_n$, and $a, b \in I_n$. It follows that $a + b \in I_n \subseteq I$.
- Now assume that $a \in I$. Then $a \in I_k$ for some k. Since I_k is an ideal, for all $r \in R$, we have $ra \in I_k \subseteq I$. $\square$

Ascending chain condition for a PID

Lemma (45.10, ascending chain condition for a PID)

Let D be a PID. Let $I_1 \subseteq I_2 \subseteq \cdots$ be an ascending chain of ideals. Then there is a positive number N such that $I_n = I_N$ for all $n \geq N$.

Remarks

- The statement can also be given as: In a PID, every strictly ascending chain of ideals must be of finite length.
- We refer to this property of a PID by saying that the ascending chain condition (ACC) holds for ideals in a PID.

Proof of Theorem 45.11

We first show that every nonzero non-unit element a has an irreducible factor.

- Suppose a is irreducible. Then there is nothing to be done. So let us assume that a is not an irreducible.
- Then we have $a = a_1 b_1$, where neither a_1 nor b_1 is a unit.
- This implies that $\langle a \rangle \subsetneq \langle a_1 \rangle$.
- If a_1 is an irreducible, then we are done. If not, then $a_1 = a_2 b_2$ for some non-unit a_2 and b_2, and we have $\langle a_1 \rangle \subsetneq \langle a_2 \rangle$.
- Continuing this way, we obtain a sctrictly ascending chain of ideals $\langle a \rangle \subsetneq \langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \cdots$.
- By ACC, this chain of ideals can not go on forever.
- This means that at some point a_n must be an irreducible, which is what we are looking for.

Proof of Theorem 45.11, continued

We now show that every nonzero non-unit element a is a product of irreducibles.

- If a is an irreducible, there is nothing to be done. So let us assume that a is not an irreducible.
- Previously we have shown that a has an irreducible factor, say, $a = p_1 a_1$ for some irreducible p_1 and a_1 is not a unit. Then $\langle a \rangle \subsetneq \langle a_1 \rangle$.
- If a_1 is an irreducible, we are done; otherwise, $a_1 = p_2 a_2$ for some irreducible p_2 and some non-unit a_2. We have $\langle a \rangle \subsetneq \langle a_1 \rangle \subsetneq \langle a_2 \rangle$.
- Continuing this way, we obtain a strictly ascending chain of ideals $\langle a \rangle \subsetneq \langle a_1 \rangle \subsetneq \langle a_2 \rangle \subsetneq \cdots$.
- By ACC, this process terminates at some point, i.e., $a = p_1 \cdots p_r$, where p_i are all irreducibles. $\square$

Analogue of Theorem 27.25

Lemma (45.12)

An ideal $\langle p \rangle$ in a PID is a maximal ideal if and only if p is an irreducible.

Proof.

The proof follows exactly the proof of Theorem 27.25, where we show that an ideal $\langle p(x) \rangle$ in $F[x]$ is a maximal ideal if and only if $p(x)$ is an irreducible polynomial. $\square$

Analogue of Theorem 27.27

Lemma (45.13)

In a PID, if an irreducible p divides ab, then either $p|a$ or $p|b$.

Proof.

The proof follows exactly the proof of Theorem 27.27, where we show that if an irreducible polynomial $p(x)$ in $F[x]$ divides $r(x)s(x)$, then $p(x)|r(x)$ or $p(x)|s(x)$. $\square$

Corollary (45.14)

In a PID, if an irreducible p divides $a_1 \dots a_n$, then $p|a_i$ for at least one i.

Prime

Definition

A nonzero non-unit element p of an integral domain D is a prime if $p|ab$ implies $p|a$ or $p|b$.

Remarks

- In $\mathbb{Z}$, an integer prime p has two properties
  - Only positive divisors of p are 1 (unit) and p itself.
  - If $p|ab$, then $p|a$ or $p|b$.
- In a general integral domain, an element with the first property is called an irreducible, while an element with second property is a prime.
- In an integral domain, a prime is always an irreducible, but an irreducible may not be a prime. (Exercise 25.)
- In a UFD, an element is an irreducible if and only if it is a prime. (Exercise 26.)

Examples of irreducibles that are not primes

- In $\mathbb{Z}[\sqrt{-5}]$, $2, 3, 1 \pm \sqrt{-5}$ are all irreducibles, but neither of them is a prime. (We have $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, but 2 does not divide $1 + \sqrt{-5}$ nor $1 - \sqrt{-5}$ in $\mathbb{Z}[\sqrt{-5}]$.)
- Let F be a field and $D = F[x^2, xy, y^2]$. Then x^2, xy, y^2 are all irreducibles, but neither of them is a prime. (We have $(xy)|(x^2)(y^2)$, but xy does not divide x^2 nor y^2.)

Proof of PID $\Rightarrow$ UFD, second part

We have shown that every nonzero non-unit element is a product of irreducibles. We now show the uniqueness.

- Assume that $a = p_1 \dots p_r$ and $a = q_1 \dots q_s$ are two factorizations into products of irreducibles.
- By Corollary 45.14, p_1 divides one of q_i. By rearranging the index, we assume that p_1 divides q_1.
- Then $q_1 = p_1 u_1$ for some $u_1 \in D$.
- Since q_1 is an irreducible, u_1 must be a unit. That is, p_1 and q_1 are associates.
- We then have $p_2 \dots p_r = u_1 q_2 \dots q_s$.
- Applying the same argument to p_2, we find $q_2 = p_2 u_2$ for some unit u_2, and $p_3 \dots p_r = u_1 u_2 q_3 \dots q_s$.
- Continuing this way, we find $r = s$ and p_i are associates of q_i for each i. $\square$

D is a UFD $\Rightarrow D[x]$ is a UFD

Theorem (45.29)

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

Corollary (45.30)

If F is a field, then $F[x_1, \ldots, x_n]$ is a UFD.

Remark

The above corollary gives an example of a UFD that is not a PID.
Let I be the set of all polynomials in $F[x, y]$ whose constant term is zero. Then I is not a principal ideal. Thus, $F[x, y]$ is a UFD, but not a PID.

Homework

Problems 4, 5, 10, 24, 25, 26, 30, 32 of Section 45.