Contents

Section 1. Ring

Lecture 0904

1.1 Definition: Ring

A ***ring*** R is an abelian group $\langle R, +\rangle$ which has another operation $\cdot$ such that

(a) $'\cdot'$ is associative.

(b) $(a+b)\cdot c = a\cdot c + b\cdot c$ and $c\cdot(a+b) = c\cdot a + c\cdot b$ for all $a, b, c \in R$.

Example 1.2 $G = \langle \mathbb{Z}, +R = \rangle \to \langle \mathbb{Z}, +, \cdot\rangle$: a ring

1.3 Definition

R is called a ***commutative ring*** if for every $a, b \in R$, $a\cdot b = b\cdot a$.

Example 1.4 $R = \langle (M^{\infty}(\mathbb{Z})), +, \cdot\rangle$ is NOT commutative.

1.5 Definition

An element $1_R \in R$ is called a ***unity*** if for every $a \in R$ $a\cdot a = a\cdot 1 = a$.

1.6 Proposition

1_R is unique in R.

1.7 Definition

An element $u \in R$ is called a ***unit element*** if there exists $u' \in R$ such that $u\cdot u' = 1_R$.

1.8 Definition

Suppose R, R' are two rings. $f : R \to R'$ is called a ***ring homomorphism*** if

(a) $f(a +_R b) = f(a) +_{R'} f(b)$.

(b) $f(a \cdot_R b) = f(a) \cdot_{R'} f(b)$.

Remark The ring homomorphism f is injective if $\ker f = \{r \in R | f(r) = 0_{R'}\} = \{0_R\}$.

1.9 Definition

Any subgroup I of R is called ***ideal*** of R if

(a) $I \subset R$

(b) $R\cdot I = I\cdot R \subset I$

Example 1.10 Suppose f is a ring homomorphism. Then $\forall \alpha \in R, \forall r \in \ker f$, $\alpha\cdot r \in R$ and $f(\alpha\cdot r) = f(\alpha)f(r) = 0$. That is, $\ker f$ is an ideal of R.

1.11 Definition

An nonzero element $\alpha \in R$ is called a ***zero divisor*** if there exists a nonzero element $\beta \in R$ such that $\alpha\cdot\beta = 0$.

1.12 Definition

R is called an ***integral domain*** if R is a commutative ring with 1_R and no zero devisors.

1.13 Proposition: Cancellation laws

Suppose R is a integral domain. for all nonzero element $a, b \in R$, $ac = ab \implies a(b-c) = 0 \implies b = c$.

Lecture 0909

1.14 Definition

By a ***division ring***, we mean a ring R with unity 1 such that $\forall r \in R$, r has multicative inverse r' such that $r\cdot r' = 1$.

1.15 Proposition

If a ring R is a division ring, then r has no zero divisor.

1.16 Definition

By a ***field***, we mean a ring R such that R is a integral domain and that every nonzero element $r \in R$ has an inverse in R.

1.17 Proposition

A commutative division ring is a field.

1.18 Theorem

(a) Every finite integral domain is a feild.

(b) Every finite division ring is a field.

Proof) (a) Let R be a finite integral domain. We may assume $R = \{a_1, a_2, \dots, a_n\}$. Given a nonzero element $r \in R$, define $\psi : R \to R$ by $\psi(a_i) = ra_i$. For $\alpha, \beta \in R$, $r\alpha = r\beta \implies r(\alpha - \beta) = 0$, which means $a = b$ since R has no zero divisors. Then there exists a $1 \le i \le n$ such that $ra_i = 1$. $\square$

1.19 Definition

$n \in \mathbb{Z}^+$ is called the ***characteristic*** of R if there exists a number s.t. $n \cdot r = 0$ for all $r \in R$. n is the smallest such number.

1.20 Corollary

If R is a ring with unity 1, the characteristic of R is the smallest number $n \cdot 1 = 0$.

1.21 Lemma

$\mathbb{Z}^n$ is an integral domain $\iff$ n is a prime number.

Proof) $(\Rightarrow)$ If n is not prime, then $n = n_1 n_2$ for some $1 < n_1, n_2 < n$. It implies that $n_1 n_2 \equiv 0 \mod n$, i.e., n_1, n_2 are zero divisors.
$(\Leftarrow)$ Suppose, for contradiction, $\mathbb{Z}_p$ is not integral domain. There exists some nonzero elements $n_1, n_2 \in \mathbb{Z}_p$ such that $n_1 n_2 \equiv 0 \mod p$. Then $p | n_1$ or $p | n_2$, which means $n_1 = 0$ or $n_2 = 0$. $\square$

1.22 Lemma

Let $\mathcal{R} \subset \mathbb{Z}$ be an nonempty ideal of $\mathbb{Z}$. Then $\mathcal{R} = n\mathbb{Z} = \{na : a \in \mathbb{Z}\}$ for some $n \in \mathbb{Z}^+$.

Proof) Let r be the smallest number in $\mathcal{R}$. By the division algorithm, $r = nq + s$ for some n, q, s. since $r, nq \in \mathcal{R}$, $s = 0$. Thus $r = nq \in n\mathbb{Z} \implies \mathcal{R} \subset n\mathbb{Z}$. The other direction is trivial. $\square$

1.23 Theorem

$\mathbb{Z}_n$ is a field $\iff$ n is a prime number p. In this case,

(a) $\mathbb{Z}_p$ is called a ***finite field***.

(b) Every finite field F contains $\mathbb{Z}_p$ for some prime p.

Proof) Consider a ring homomorphism: $\psi : \mathbb{Z} \to F$ given by

$$\psi(n) = \begin{cases} n \cdot 1_F = 1_F + \cdots + 1_F & \text{for } n > 0 \\ -|n| \cdot 1_F = (-1_f) + \cdots + (-1_F) & \text{for } n < 0 \\ 0_F & \text{for } n = 0 \end{cases}$$

Then $n\mathbb{Z} = \ker\psi \subset \mathbb{Z} = R \implies \mathbb{Z}/\ker\psi \simeq \psi(\mathbb{Z}) \subset F$ for some $n \in \mathbb{Z}$. Since the field F has no zero devisor, n must be a prime number. $\square$

1.24 Lemma

For all nonzero number $a \in \mathbb{Z}$, $a^{p-1} \equiv 1 \mod p$.

Proof)

$\square$

$\mathbb{Z}_n^* = \{\overline{r} \in \mathbb{Z}_n : (r, n) = 1\}$. $|\mathbb{Z}_n^*| = \psi(n) =$ the number of $\{r \in \mathbb{N} : (r, n) = 1\}$.

1.25 Theorem

$\mathbb{Z}_n^*$ forms a group with $\cdot$.

Proof) since $(a, n) = 1$, for some $\alpha, \beta \in \mathbb{Z}$, $\alpha a + \beta n = 1 \implies \alpha a \equiv 1 \mod n \implies \overline{a}$ has inverse $\overline{\alpha}$ in $\mathbb{Z}_n^*$. $\square$

1.26 Theorem

If $a \in \mathbb{Z}$, $(a, n) = 1$, then $a^{\psi(1)} \equiv 1 \mod n$.

Proof) $G = \mathbb{Z}_n^*$ is a group by the pervious thm, of order $|G| = \psi(n)$, by the Lagrange thm, $a^{|G|} = a^{\psi(n)} \equiv 1 \mod n$. $\square$

1.27 Theorem

If $(a, m) = 1$, then $ax \equiv b \mod n$ has a unique solution in $\mathbb{Z}_m$.

Proof) By the previous thm, $\mathbb{Z}_m^*$ is a group. $\overline{a} \in \mathbb{Z}_m^* \implies \exists \overline{a'} \in \mathbb{Z}_m^*$ s.t. $\overline{a} \cdot \overline{a'} = \overline{1} \mod m$. Then, $x \equiv \overline{a'} \cdot \overline{b}$ is the unique solution. $\square$

1.28 Theorem

Let $d = \gcd(a, m)$. Then $ax \equiv b \mod m$ has a solutuin $\iff$ $d | b$. In this case, there are d-solutions.

Proof) $(\Rightarrow)$ Assume $a = da_1$, $m = dm_1$. $ax \equiv b \mod m$ has a solution $x_0 \implies ax_0 \equiv b \mod m \implies m | (ax_0 - b) \implies d | dm_1 | da_1 x_0 - b \implies d | b$.
$(\Leftarrow)$ $d | b \implies b = b_1 d$, $a = a_1 d$, $m = m_1 d$. $ax \equiv b \mod m \implies a_1 dx \equiv bd \mod md \implies a_1 x \equiv b_1 \mod m_1 \implies$ there exists a unique solution in $\mathbb{Z}_{m_1}$. Consider a ring-homo $\phi : \mathbb{Z}_m \to \mathbb{Z}_{m_1}$. Then $\phi^{-1}(x) = \{x, x + m_1, \dots, x + (d-1)m_1\}$. $\square$

HW1: p189 #11,13,15,17,19,21,22,27 30

Lecture 0911

1.29 Theorem: Division algorithm

Let $F[x] = \{\sum_{i=0}^{n} a_i x^i \mid a_i \in F, n \geq 0\}$.

(a) For all $f(x), g(x) \in F[x]$, $f(x) = q(x)g(x) + r(x)$ for $\deg(r(x)) < \deg(g(x))$.

(b) For all $f(x) \in F[x]$, 'a' is a root of $f(x)$, i.e., $f(a) = 0 \iff (x-a) \mid f(x) \iff f(x) = (x-a)f'(x)$.

(c) Every finite multiplicative group of a field F must be cyclic.

(d) (Eisenstein crieteria) For all $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in Q[x]$ is ***iwed??*** if there exists a prime $p \in \mathbb{Z}$ such that $p \nmid a_n$, $p \mid a_i$ for $0 \leq i \leq n-1$, and $p^2 \nmid a_0$.

Recall that $f(x)$ is ***rdasd??*** in $F[x]$ if $f(x) = f_1(x)f_2(x)$ in $F[x]$ and $\deg f_i(x)$ is non-zero or $f_i(x)$ is not constant. Otherwise, $f(x)$ is said to be ***????***.

HW2: p207 # 12,14,15,16,17,24,27, p218 # 14,16,34,35,36,37