PMATH 336 Introduction to Group Theory

Keven Qiu
Instructor: Wentang Kuo
Fall 2024

Chapter 1

Rings, Fields, and Groups

Definition: Cartesian Product

For a set S, we write $S \times S = \{(a, b) : a \in S, b \in S\}$.

Definition: Binary Operation

A binary operation on S is a map $* : S \times S \to S$, where for $a, b \in S$, we denote $*(a, b) = a * b$.

E.g. For $S = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, there are $* : \times, +$.

Definition: Ring (With Identity)

A set R together with two binary operations $+$ and $\times$, where for $a, b \in R$, we often write $a \times b = a \cdot b = ab$ and $a + b$ and two distinct elements 0 and 1, such that

1. $+$ is associative: $(a + b) + c = a + (b + c)$ for all $a, b, c \in R$
2. $+$ is commutative: $a + b = b + a$ for all $a, b \in R$
3. 0 is an additive identity: $0 + a = a$ for all $a \in R$
4. Every element has an additive inverse: $\forall a \in R$, $\exists b \in R$ such that $a + b = 0$
5. $\cdot$ is associative: $(ab)c = a(bc)$ for all $a, b, c \in R$
6. 1 is a multiplicative identity: $1 \cdot a = a \cdot 1 = a$ for all $a \in R$
7. $\cdot$ is distributive over $+$: $a(b + c) = ab + ac$ for all $a, b, c \in R$

Note that we do not assume that $ab = ba$.

Definition: Commutative Ring

A set R that is a ring and $\cdot$ is commutative.

Definition: Right(Left) Inverse

For $a \in R, a \neq 0$, we say a has a right(left) inverse if $\exists b \in R$, $ab = 1$ ($ba = 1$).

Definition: Unit (Invertible)

We say a is a unit/invertible if a has the same right and left inverse, $ab = ba = 1$.

Definition: Field

A commutative ring that satisfies every non-zero element is a unit.

Remark: For some non-commutative ring, there exists $a \in R$, a has a right inverse, but it has no left inverse. We have $ab = ca = 1$, but $b \neq c$.

E.g. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are commutative rings. $\mathbb{Z}$ is not a field, take 2, the inverse is $\frac{1}{2}$, but $\frac{1}{2} \notin \mathbb{Z}$. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all fields.

$\mathbb{F}_p = \mathbb{Z}_p$ where p is prime, then this is a field. $\mathbb{Z}_m$ where $m \in \mathbb{N}$ and m is not prime is a ring, but not a field.

E.g. If R is a ring, then $R[x]$ (the set of all polynomials in x with coefficients in R) is a ring and not a field. x has no inverse.

Proposition

In $R[x]$, the set of units in $R[x]$ is the same as that in R.

So the set of units in $\mathbb{Z}[x]$ is the set of units in $\mathbb{Z}$.

Proposition

If R is a ring and $n \in N$, then $M_n(R)$ (the set of all $n \times n$ matrices with entries in R) is a ring. It is usually non-commutative.

E.g. Let R and S be rings. Then

$$R \times S = \{(r, s) : r \in R, s \in S\}$$

Define $(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$ and $(r_1, s_1) \cdot (r_2, s_2) = (r_1 r_2, s_1 s_2)$. Then $(R \times S, +, \cdot)$ is a ring with $0_{R \times S} = (0_R, 0_S)$ and $1_{R \times S} = (1_R, 1_S)$.

Theorem (Uniqueness of Inverse)

Let R be a commutative ring. Let $a \in R$, then

1. The additive inverse of a is unique. ($a + b = 0 = a + c \implies b = c$)
2. For $a \neq 0$, if a has an inverse, then it is unique. ($ab = 1 = ac \implies b = c$)

Proof. 1.

$$\begin{aligned} b &= 0 + b \\ &= (c + a) + b \\ &= c + (a + b) \\ &= c + 0 \\ &= c \end{aligned}$$

2. Similar.

Definition: Additive Inverse

For $a \in R$, denote $-a$ as the unique additive inverse of a.

Definition: Inverse

For $a \in R$, if a has an inverse, denote a^{-1} or $\frac{1}{a}$ as the inverse of a.

Theorem (Cancellation)

Let R be a ring, then for all $a, b, c \in R$,

1. If $a + b = a + c$, then $b = c$.
2. If $a + b = a$, then $b = 0$.
3. If $a + b = 0$, then $b = -a$.

Let F be a field, then for all $a, b, c \in F$,

1. If $ab = ac$, then either $a = 0$ or $b = c$.
2. If $ab = a$, the neither $a = 0$ or $b = 1$.
3. If $ab = 1$, then $b = a^{-1}$.
4. If $ab = 0$, then either $a = 0$ or $b = 0$.

Proof. 1. $b = 0 + b = (-a + a) + b = -a + (a + b) = -a + (a + c) = (-a + a) + c = 0 + c = c$.

2. $a + b = a + 0$, then it follows from 1.

3. $a + b = 0 = a + (-a)$, then it follows from 1.

4. Recall $A \implies B \vee C$ is the same as $A \wedge \neg B \implies C$. So assume $a \neq 0$. We have $ab = ac$. Since $a \neq 0$ and F is a field, a has the inverse a^{-1}. Thus,

$$\begin{aligned} b = 1 \cdot b &= (a^{-1} \cdot a)b \\ &= a^{-1}(ab) \\ &= a^{-1}(ac) \\ &= (a^{-1}a)c \\ &= 1 \cdot c = c \end{aligned}$$

5, 6, 7 follows from 4.

Theorem

Let R be a ring and $a \in R$, then

1. $0 \cdot a = 0$.
2. $(-1) \cdot a = -a$.

Proof. 1. $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$. By cancellation theorem (2), $0 \cdot a = 0$.

2. $0 = 0 \cdot a = (1 + (-1)) \cdot a = 1 \cdot a + (-1) \cdot a$. Since $a + (-1) \cdot a = 0$, then by cancellation theorem (3), $(-1) \cdot a = -a$.

Definition: Group

A set G with a binary operation $\cdot : G \times G \to G$ satisfying the following conditions:

1. For all $f, g, h \in G$, $(fg)h = f(gh)$
2. There exists an element e_ℓ (ℓ stands for left) called an identity such that for all $g \in G$,
   (a) $e_\ell \cdot g = g$
   (b) there exists an element g_ℓ^{-1} such that $g_\ell^{-1} \cdot g = e_\ell$

Chapter 2

Subgroups and Cyclic Groups

Chapter 3

Symmetric Groups

Chapter 4

Homomorphisms

Chapter 5

Cosets and Normal Subgroups

Chapter 6

Free and Finite Abelian Groups

Chapter 7

Isometrics and Symmetric Groups

Chapter 8

Group Actions

Chapter 9

Sylow Theorems