Abstract Algebra

Jatinder Singh

September, 2022

Contents

Chapter 1

Groups

Definition 1.1. *A binary operation* $\bullet$ *on a set* S *is a function* $\bullet : S \times S \to S$. *Notation:* $a \bullet b := (a, b) \in S \times S$.

Definition 1.2. *Let* S *be a set and* $\bullet : S \times S \to S$ *be a binary operation on* S. *An element* $e \in S$ *is an* ***identity element*** *of the set* S *if* $s \bullet e = s$ *and* $e \bullet s = s$, $\forall s \in S$.

Theorem 1.3. *Let* S *be a set and* $\bullet : S \times S \to S$ *be a binary operation on* S. *Then, there is at most one identity element, implying that if there is an identity element of the set* S *then it is unique.*

Definition 1.4. *A pair* $(G, \bullet)$ *consisting of a set* G *and a binary operation* $\bullet : G \times G \to G$ *is a group if the* Three Group Axioms *hold:*

1. *(Associativity): The binary operation* $\bullet$ *is associative. So*

$$a \bullet (b \bullet c) = (a \bullet b) \bullet c, \ \forall a, b, c \in G$$

2. *(Identity)* G *has an identity element. Since identity element is unique, it is usually denoted by* e. *So*

3. *(Inverse) Every element of* G *has an inverse. So*

$$\forall a \in G, \exists b \in G \ni a \bullet b = b \bullet a = e$$

Chapter 2

The Symmetric Group

Definition 2.1. *A bijection whose domain and co-domain are equal is called a* ***permutation****. The set of permutations on* A, (S_A) *is the set of all bijections from a finite set A to itself. So* $S_A = \{\sigma : \sigma \text{ is a bijection from } A \text{ to } A\}$.

Theorem 2.2. *Given any set* A, S_A *is a group under function composition.*

Definition 2.3. *If* $A = \{1, 2, 3, \cdots, n\}$ *then* S_A *is called the symmetric group on* n *numbers and is written as* S_n

Theorem 2.4. *Disjoint cycles commute.*

Theorem 2.5. *Let* $\sigma \in S_n$*. If* $\sigma \neq I$*, then* σ *can be written uniquely (upto the order of the cycles) as a single cycle or a finite product of disjoint cycles.*

Definition 2.6. *A 2-cycle is called a transposition.*

Theorem 2.7. *Every transposition is its own inverse.*

Theorem 2.8. *Any cycle in* S_n *can be written as the product of transpositions.*

Theorem 2.9. *Every permutation in* S_n *can be written as the product of transpositions.*

Lemma 2.10. *Let* $I = \sigma_1\sigma_2\cdots\sigma_k$ *where* $\sigma_1, \sigma_2, \ldots, \sigma_k$ *are transpositions, then* k *is even.*

Theorem 2.11. *Let* $\sigma \in S_n$.

Definition 2.12. *We say a permutation is even if it can be written as a product of an even number of transpositions. Likewise, a permutation is odd if it can be written as a product of an odd number of transpositions.*

Definition 2.13. *The set of even permutations in S_n is denoted A_n (alternating group of degree n).*

Theorem 2.14. *A_n is a subgroup of S_n.*

Theorem 2.15. *For $n \geq 2$, $|A_n| = \dfrac{n!}{2}$.*

Chapter 3

Subgroups

3.1 Criteria for Subgroups

Definition 3.1. *A subset H of a group G is a* ***subgroup*** *of G if H is a group using the same operation as in G.*

Theorem 3.2. *If H is a subgroup of a group G then*

1. *the identity element of H is the same as that of G;*
2. *for any $a \in H$, inverse of a in H is the same as the inverse of a in G.*

Theorem 3.3 (Subgroup Three Step Test)**.** *A subset H of a group G is a subgroup of G if and only if*

(i) *H is closed under the operation from G;*

(ii) *H contains the identity element e from G; and*

(iii) $\forall a \in H, a^{-1} \in H$.

Theorem 3.4 (Subgroup Two Step Test)**.** *A nonempty subset H of a group G is a subgroup of G if and only if*

(i) *H is closed under the operation from G;*

(ii) $\forall a \in H, a^{-1} \in H$.

Theorem 3.5 (Subgroup One Step Test)**.** *A nonempty subset H of a group G is a subgroup of G if and only if $\forall a, b \in H, ab^{-1} \in H$.*

Theorem 3.6. *The intersection of two subgroups of a group is a subgroup.*

Theorem 3.7. *For every integer $n \geq 0$, $n\mathbb{Z}$, is a subgroup of $\mathbb{Z}$. Moreover every subgroup of $\mathbb{Z}$ is of the form $m\mathbb{Z}$ for some integer $m \geq 0$.*

Chapter 4

Integer Powers of Elements in a Group

4.1 Power of Elements in a Group

Definition 4.1. *Let G be a group with identity e, and let $a \in G$. Then for each integer m, we define a^m as follows:*

- $a^0 = e$;
- $a^m = a^{m-1}a, \forall m \geq 1$;
- $a^{-m} = (a^{-1})^m, \forall m \geq 1$.

Lemma 4.2. *Let G be a group and let $a, b \in G$ such that $ab = ba$. Then $b^n a = ab^n, \forall n \in \mathbb{N}$.*

Theorem 4.3. *Let G be a group with identity e, and let $a, b \in G$ such that $ab = ba$. Then $(ab)^m = a^m b^m$ for every integer m.*

Theorem 4.4 (Laws of Exponents)**.** *Let G be a group. For every $a \in G$ and every $m, n \in \mathbb{Z}$;*

(a) $a^{-m} = (a^{-1})^m = (a^m)^{-1}$;

(b) $a^m a^n = a^{m+n}$;

(c) $(a^m)^n = a^{mn}$.

4.2 Order of an Element

Definition 4.5 (Order of an Element)**.** *Let G be a group and $a \in G$. If there exists a positive integer n such that $a^n = e$, then a is said to be of finite order. If no such integer exists, then a is said to be of infinite order. If a is of finite order, then the least positive integer n such that $a^n = e$ is called the **order** of a.*
Notation: *The order of an element a is denoted by $O(a)$ or $|a|$*

Theorem 4.6. *Let G be a group and $a, b \in G$. Then*

(a) $O(a) = 1 \iff a = e$;

(b) $O(a) = O(a^{-1})$;

(c) *a and gag^{-1} have the same order for all $g \in G$;*

(d) $O(ab) = O(ba)$;

(e) *Suppose a is of infinite order. Then $a^n = e \implies n = 0$;*

(f) *Suppose a is of infinite order. Then $a^i = a^j \iff i = j, \forall i, j \in \mathbb{Z}$;*

(g) *Suppose a and b have finite order and $ab = ba$. Then $O(ab) \mid O(a) \cdot O(b)$*

Theorem 4.7. *If G is a group and $a \in G$ is an element of order n, then*

(a) $a^t = e \iff n \mid t$;

(b) $a^i = a^j \iff n \mid i - j \iff i \equiv j \pmod{n}$.

Theorem 4.8. *In a finite group G each element is of finite order. In fact, the order of an element is at most $|G|$.*

Chapter 5

Cyclic Group

Definition 5.1. *Let G be a group and let $a \in G$. The* ***cyclic subgroup generated by*** *a, denoted $\langle a \rangle$ is defined by*

$$\langle a \rangle = \{a^n : n \in Z\}$$

if the group operation is written in multiplicative notation or

$$\langle a \rangle = \{na : n \in Z\}$$

if the group operation is written in additive notation.

Definition 5.2. *A group G is a* ***cyclic group*** *if $G = \langle a \rangle$ for some $a \in G$.*

Theorem 5.3. *Let G be a group and $a \in G$. Then the following statements are equivalent;*

(a) $O(a) = n$;

(b) $|< a >| = n$.

Theorem 5.4. *Let G be a group and $a \in G$ and $O(a) = n$. Let $k \in \mathbb{Z}$. Then*

(a) $< a^k > = < a^{\gcd(k,n)} >$

(b) *sd*

Definition 5.5. *If a group contains some element a such that $G = < a >$ then G is called a* ***cyclic*** *group and a is called a* ***generator*** *of G.*

Theorem 5.6. *Let G be a finite group of order n and let $a \in G$. Then $O(a) = n \iff G = < a >$.*

Theorem 5.7. *Every cyclic group is abelian.*

Theorem 5.8. *Every subgroup of a cyclic group is cyclic.*

Theorem 5.9. *Let G be a finite cyclic group of order n. For each positive integer divisor m of n there is exactly one subgroup of G of order m and these are the only subgroups of G.*

Theorem 5.10. *Let G be a cyclic group of order n and suppose $G = < a >$. Then the set of generators of $G = \{a^k : 1 \leq k < n$ and $\gcd(k, n) = 1\}$.*

Corollary 5.10.1. *The generators of $\mathbb{Z}_n$ are the integers r such that $1 \leq r < n$ and $\gcd(r, n) = 1$.*

Theorem 5.11. *The subgroups of $\mathbb{Z}$ are exactly $n\mathbb{Z}$ for $n = 0, 1, 2, 3, \cdots$.*

Chapter 6

Cosets and Lagrange's Theorem

Definition 6.1. *Let H be a subgroup of a group G and let $g \in G$. The left coset of H in G determined by g is defined as the following set:*

$$gH = \{gh : h \in H\}$$

The right coset is defined similarly by

$$Hg = \{hg : h \in H\}$$

Remark. *Since $eH = He = H$, the subgroup H is both a left and right coset.*

Theorem 6.2. *If G is an abelian group and H is a subgroup of G then any left coset gH is equal to the right coset Hg.*

Theorem 6.3. *Let H be a subgroup of a group G and suppose $g_1, g_2 \in G$. The the following statements are equivalent;*

(a) $g_1 H = g_2 H$;

(b) $g_2 \in g_1 H$;

(c) $g_1^{-1} g_2 \in H$;

(d) $g_2 H \subseteq g_1 H$;

(e) $H g_1^{-1} = H g_2^{-1}$.

Theorem 6.4. *Distinct left cosets of H in G are pairwise disjoint.*

Theorem 6.5. *Let H be a subgroup of a group G. Then*

(a) *If $g \in H$ then $gH = H$;*

(b) *If $g \notin H$ then $gH \cap H = \varnothing$.*

Theorem 6.6. *Let H be a subgroup of a group G. Then the left cosets of H in G, partition G.*

Theorem 6.7. *Let H be a subgroup of a group G. The number of left cosets of H in G is the same as the number of right cosets of H in G.*

Theorem 6.8. *Let H be a subgroup of a group G and let $g \in G$. Then $|H| = |gH|$.*

Definition 6.9. *Let G be a group and H be a subgroup of G. The index of H in G is the number of left cosets of H in G, denoted by $[G : H]$.*

Theorem 6.10 (Lagrange's Theorem)**.** *Let G be a finite group and let H be a subgroup of G. Then $|G|/|H| = [G : H]$. In particular the number of elements in H must divide the number of elements in G.*

Corollary 6.10.1. *Let G be a finite group of order n. Then the order of every element of G is divisor of n.*

Theorem 6.11. *Every group of prime order p is cyclic.*

Theorem 6.12. *Let G be a group of order $n > 1$. Then G, contains a subgroup of prime order p.*

Chapter 7

Normal Subgroups and Quotient Groups

Definition 7.1. *A subgroup H of a group G is normal in G if $gH = Hg$ for all $g \in G$.*

Theorem 7.2. *For any group G, $\{e\}$ is a normal subgroup of G.*

Theorem 7.3. *Let H be a subgroup of G. Then H is normal if and only if $\{$left cosets$\} = \{$right cosets$\}$.*

Theorem 7.4. *Let G be a finite group and let H be a subgroup of G with index 2. Then H is a normal subgroup of G.*

Theorem 7.5. *Any subgroup of an abelian group is normal.*

Theorem 7.6. *Let G be a group and H be a subgroup of G. Then the following statements are equivalent;*

(a) *The subgroup H is normal in G;*

(b) $\forall g \in G, gHg^{-1} \subseteq H$;

(c) $\forall g \in G, gHg^{-1} = H$.

Theorem 7.7. *H is a normal subgroup of $G \iff \forall g \in G, \forall h \in H, ghg^{-1} \in H$.*

Theorem 7.8. *Intersection of two normal subgroups is normal.*

Theorem 7.9. *Let H be a subgroup of a group G and let $g \in G$. Then*

(a) gHg^{-1} *is a subgroup of* G*.*

(b) $|H| = |gHg^{-1}|$

(c) *If* G *has exactly one subgroup* H *of order* k *then* H *is normal in* G*.*

Theorem 7.10. *Let* G *be a group and let* H *be a noraml subgroup of* G*. Let* $g \in G$ *and* $h \in H$*. Then* $\exists h' \in H \ni hg = gh'$ $($*or* $gh = h'g)$*.*

Theorem 7.11. *Let* G *be a group and let* H *be a noraml subgroup of* G*. Let* $x_1 \in g_1H$ *and* $x_2 \in g_2H$*. Then* $x_1x_2 \in g_1g_2H$

Definition 7.12. *Let* A *adn* B *be two sets of a group* G*. Then the composition* $A \circ B$ *is defined as the set*

$$A \circ B = \{ab : a \in A, b \in B\}$$

Theorem 7.13. *Suppose* H *is a subgroup of a group* G*. The following are equivalent;*

(a) $\forall x, y \in G, \exists g \in G \ni xH \circ yH = gH$*;*

(b) $\forall x, y \in G, xH \circ yH = xyH$*;*

(c) H *is a normal subgroup of* G*.*

Theorem 7.14. *Let* H *be a normal subgroup of* G*. The cosets of* H *in* G *form a group under the operation of set composition.*

Chapter 8

Cosets and Quotient Groups

Definition 8.1. *Let G be a group and H a subgroup of G. The* ***left coset*** *of H with representative $g \in G$ is defined as the following set:*

$$gH = \{gh : h \in G\}$$

Right cosets are defined similarly by

$$Hg = \{hg : h \in H\}.$$

Remark. *Since $eH = H = He$, the subgroup H is both a left and right coset.*

Theorem 8.2. *Let H be a subgroup of a group G and suppose that $g_1, g_2 \in G$. The following conditions are equivalent;*

(a) $g_1 H = g_2 H$;

(b) $g_2 \in g_1 H$;

(c) $g_1^{-1} g_2 \in H$;

(d) $g_2 H \subseteq g_1 H$;

(e) $H g_1^{-1} = H g_2^{-1}$;

Theorem 8.3. *Let H be a subgroup of a group G. Then the left cosets of H in G, partition G. That is, the group G is the disjoint union of the left cosets of H in G.*

Definition 8.4. *Let G be a group and H be a subgroup of G. The* ***index*** *of H in G is the number of left cosets of H in G, and is denoted by $[G : H]$.*

Theorem 8.5. *Let H be a subgroup of a group G. The number of left cosets of H in G is the same as the number of right cosets of H in G.*

Lemma 8.6. *Let H be a subgroup of a group G with $g \in G$. Then $|H| = |gH|$.*

Theorem 8.7 (Lagrange's theorem)**.** *Let G be a finite group and let H be a subgroup of G. Then $|G|/|H| = [G : H]$ is the number of distinct left cosets of H in G. In particular, the number of elements in H must divide the number of elements in G.*

Theorem 8.8. *Let G be a finite group of order n. Then the order of every element of G is a divisor of n.*

Theorem 8.9. *Every group of prime order p is cyclic.*

Theorem 8.10. *Let G be a group of order $n > 1$. Then G contains a subgroup of prime order p.*

8.1 Normal Subgroups

Definition 8.11. *A subgroup H of a group G is **normal** in G if $gH = Hg$ for all $g \in G$. That is, a normal subgroup of a group G is one in which the right and left cosets are precisely the same.*

Theorem 8.12. *Let G be a group, and let H be a subgroup of G with index 2. Then H is a normal subgroup of G.*

Theorem 8.13. *Let H be a subgroup of G. Then H is normal if and only if $\{$left cosets$\}$ = $\{$right cosets$\}$.*

Theorem 8.14. *Let G be a group and H be a subgroup of G. Then the following statements are equivalent;*

(a) *The subgroup H is normal in G;*

(b) $\forall g \in G, gHg^{-1} \subseteq H$;

(c) $\forall g \in G, gHg^{-1} = H$.

Theorem 8.15. *Let G be a group and H be a subgroup of G. Then the subgroup H is normal in G iff $\forall g \in G, \forall h \in H, ghg^{-1} \in H$.*

Theorem 8.16. *Every subgroup of an abelian group is normal.*

8.2 Quotient Group

Chapter 9

Isomorphism

Chapter 10

Homomorphism

Definition 10.1. *A **homomorphism** between groups* $(G, \circ)$ *and* $(G', \bullet)$ *is a function* $f : G \to G'$ *such that*

$$f(g_1 \circ g_2) = f(g_1) \bullet f(g_2)$$

for all $g_1, g_2 \in G$.

Theorem 10.2. *Let* $f : G \to G'$ *be a homomorphism of groups and let* e *and* e' *be identity elements of* G *and* G' *respectively and let* H *be a subgroup of* G. *Then*

(a) $f(e) = e'$;

(b) $f(g^{-1}) = (f(g))^{-1}, \forall g \in G$;

(c) $f(H)$ *is a subgroup of* G';

(d) *If* H *is cyclic, then* $f(H)$ *is cyclic;*

(e) *If* H *is abelian, then* $f(H)$ *is abelian;*

(f) *If* T *is a subgroup of* G' *then* $f^{-1}(T) = \{g \in G : f(g) \in T\}$ *is a subgroup of* G. *Furthermore, if* T *is normal in* G' *then* $f^{-1}(T)$ *is normal in* G;

Definition 10.3. *Let* $f : G \to G'$ *be a homomorphism of groups and let* e' *is the identity element of* G'. *The set* $f^{-1}(\{e\})$ *is called the **kernal** of* f, *and is denoted by* $ker(f)$.

Theorem 10.4. *Let* $f : G \to G'$ *be a homomorphism of groups. Then* $ker(f)$ *is a normal subgroup of* G.