

## 1. QUOTIENT RINGS AND IDEALS

Let  $R$  and  $S$  be rings, i.e. they're equipped with addition and multiplication

$$(R, +_R, \cdot_R), \quad (S, +_S, \cdot_S)$$

where the multiplications are associative and the additions make  $R$  and  $S$  abelian groups. Moreover, the addition and multiplication satisfies the distributive law. Recall that a map  $\phi : R \longrightarrow S$  is called a *ring homomorphism* if it satisfies

- $\phi(a +_R b) = \phi(a) +_S \phi(b)$  for all  $a, b \in R$ .
- $\phi(a \cdot_R b) = \phi(a) \cdot_S \phi(b)$  for all  $a, b \in R$ .
- $\phi(0_R) = \phi(0_S)$  where  $0_R$  and  $0_S$  denote the additive identities of  $R$  and  $S$ , respectively.

This is a consequence of the first property.

- If  $R$  is a ring with multiplicative unity  $1_R$ , then we have  $\phi(1_R) = 1_{\phi(R)}$ . This is also a consequence of the second property. Here  $\phi(R)$  denotes the image of  $R$  under  $\phi$  in  $S$ .  $\phi(R)$  is itself a subring of  $S$  with multiplicative unity (why?). It is not true, however, that  $\phi(1_R)$  is the multiplicative unity for  $S$  as one can see easily from the following example:

$$\phi : \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}, \quad n \mapsto (n, 0)$$

where the ring structures are given by the most obvious ones.

From now on, I will omit the subscripts on  $+_R, \cdot_R$  and simply write  $a+_R b = a+b$  and  $a\cdot_R b = ab$ .

We also have the following immediate consequence:

If  $R' \subset R$  and  $S' \subset S$  are subrings, then  $\phi(R')$  and  $\phi^{-1}(S')$  are subrings of  $S$  and  $R$ , respectively. Roughly speaking, the *homomorphisms* are those mappings which preserve the structure of the objects that it is mapping from and to.

Among the subrings of the type  $\phi^{-1}(S')$ , the following one is distinguished

**Definition 1.1.** Let  $\phi : R \longrightarrow S$  be a ring homomorphism. The subring

$$\phi^{-1}(0') = \{ r \in R \mid \phi(r) = 0 \}$$

is called the *kernel* of  $\phi$  and denoted by  $\text{Ker}(\phi)$ .

Recall that a subgroup  $H$  of a group  $G$  induces a well-defined group structure on the set of cosets  $G/H = \{ gH \mid g \in G \}$  if and only if  $H$  is a normal subgroup of  $G$ , i.e. for all  $g \in G$  and  $h \in H$ , we have  $g^{-1}hg \in H$ . ( Here we used the multiplicative notation for the group structure of  $G$  ). In a given ring  $R$ , any subring  $H$  of  $R$  will be a normal subgroup of the abelian group  $(R, +)$ , hence the quotient  $R/H$  is well-defined as an additive group. Then

what will be the corresponding equivalent condition for the set of cosets  $R/H$  to be a ring? The answer is given by the following definition:

**Definition 1.2.** An additive subgroup  $N$  of a ring  $R$  is called an *ideal* if it satisfies

$$aN \subset N \quad \text{and} \quad Nb \subset N \quad \text{for all } a, b \in R$$

**Proposition 1.1.** Let  $H$  be a subring of the ring  $R$ . The following two conditions are equivalent

1) Multiplication of additive cosets of  $H$  is well-defined by the equation

$$(a + H)(b + H) = ab + H, \quad \text{for all } a, b \in R$$

2)  $H$  is an ideal of  $R$ .

**Example 1.1.** Kernels,  $\phi : \mathbb{Z} \rightarrow \mathbb{Z}_n, n\mathbb{Z}, C(\mathbb{R}, \mathbb{R})\dots$

**Definition 1.3.** Let  $N$  be an ideal of a ring  $R$ . Then the *quotient ring* is  $(R/N, +^\dagger, \cdot^\dagger)$  where

$$(a + N) +^\dagger (b + N) = (a + b) + N, \quad (a + N) \cdot^\dagger (b + N) = ab + N$$

for all  $a, b \in R$ .

## 2. FUNDAMENTAL HOMOMORPHISM THEOREM

Recall that an ideal  $N$  of a ring  $R$  gives a canonical ring structure on  $R/N$ , i.e. the mapping  $\gamma : R \rightarrow R/N$  given by  $\gamma(x) = x + N$  is a ring homomorphism with kernel  $N$ . The following theorem is an immediate consequence of the 1st isomorphism theorem

**Theorem 2.1.** Let  $\phi : R \rightarrow S$  be a ring homomorphism with kernel  $N$ . Then  $\phi(R)$  is a ring and the map  $\mu : R/N \rightarrow \phi(R)$  given by  $\mu(x + N) = \phi(x)$  is an isomorphism. Also we have  $\phi = \mu \circ \gamma$ .

**Example 2.1.** 0) The kernel of any ring homomorphism is an ideal.

- 1) **Frobenius homomorphism:** Let  $R$  be a commutative ring with unity of prime characteristic  $p$ . The map  $\phi_p : R \rightarrow R$  given by  $\phi_p(a) = a^p$  is a homomorphism.
- 2) Let  $N, I$  be ideals of  $R, S$ , respectively. A ring homomorphism  $\phi : R \rightarrow S$  induces a natural homomorphism  $\phi_* : R/N \rightarrow S/I$  if and only if  $\phi(N) \subset I$ .
- 3) **Ninradical:** An element  $a$  of a ring  $R$  is called *nilpotent* if there exists an  $n \in \mathbb{N}$  such that  $a^n = 0$ . The collection of all nilpotent elements in a commutative ring  $R$

$$N = \{ a \in R \mid \exists n \in \mathbb{N} \text{ such that } a^n = 0 \}$$

is an ideal and is called the *nilradical* of  $R$ . Also written as  $\sqrt{0}$ .

4) **Radical:** For an ideal  $N$  of a commutative ring  $R$ , the set

$$\sqrt{N} = \{ a \in R \mid \exists n \in \mathbb{N} \text{ such that } a^n \in N \}$$

is an ideal of  $R$ , called the *radical* of  $N$ .

### 3. PRIME AND MAXIMAL IDEALS

A commutative ring  $R$  has at least two ideals: the *improper ideal*  $R$  and the *trivial ideal*  $0 = \{0\}$ . These ideals do not give any further interesting structures since  $R/R = 0$  and  $R/0 = R$ . Hence we will always consider *proper nontrivial ideal* which is an ideal  $N$  of  $R$  such that  $N \neq R$  and  $N \neq \{0\}$ . One can observe that

- 1): If  $R$  is a ring with unity and  $N$  is an ideal of  $R$  containing a unit, then  $N = R$ .
- 2): A field contains no proper nontrivial ideals.

In particular, which ideals will give, when we form the quotient ring, a field or an integral domain? The above observation gives a hint and the answer is given by

**Definition 3.1.** A *maximal ideal* of a ring  $R$  is an ideal  $M$  such that  $M \neq R$  and there is no proper ideal  $N$  of  $R$  such that  $M \subsetneq N$ . A *prime ideal* of a ring  $R$  is an ideal  $P$  such that  $P \neq R$  and, for any  $a, b \in R$ ,  $ab \in P$  implies  $a \in P$  or  $b \in P$ .

**Theorem 3.1.** For an ideal  $N$  of a commutative ring  $R$ , we have

- 1)  $R/N$  is a field if and only if  $N$  is a maximal ideal.
- 2)  $R/N$  is an integral domain if and only if  $N$  is a prime ideal.
- 3) If  $N$  is a maximal ideal, then  $N$  is a prime ideal.

### 4. PRIME FIELDS

If a commutative ring  $R$  has the unity, then the ring structure of  $R$  guarantees that any element that can be obtained from the unity by successive addition or multiplication is contained in  $R$ . Precisely this means

The mapping  $\phi : \mathbb{Z} \longrightarrow R$  given by  $k \mapsto k \cdot 1$  is a ring homomorphism.

The kernel of  $\phi$  will be an ideal of  $\mathbb{Z}$ , and we know that all ideals of  $\mathbb{Z}$  is of the form  $n\mathbb{Z}$  for some  $n \in \mathbb{Z}_{\geq 0}$  ( why? ). This  $n$  should be determined by the structure of  $R$ , or more precisely, by the characteristic of  $R$ .

- If  $R$  is a ring with unity and  $\text{char}(R) = n$  for some  $n \in \mathbb{N}$ , then  $R$  contains a subring isomorphic to  $\mathbb{Z}_n$ .

- If  $R$  is a ring with unity and  $\text{char}(R) = 0$ , then  $R$  contains a subring isomorphic to  $\mathbb{Z}$ .
- If  $F$  is a field with  $\text{char}(F) = p$  for some  $n \in \mathbb{N}$ , then  $F$  contains a subfield isomorphic to  $\mathbb{Z}_p$ .
- If  $F$  is a field with  $\text{char}(F) = 0$ , then  $F$  contains a subfield isomorphic to the quotient field of  $\mathbb{Z}$ , i.e.  $\mathbb{Q}$ .

In the sense which is clear by the above observation, the fields  $\mathbb{Z}_p$  and  $\mathbb{Q}$  are called the *prime fields*.

## 5. PID AND UFD

### **Definition 5.1.**

- 1) If  $R$  is a commutative ring with unity, an ideal  $N$  of  $R$  is called a *principal ideal* if there exists  $a \in R$  such that  $N = \langle a \rangle = \{ra \mid r \in R\}$ .  $R$  is called a *principal ideal domain* if all ideals of  $R$  are principal.
- 2) If  $R$  is a commutative ring with unity,  $R$  is called a *unique factorization domain* if every element  $a \in R$  can be written uniquely as the product of irreducible elements of  $R$  up to the multiplication order and a unit factor.

**Theorem 5.1.** *The polynomial ring  $F[x]$  over a field  $F$  is a PID.*

**Theorem 5.2.** *A nonzero ideal  $\langle p(x) \rangle$  of  $F[x]$  is maximal if and only if  $p(x)$  is irreducible over  $F$ .*

**Theorem 5.3.** *Let  $p(x)$  be an irreducible polynomial in  $F[x]$ . If  $p(x)$  divides  $r(x)s(x)$ , then  $p(x)$  divides either  $r(x)$  or  $s(x)$ .*