Abstract Algebra

Module 4

Section 26 : Homomorphisms & Factor Rings

June 14, 2021

Ring

Ring $\langle R, +, \cdot \rangle$

- Set R
- Ring Addition, $+$
  - Addition is associative.
  - Addition is commutative.
  - Existence of Additive Identity
  - Existence of Additive Inverses
- Ring Multiplication, $\cdot$
  - Multiplication is associative
  - Multiplication is distributive over Addition

Ring - Examples

Integer Ring, $\langle \mathbb{Z}, +, \times \rangle$

Integers together with usual Addition and Multiplicaiton

Matrix Space, $\langle M_n(R), +, \times \rangle$

- Ring R
- $M_n(R) = \{(a_{ij}) : 1 \leq i, j \leq n, a_{ij} \in R\}$
- $A + B = C, \; c_{ij} = a_{ij} + b_{ij}$
- $AB = C, \; c_{ij} = \sum_k a_{ik} b_{kj}$

Function Space, $\langle F, +, \times \rangle$

- R Ring
- $F = \{f : R \to R\}$
- $(f + g)(x) = f(x) + g(x)$
- $fg(x) = f(x)g(x)$

Ring Homomorphism

$\phi : R \rightarrow R'$

- R, R' Rings
- Function, $\phi : R \rightarrow R'$
- ϕ preserves all binary operations
  Addition, $\phi(x + y) = \phi(x) + \phi(y)$
  Multiplication, $\phi(xy) = \phi(x)\phi(y)$

Ring Homomorphism - Examples

$\phi : \mathbb{Z} \to \mathbb{Z}_n,\ \phi(m) \simeq m \pmod{n}$

- $\mathbb{Z}_n, \mathbb{Z}$ Rings
- $\phi(a+b) = \phi(a) + \phi(b)$
- $\phi(ab) = \phi(a)\phi(b)$

Evaluation Homomorphism

- R Ring
- $F = \{f : R \to R\}$
- $\phi_\alpha : F \to R,\ \phi_\alpha(f) = f(\alpha),$ where $\alpha \in R$
- $\phi_\alpha(f+g) = (f+g)(\alpha) = f(\alpha) + g(\alpha) = \phi_\alpha(f) + \phi_\alpha(g)$
- $\phi_\alpha(fg) = (fg)(\alpha) = f(\alpha)g(\alpha) = \phi_\alpha(f)\phi_\alpha(g)$
- ϕ_α evaluate each function in F at α.

Ring Homomorphism - Examples

Projection Homomorphism, $\pi_i : R_1 \times R_2 \times \cdots \times R_n \to R_i$

- $R_1, R_2, \cdots, R_n$ Rings ‘
  - $R_1 \times R_2 \times \cdots \times R_n$ Ring
  - $A + B = (a_1 + b_1, a_2 + b_2, \cdots, a_n + b_n)$
  - $AB = (a_1 b_1, a_2 b_2, \cdots, a_n b_n)$
- Function $\pi_i : R_1 \times R_2 \times \cdots \times R_n \to R_i,\ \pi_i(A) = a_i$ where $A = (a_1, a_2, \cdots, a_n)$ and $a_j \in R, \forall j$
- Preserves Ring Addition $\pi_i(A + B) = a_i + b_i = \pi_i(A) + \pi_i(B)$
- Preserves Ring Multiplication $\pi_i(AB) = a_i b_i = \pi_i(A)\pi_i(B)$

Properties of Ring Homomorphism

1. Preserves Additive Identity

$$\phi(0) = 0' \text{ of } R'$$

2. Preserves Additive Inverses

$$\phi(-a) = -\phi(a)$$

3. Preserves subRings

$$S \leq R \implies \phi(S) \leq R'$$

4. Preserves Multiplicative Identity (to its range)

$$\phi(1) = 1' \text{ of } \phi[R]$$

Kernel of Ring Homomorphism, $\ker(\phi)$

Definition

$$\ker(\phi) = \{a \in R : \phi(a) = 0'\}$$

Theorem

$$\phi^{-1}(\phi(a)) = a + H = H + a \textit{ where } \ker(\phi) = H$$

Theorem

$$\phi : R \to R' \textit{ is injective} \iff \ker(\phi) = \{0\}$$

Proof : $\phi^{-1}(\phi(a)) = a + H$

$$\{x \in R : \phi(a) = \phi(x)\} = a + H$$

Sufficient Part

$$\begin{aligned}
x \in \phi^{-1}(\phi(a)) \implies \ & \phi(x) = \phi(a) \\
& \phi(-a) + \phi(x) = \phi(-a) + \phi(a) \\
& \phi(-a + x) = 0' \\
\implies -a + x \in \ker(\phi) & \implies x \in a + H \\
& \implies \phi^{-1}(\phi(a)) \subset a + H
\end{aligned}$$

Proof : $\phi^{-1}(\phi(a)) = a + H$

Necessary Part

$$
\begin{aligned}
x \in a + H &\implies x = a + y,\ \ y \in \ker(\phi) \\
\phi(a+y) = \phi(a) + \phi(y) &= \phi(a) + 0' = \phi(a) \\
&\implies a + y \in \phi^{-1}(\phi(a)) \\
&\implies a + H \subset \phi^{-1}(\phi(a))
\end{aligned}
$$

Proof : $\phi : R \to R'$ is injective $\iff$ $\ker(\phi) = \{0\}$

Sufficient Part

$$\begin{aligned}\phi \text{ injective },\ \phi(0) = 0' &\implies \phi^{-1}(\phi(0)) = \{0\}\\ &\implies \ker(\phi) = \{0\}\end{aligned}$$

Necessary Part

$$\begin{aligned}\ker(\phi) = \{0\},\ a \in R &\implies \phi^{-1}(\phi(a)) = a + \ker(\phi)\\ &\implies \phi^{-1}(\phi(a)) = \{a\}\\ &\implies \phi \text{ is injective}\end{aligned}$$

Note 1 : Always $\phi(\phi^{-1}(b)) = b$, but $\phi^{-1}(\phi(b)) = b$ if ϕ injective

Note 2 : $a + \ker\phi = a + \{0\} = \{a + 0\} = \{a\}$ †[1]

[1] $a + \{b, c\} = \{a + b, a + c\}$

Quotient Ring

- $\phi : R \to R'$, then $\ker(\phi) \leq R$
- $\langle R/H, +, \times \rangle$ is a ring where $H = \ker(\phi)$
  - $R/H = \{a + H : a \in R\}$
  - $(a + H) + (b + H) = (a + b) + H$
  - $(a + H)(b + H) = (ab) + H$
- Canonical Homomorphism, $\gamma_H : R \to R/H,\ a \xrightarrow{\gamma_H} a + H$
- Isomorphism, $\mu : R/H \to \phi[R],\ a + H \xrightarrow{\mu} \phi(a)$
- Unique Isomorphism, μ such that $\phi = \mu \circ \gamma_H$

$$\begin{tikzcd}
R \arrow[rr, "\phi"] \arrow[dr, "\gamma_H"'] & & R' \\
& R/H \arrow[ur, dotted, "\mu"'] &
\end{tikzcd}$$

Left Coset Addition well-defined

- Let $\phi : R \to R'$ be ring homomorphism and $H = \ker(\phi)$
- $\langle H, +_{|H} \rangle \underset{N}{\leq} \langle R, + \rangle$ since R is abelian group
- $a + H = H + a, \ \forall a \in R$

$(a + H) + (b + H) \subset (a + b) + H$

Let $a, b \in R$, Then $a + h_1 \in a + H$, and $b + h_2 \in b + H$
$(a+h_1)+(b+h_2) = a+(h_1+b)+h_2 = a+(b+h_3)+h_2 = a+b+h_4$
$\implies (a + H) + (b + H) \subset (a + b) + H$

$(a + b) + H \subset (a + H) + (b + H)$

Let $a, b \in R, \ h \in H$. Then $a + b + h \in (a + b) + H$.
$a + b + h = (a + 0) + (b + h) \in (a + H) + (b + H)$.
$\implies (a + b) + H \subset (a + H) + (b + H)$

Left Coset Multiplication is well-defined : $\ker(\phi)$

- $\ker(\phi) = H \leq R$ since $\phi : R \to R'$ is a ring homomorphism.

$(a+H)(b+H) \subset (ab)+H$

Let $c = (a+h_1)(b+h_2) = (ab + ah_2 + h_1b + h_1h_2)$

$$
\begin{aligned}
\phi(c) &= \phi(ab) + \phi(ah_2) + \phi(h_1b) + \phi(h_1h_2) \\
&= \phi(a)\phi(b) + \phi(a)\phi(h_2) + \phi(h_1)\phi(b) = \phi(h_1)\phi(h_2) \\
&= \phi(a)\phi(b) + \phi(a)0' + 0'\phi(b) + 0' \\
&= \phi(a)\phi(b) = \phi(ab) \\
\implies & (a+H)(b+H) \subset (ab)+H
\end{aligned}
$$

$(ab)+H \subset (a+H)(b+H)$

Let $c = ab + h_1$.

$\phi(c) = \phi(ab) = \phi(a)\phi(b) = \phi(a+H)\phi(b+H) = \phi((a+H)(b+H))$

$\implies (ab)+H \subset (a+H)(b+H)$

Factor Ring : $\langle R/H, +, \times \rangle$

- Set $R/H = \{a + H : a \in R\}$
- Addition, $(a + H) + (b + H) = (a + b) + H$ is well-defined
  - Addition is associative, since $(a + b) + c = a + (b + c)$
  - Addition is commutative, since $a + b = b + a$
  - Existence of Additive Identity, $0 + H$
  - Existence of Additive Inverse of $a + H = (-a) + H$
- Multiplication, $(a + H)(b + H) = (ab) + H$ is well-defined
  - Multiplication is associative, since $(ab)c = a(bc)$
  - Multiplication is distributive, since $a(b + c) = ab + ac$

Left Coset Multiplication is well-defined : $H \underset{ideal}{\leq} R$

$$(a+H)(b+H) = ab + H \implies ah, bh \in H$$

$$\begin{aligned}
(a+h_1)(b+h_2) \in ab + H &\implies (ab + ah_2 + bh_1 + h_1h_2) \in ab + H \\
&\implies ab + (ah_2 + bh_1 + h_1h_2) \in ab + H \\
&\implies ah_2 + bh_1 \in H, \ \forall h_1, h_2 \in H \\
&\implies ah, bh \in H, \ \forall h \in H
\end{aligned}$$

$$ah, bh \in H \implies (a+H)(b+H) = ab + H$$

$$\begin{aligned}
(a+h_1)(b+h_2) =& (ab + ah_2 + bh_1 + h_1h_2) \\
ah_2, bh_1, h_1h_2 \in H \implies& (a+H)(b+H) = ab + H
\end{aligned}$$

Ideal vs Normal

Definition (Normal Subgroup)

Let N be a subgroup of group G.
N is normal subgroup of G, if $gN = Ng$, $\forall g \in G$

Definition (Ideal)

Let N be an additive subgroup $\langle N, +_{|_N} \rangle$ of ring $\langle R, +, \times \rangle$.
N is an ideal of R, if $aN \subset N$ and $Nb \subset N$ $\forall a, b \in R$

Ideal - Example

$n\mathbb{Z} \underset{ideal}{\leq} \mathbb{Z}$

- $\langle n\mathbb{Z}, +\rangle \leq \langle \mathbb{Z}, +\rangle$.
  - $nm + ns \in n(m + s) \in n\mathbb{Z}$
  - Additive Identity, $0 = n0$
  - Additive Inverses of $nm = n(-m) = -nm$
- $aN \subset N$ and $Nb \subset N$
  - $s(nm) = n(ms) \in n\mathbb{Z}$ and $(nm)s = n(ms) \in n\mathbb{Z}$

Factor Ring $\langle R/N, +, \times \rangle$

- $N \underset{ideal}{\leq} R$
- Addition, $(a+N)+(b+N)=(a+b)+N$
- Multiplication, $(a+N)(b+N)=ab+N$

Theorem (Cannonical Homomorphism)

Let $N \underset{ideal}{\leq} R$. Let $\gamma : R \to R/N$ given by $\gamma(x) = x + N$ is a ring homomorphism with kernel N.

Theorem (Fundamental Homomorphism)

Let $\phi : R \to R'$ be a ring homomorphism with kernel N. Then there exists a cannonical homomorphism $\gamma_N : R \to R/N$ given by $\gamma_N(x) = x + N$ and a unique ring isomorphism $\mu : R/N \to R'$ given by $\mu(x+N) = \phi(x)$. That is, $\mu \circ \gamma_N = \phi$.

Frobeinus Homomorphism

Definition (Frobeinus Homomorphism)

Let R be a commutative ring with unity and characteristic p.
$\phi_p : R \to R$ given by $\phi_p(a) = a^p$ is a ring homomorphism

$\phi_7 : \mathbb{Z}_7 \to \mathbb{Z}_7,\ a \to a^p \pmod p$

$$\phi_7(5) = \phi_7(3) + \phi_7(2) = 3 + 2 = 5$$

$$\phi_7(6) = \phi_7(3)\phi_7(2) = 3 \times 2 = 6$$

Frobenius Homomorphism on $\mathbb{Z}_p$ is the identity map by Fermat's Little Theorem.

Nilradical Ideal

Definition (Nilradical)

An element $a \in R$ is nilradical if $a^n = 0$ for some positive integer n. The set of all nilradical elements of commutative ring R with an ideal is the nilradical of R.

Thank You