Sections 7.1 7.2 Rings

Recall

- A zero divisor is an element $a \in R$, $a \neq 0$, $ab = 0$ for some $b \in R$
- A unit in a ring R (with $1 \neq 0$) is an element $a \in R$ with $ab = 1$ for some $b \in R$. We write $a^{-1} = b$.
- An integral domain is a commutative ring with $1 \neq 0$ that has no zero divisors.

Example $\mathbb{Z}$ is integral domain; no zero divisors; units $1, -1$.

Significant properties of integral domains:

① $ab = 0 \iff a = 0$ or $b = 0$

② Cancellation: If $a \neq 0$, then:

$ab = ac \Rightarrow b = c$ $\quad$ $ab = ac \iff ab - ac = 0 \iff a(b-c) = 0 \iff b - c = 0 \iff b = c$

$ba = ca \Rightarrow b = c$

$ab = ca \Rightarrow$ (no conclusion)

A division ring is a ring with 1 for which all non-zero elements are units. A field is a commutative division ring.

Corollary 3 Any finite integral domain is a field.

- A subring of R is a subset $S \subseteq R$ that is a ring under the operations of R.

How to show $S \subseteq R$ is a subring.

① Show S is a subgroup of R under $+$.

② Show S is closed under multiplication

Example The Quaternions (A Division Ring)

$$\mathbb{H} = \left\{ \begin{bmatrix} z & w \\ -\bar{w} & \bar{z} \end{bmatrix} \mid w, z \in \mathbb{C} \right\} = \left\{ \begin{bmatrix} a+bi & c+di \\ -c+di & a-bi \end{bmatrix} \mid a, b, c, d \in \mathbb{R} \right\}$$

Check $\mathbb{H}$ is a subring of $M_2(\mathbb{C})$ $\quad$ {use $\overline{z+w} = \bar{z} + \bar{w}$, $\overline{zw} = \bar{z}\bar{w}$.}

Check $\begin{bmatrix} z & w \\ -\bar{w} & \bar{z} \end{bmatrix}^{-1} = \dfrac{1}{|z|^2 + |w|^2} \begin{bmatrix} \bar{z} & -w \\ \bar{w} & z \end{bmatrix} \in \mathbb{H}$.

Note $Q_8 = \left\{ \underbrace{\pm\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}}_{1}, \underbrace{\pm\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}}_{i}, \underbrace{\pm\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}}_{j}, \underbrace{\pm\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}}_{k} \right\} = \{\pm 1, \pm i, \pm j, \pm k\}$

Text $\mathbb{H} = \{ a + bi + cj + dk \mid a, b, c, d \in \mathbb{R},\ i, j, k \in Q_8 \}$

Multiplication defined with $i^2 = j^2 = k^2 = 1$, $ij = k$, etc.

New Rings from Old Suppose $\mathbb{R}$ is a ring. So are the following

(a) $M_n(\mathbb{R})$ = $n \times n$ matrices, entries in $\mathbb{A}$.

(b) Given a set X, $R_X = \{ f \mid f : X \to \mathbb{R} \}$ = (all functions from X to A) is a ring under operations

$f + g$ is function $(f+g)(x) = f(x) + g(x)$

fg is function $(fg)(x) = f(x)\, g(x)$

(c) $R[x]$ $\{ a_0 + a_1 x + a_2 x^2 + \cdots a_k x^k \mid k \in \mathbb{Z}^+,\ a_i \in A \}$
= polynomials with coefficients in A.
Operations are usual addition and multiplication of polynomials

(d) Read about group rings.

Section 7.3 Ring Homomorphisms and Quotients

Definition Suppose R and S are rings.

(1) A ring homomorphism $\varphi : R \to S$ is a map for which

$\varphi(x+y) = \varphi(x) + \varphi(y) \quad \forall x, y \in R$

$\varphi(xy) = \varphi(x)\, \varphi(y) \quad \forall x, y \in R$

(2) $\operatorname{Ker} \varphi = \{ x \in R \mid \varphi(x) = 0 \}$

(3) If φ is bijective, its called an isomorphism; $R \cong S$.

Proposition 5 Given homomorphism $\varphi : R \to S$,

$\varphi(R)$ is subring of S

$\ker \varphi$ is subring of R

Property of $\ker \varphi$: $x \in \ker \varphi \implies rx \in \ker \varphi \quad \forall r \in R$.

$x = 0 \implies rx = 0$ $(r \ker\varphi \subseteq \ker\varphi)$

Definition A subring $I \leq R$ is an ideal if $x \in I \implies rx \in I$ and $xr \in I$ for all $r \in R$, that is $rI \subseteq I$ when $rI = \{ rx \mid x \in I \}$
$Ir = \{ xr \mid x \in I \}$.

Thus every kernel is an ideal.

Quotient Rings

Definition Suppose $I \subseteq R$ is an ideal. Then $R/I = \{ r+I \mid r \in R \}$ is called a *quotient ring*.

This is a ring under the following operations:

$$(r+I) + (s+I) = (r+s) + I$$
$$(r+I)(s+I) = rs + I$$

Proof Under $+$, R is abelian, so $I \trianglelefteq R$ and R/I is an abelian group under $+$.

Show multiplication is well-defined.

Suppose $r+I = r'+I$ $r'-r \in I$ $r' = r+\alpha$ $\alpha \in I$
 $s+I = s'+I$ $s'-s \in I$ $s' = s+\beta$ $\beta \in I$

Must verify $(r+I)(s+I) \stackrel{?}{=} (r'+I)(s'+I)$

$$rs + I \stackrel{?}{=} r's' + I$$
$$rs + I \stackrel{?}{=} (r+\alpha)(s+\beta) + I$$
$$= (rs + \underbrace{r\beta + \alpha s + \alpha\beta}_{\in I}) + I$$
$$= rs + I$$

$$(r'+I)(s'+I) = r's' + I = (r+\alpha)(s+\beta) + I$$
$$= (rs + \underbrace{r\beta + \alpha s + \alpha\beta}_{\in I}) + I =$$
$$= rs + I = (r+I)(s+I)$$

Easy to check mult is associative; distributive property.

Note $I = 0 + I$ is zero element of R/I.

Observation: $\pi : R \longrightarrow R/I$, where $\pi(r) = r+I$ is a ring homomorphism with kernel I.

Thus every ideal is the kernel of some ring homomorphism.

Next Time: Isomorphism Theorems for quotient rings.