Abstract Algebra

Module 4

Section 24 : Noncommutative Examples

June 14, 2021

$M_n(F)$: Ring of $n \times n$ Matrices

Definition

- Set of all $n \times n$ matrices with entries in field F

$$A_{n\times n} = (a_{ij})_{n\times n} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

- Matrix Addition, $A + B = C$

$$(a_{ij})_{n\times n} + (b_{ij})_{n\times n} = (c_{ij})_{n\times n} \text{ where } c_{ij} = a_{ij} + b_{ij}$$

- Matrix Multiplication, $A \cdot B = C$

$$(a_{ij})_{n\times n} \cdot (b_{ij})_{n\times n} = (c_{ij})_{n\times n} \text{ where } c_{ij} = \sum_{k=0}^{n} a_{ik} b_{kj}$$

$\langle M_n(F), +, \cdot \rangle$: Noncommutative Ring with Unity

$\langle M_n(R), +, \cdot \rangle$ is well-defined only if R is a ring.

1. Addition is associative

$$A + (B + C) = (A + B) + C, \quad \forall A, B, C \in M_n(F)$$

2. Addition is commutative

$$A + B = B + A, \quad \forall A, B \in M_n(F)$$

3. Existence of Additive Identity

$$\text{Zero Matrix, } 0 = (0)_{n\times n}$$

$$\text{Then, } A + 0 = A, \quad \forall A \in M_n(F)$$

4. Existence of Inverse Matrices

$$A \in M_n(F), \text{ Inverse } A' = (-a_{ij})_{n\times n}$$

$$\text{Then, } A + A' = 0$$

$\langle M_n(F), +, \cdot \rangle$: Noncommutative Ring with Unity

5. Multiplication is associative

$$A \cdot (B \cdot C) = (A \cdot B) \cdot C, \quad \forall A, B, C \in M_n(F)$$

6. Multiplication is distributive over Addition

$$A \cdot (B + C) = A \cdot B + A \cdot C, \quad \forall A, B, C \in M_n(F)$$

$$(B + C) \cdot A = B \cdot A + C \cdot A, \quad \forall A, B, C \in M_n(F)$$

7. Existence of Multiplicative Identity, Unity

$$\text{Identity Matrix, } I = (\delta_{ij})_{n \times n}$$

$$\text{Then, } A \cdot I = A = I \cdot A, \quad \forall A \in M_n(F)$$

8. Multiplication is non-commutative

$$AB \neq BA, \quad \forall A, B \in M_n(F)$$

$End(A)$: Endomorphism of A

- $\langle A, * \rangle$: Abelian Group
- $End(A)$: set of all homomorphisms from A into A

$$\phi \in End(A),\ \text{Then } \phi(xy) = \phi(x)\phi(y)$$

- Function Addition

$$(\phi + \psi)(x) = \phi(x) + \psi(x), \quad \forall \phi, \psi \in End(A)$$

- Function Composition

$$(\phi \cdot \psi)(x) = \phi \circ \psi(x) = \phi(\psi(x)), \quad \forall \phi, \psi \in End(A)$$

$End(A)$: Noncommutative Ring

$\langle End(A), +, \circ \rangle$ is well-defined only if A is an abelian group.

Let $\theta, \phi, \psi \in End(A)$, $x \in A$

1. Addition is associative

$$\begin{aligned}(\theta + (\phi + \psi))(x) &= \theta(x) + (\phi + \psi)(x) \\ &= \theta(x) + (\phi(x) + \psi(x)) \\ &= (\theta(x) + \phi(x)) + \psi(x) \\ &= ((\theta + \phi) + \psi)(x)\end{aligned}$$

2. Addition is commutative

$$\begin{aligned}(\phi + \psi)(x) &= \phi(x) + \psi(x) \\ &= \psi(x) + \phi(x) \\ &= (\psi + \phi)(x)\end{aligned}$$

$End(A)$: Noncommutative Ring

3. Existence of Additive Identity
   Consider, the trivial homomorphism 0. Then $0 \in End(A)$.

$$\begin{aligned}(\phi + 0)(x) &= \phi(x) + 0(x) \\ &= \phi(x) + e, \quad \because 0(x) = e,\ \forall x \in A \\ &= \phi(x)\end{aligned}$$

4. Existence of Additive Inverses
   Let $\phi \in End(A)$.
   Consider $\phi' : A \to A$ defined by $\phi'(x) = -\phi(x)$.

$$\begin{aligned}(\phi + \phi')(x) &= \phi(x) + \phi'(x) \\ &= \phi(x) + (-\phi(x)) \\ &= e \\ &= 0(x)\end{aligned}$$

$End(A)$: Noncommutative Ring

5. Multiplication is associative
   Let $\theta, \phi, \psi \in End(A)$.

$$\begin{aligned}(\theta(\phi\psi))(x) &= \theta \circ \phi\psi(x) \\ &= \theta \circ \phi \circ \psi(x) \\ &= \theta\phi \circ \psi(x) \\ &= ((\theta\phi)\psi)(x)\end{aligned}$$

6. Multiplication is distributive over Addition
   6.1 Multiplication is left-distributive over Addition

$$\begin{aligned}(\theta(\phi + \psi))(x) &= \theta \circ (\phi + \psi)(x) \\ &= \theta((\phi + \psi)(x)) \\ &= \theta(\phi(x) + \psi(x)) \\ &= \theta(\phi(x)) + \theta(\psi(x)) \\ &= \theta\phi(x) + \theta\psi(x)\end{aligned}$$

$End(A)$: Noncommutative Ring

6. Multiplication is distributive over Addition
   6.2 Multiplication is right-distributive over Addition

$$\begin{aligned}((\phi+\psi)\theta)(x) &= (\phi+\psi)\circ\theta(x)\\ &= (\phi+\psi)(\theta(x))\\ &= \phi(\theta(x))+\psi(\theta(x))\\ &= \phi\theta(x)+\psi\theta(x)\end{aligned}$$

7. Existence of Multiplicative Identity
   Consider the identity map, $id : A \to A$. Then $id \in End(A)$.

$$\phi id(x) = \phi(id(x)) = \phi(x)$$

$$id\phi(x) = id(\phi(x)) = \phi(x)$$

Examples : $End(\mathbb{Z}_m \times \mathbb{Z}_n)$

$End(\mathbb{Z}_m \times \mathbb{Z}_n)$ is noncommutative

- abelian group $\mathbb{Z}_m \times \mathbb{Z}_n$
- $\phi, \psi \in End(\mathbb{Z}_m \times \mathbb{Z}_n)$

$$\phi(m, n) = (m + n, 0)$$

$$\psi(m, n) = (n, 0)$$

- $\phi\psi \neq \psi\phi$.

Examples : Weyl Algebra

Weyl Algebra, $End(F[x])$ are noncommutative

- field of characteristic zero, F
- abelian group, $F[x]$
- $X, Y \in End(F[x])$

$$X(a_0 + a_1 x + \cdots + a_n x^n) = a_0 x + a_1 x^2 + \cdots + a_n x^{n+1}$$

$$Y(a_0 + a_1 x + \cdots + a_n x^n) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}$$

- $XY \neq YX$.
- **Weyl Algebra** : The subring of $End(F[x])$ generated by X, Y

Summary : $\langle End(A), +, \circ \rangle$

$\langle End(A), +, \circ \rangle$ is well-defined

1. $\phi, \psi \in End(A)$
   1.1 $\phi : A \to A$ is well defined by $x \to \phi(x)$
   1.2 $\phi : A \to A$ is a homomorphism ie, $\phi(xy) = \phi(x)\phi(y)$
   1.3 $\psi : A \to A$ is well defined by $x \to \psi(x)$
   1.4 $\psi : A \to A$ is a homomorphism ie, $\psi(xy) = \psi(x)\psi(y)$
2. $\phi + \psi \in End(A)$
   2.1 $\phi + \psi : A \to A$ is well-defined by $x \to \phi(x) + \psi(x)$
3. $\phi + \psi \in End(A)$
   3.1 $\phi \circ \psi : A \to A$ is well-defined by $x \to \phi(\psi(x))$

$\langle End(A), +, \circ \rangle$ is non-commutative ring with unity

1. Additive Identity, $0 =$ Trivial Homomorphism, $x \to e$
2. Multiplicative Identity/Unity, $1 = id_A$ (Identity Map), $x \to x$

Group Ring, RG

The set of all formal sums, RG

- $\langle G, \cdot \rangle$ be a multiplicative group
- $\langle R, +, \times \rangle$ be commutative ring with nonzero unity
- Elements of RG are of the form $\sum_{i \in I} a_i g_i$
  where $a_i \in R$, $g_i \in G$ and all except finite a_i are zero.

Example : $\mathbb{Z}_6 S_3$

- $\langle \mathbb{Z}_6, +_6, \times_6 \rangle$ is a ring (but not an integral domain)
- $\langle S_3, \circ \rangle$ is a symmetric group of permutations of $\{1, 2, 3\}$
- Let $x = 2\mu_1 + 0\mu_2 + 1\mu_3 + 2\rho_0 + 5\rho_1 + 2\rho_2$
- Clearly, $x \in \mathbb{Z}_6 S_3$

Group Ring, RG

Group Ring, RG is an Abelian group

- Set $RG = \left\{ \sum_{i \in I} a_i g_i : a_i \in R,\ g_i \in G \right\}$
  where all expect finte a_i are zero
- Addition in RG

$$\sum_{i \in I} a_i g_i + \sum_{i \in I} b_i g_i = \sum_{i \in I} (a_i + b_i) g_i$$

- Addition is closed (since ring addition is closed)
- Addition is commutative (since ring addition is commutative)
- Addition is associative (since ring addition is associative)
- Additive Identity, $0 = \sum_{i \in I} 0 g_i$
- Additive Inverse of $\sum_{i \in I} a_i g_i$ is $\sum_{i \in I} (-a_i) g_i$
  where $(-a_i)$ are the additive inverses of a_i in the ring R

Group Ring, RG

Multiplication in RG

$$\sum_{i\in I} a_i g_i \sum_{i\in I} b_i g_i = \sum_{i\in I}\left(\sum_{g_j g_k = g_i} a_j b_k\right) g_i$$

Example : $\mathbb{Z}_6 S_3$

- $x = 2\mu_1 + 0\mu_2 + 1\mu_3 + 2\rho_0 + 5\rho_1 + 2\rho_2$
- $y = 4\mu_1 + 2\mu_2 + 3\mu_3 + 2\rho_0 + 2\rho_1 + 0\rho_2$
- $xy = 1\mu_1 + 2\mu_2 + 0\mu_3 + 1\rho_0 + 4\rho_1 + 4\rho_2$ (by SageMath)

$\rho_1\mu_1 = (2,3)(1,2,3) = (1,3,2) = \mu_2$

	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

Computation in $\mathbb{Z}_6 S_3$: by Hand

- $x = 2\mu_1 + 0\mu_2 + 1\mu_3 + 2\rho_0 + 5\rho_1 + 2\rho_2$
- $y = 4\mu_1 + 2\mu_2 + 3\mu_3 + 2\rho_0 + 2\rho_1 + 0\rho_2$

$$\begin{aligned}
xy =& 2\mu_1\mu_1 \quad + 4\mu_1\mu_2 \quad + 4\mu_1\rho_0 + 4\mu_1\rho_1 \quad + \\
& 4\mu_3\mu_1 \quad + 2\mu_3\mu_2 \quad + 3\mu_3\mu_3 \quad + 2\mu_3\rho_0 + 2\mu_3\rho_1 \quad + \\
& 2\rho_0\mu_1 + 4\rho_0\mu_2 + 4\rho_0\rho_0 + 4\rho_0\rho_1 + \\
& 2\rho_1\mu_1 \quad + 4\rho_1\mu_2 \quad + 3\rho_1\mu_3 \quad + 4\rho_1\rho_0 + 4\rho_1\rho_1 \quad + \\
& 2\rho_2\mu_1 \quad + 4\rho_2\mu_2 \quad + 4\rho_2\rho_0 + 4\rho_2\rho_1 \\
=& 1\mu_1 + 2\mu_2 + 0\mu_3 + 1\rho_0 + 4\rho_1 + 4\rho_2
\end{aligned}$$

Computation in $\mathbb{Z}_6 S_3$: by Hand

- $x = 2\mu_1 + 0\mu_2 + 1\mu_3 + 2\rho_0 + 5\rho_1 + 2\rho_2$
- $y = 4\mu_1 + 2\mu_2 + 3\mu_3 + 2\rho_0 + 2\rho_1 + 0\rho_2$

$$
\begin{aligned}
xy =& 2 \quad \rho_0 + 4 \quad \rho_2 + 4\mu_1 \quad + 4 \quad \mu_3 + \\
& 4 \quad \rho_2 + 2 \quad \rho_1 + 3 \quad \rho_0 + 2\mu_3 \quad + 2 \quad \mu_2 + \\
& 2 \quad \mu_1 + 4 \quad \mu_2 + 4 \quad \rho_0 + 4 \quad \rho_1 + \\
& 2 \quad \mu_2 + 4 \quad \mu_3 + 3 \quad \mu_1 + 4\rho_1 \quad + 4 \quad \rho_2 + \\
& 2 \quad \mu_3 + 4 \quad \mu_1 + 4\rho_2 \quad + 4 \quad \rho_0 \\
=& 1\mu_1 + 2\mu_2 + 0\mu_3 + 1\rho_0 + 4\rho_1 + 4\rho_2
\end{aligned}
$$

Group Ring, RG

$\langle RG, +, \times \rangle$ is a ring - Group Ring

$$RG = \left\{ \sum_{i \in I} a_i g_i : a_i \in R,\ g_i \in G \right\}$$

$$\sum_{i \in I} a_i g_i + \sum_{i \in I} b_i g_i = \sum_{i \in I} (a_i + b_i) g_i$$

$$\sum_{i \in I} a_i g_i \times \sum_{i \in I} b_i g_i = \sum_{i \in I} \left(\sum_{g_j g_k = g_i} a_j b_k \right) g_i$$

- multiplication is associative $x(yz) = (xy)z$
- multiplication is distributive over addition
    1. left distributive, $x(y + z) = xy + xz$
    2. right distributive, $(x + y)z = xz + yz$

Complex Field

Complex Numbers

- $\mathbb{C} = \mathbb{R} \times \mathbb{R} = \mathbb{R}^2$
  - $(1, 0) = 1$ and $(0, 1) = i$
  - $(u, v) = u(1, 0) + v(0, 1) = u + iv$
- Addition Operation (usual)
  $(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$
- Multiplicaiton Operation (complicated ?)
  $(a_1, a_2) \times (b_1, b_2) = (a_1 b_1 - a_2 b_2, a_1 b_2 + a_2 b_1)$

Complex Numbers

Multiplication in $\mathbb{R}^2$

- No candidates for usual multiplication.
- Multiplicaiton Operation (expectation)
  $(a_1 + a_2 i) \times (b_1 + b_2 i) = a_1 b_1 + a_1 b_2 i + a_2 i b_1 + a_2 i b_2 i$
- Assuming some commutativity and preserving unity 1.
  $(a_1 + a_2 i) \times (b_1 + b_2 i) = (a_1 b_1 + a_2 b_2 i^2) + (a_1 b_2 + a_2 b_1) i$
- $(u, v) = u + iv$ where $i^2 = -1$

Quaternions - $\langle \mathbb{H}, +, \cdot \rangle$

- $\mathbb{H} = \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R} = \mathbb{R}^4$
  - $(u, v, w, x) = u + vi + wj + xk$
  - $i^2 = j^2 = k^2 = -1$
  - $ijk = -1$
    - $ijk = jki = kij = -1$
    - $ikj = jik = kji = 1$
    - $ij = -ji$
- Addition Operation (usual)
  $$(a_1, a_2, a_3, a_4) + (b_1, b_2, b_3, b_4) = (a_1 + b_1, a_2 + b_2, a_3 + b_3, a_4 + b_4)$$
- Multiplication Operation (simlified)
  $$(a_1, a_2, a_3, a_4) \times (b_1, b_2, b_3, b_4) = (a_1 b_1 - a_2 b_2 - a_3 b_3 - a_4 b_4, a_1 b_2 + a_2 b_1 + a_3 b_4 - a_4 b_3, a_1 b_3 - a_2 b_4 + a_3 b_1 + a_4 b_2, a_1 b_4 + a_2 b_3 - a_3 b_2 + a_4 b_1)$$

Quaternions - $\langle \mathbb{H}, +, \cdot \rangle$

- $\mathbb{H} = \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R} = \mathbb{R}^4$
  - $(u, v, w, x) = u + vi + wj + xk$
  - $i^2 = j^2 = k^2 = -1$
  - $ijk = -1$
    - $ijk = jki = kij = -1$
    - $ikj = jik = kji = 1$
    - $ij = -ji$
- Addition Operation (usual)

$$(a_1 + a_2 i + a_3 j + a_4 k) + (b_1 + b_2 i + b_3 j + b_4 k) = \\ (a_1 + b_1) + (a_2 + b_2)i + (a_3 + b_3)j + (a_4 + b_4)k$$

- Multiplication Operation (simlified)

$$\begin{aligned}(a_1 + a_2 i + a_3 j + a_4 k) \times (b_1 + b_2 i + b_3 j + b_4 k) = \\ a_1 b_1 + a_1 b_2 i + a_1 b_3 j + a_1 b_4 k + \\ a_2 b_1 i + a_2 b_2 i^2 + a_2 b_3 ij + a_2 b_4 ik + \\ a_3 b_1 j + a_3 b_2 ji + a_3 b_3 j^2 + a_3 b_4 jk + \\ a_4 b_1 k + a_4 b_2 ki + a_4 b_3 kj + a_4 b_4 k^2\end{aligned}$$

Quaternions - $\langle \mathbb{H}, +, \cdot \rangle$

- $\mathbb{H} = \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R} = \mathbb{R}^4$
  - $(u, v, w, x) = u + vi + wj + xk$
  - $i^2 = j^2 = k^2 = -1$
  - $ijk = -1$
    - $ijk = jki = kij = -1$
    - $ikj = jik = kji = 1$
    - $ij = -ji$
- Addition Operation (usual)

$$(a_1 + a_2 i + a_3 j + a_4 k) + (b_1 + b_2 i + b_3 j + b_4 k) = (a_1 + b_1) + (a_2 + b_2)i + (a_3 + b_3)j + (a_4 + b_4)k$$

- Multiplication Operation (simlified)

$$\begin{aligned}(a_1 + a_2 i + a_3 j + a_4 k) \times (b_1 + b_2 i + b_3 j + b_4 k) = {} & a_1 b_1 + a_1 b_2 i + a_1 b_3 j + a_1 b_4 k + \\ & a_2 b_1 i - a_2 b_2 + a_2 b_3 k - a_2 b_4 j + \\ & a_3 b_1 j - a_3 b_2 k - a_3 b_3 + a_3 b_4 i + \\ & a_4 b_1 k + a_4 b_2 j - a_4 b_3 i - a_4 b_4\end{aligned}$$

Quaternions - $\langle \mathbb{H}, +, \cdot \rangle$

- $\mathbb{H} = \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R} = \mathbb{R}^4$
  - $(u, v, w, x) = u + vi + wj + xk$
  - $i^2 = j^2 = k^2 = -1$
  - $ijk = -1$
    - $ijk = jki = kij = -1$
    - $ikj = jik = kji = 1$
    - $ij = -ji$
- Addition Operation (usual)
- Multiplication Operation (simlified)
- Additive Identity, $0 = (0, 0, 0, 0)$
- Multiplicative Identity, $1 = (1, 0, 0, 0)$
- Additive Inverse of $(a_1, a_2, a_3, a_4) = (-a_1, -a_2, -a_3, -a_4)$
- Multiplicative Inverse of (a_1, a_2, a_3, a_4)

$$\left(\frac{a_1}{|a|^2}, \frac{-a_2}{|a|^2}, \frac{-a_3}{|a|^2}, \frac{-a_4}{|a|^2}\right) \text{ where } |a|^2 = a_1^2 + a_2^2 + a_3^2 + a_4^2$$

$\mathbb{H}$ is a subring of $M_2(\mathbb{C})$

Ring Homomorphism

$$\phi : \mathbb{H} \to M_2(\mathbb{C}) \text{ defined by } \phi(a,b,c,d) = \begin{bmatrix} a+bi & c+di \\ -c+di & a-bi \end{bmatrix}$$

$$\phi\left((a,b,c,d)+(e,f,g,h)\right) = \phi\left(a,b,c,d\right)) + \phi\left(e,f,g,h\right))$$

$$\phi\left((a,b,c,d)\times(e,f,g,h)\right) = \phi\left(a,b,c,d\right)) \times \phi\left(e,f,g,h\right))$$

Different Form

$$\phi(a,b,c,d) = a\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + b\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} + c\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} + d\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

ϕ preserves multiplication

$$\phi(a,b,c,d) = a\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} + b\begin{bmatrix}i & 0\\ 0 & -i\end{bmatrix} + c\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix} + d\begin{bmatrix}0 & i\\ i & 0\end{bmatrix}$$

- $\phi(i)^2 = \phi(j)^2 = \phi(k)^2 = \phi(-1) = -1\phi(1)$
- $\phi(i) = \phi(jk) = \phi(j)\phi(k)$

ϕ preserves multiplication

$$\phi(a, b, c, d) = aA + bB + cC + dD$$

- $\phi(i)^2 = \phi(j)^2 = \phi(k)^2 = \phi(-1) = -1\phi(1)$
- $B^2 = C^2 = D^2 = -1A$
- $\phi(i) = \phi(jk) = \phi(j)\phi(k)$
- $B = CD$

Strictly Skew Field $\langle \mathbb{H}, +, \cdot \rangle$

1. $\mathbb{H} = \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}$
2. Usual Addition
   - 2.1 Addition is Associative
   - 2.2 Addition is Commutative
   - 2.3 Additive Identity $(0,0,0,0) = 0 + 0i + 0j + 0k$
   - 2.4 Additive Inverse of (a,b,c,d) is $(-a,-b,-c,-d)$
3. Multiplication
   - 3.1 Multiplication is associative since $\mathbb{H} \leq M_2(\mathbb{C})$
   - 3.2 Multiplication is not commutative $ij \neq ji$
     ie, $(0,1,0,0)(0,0,1,0) \neq (0,0,1,0)(0,1,0,0)$
   - 3.3 Multiplication Identity, Unity $(1,0,0,0) = 1 + 0i + 0j + 0k$
   - 3.4 Multiplicative Inverse of (a,b,c,d) is $\left(\frac{a}{m}, -\frac{b}{m}, -\frac{c}{m}, -\frac{d}{m}\right)$
     where $m = a^2 + b^2 + c^2 + d^2$

Next Topic : Wedderburn's Theorem

Theorem (Wedderburn)

Every finite division ring is a field.