

DISCRETE MATHEMATICS AND APPLICATIONS

Abstract Algebra 3

Mohd Sham Mohamad (mohdsham@ump.edu.my) Adam Shariff Adli Aminuddin (adamshariff@ump.edu.my)

Faculty of Industrial Sciences & Technology



Chapter Description

Chapter Outline

5.6 Rings5.7 Commutative Rings5.8 Field

Aims

 Define properties and give some examples of rings and fields.



References

- 1. Rosen K.H., Discrete Mathematics & Its Applications, (Seventh Edition), McGraw-Hill, 2011
- 2. Epp S.S, Discrete Mathematics with Applications, (Fourth Edition), Thomson Learning, 2011
- 3. Ram Rabu, Discrete Mathematics, Pearson, 2012
- Walls W.D., A beginner's guide to Discrete Mathematics, Springer, 2013
- 5. Chandrasekaren, N. & Umaparvathi, M., Discrete Mathematics, PHI Learning Private Limited, Delhi, 2015



Rings

A ring is a nonempty set *R* together with two binary operations + and \cdot (which we call as addition and multiplication) that satisfy the following conditions. $\forall a, b, c \in R$,

- (i) *R* is abelian group under addition + (i.e. $\langle R, + \rangle$ is abelian).
- (ii) Multiplication is associative (i.e. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$).
- (iii) Left distributive law, $a \cdot (b+c) = (a \cdot b) + (a \cdot c) \&$

right distributive law, $(a+b) \cdot c = (a \cdot c) + (b \cdot c)$ hold.



Rings: Example 1

 $\left< \mathbb{Z}_6, +, \cdot \right>$

- (i) \mathbb{Z}_6 is an abelian group under addition +
- (ii) Multiplication is associative $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, $a, b, c \in \mathbb{Z}_6$ by properties of integers
- (iii) Left distributive law, $a \cdot (b+c) = (a \cdot b) + (a \cdot c) \&$

right distributive law, $(a+b) \cdot c = (a \cdot c) + (b \cdot c)$ hold

Try:

If a = 2, b = 3, c = 5 show that it satisfy Left and Right distributive law



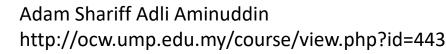
Rings: Example 2

 $\left\langle M_{2}(\mathbb{Z}),+,\cdot
ight
angle$

- (i) $M_2(\mathbb{Z})$ is an abelian group under addition.
- (ii) Multiplication is associative $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, $a, b, c \in M_2(\mathbb{Z})$ by properties of matrices
- (iii) Left distributive law, $a \cdot (b+c) = (a \cdot b) + (a \cdot c) \&$

right distributive law, $(a+b) \cdot c = (a \cdot c) + (b \cdot c)$ hold

If $a = \begin{bmatrix} 2 & 1 \\ 2 & 3 \end{bmatrix}$, $b = \begin{bmatrix} 1 & 1 \\ 3 & 3 \end{bmatrix}$, $c = \begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix}$ show that it satisfy Left and Right distributive law



Commutative Rings

A ring in which the multiplication is commutative is a commutative ring.

Example

Let *G* be the group of isomorphism $\phi : \mathbb{Z}_{rs} \to \mathbb{Z}_r \times \mathbb{Z}_s$ where gcd(r, s) = 1.

Clear that $\phi(n \cdot 1) = n(1 \cdot 1)$ is an additive group isomorphism.

To check the multiplicative, use the unity (1,1) in the ring $\mathbb{Z}_r \times \mathbb{Z}_s$ and compute

$$\phi(m,n) = (mn) \cdot (1,1) = [m \cdot (1,1)][n \cdot (1,1)] = \phi(m)\phi(n) \text{ and}$$

$$\phi(n,m) = (nm) \cdot (1,1) = [n \cdot (1,1)][m \cdot (1,1)] = \phi(n)\phi(m).$$



Commutative Rings: Example

1. $\langle \mathbb{Z}_6, +, \cdot \rangle$ is a commutative ring.

 \mathbb{Z}_{6}^{*} is commute under multiplication.

2. $\langle M_2(\mathbb{Z}), +, \cdot \rangle$ is not a commutative ring.

Matrices is not necessary commute under multiplication of matrices.





A field is a commutative division ring.

Some terminologies:

1. Ring with unity

A ring with multiplicative identity.

2. Unit

Let R be a ring with unity 1. An element u in R is a unit of R if it has a multiplicative inverse in R.

3. Division ring

If every nonzero element of R is a unit, the R is a division ring/skew field.



Field: Example 1

In the ring $M_2(\mathbb{C})$, let

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \ j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ and } k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

The set H of real quaterions consists of all matrices of the form

$$a1 + b\tilde{i} + c\tilde{j} + d\tilde{k} = \begin{pmatrix} a + ib & c + di \\ -c + di & a - bi \end{pmatrix}$$

where $a, b, c, d \in \mathbb{R}$. It is easy to verify that *H* is closed under the usual addition of matrices. Note that multiplication is not commutative in this ring; e.g., ij = k = -ji. It is possible to show nevertheless that *H* is not only a ring with identity but a division ring.



Field: Example 2

- 1. Show that $\langle \mathbb{Z}_5, +, \cdot \rangle$ is a field. \mathbb{Z}_6^* is commute under multiplication.
- 2. Show that $\langle M_2(\mathbb{R}), +, \cdot \rangle$ is not a field. $\langle M_2(\mathbb{R}), +, \cdot \rangle$ is a division ring but not field since $\langle M_2(\mathbb{R}), +, \cdot \rangle$ is not commutative.

