Lecture 11: Unique Factorization Domains

Prof. Dr. Ali Bülent EKİN
Doç. Dr. Elif TAN

Ankara University

Units and Associates

It is well known that the fundamental theorem of arithmetic holds in $\mathbb{Z}$. Motiveted the unique factorization into primes (irreducibles) in $\mathbb{Z}$, we investigate the integral domains which have this property.

Definition

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

- a **divides** b (a is a **factor** of b), denoted by $a \mid b$, if $\exists\ c \in R$ such that $b = ac$.
- $0_R \neq a$ is a **unit** of R, if $u \mid 1_R$, that is, $u \in U(R)$.
- a and b are **associates** in R, denoted by $a \approx b$, if $a = bu$ where $u \in U(R)$.

Examples:

1. The only units of $\mathbb{Z}$ are 1 and -1. Thus the only associates of 17 in $\mathbb{Z}$ are 17 and -17.

2. The only units of $\mathbb{Z}[i]$ are $1, -1, i, -i$. Thus the only associates of $1+i$ are $1+i, -1+i, 1-i$ and $-1-i$.

3. All units of $F[x]$ are F^*. The associates of a nonconstant $f(x)$ is $uf(x)$ where u is a unit in F.

Remarks:

1. Let R be a commutative ring with unity and $a, b \in R$. The relation $\approx$ defined by
$$a \approx b \Leftrightarrow a = bu, \;\; u \in U\left(R\right),$$
is an equivalence relation.
2. Let D be an integral domain and $a, b \in D$. Then we have the followings:
    - $a \approx b \Leftrightarrow a \mid b$ and $b \mid a$.
    - $a \mid b \Leftrightarrow \langle b \rangle \subseteq \langle a \rangle$.
    - $a \approx b \Leftrightarrow \langle a \rangle = \langle b \rangle$.

Greatest common divisor

Definition

Let D be an integral domain and let a, b be nonzero elements in D.

- If there exists $0_D \neq d \in D$ such that $d \mid a$ and $d \mid b$, then d is called a **common divisor** of a and b.
- An element $0_D \neq d \in D$ is called a **greatest common divisor** of a and b, denoted by $\gcd(a, b)$, if
  1. d is a common divisor of a and b,
  2. If t is a common divisor of a and b, then $t \mid d$.
- a and b are called **relatively prime** if their only common divisors are units.

Greatest common divisor

Remark: The gcd of two elements need not be unique, actually the gcd of two elements may not even exist.

Example: In the ring of even integers $2\mathbb{Z}$, 2 and no other even integer have a gcd.
In F, there exists a gcd (a, b), since $a \mid b$ and $b \mid a$, for all nonzero $a, b \in F$.

Theorem

Let R be a PID and let $a, b \in R$ (not both zero). Then there exists a $\gcd(a, b)$. *Moreover,*

$$\gcd(a, b) = d \Rightarrow \exists\ x, y \in R \text{ such that } d = ax + by.$$

Definition

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

- A nonzero element c that is not a unit in R is called **irreducible** element if $c = ab$ implies either a or b is a unit. If c is not irreducible, then c is called **reducible.**
- A nonzero element p that is not a unit in R is called **prime** element if $p \mid ab$ implies either $p \mid a$ or $p \mid b$.

Remark: Let D be an integral domain. A nonzero and a nonunit element $c \in D$ is **irreducible** $\Leftrightarrow$ the only divisors of c are the associates of c and the units of D.

Example: $\overline{3}$ is not irreducible in $\mathbb{Z}_6$, but prime.

Irreducible and prime elements

Theorem

Let R be an integral domain and let $p \in R$. Then

$$p \text{ is prime} \Rightarrow p \text{ is irreducible.}$$

Remark: Converse of this theorem need not be true. For example $3 = 1 + 0i\sqrt{5} \in \mathbb{Z}i\sqrt{5}$ is irreducible, but not prime. (See malik, 362)

The following theorem gives information when the converse is true.

Theorem

Let R be a PID and let $p \in R$. Then

$$p \text{ is prime} \Leftrightarrow p \text{ is irreducible.}$$

Unique Factorization Domains

Definition

Let D be an integral domain. D is called an **unique factorization domain (UFD)** if

1. Every nonzero and nonunit element of D can be factored into a product of a finite number of irreducibles, that is,

$$a = p_1 p_2 \dots p_r$$

2. If $p_1 p_2 \dots p_r$ and $q_1 q_2 \dots q_s$ are two factorization of $a \in D$ into irreducibles, then $r = s$ and q_j can be renumbered so that p_i and q_i are associates.

D is UFD $\Leftrightarrow$ Every nonzero and nonunit element of D can be uniquely expressible (except unit factors and order of factors) as a product of a finite number of irreducibles.

Theorem

Every PID is a UFD.

Example: Since $\mathbb{Z}$ is a PID, hence $\mathbb{Z}$ is a UFD.
In $\mathbb{Z}$, we have

$$12 = (2)(2)(3) = (-2)(-2)(3) = (2)(-2)(-3),$$

where 2 and -2 are associates, 3 and -3 are associates. So except for order and associates, the irreducible factors of 12 are same.