PMATH 336 Introduction to Group Theory

Keven Qiu
Instructor: Wentang Kuo
Fall 2024

Contents

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 called an identity such that for all $g \in G$,
   (a) $e \cdot g = g$
   (b) there exists an element g^{-1} such that $g^{-1} \cdot g = g \cdot g^{-1} = e$

Remark: In this class, we use the left identity, but we can show that we can use either left or right. Note that commutativity is not implied.

Definition: Order of G

The cardinality of G denoted by $|G|$.

If $|G| = n$ is finite, we say G is a finite group. If $|G| = \infty$, G is an infinite group.

Definition: Abelian Group

A group G where for every $a, b \in G$, $ab = ba$.

If the group is Abelian, we sometimes use $+$ as the binary operation notation. The identity will be denoted by 0. For all $k \in \mathbb{Z}, a \in G$, then $ka := \underbrace{a + a + \cdots + a}_{k}$.

In general, we use 1 or e as the identity of G. So $a^k = \underbrace{a \cdots a}_{k}$. $a^0 = 1$ or e and $a^{-k} = \underbrace{a^{-1} \cdots a^{-1}}_{k}$.

Theorem

Let G be a group with identity e and $a, b, c \in G$.

1. If $ab = ac$ or $ba = ca$, then $b = c$.
2. If $ab = e$, then $a^{-1} = b$ and $b^{-1} = a$.
3. If $ab = a$, then $b = e$.
4. If $ba = a$, then $b = e$.

Proof. 1. Let a^{-1} be an inverse of a.

$$b = eb = (a^{-1}a)b = a^{-1}(ab) = a^{-1}(ac) = (a^{-1}a)c = ec = c$$

2 and 3 are similar.

Corollary

The identity and the inverse are unique.

If $e_1, e_2 \in G$ such that for any $g \in G$, $e_1 g = g e_1, e_2 g = g e_2$, then $e_1 = e_2$. If for $g \in G$, $b_1, b_2 \in G$ such that $b_1 g = g h_1 = e = b_2 g = g b_2$, then $b_1 = b_2$.

E.g. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all Abelian groups with infinite orders. Note that the binary operation is addition.

Let R be a ring. We define

$$R^* = \text{the set of all invertible elements/units in } R$$

Then R^* is a group with binary operation being multiplication. Addition does not work, take 1 and -1, if we add $1 + (-1) = 0$ does not have an inverse and is not in R^*.

Definition: Groups of Units Modulo n

$$U_n = \mathbb{Z}_n^* = \{[b]_n : 1 \le b \le n, \gcd(b, n) = 1\}$$

$\mathbb{Z}^* = \{1, -1\}$ is a finite group. $\mathbb{Q}^* = \{r \in \mathbb{Q} : r \neq 0\} = \mathbb{Q} \setminus \{0\}$. $\mathbb{R}^* = \mathbb{R} \setminus \{0\}, \mathbb{C}^* = \mathbb{C} \setminus \{0\}$ are infinite groups.

$\mathbb{Z}_m^* = \{[b]_m : 1 \le b \le m, \gcd(b, m) = 1\}$. $|\mathbb{Z}_m^*| = \phi(m)$

Definition: Euler's Phi Function ϕ

If $m = p_1^{k_1} \cdots p_\ell^{k_\ell}$, then

$$\phi(m) = (p_1^{k_1} - p_1^{k_1 - 1}) \cdots (p_\ell^{k_\ell} - p_\ell^{k_\ell - 1})$$

$|\mathbb{Z}_{10}^*| = |\{1, 3, 7, 9\}| = 4 = (5^1 - 5^0)(2^1 - 2^0)$.
$|\mathbb{Z}_{100}^*| = (5^2 - 5^1)(2^2 - 2^1) = 20(2) = 40$.

Recall that $M_n(R)$ where R is a ring is non-commutative. We can define

$$M_n(R)^* = GL_n(R)$$

Definition: General Linear Group

Let R be a ring. The set of $n \times n$ matrices A such that $\det(A) \neq 0$.

$$M_n(R)^* = GL_n(R)$$

Note that $M_1(R)^* = GL_1(R) = R^*$. If R is commutative, $GL_1(R)^* = R^*$ is Abelian. However, if $n \geq 2$, $GL_n(R)$ must be non-Abelian.

$GL_n(\mathbb{Z}_p)$ is finite. $GL_n(\mathbb{Q}), GL_n(\mathbb{R}), GL_n(\mathbb{C}), GL_n(\mathbb{Z})$ are infinite.

$GL_n(\mathbb{Z})$ is infinite for $n \geq 2$. Take $n = 2$. If the matrix is $\begin{pmatrix} n & n-1 \\ n+1 & n \end{pmatrix} \in GL_2(\mathbb{Z})$. So we have infinitely many elements in $GL_2(\mathbb{Z})$.

If G is finite, we would like to know $|G|$.

Proposition

$|GL_n(\mathbb{Z}_p)| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$.

Proof. For a matrix $A = (v_1, v_2, \ldots, v_n)^T$ where $v_i \in M_{1 \times n}(\mathbb{Z}_p)$. $A \in GL_n(\mathbb{Z}_p)$ if and only if $v_1, \ldots, v_n$ are linearly independent if and only if for all i where $2 \leq i \leq n$, $v_i \notin \text{Span}\{v_1, \ldots, v_{i-1}\}$. Therefore, the number of choices for v_1 is $p^n - 1$. The number of choices for v_2 is $p^n - p$. For v_3 is $p^n - p^2$. For v_n, there are $p^n - p^{n-1}$.

Definition: Special Linear Group

$$SL_n(R) = \text{the set of all } n \times n \text{ matrices } A \text{ with entries in } R \text{ and } \det(A) = 1$$

Proposition

$|SL_n(\mathbb{Z}_p)| = |GL_n(\mathbb{Z}_p)| / (p - 1)$.

Recall s

Definition: Permutation

For a set S, the set of permutations $\text{Perm}(S) = \{f : S \to S : f \text{ is bijective}\}$, $\text{Perm}(S)$ is a group with the composition as its binary operation and the identity bijection as its identity.

Proposition

$|\text{Perm}(S)| = |S|!$.

Definition: n Symmetric Group

Let $S = \{1, 2, \ldots, n\}$. Then $S_n = \text{Perm}(\{1, 2, \ldots, n\})$.

Definition: Operation/Multiplication Table

For a finite group, we can specify its operation $*$ by making a table showing the value of the product $a * b$ for each pair $a, b \in G^2 = G \times G$.

E.g. $U_{12} = \{1, 5, 7, 11\}$.

a/b	1	5	7	11
1	1	5	5	7
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Proposition

If G and H are groups, then $G \times H$ is also a group.
The order is $|G \times H| = |G|\,|H|$.

$(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$.

Definition: Order of a in G

Let G be a group and $a \in G$, the order of a in G, denoted by $|a|$ or $ord(a)$, is the smallest positive integer n such that $a^n = e$.
If there is no positive integer, $|a| = \infty$.

If $|a|$ is finite, then we say a has a finite order, otherwise it has infinite order.

$ord(e) = 1$ and in the previous example, $ord(5) = ord(7) = ord(11) = 2$.

E.g. If $G = \mathbb{Z}$ and for all $n \in \mathbb{Z}, n \neq 0$, the order n is infinite.

E.g. If $G = \mathbb{Z}_n$ and $a \in G$, then $|a| = \frac{n}{\gcd(a,n)}$.

E.g. If $G = \mathbb{C}^*$, $|C^*| = \infty$. If $z \in \mathbb{C}^*$, we can write $z = re^{i\theta}$ where $r > 0, \theta \in \mathbb{R}$. What choices of r and θ make $ord(z)$ finite?

By De Mouvre's Theorem, $z^n = r^n e^{in\theta}$. If $|z| = n$, then

$$z^n = r^n e^{in\theta} = 1$$

This implies $r = 1$ and θ/π is rational. Thus, $|z|$ is finite if and only if $r = 1$ and $\theta = s\pi$ where $s \in \mathbb{Q}$.

Proposition

For $a \in G, b \in H$, then $|(a, b)| = lcm(|a|, |b|)$.

Proof. If $|a| = n, |b| = m$, then for $k \in \mathbb{N}$ we have $(a, b)^k = (a^k, b^k) = (e_G, e_H)$ if and only if $a^k = e_G, b^k = e_H$ if and only if $n|k$ and $m|k$ if and only if $lcm(m, n)|k$. Thus, the smallest positive value of k is $lcm(n, m)$.

Claim: Let G be a group and $a \in G$. $\forall m \in \mathbb{Z}, a^m = e$, then $ord(a)|m$.

Proof. (Claim) Let $n = ord(a)$. Since $a^m = e$, then $ord(a) < \infty$. By the division algorithm, there exists $q, r \in \mathbb{Z}$ where $q \leq r < n$ such that $m = qn + r$.

$$\begin{aligned} e = a^m &= a^{qn+r} \\ &= (a^n)^q \cdot a^r \\ &= e^q \cdot a^r \\ &= a^r \end{aligned}$$

By the definition of $|a|$, $r = 0$, which shows $n|m$.

Definition: Conjugate

Let G be a group. For $a, b \in G$, we say a and b are conjugate in G, written as $a \sim b$, when $b = xax^{-1}$ for some $x \in G$.

Definition: Conjugate Class Cl

$$Cl(a) = Cl_G(a) = \{b \in G : b \sim a\} = \{xax^{-1} : x \in G\}$$

Remark: The binary relation $\sim$ is an equivalence relation on G. For all $a, b, c \in G$, we have $a \sim a$, $a \sim b, b \sim a$ and $a \sim b, b \sim c \implies a \sim c$.

Remark: If $a \sim b$, then $|a| = |b|$.

E.g. Consider two groups G and H, when and how can we view them as the same ones. Take $G = \mathbb{Z}^* = \{-1, 1\}$ and $H = \mathbb{Z}_2 = \{0, 1\}$. To view two groups as the same, they must share the operation tables. If ϕ maps 1 to 0 and -1 to 1, then under ϕ, their operation table are the same.

a/b	1	-1
1	1	-1
-1	-1	1

a/b	0	1
0	0	1
1	1	0

Definition: Homomorphism

Let G and H be groups and $\phi : G \to H$, we say ϕ is a homomorphism if for any $a, b \in G$, $\phi(ab) = \phi(a)\phi(b)$.

Definition: Isomorphism

If ϕ and ϕ^{-1} are homomorphisms (ϕ is a bijection), then ϕ is an isomorphism and G and H are isomorphic, denoted by $G \cong H$.

E.g. $\mathbb{Z}^* \cong \mathbb{Z}_2$.

E.g. $U_{12} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Chapter 2

Subgroups and Cyclic Groups

Definition: Subgroup

A subgroup H of a group G is a subset which is also a group under the same binary operation, denoted $H \leq G$.

For any group G, G and $\{e\}$ are subgroups of G. $\{e\}$ is called the trivial subgroup.

Definition: Proper Subgroup

H is a proper subgroup of G if $H \leq G$ and $H \neq G$, denoted $H < G$.

E.g. $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$. $\mathbb{Z}^* < \mathbb{Q}^* < \mathbb{R}^* < \mathbb{C}^*$.

E.g. If we denote $\mathbb{Z}_n = \{0, \ldots, n-1\}$, $\mathbb{Z}_n$ is not a subgroup of $\mathbb{Z}$.

U_n is not a subgroup of $\mathbb{Z}_n$ under the binary operation $+$ (U_n has no 0, which is the identity in $\mathbb{Z}_n$).

Theorem Subgroup Test I)

Let G be a group and $H \subseteq G$, then $H \leq G$ if and only if

1. H contains the identity e.
2. H is closed under operation, i.e. $a, b \in H$ then $ab \in H$.
3. H is closed under inversion, i.e. $a \in H$ then $a^{-1} \in H$.

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