Theorems and Definitions in Group Theory

Shunan Zhao

Contents

1 Basics of a group

1.1 Basic Properties of Groups

Definition 1.1.1 (Definition of a Group)**.** A set G is a group if and only if G satisfies the following:

1. G has a binary relation $\cdot : G \times G \to G$ so that $\forall g, h \in G, g \cdot h \in G$. We write $\cdot(g, h) = g \cdot h$. (Closure.)

2. $\forall g, h, k \in G, g \cdot (h \cdot k) = (g \cdot h) \cdot k$. (Associative.)

3. $\exists e \in G,$ s.t. $e \cdot a = a = a \cdot e$. e is called an identity element of G.

4. $\forall g \in G, \exists g^{-1} \in G,$ s.t. $g \cdot g^{-1} = e = g^{-1} \cdot g$. g^{-1} is called an inverse of g.

Definition 1.1.2. If $\forall g, h \in G$, we also have $g \cdot h = h \cdot g$, then we say that G is an abelian group.

Theorem 1.1.1. Let G be a group. Then,

- $\forall a \in G, aG = G = Ga$, where $Ga = \{ga : g \in G\}$ and $aG = \{ag : g \in G\}$

- If $a, x, y \in G$, then $ax = ay \implies x = y$.

- If $a, x, y \in G$, then $xa = ya \implies x = y$.

Theorem 1.1.2. G is a group. Then:

- G has only one identity element.

- Each $g \in G$ has only one inverse g^{-1}.

1.2 Properties of Inverses

Theorem 1.2.1. G is a group.

- If $g \in G$, then $(g^{-1})^{-1} = g$.

- If $g, h \in G$, then $(gh)^{-1} = h^{-1}g^{-1}$.

Theorem 1.2.2. Let G be a set with the following axioms:

1. **Closure:** $g, h \in G \implies gh \in G$.

2. **Associativity:** $\forall g, h, k \in G, g(hk) = (gh)k$.

3. $\exists e \in G, \forall g \in G, eg = g$. ($e$ is a left identity.)

4. $\forall g \in G, \exists * g \in G, *gg = e$. ($*g$ is a left inverse.)

Then, G is a group. The same applies for a right inverse and a right identity.

1.3 Direct Product of Groups

Theorem 1.3.1. *Let G and H be two groups. Define the direct product of G and H as $G \times H = \{(g, h) : g \in G, h \in H\}$. Then, $G \times H$ is a group with the component-wise binary operation.*

Definition 1.3.1. Let $\mathbb{C} = \mathbb{R} \times \mathbb{R} = \{(a, b) : a, b \in \mathbb{R}\}$. We define addition and multiplication in $\mathbb{C}$ as:

- **Addition:** We want to use the component wise addition from $(\mathbb{R}, +)$. Thus, $(a, b) + (c, d) = (a + b, c + d)$. Then, $\mathbf{0} = (0, 0)$ and $(a, b)^{-1} = -(a, b) = (-a, -b)$.
- **Multiplication:** Define multiplication by $(a, b)(c, d) = (ac - bd, ad + bc)$. Then, the multiplicative identity is $(1, 0)$. Furthermore, define $i = (0, 1)$. Then, the multiplicative inverse is $z^{-1} = \frac{\bar{z}}{|z|^2}$.

Definition 1.3.2. Define $\mathbb{H} = \mathbb{C} \times \mathbb{C} = \{(z, w) : z, w \in \mathbb{C}\}$. We define addtion component-wise and multiplication by $(z, w)(u, v) = (zu - w\bar{v}, zv - w\bar{u})$. The multiplicative identity is $(1, 0)$ and $h^{-1} = \frac{\bar{h}}{|h|^2}$.

2 Equivalence Relations and Disjoint Partitions

Definition 2.0.3. Let X be a set and R be a relation on X. R is called an equivalence relation on X if and only if the following axioms hold:

1. For each $x \in X, x\mathrm{R}x$ (R is reflexive).
2. $\forall x, y \in X$, if $x\mathrm{R}y$, then $y\mathrm{R}x$ (R is symmetric).
3. If $x\mathrm{R}y$ and $y\mathrm{R}z$, then $x\mathrm{R}z$ (R is transitive).

Definition 2.0.4. $\forall x \in X, \mathrm{R}[x] = \{y \in X : y\mathrm{R}x\}$ is called an equivalence class.

Theorem 2.0.2. *Let R be an equivalence relation on X. Then, $\mathrm{R}[x] = \mathrm{R}[z] \iff x\mathrm{R}z$*

Theorem 2.0.3. *Let R be an equivalence relation on a set X. Let $D_R = \{\mathrm{R}[x] : x \in X\}$. Then, D_R has the following properties:*

1. $\mathrm{R}[x] \neq \emptyset$, since $x\mathrm{R}x \implies x \in \mathrm{R}[x]$.
2. If $\mathrm{R}[x] \cap \mathrm{R}[y] \neq \emptyset$, then $\mathrm{R}[x] = \mathrm{R}[y]$.
3. $X = \bigcup_{x \in X} \mathrm{R}[x]$.

Definition 2.0.5. Let X be a set. The power set of X is $\mathrm{P}(X) = \{S : S \subseteq X\}$.

Definition 2.0.6 (Disjoint Partition)**.** A subset $\mathfrak{D} \subseteq \mathrm{P}(X)$ is a disjoint partition of X if and only if $\mathfrak{D}$ satisfies the following axioms:

1. $\forall D \in \mathfrak{D}, D \neq \emptyset$.
2. If $D, \tilde{D} \in \mathfrak{D}$ and $D \cap \tilde{D} \neq \emptyset$, then $D = \tilde{D}$.

3. $X = \bigcup_{D \in \mathfrak{D}} D$.

Corollary 2.0.4. If R is an equivalence relation on a set X, then $\mathfrak{D}_R = \{\mathrm{R}[x] : x \in X\}$ is a disjoint partition of X.

Theorem 2.0.5. Let $\mathfrak{D}$ be a disjoint partition of a set X. Define a relation on X, $\mathrm{R}_{\mathfrak{D}}$ as follows:

$$x \mathrm{R}_{\mathfrak{D}} y \iff \exists D \in \mathfrak{D} \text{ so that } x, y \in D.$$

Then, $\mathrm{R}_{\mathfrak{D}}$ is an equivalence relation.

3 Elementary Number Theory

3.1 GCD and LCM

Axiom 3.1.1 (The Well Ordering Principle)**.** Every non-empty subset of $\mathbb{N}$ has a smallest element.

Theorem 3.1.1 (Division Algorithm)**.** Let $a, b \in \mathbb{Z}, b \neq 0$. Then, $\exists! q, r \in \mathbb{Z}$ s.t. $a = bq + r, 0 \leq r < |b|$.

Definition 3.1.1. Let $a, b \in \mathbb{Z}$, not both zero. Then, $c > 0, c \in \mathbb{N}$ is a greatest common divisor of a and $b \iff c$ satisfies the following properties $(a, b \in \mathbb{Z}, a \neq 0 \neq b)$:

1. $c|a$ and $c|b$.
2. If $x|a$ and $x|b$, then $x|c$.

Theorem 3.1.2. There exists a GCD of a and b, say c, and $c = \lambda a + \mu b,\ \lambda, \mu \in \mathbb{Z}$. Furthermore, c is smallest $n \in \mathbb{N}$ s.t. $n = \lambda a + \mu b$.

Definition 3.1.2. Let $a, b \in \mathbb{Z}, a > 0, b > 0$. $d \in \mathbb{Z}$ and $d > 0$ is a least common multiple of a and b if and only if d satisfies the folloing properties:

1. $a|d$ and $b|d$.
2. If $a|x$ and $b|x$, then $d|x$.

Theorem 3.1.3. Assume $a, b \in \mathbb{Z}, a > 0, b > 0$. Then, $d = \dfrac{ab}{\gcd(a, b)}$ is the LCM of a and b.

3.2 Primes and Euclid's Lemma

Definition 3.2.1. $p \in \mathbb{N}, p$ is a prime $\iff n|p \implies n = 1$ or $n = p$.

Theorem 3.2.1. Let $p \in \mathbb{N}$. p is a prime if and only if $\forall n \in \mathbb{N}, p|n$ or $\gcd(n, p) = 1$ (relatively prime).

Theorem 3.2.2. For $a, b, c \in \mathbb{N}$, if $a|bc$ and $\gcd(a, b) = 1$, then $a|c$.

Corollary 3.2.3 (Euclid's Lemma)**.** If p is a prime and $p|ab$, then $p|a$ or $p|b$.

4 Exponents and Order

4.1 Exponents

Definition 4.1.1. G is a group and $a \in G$. We define $a^0 = e$, $a^1 = a$ and $a^{n+1} = a^n \cdot a$, for $n \in \mathbb{N}^+$. Also, if $m > 0$, define $a^{-m} = (a^{-1})^m$.

Theorem 4.1.1 (Properties of Exponents)**.** G is a group and $a, b \in G$ and $m, n \in \mathbb{N}$. Then, we have

1. $e^n = e$
2. $a^{m+n} = a^m a^n$
3. $(a^m)^n = a^{mn}$
4. Let $ab = ba$. Then, $ab^n = b^n a$ and $(ab)^n = a^n b^n = b^n a^n$.
5. $a^{-m} = (a^m)^{-1}$
6. If $0 \leq m \leq n$, then $a^{n-m} = a^n a^{-m}$.
7. $(a^{-1}ba)^n = a^{-1}b^n a$

4.2 Order

Definition 4.2.1. G is a group and $a \in G$. If there is a positive integer $n > 0$ s.t. $a^n = e$, we say a has finite order. If a has finite order, then the smallest $n > 0$ s.t. $a^n = e$ is called the order of a. We write $o(a)$ as the order of a. If $\forall n \in \mathbb{N}^+, a^n \neq e$, then we say a has infinite order and we write $o(a) = \infty$. If $o(a) \neq \infty$, then a has finite order.

Theorem 4.2.1. Let G be a group and $a \in G, m > 0$. Then,

1. If $a^m = e$, then $o(a)|m$.
2. Let $o(a) = \infty$. If $a^k = e$, then $k = 0$.
3. $o(a) = \infty \iff a^m = a^n \implies m = n$.
4. If $o(a) \neq \infty$, then $o(a^k) \neq \infty$ and $o(a^k)|o(a)$.

Theorem 4.2.2. Let G be a group, $a \in G$, $o(a) \neq \infty$ and $k \in \mathbb{N}$. Then,

1. If $d = \gcd(o(a), k)$, then $o(a^k) = o(a^d)$.
2. $o(a^k) = \dfrac{o(a)}{\gcd(o(a), k)}$

5 Integers Modulo n

5.1 Integers Modulo n

Definition 5.1.1. Let $a, b \in \mathbb{Z}$. Define $a \equiv b(n)$ (a is congruent to b modulo n) if and only if $a = b + nt,\ t \in \mathbb{Z}$. Or, $n|a - b$.

Theorem 5.1.1. a is congruent to b modulo n is an equivalence relation on $\mathbb{Z}$.

Definition 5.1.2. The equivalence classes of $\equiv (n)$ are denoted as $[x]_n$, where $[x]_n = \{z \in \mathbb{Z} : z \equiv x(n)\}$. $\mathbb{Z}_n = \{[x]_n : x \in \mathbb{Z}\}$ is the set of integers modulo n.

Theorem 5.1.2. $\mathbb{Z}_n = \{[r]_n : 0 \leq r < n\} = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$, and all these elements are distinct (i.e. $|\mathbb{Z}_n| = n$).

5.2 Addition and Multiplication of $\mathbb{Z}_n$

Definition 5.2.1 (Addition on $\mathbb{Z}_n$)**.** Let $[x]_n, [y]_n \in \mathbb{Z}_n$. Define $[x]_n \oplus [y]_n = [x+y]_n$.

Lemma 5.2.1. Let $a \equiv b(n)$ and $c \equiv d(n)$. Then, $(a+c) \equiv (b+d)(n)$.

Theorem 5.2.2. $\mathbb{Z}_n$ is an additive group with group operation $[x]_n \oplus [y]_n = [x+y]_n$. The identity is $[0]_n$ and the inverse of $[x]_n$ is $[-x]_n$. $\mathbb{Z}_n$ is an abelian group, since $\mathbb{Z}$ is abelian.

Theorem 5.2.3. In general, $\mathbb{Z}_n = \langle [1]_n \rangle$, where $[1]_n^r = [r]_n$.

Definition 5.2.2 (Multiplication on $\mathbb{Z}_n$)**.** Define $[x]_n \odot [y]_n = [xy]_n$.

Lemma 5.2.4. If $a \equiv b(n)$ and $c \equiv d(n)$, then $ac \equiv bd(n)$.

Theorem 5.2.5. $\mathbb{Z}_n$ under the multiplication $[x]_n \odot [y]_n = [xy]_n$ satisfies all the properties of a multiplicative group, except for, in general, the inverse.

Theorem 5.2.6. $\mathbb{Z}_n$ under $\odot$ multiplication has the following property: $[x]_n$ has a multiplicative inverse $\iff \gcd(x, n) = 1$.

Definition 5.2.3. In $\mathbb{Z}_n$, define $U(n) = \{[r]_n : \gcd(r, n) = 1, 0 \leq r < n\}$. $U(n)$ is called the set of units (multiplicative inverses) of $\mathbb{Z}_n$ with respect to multiplication.

Theorem 5.2.7. $U(n)$ is a multiplicative group (abelian) under $\odot$.

6 Subgroups

6.1 Properties of Subgroups

Definition 6.1.1. Let G be a group. A subset $S \subseteq G$ is called a subgroup of G if and only if S is a group under the same group operations as G. We write $S \leqslant G$.

Theorem 6.1.1. Let G be a group and $S \subseteq G$. Then,

1. If $t, s \in S$, then $st \in S$ (Closure).
2. $e \in S$.
3. If $s \in S$, then $s^{-1} \in S$.

Corollary 6.1.2 (Second test for subgroups)**.** Let $S \subseteq G$, G is a group. $S \leqslant G \iff S \neq \emptyset$ and $s, t \in S \implies st^{-1} \in S,\ \forall s, t \in S$.

6.2 Subgroups of $\mathbb{Z}$

Theorem 6.2.1. Let $S \subseteq \mathbb{Z}$. $S \leqslant \mathbb{Z} \iff S = m\mathbb{Z},\ m > 0$.

Corollary 6.2.2. If m is the smallest integer greater than 0 in $S \neq \{0\},\ S \leqslant \mathbb{Z}$, then $S = m\mathbb{Z}$.

Theorem 6.2.3 (Test for finite subgroups)**.** G is a group and $S \subseteq G$, S finite. Then, $S \leqslant G \iff S \neq \emptyset$ and S satisfies property 1 of subgroups.

6.3 Special Subgroups of a Group G

Definition 6.3.1. Let G be a group. Then, we define the following:

1. The centre of G is $Z_G = Z(G) = \{z \in G : za = az,\ \forall a \in G\}$.
2. If $a \in G$, then $C(a) = \{z \in G : za = az\}$, is called the centralizer of a.
3. $S = \{e\}$ is called the trivial subgroup.
4. S is called a proper subgroup of $G \iff S \neq G$.

Theorem 6.3.1. If G is a group, then Z_G is an abelian subgroup of G.

Theorem 6.3.2. In any group G, $C(a) \leqslant G$ for each $a \in G$.

Definition 6.3.2. Let G be a group. Then, $T = \{g \in G : o(g) \neq \infty\}$ is the Torsion subset of G.

Theorem 6.3.3. Let A be an abelian group. Then, $T \leqslant A$ is called the Torsion subgroup of A.

6.4 Creating New Subgroups from Given Ones

Theorem 6.4.1. G is a group and $P, Q \leqslant G$. Then,

1. $P \cap Q \leqslant G$. In fact, if $\{P_\alpha\}_{\alpha \in I}$ is a collection of subgroups, then $\bigcap_{\alpha \in I} P_\alpha$ is also a subgroup.
2. $P \cup Q \leqslant G \iff P \leqslant Q$ or $Q \leqslant P$.
3. $PQ \leqslant G \iff PQ = QP$.

Theorem 6.4.2. G is a group, $P, Q \leqslant G$. Then every element $g \in G$ can be represented uniquely as $g = pq$, where $p \in P,\ q \in Q$ if and only if $G = PQ$ and $P \cap Q = \{e\}$.

7 Cyclic Groups and Their Subgroups

7.1 Cyclic Subgroups of a Group

Definition 7.1.1. Let G be a group and let $a \in G$. Define $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$.

Theorem 7.1.1. Let G be a group and $a \in G$. Then, we have:

1. $\langle a \rangle \leqslant G$.
2. $\langle a \rangle$ is the smallest subgroup of G containing a. (If $S \leqslant G$ and $a \in S$, then $\langle a \rangle \subseteq S$.)
3. $\langle a^{-1} \rangle = \langle a \rangle$.
4. Let $o(a) = n \neq \infty$. Then, $\langle a \rangle = \{a^k : 0 \leq k < n\}$.
5. If $o(a) = \infty$, then $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$, where $a^r = a^s \implies s = r$.

7.2 Cyclic Groups

Definition 7.2.1. Let G be a group. We say G is a cyclic group $\iff \exists a \in G$ s.t. $G = \langle a \rangle$. In this case, a is called a generator of G.

7.3 Subgroups of Cyclic Groups

Theorem 7.3.1. Let $G = \langle a \rangle$. Then, $S \leqslant \langle a \rangle = G \iff S = \langle a^k \rangle,\ k \geq 0$.

Corollary 7.3.2. If $G = \langle a \rangle$ and $S \leqslant G,\ S \neq \{e\}$, then $S = \langle a^k \rangle$, where k is the smallest integer greater than 0 s.t. $a^k \in S$.

Theorem 7.3.3. Let $G = \langle a \rangle$ and $o(a) = n \neq \infty$. Then, a^k is a generator of $\langle a \rangle$ (i.e. $\langle a^k \rangle = \langle a \rangle$) $\iff \gcd(n, k) = 1$. Hence, $S = \langle a^k \rangle$ is a proper subgroup of $G \iff \gcd(n, k) \neq 1$.

Definition 7.3.1. If G is a finite group of n elements, we say G has order n and we write $o(G) = n$. For cyclic groups $G = \langle a \rangle$, we have $o(G) = o(\langle a \rangle) = o(a)$.

Theorem 7.3.4. Let $G = \langle a \rangle$ be a cyclic group. Then,

- Let $o(a) = n = o(G)$. If $S \leqslant G$, then $o(S)|o(G)$. (A special case of Legrange's theorem.)
- Let $o(a) = \infty$. Then, $\langle a^r \rangle = \langle a^s \rangle \iff r = \pm s,\ r, s \in \mathbb{Z}$.

Theorem 7.3.5. Let $G = \langle a \rangle$ and $o(a) = n \neq \infty$. If $d|n$, then there exists exactly one subgroup S s.t. $o(S) = d$. If $d \neq n$ and $d \neq 1$, then S is a proper, non-trivial subgroup.

Definition 7.3.2 (Euler-Phi Function)**.** The function $\phi : \mathbb{Z} \to \mathbb{N}$ is defined by $\phi(n) = |U(n)|$. (The number of positive integers less than or equal to n that are coprime to n.)

Theorem 7.3.6. Let $G = \langle a \rangle$ with $o(a) = n \neq \infty$. Then, if $d|n$, then $|\{x \in G : o(x) = d\}| = \phi(d)$.

Corollary 7.3.7. Let G be a finite group with $o(G) = n$. Then, $\phi(d) \mid |\{x \in G : o(x) = d\}|$.

Theorem 7.3.8. If G is a cyclic group and $\exists g \in G$, s.t. $o(g) = \infty$, then $\forall x \in G, o(x) \neq \infty \implies x = e$.

7.4 Direct Product of Cyclic Groups

Theorem 7.4.1. Let $G_1, \ldots, G_n$ be groups and $(g_1, \ldots, g_n) \in \prod_{i=1}^{n} G_i = G_1 \times \cdots \times G_n$. If $o(g_i) = r_i \neq \infty,\ (1 \leq i \leq n)$, then $o(g_1, \ldots, g_n) = \text{lcm}(o(g_1), \ldots, o(g_n)) \neq \infty$.

Theorem 7.4.2. Let $G_1, \ldots, G_n$ be groups. Then,

- If $\prod_{i=1}^{n} G_i$ is a cyclic group with generators $(g_1, \ldots, g_n)$, then each group G_i is a also a cyclic group with generators g_i.
- $\mathbb{Z} \times \mathbb{Z}$ is a not a cyclic group even though $\mathbb{Z}$ is!

Theorem 7.4.3. Let G_i be finite groups, $1 \leq i \leq n$. $\prod_{i=1}^{n} G_i$ is cyclic with generators $(g_1, \ldots, g_n) \iff$

1. Each G_i is cyclic with generator g_i.
2. $o(g_1) \cdots o(g_n) = \text{lcm}(o(g_1), \ldots, o(g_n))$, or equivalently $\gcd(o(g_i), o(g_j)) = 1,\ i \neq j$.

8 Subgroups Generated by a Subset of a Group G

Definition 8.0.1. Let G be a group and suppose $M \subseteq G$. Then, $\bigcap_{M \subseteq S \leqslant G} S$ is the smallest subgroup containing M. We denote this subgroup by $\langle M \rangle$.

Theorem 8.0.4. Let G be a group and $M \subseteq G$. Then, $\langle M \rangle = \bigcup_{n=1}^{\infty} [M \cup M^{-1}]^n$.

Corollary 8.0.5. Let A be an abelian group and $M = \{m_1, \ldots, m_t\} \subseteq A$. Then, $\langle M \rangle = \{x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} : x_i \in M\} = \{m_1^{t_1} \cdots m_t^{t_t} : t_i = \pm 1, m_i \in M, t \geq 1\}$.

Definition 8.0.2 (Dihedral Group)**.** Let G be a group and $M = \{\sigma, \delta\}$, where $o(\sigma) = 2,\ o(\delta) = n$, and $\sigma\delta = \delta^{-1}\sigma$.

Theorem 8.0.6. $\langle\{\sigma, \delta\}\rangle = \{e, \delta^1, \ldots, \delta^{n-1}\} \cup \{\sigma, \sigma\delta, \ldots, \sigma\delta^{n-1}\} = D_n$ (Dihedral group with $2n$ elements). Note that $D_n = \langle\delta\rangle \cup \sigma\langle\delta\rangle$.

9 Symmetry Groups and Permutation Groups

9.1 Bijections

Definition 9.1.1. Let X, Y be sets and $f : X \to Y$ a function. Then,

1. If $S \subseteq X$, then $f(S) = \{f(s) : s \in S\}$.
2. If $T \subseteq Y$, then $f^{-1}(T) = \{x \in X : f(x) \in T\}$.
3. f is injective one-to-one if and only if $\forall x, y \in X, f(x) = f(y) \implies x = y$.

4. f is surjective (onto) if and only if $\forall y \in Y, \exists x \in X,$ s.t. $f(x) = y$.

5. f is a bijection if and only if f is injective and surjective.

Theorem 9.1.1. Let $f : X \to Y$ be a function.

1. f is injective $\iff$ $\exists g : Y \to X$ s.t. $g \circ f = \mathrm{id}_X$. In other words, f has a left inverse.

2. f is surjective $\iff$ $\exists h : Y \to X$ s.t. $f \circ h = \mathrm{id}_Y$. In other words, f has a right inverse.

3. f is is bijective $\iff$ $\exists k : Y \to X$ s.t. $k \circ f = \mathrm{id}_X$ and $f \circ k = \mathrm{id}_Y$. I.e. k is the inverse of f.

Theorem 9.1.2. Let X be a set with $X = \{x_1, \ldots, x_n\}$. If $f : X \to X$ is a function, then f is injective $\iff$ f is surjective.

9.2 Permutation Groups

Definition 9.2.1. Let X be a set. Define $S_X = \{f \mid f : X \to X \text{ is a bijection }\}$.

Theorem 9.2.1. For any set X, S_X is a group under composition of functions, where the identity is $1 = \mathrm{id}_X : X \to X$.

Theorem 9.2.2. If X is a set and $|X| \geq 3$, then S_X is non-abelian.

Definition 9.2.2. S_X is called the symmetry group on X. If $X = \{1, \ldots, n\}$, we write $S_X = S_n$. Here, S_n is called the permutation group on X and $|S_n| = n!$.

Definition 9.2.3. If $f \in S_n$, we denote f as:

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ a_1 & a_2 & a_3 & \cdots & a_n \end{pmatrix}$$

i.e. $f(i) = a_i$.

9.3 Cycles

Definition 9.3.1. A permutation $\varphi \in S_n$ is called a cycle if and only if $\varphi = (a_1 \ldots a_\ell)$, which means that:

$$\varphi(x) = \begin{cases} a_{i+1} & x = a_i,\ (1 \leq i \leq \ell - 1) \\ a_1 & x = a_\ell \\ x & x \neq a_i,\ \forall i \end{cases}$$

ℓ is called the length of φ.

Theorem 9.3.1 (Properties of Cycles)**.** We have the following results for cycles:

1. $(a_1 \ldots a_\ell)^{-1} = (a_\ell \ldots a_1)$. i.e. the inverse of a cycle is a cycle.

2. 2 cycles do not produce another cycle, in general.

3. 2 cycles do not necessarily commute.

Theorem 9.3.2. When do 2 cycles commute?

1. If $\varphi \in S_n$, then $\varphi(a_1 \dots a_\ell)\varphi^{-1} = (\varphi(a_1) \dots \varphi(a_\ell))$, or $\varphi(a_1 \dots a_\ell) = (\varphi(a_1) \dots \varphi(a_\ell))\varphi$.
2. If $\varphi \in S_n$ and $\varphi(a_i) = a_i,\ (1 \leq i \leq n)$, then $\varphi(a_1 \dots a_\ell) = (a_1 \dots a_\ell)\varphi$.
3. Let $\theta_1 = (a_1 \dots a_\ell)$ and $\theta_2 = (b_1 \dots b_k)$. If $\{a_i\}_1^\ell \cap \{b_i\}_1^k = \emptyset$, then $\theta_1\theta_2 = \theta_2\theta_1$.

Corollary 9.3.3. If $\theta = (a_1 \dots a_\ell)$ is a cycle, then $o(\theta) = \ell$, the length of θ.

9.4 Orbits of a Permutation

Definition 9.4.1. Let $\varphi \in S_n$. Then, the set $O_\varphi(i) = \{\varphi^m(i) : m \in \mathbb{Z}\}$ is called the orbit of i under φ. Note that $O_\varphi(i) \subseteq X = \{1, \dots, n\}$, so $O_\varphi(i)$ is finite and hence there exists a smallest integer $\ell > 0$ s.t. $\varphi^\ell(i) = i$. ℓ is called the length of the orbit.

Theorem 9.4.1. Suppose $\varphi \in S_n$ and $O_\varphi(i)$ is an orbit with length $\ell > 0$. Then, $O_\varphi(i) = \{i, \varphi(i), \dots, \varphi^{\ell-1}(i)\}$

Theorem 9.4.2. Let $\varphi \in S_n$. Then, the set of orbits of φ, $O_\varphi = \{O_\varphi(i) : 1 \leq i \leq n\}$ forms a disjoint partition of X.

Theorem 9.4.3. Let $\varphi \in S_n$ with an orbit $O_\varphi(i)$ of length ℓ. The orbit determines a cycle $\theta = (i\ \varphi(i) \dots \varphi^{\ell-1}(i))$ of length ℓ so that $\varphi(x) = \theta(x)$ if $x \in O_\varphi(i)$.

Definition 9.4.2. We define $\mathscr{C}$ = set of cyles.

Theorem 9.4.4 (Cycle Decomposition Theorem)**.** Let $\varphi \in S_n$, let $O_\varphi = \{O_\varphi(t_i) : 1 \leq i \leq p\}$ be the set of distinct orbits of φ. Let θ_i be the cycle determined by the orbit $O_\varphi(t_i),\ 1 \leq i \leq p$. Then, $\varphi = \theta_p \cdots \theta_1$, where $\theta_i\theta_j = \theta_j\theta_i,\ i \neq j$. Hence, $S_n = \langle \mathscr{C} \rangle = \bigcup_{n=1}^{\infty} \mathscr{C}^n$, since $\mathscr{C}^{-1} = \mathscr{C}$.

Theorem 9.4.5. Let $\varphi \in S_n$ with cycle decomposition $\varphi = \theta_2\theta_1$. Then $o(\varphi) = \mathrm{lcm}(o(\theta_1), o(\theta_2))$. Furthermore, if $\varphi = \theta_n \cdots \theta_1$, where $\theta_i\theta_j = \theta_j\theta_i,\ i \neq j$, then $o(\varphi) = \mathrm{lcm}(o(\theta_1), \dots, o(\theta_n))$.

9.5 Generators of S_n

Theorem 9.5.1. $S_n = \langle \mathscr{C} \rangle$

Theorem 9.5.2. G is a group and $G = \langle M \rangle$. Let $N \subseteq G$. Then, $G = \langle N \rangle \iff M \subseteq \langle N \rangle$.

Definition 9.5.1. In S_n, let T be the set of transpositions.

Theorem 9.5.3.

$$S_n = \langle T \rangle = \bigcup_{i=1}^{\infty} T^i,\ (T^{-1} = T).$$

Corollary 9.5.4.

$$(a_1 \dots a_\ell) = (a_1\ a_2)(a_2\ a_3) \cdots (a_{\ell-1}\ a_\ell)$$

Theorem 9.5.5. In S_n, let $T_1 = \{(1\ x) : 1 < x \leq n\}$. Then, $S_n = \langle T_1 \rangle$.

Corollary 9.5.6. If $(a\ b) \in S_n$, then $(a\ b) = (1\ a)(1\ b)(1\ a)$.

Definition 9.5.2 (The Alternating Group)**.** Let $\tilde{X}^n = \{x_1, \ldots, x_n : x_i \neq x_j,\ (i \neq j)\}$ Define $P : \tilde{X}^n \to \mathbb{N}$ by $P(x_1, \ldots, x_n) = \prod\limits_{1 \leq i < j \leq n} (x_i - x_j)$.

Theorem 9.5.7. We have the following results:

1. $P(\varphi)(\psi)(x_1, \ldots, x_n) = P(\varphi)(x_{\psi(1)}, \ldots, x_{\psi(n)})$.
2. If τ is a transposition, then $P(\tau) = -P$.
3. If $\varphi \in S_n$, $\varphi = \tau_n \cdots \tau_1$, where τ_i is a transposition. Then, $P(\varphi) = (-1)^n P$.

Definition 9.5.3. Let $P : \tilde{X}^n \to \mathbb{N}$ be given. Then, we define $G(P) = \{\varphi \in S_n : P(\varphi) = P\}$.

Theorem 9.5.8. We have the following results:

1. $G(P) \leqslant S_n$.
2. $G(P) = \{\varphi \in S_n : \varphi$ is the product of an even number of transpositions.$\}$

Definition 9.5.4. $G(P)$ is called the alternating group on n-letters. We write A_n for $G(P)$.

Theorem 9.5.9 (Generators for A_n)**.** $A_n = \langle \{(1\ a\ b)\} \rangle$, if $n \geq 3$.

Corollary 9.5.10. If $(a\ b\ c) \in S_n$, then $(a\ b\ c) = (a\ c)(a\ b)$.

10 Homorphisms

10.1 Homomorphisms, Epimorphisms, and Monomorphisms

Definition 10.1.1. Let G and H be groups. Then, a function $\varphi : G \to H$ is a **homomorphism** $\iff$ $\varphi(ab) = \varphi(a)\varphi(b)$. We also say φ is an **epimorphism** if and only if φ is surjective and φ is a **monomorphism** if and only if φ is injective. If φ is surjective and injective, we say φ is an isomorphism.

Definition 10.1.2. Let G be a group. An isomorphism $\varphi : G \to G$ is called an automorphism. We write $\text{Auto}(G) = \{\varphi : G \to G \mid \varphi$ is an automorphism.$\}$.

Theorem 10.1.1. Let $\varphi : G \to H$ be a homomorphism. Then, we have:

1. If φ is an isomorphism, then φ^{-1} is also a homomorphism.
2. $\text{Auto}(G)$ is a group under functional composition.
3. φ is an isomorphism $\iff$ $\exists$ a homomorphism $\psi : H \to G$ s.t. $\varphi \circ \psi = I_H$ and $\psi \circ \varphi = I_G$.

Theorem 10.1.2. Let $\varphi : G \to H$ be a homorphism. Then,

1. $\varphi(e) = e$.
2. $\varphi(a^{-1}) = (\varphi(a))^{-1}$.
3. $\varphi(a^n) = \varphi(a)^n$.
4. $\varphi(\langle a \rangle) = \langle \varphi(a) \rangle$.
5. If $S \leqslant G$, then $\varphi(S) \leqslant H$.
6. If $T \leqslant H$, then $\varphi^{-1}(T) \leqslant G$.
7. If $a \in G$ and $o(a) = n \neq \infty$, then $o(\varphi(a)) | o(a)$.

Definition 10.1.3. Let $\varphi : G \to H$ be a homomorphism. Then, the set $\ker \varphi = \{g \in G : \varphi(g) = e\}$ is called the kernel of φ.

Corollary 10.1.3. Let $\varphi : G \to H$ be a monomorphism and $o(a) = n$. Then, $o(\varphi(a)) = o(a)$.

Theorem 10.1.4. Let $\varphi : G \to H$ be a homomorphism. Then,

1. $\ker \varphi \leqslant G$.
2. φ is a monomorphism $\iff \ker \varphi = \{e\}$.

Definition 10.1.4. Let G be a group. Then, $I_{nn}(G) = \{\varphi_g : g \in G,\ \varphi_g(x) = gxg^{-1},\ \forall x \in G\}$ is called the set of inner Automorphisms.

10.2 Classification Theorems

Theorem 10.2.1. We have the following two classification results:

1. Any 2 infinite cyclic groups are isomorphic. Hence, up to isomorphism $\mathbb{Z}$ is the only cyclic group. i.e. if $o(a) = \infty$, then $\langle a \rangle \cong \mathbb{Z}$. Or, $\mathbb{Z}$ is the unique infinite cyclic group.
2. Two finite cyclic groups, $\langle a \rangle$ and $\langle b \rangle$, are isomorphic if and only if $o(a) = o(b)$, or $|\langle a \rangle| = |\langle b \rangle|$. Hence, up to isomorphism, the only finite cyclic groups are $\mathbb{Z}_n$.

Theorem 10.2.2 (Cayley's Theorem)**.** Every group G is isomorphic to a subgroup of a permutation group, namely S_G.

Theorem 10.2.3 (Product Isomorphism Theorem)**.** Let G be a group with subgroup P and Q. If we have:

1. $G = PQ$
2. $P \cap Q = \{e\}$ and $pq = qp$, $\forall p \in P, \forall q \in Q$

Then, $G \cong P \times Q$.

11 Cosets and Lagrange's Theorem

11.1 Cosets

Definition 11.1.1. Let G be a group and $S \leqslant G$. Then, for each $g \in G$, the set Sg (gS) is called a right coset (left coset) of G.

Theorem 11.1.1. Let G be a group and $S \leqslant G$. Then:

1. $Sg_1 = Sg_2 \iff g_1 g_2^{-1} \in S \iff g_2^{-1} g_1 \in S$.
2. $S = Se = eS$ is a coset and so $Sg = S \iff g \in S$.
3. $|Sg| = o(S) = |gS|$.

Theorem 11.1.2. Let G be a group and $S \leqslant G$. Then, $\{Sg : g \in G\}$ and $\{gS : g \in G\}$ are disjoint partitions of G.

11.2 Lagrange's Theorem

Theorem 11.2.1 (Lagrange's Theorem)**.** Let G be a finite group and $S \leqslant G$. Then, $o(S)|o(G)$.

Definition 11.2.1. The index of S relative to G is written as $[G : S]$. Note, $[G : S] = \frac{o(G)}{o(S)}$, which is the number of left cosets of S (and the number of right cosets of S).

Corollary 11.2.2. Let G be a finite group and $g \in G$. Then, $o(g)|o(G)$.

Corollary 11.2.3. If G is a finite group and $g \in G$, then $g^{o(G)} = e$, $\forall g \in G$.

Corollary 11.2.4 (Euler's Theorem)**.** If $\gcd(n, k) = 1$, then $k^{\phi(n)} \equiv 1(n)$. i.e. In $\mathbb{Z}_n$, $[k^{\phi(n)}]_n = [1]_n$.

Corollary 11.2.5 (Fermat's Little Theorem)**.** If p is prime, then $k^{p-1} \equiv 1(p)$, for $k \in \mathbb{Z}$ s.t. $\gcd(p, k) = 1$.

Corollary 11.2.6. Let G be a group. Then, G is a cyclic group with no proper non-trivial subgroups if and only if $o(G)$ is a prime.

Theorem 11.2.7. If $H, K \leqslant G$, where G is a finite group, then $|HK| = \dfrac{o(H)o(K)}{o(H \cap K)}$.

Corollary 11.2.8. If G is a finite group, $H, K \leqslant G$, and $H \cap K = \{e\}$, then $|HK| = o(H)o(K)$.

Theorem 11.2.9 (The converse of Lagrange's Theorem)**.** If $d|o(G)$, then there exists a subgroup S s.t. $o(S) = d$ is true if G is abelian, but is not true if G is not abelian.

Theorem 11.2.10 (The First Sylow Theorem)**.** If G is a finite group and $p^n|o(G)$, where p is a prime, then $\exists S \leqslant G$, with $o(S) = p^n$.

12 Normal Subgroups

12.1 Introduction to Normal Subgroups

Definition 12.1.1. Let G be a group and $N \leqslant G$. N is called a normal subgroup of G if and only if $Ng = gN$, $\forall g \in G$. Or, equivalently, $gNg^{-1} = N$, $\forall g \in G$. We write $N \lhd G$ for N to be a normal subgroup of G.

Theorem 12.1.1 (Tests for Normal Subgroups)**.** Let G be a group and $N \leqslant G$. Then,

1. $N \lhd G \iff gNg^{-1} \subseteq N$, $\forall g \in G$.
2. If $[G : N] = 2$, then $N \lhd G$.

Theorem 12.1.2. Let G be a group. Then,

1. $Z(G) = Z_G \lhd G$.
2. If $\varphi : G \to H$ is a homomorphism, then $\ker \varphi \lhd G$.

Theorem 12.1.3 (Operations on Normal Subgroups)**.** Let $M, N \leqslant G$, where G is a group. Then,

1. If $N \lhd G$, then $M \cap N \lhd M$.
2. If $N \lhd G$, then $MN \leqslant G$ and $N \lhd MN$.
3. If both M and N are normal, then $M \cap N$ and MN are normal subgroups of G.

12.2 Quotient Groups

Theorem 12.2.1. Let $N \lhd G$, G is a group. Let $G/N = \{Ng : g \in G\}$. Define a binary relation on G/N by $(Ng_1)(Ng_2) = Ng_1g_2$. Then, G/N is a group.

Definition 12.2.1. If $N \lhd G$, where G is a group, then the set of cosets, G/N, we say G modulo N, is a group with identity Ne and inverses $Ng^{-1} = (Ng)^{-1}$. G/N is called the quotient group of G and N. If G is finite, then $o(G/N) = [G : N] = {}^{o(G)}/_{o(N)}$. In general, G/N inherits properties from G.

Theorem 12.2.2. Let G be a group and $N \lhd G$. Then,

1. If G is abelian, then so is G/N.
2. If G is cyclic, then so is G/N.

Theorem 12.2.3. Let A be an abelian group and let $T = \{a \in A : o(a) \neq \infty\}$ be the Torsion subgroup. Then, A/T is Torsion-free, i.e. all elements of A/T have infinite order.

Theorem 12.2.4 (The $G/Z(G)$ Theorem)**.** Let G be a group and we know that $Z(G) \lhd G$. If $G/Z(G)$ is cyclic, then G is abelian.

Corollary 12.2.5. Let G be a group, $N \lhd G$ and $N \subseteq Z(G)$. If G/N is cyclic, then G is abelian.

13 Product Isomorphism Theorem and Isomorphism Theorems

13.1 Product Isomorphism Theorem

Theorem 13.1.1. Let G be a group and $M, N \leqslant G$. Then, G satisfies:

1. $G = MN$.
2. $M \cap N = \{e\}$.
3. $mn = nm,\ \forall m \in M, \forall n \in N$.

If and only if G also satisfies:

1. $G = MN$.
2. $M \cap N = \{e\}$.
3. M and N are normal subgroups.

Definition 13.1.1. Let M and N be subgroups of a group G. We say G is the internal direct product of M and N if and only if:

1. $G = MN$.
2. $M \cap N = \{e\}$.
3. $mn = nm,\ \forall m \in M, \forall n \in N$.

In general, we say G is the internal direct product of subgroups $N_1, \dots, N_t \iff$

1. $G = N_1 \cdots N_t$.
2. $(N_1 \cdots N_i) \cap N_{i+1} = \{e\},\ (1 \leq i \leq t-1)$.
3. $N_i \lhd G,\ \forall i = 1, \dots, t$.

Definition 13.1.2. Let N_i $(1 \leq i \leq n)$ be n subgroups of G. $\prod_{i=1}^{n} N_i = N_1 \times \cdots \times N_n$ is the external direct product of the N_i's. If G is the internal direct product of the N_i's, then we write $G = \bigoplus_{i=1}^{n} N_i$.

Theorem 13.1.2 (Product Isomorphism Theorem)**.** If $G = \bigoplus_{i=1}^{n} N_i$, then $G \cong \prod_{i=1}^{n} N_i$.

Theorem 13.1.3. Let G be a group and $o(G) = p^2$, where p is a prime. Then, $G \cong \mathbb{Z}_{p^2}$ or $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$ and hence G is abelian.

13.2 Isomorphism Theorems

Theorem 13.2.1. Suppose G is a group and $N \lhd G$. The map $\varphi_N : G \to G/N$ defined by $\varphi_N(g) = Ng$ is an epimorphism whose kernel is N.

Corollary 13.2.2. Let G be a group. Then, $N \lhd G \iff N$ is the kernel of some homomorphism $\varphi : G \to H$.

Theorem 13.2.3 (Fundamental Homomorphism Theorem)**.** If $\varphi : G \to H$ is a homomorphism, then $G/\ker\varphi \cong \varphi(G)$.
If φ is an epimorphism, then $G/\ker\varphi \cong H$.

Theorem 13.2.4 (Second Isomorphism Theorem)**.** G is a group, $M \leqslant G$ and $N \lhd G$. Then,

1. $M \cap N \lhd M$.
2. $MN \leqslant G$ and $N \lhd MN$.
3. $MN/N \cong M/M \cap N$.

Theorem 13.2.5 (Third Isomorphism Theorem)**.** Let G be a group and M and N are both normal subgroups of G with $N \leqslant M$. Then,

1. $M/N \lhd G/N$.
2. $G/M \cong (G/N)/(M/N)$.

Theorem 13.2.6 (Basis Theorem)**.** Let A be an abelian group, with $A = \langle M \rangle$, and M is finite, i.e. A is a finitely generated abelian group. Then, $A \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r} \times \mathbb{Z}^S$, where $m_1 | m_2 | \cdots | m_{r-1} | m_r$ $(m_i | m_{i+1},\ 1 \le i \le r-1)$. Here, $T = \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r}$ is called the Torsion subgroup and the m_i are called the Torsion coefficients. The S is called the rank of A, or the Betti number. If $S = 0$, we have a finite abelian group. If $r = 0$, we have $A \cong \mathbb{Z}^S$ and we have a free abelian group of rank S.

Theorem 13.2.7 (The Fundamental Theorem of Finitely Generated Abelian Groups)**.** Let A be a finitely generated abelian group. If $A \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r} \times \mathbb{Z}^S \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_t} \times \mathbb{Z}^W$, then $r = t$, $m_i = n_i$ $(1 \le i \le r)$, and $S = W$. If A is a finite abelian group, A has type $(m_1, m_2, \ldots, m_r)$ if and only if $A \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_r}$, with $m_i | m_{i+1}$ $(1 \le i \le r-1)$.