Chapter 14 Ideals and Factor Rings

Definition A subring A of a ring R is a (two-sided) ideal if $ar, ra \in A$ for every $r \in R$ and every $a \in A$. [An ideal is a subring with left and right absorbing power!]

Theorem 14.1 A non-empty subset A of a ring R is an ideal if

1. $a - b \in A$ whenever $a, b \in A$, and
2. $ra, ar \in A$ whenever $a \in A, r \in R$.

Example $\{0\}$, $n\mathbb{Z}$ in $\mathbb{Z}$, $\langle f(x)\rangle$ in $\mathbb{R}[x]$, $\langle\{2, x\}\rangle = (2\mathbb{Z})[x] \subseteq \mathbb{Z}[x]$.

Theorem 14.2 Let R be a ring, and A be a subring. The set of cosets $\{r + A : r \in R\}$ is a ring under the operations

$$(x + A) + (y + A) = (x + y) + A \text{ and } (x + A)(y + A) = xy + A$$

is a ring (known as the factor ring) if and only if A is an ideal.

Proof. Key step is to show that the multiplication is well-defined if and only if A is an ideal.

If A is an ideal, then ...

If there are $a \in A, r \in R$ such that $ar \notin A$, then ...

Examples $\mathbb{Z}/4\mathbb{Z}$, $2\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}[i]/\langle 2-i\rangle$, $\mathbb{R}[x]/\langle x^2+1\rangle$.

Definition Let A be a proper ideal of a commutative ring R.

It is a **prime ideal** $a, b \in R$ satisfying $ab \in A$ imply that $a \in A$ or $b \in A$.

It is a **maximal ideal** if there is no other ideal lying strictly between A and R.

Example $n\mathbb{Z}$ is prime if and only if n is prime; $\langle 2 \rangle$ and $\langle 3 \rangle$ are maximal ideal in $\mathbb{Z}_{36}$; $\langle x^2 + 1 \rangle$ is a maximal ideal in $\mathbb{R}[x]$.

Theorem 14.3-4 Let A be an ideal of a commutative ring R with unity.

(a) The factor ring R/A is an integral domain if and only if A is prime.

(b) The factor ring R/A is a field if and only if A is maximal.

Remark If A is maximal, then A is prime. The ideal $\langle x \rangle$ is prime in $\mathbb{Z}[x]$, but not maximal.

Chapter 15 Ring Homomorphisms

Definitions Let R_1, R_2 be rings. A function $\phi : R_1 \to R_2$ is a ring homomorphism if $\phi(a+b) = \phi(a)+\phi(b)$ and $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in R_1$. If in addition that ϕ is bijective, then ϕ is a ring isomorphism.

Theorem 15.1-2 let $\phi : R_1 \to R_2$ be a ring homomoprhism.

(1) For any $r \in R$ and positive integer n, $\phi(nr) = n\phi(r)$ and $\phi(r^n) = \phi(r)^n$.

(2) If A is a subring of R_1, then $\phi(A)$ is a subring of R_2.

(3) If A is an ideal of R_1, then $\phi(A)$ is an ideal of $\phi(R_1)$.

(4) If B is a subring/ideal of R_2, then $\phi^{-1}(B)$ is a subring/ideal of R_1. In particular, $Ker(\phi)$ is an ideal.

(5) If A is a commutative subring of R, then $\phi(A)$ is commutative.

(6) If R_1 has a unity, then $\phi(1)$ is a unity of $\phi(R_1)$.

(7) The map ϕ is injective if and only if $Ker(\phi) = \{0\}$,

Theorem 15.3 Let $\phi : R_1 \to R_2$ be a ring homomorphism. Then $x + Ker(\phi) \mapsto \phi(x)$ is an isomorphism from $R_1/Ker(\phi)$ to $\phi(R_1)$.

Theorem 15.4 Every ideal A of a ring R is the kernel of the ring homomorphism $\phi : A \mapsto R/A$ defined by $\phi(a) = a + A$.

Theorem 15.5 Let R be a ring with unity. Then $\phi : \mathbb{Z} \to R$ defined by $\phi(n) = n \cdot 1$ is a ring homomorphism. In particular, $\phi(\mathbb{Z}) = \mathbb{Z}$ or $\mathbb{Z}_n$. In the former case, R has characteristic 0; in the latter case R has characteristic n.

Corollary (a) $\phi : \mathbb{Z} \to \mathbb{Z}_n$ defined by $\phi(a) = [a]$ is a ring homomorphism.

(b) If R is a field of characteristic p, then $\{n \cdot 1 : n \in \mathbb{Z}\}$ is isomorphic to $\mathbb{Z}_p$.

Construction of the fields of quotients

Theorem 15.6 Let $\mathbb{D}$ be an integral domain. Then $(a,b) \sim (c,d)$ on $\mathbb{D} \times \mathbb{D}^*$ defined by $ad = bc$ is an equivalence relation. Suppose $\mathbb{F} = \{[(a,b)] : (a,b) \in \mathbb{D} \times \mathbb{D}^*\}$ is the set of equivalence classes of the relation. Then $\mathbb{F}$ is a field under the operations $[(a,b)] + [(c,d)] = [(ad+bc, bd)]$ and $[(a,b)][(c,d)] = [(ab,cd)]$. This is known as the field of quotients of $\mathbb{D}$.

Examples $\mathbb{D} = \mathbb{Z}, \mathbb{Z}[x], \mathbb{Z}_p[x]$ for a prime p, and $\mathbb{R}[x]$.

Construction of finite field

Theorem Suppose $\mathbb{F}$ is field, and $A = \langle f(x) \rangle \in \mathbb{F}[x]$ is a maximal ideal, where

$$f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0.$$

Then $A = \{f(x)q(x) : q(x) \in \mathbb{F}[2]\}$, and $\mathbb{F}[x]/A = \{r(x) + A : r(x) \in \mathbb{F}[x] \text{ of degree at most } m-1\}$ is a field. If $\mathbb{F} = \mathbb{Z}_p$ and $f(x)$, then $\mathbb{F}[x]/A$ has p^m elements.

Question When is $A = \langle f(x) \rangle$ maximal if $f(x) \in \mathbb{F}[x]$?