Lecture Notes on Group Theory

(ICS440 and SEC540)

Dr. Sultan Almuhammadi

November 2020

Introduction

Group theory is the mathematical study of groups. After we have studied modular arithmetic and basic concepts in number theory, it is time we proceed more abstractly to the concepts of groups and other abstract structures, like finite fields. Groups and finite fields have important applications in modern cryptography. Most of the cryptographic algorithms today are based on some concepts in group theory and finite fields.

The format of this lecture note is as follows: all concepts and issues (like definitions, theorems, notations, and other notes) are sequentially numbered in brackets [like these] so that the student may need to study and understand them in sequence. Some exercises are given at the end of each section to ensure understanding of the material.

§ 1. Groups and Subgroups

[1] Definition. Let * be a binary operator. Then the operator * is said to be ***on a set*** A if * is a function from $A \times A$ to A itself. i.e.

$$* : A \times A \to A$$

Here, A is said to be ***closed*** under the * operation.

[2] Definition. A ***group*** $(G, \cdot)$ is a nonempty set G together with a binary operation $\cdot$ on G such that the following conditions hold:

(i) *Closure:* For all $a, b \in G$ the element $a \cdot b$ is a uniquely defined element of G

(ii) *Associativity:* For all $a, b, c \in G,$ we have

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

(iii) *Identity:* There exists an *identity element* $e \in G$ such that for all $a \in G$

$$e \cdot a = a \qquad \text{and} \qquad a \cdot e = a$$

(iv) *Inverses:* For each $a \in G$ there exists an *inverse* element $a^{-1} \in G$ such that

$$a \cdot a^{-1} = e \qquad \text{and} \qquad a^{-1} \cdot a = e$$

[3] Examples.

$(\mathbf{Z}^*_5, \cdot)$ is a multiplicative group modulo 5, with $\mathbf{Z}^*_5 = \{1, 2, 3, 4\}$. We have: $e = 1$ and $1^{-1} = 1$, $2^{-1} = 3$, $3^{-1} = 2$, and $4^{-1} = 4$.

$(\mathbf{Z}_{10}, +)$ is an additive group, where $\mathbf{Z}_{10} = \{0, 1, 2, 3, .., 9\}$ and addition is taken modulo 10. Here, we have: $e = 0$ and for all $x \in \mathbf{Z}_{10}$, $x^{-1} = -x \pmod{10}$

[4] Notations.

1. Juxtaposition: we usually write "*ab*" for the product $(a \cdot b)$
2. Power (Superscript): $a^n = a \cdot a \cdot \ldots \cdot a$ (n times), and $a^0 = e$
3. Negative power: a^{-n} denotes $(a^{-1})^n$
4. Avoid juxtaposition and superscript if the operation of the group is denoted additively, and use $n(a)$ instead of a^n. For example, in $(\mathbf{Z}_{10}, +)$, it may look very confusing if we write 5^3 to denote $(5 + 5 + 5)$; therefore, we shall write 3(5) or $3 \cdot 5$ instead.

[5] Proposition. (Cancellation Property for Groups) Let G be a group, and let $a, b, c \in G$,

(a) If $ab = ac$, then $b = c$
(b) If $ac = bc$, then $a = b$

[6] Definition. A group G is said to be ***abelian*** (or ***commutative***) if $\forall a, b \in G, a \cdot b = b \cdot a$.

[7] Example. The groups $(\mathbf{Z}_{10}, +)$ and $(\mathbf{Z}^*_5, \cdot)$ are abelian.

[8] Definition. A group G is said to be a ***finite*** group if the set G has a finite number of elements. In this case, the number of elements is called the ***order*** of G, denoted by $|G|$.

[9] Definition. Let a be an element of the group G. If there exists a positive integer n such that $a^n = e$, then a is said to have a ***finite order***, and the smallest such positive integer is called the ***order*** of a, denoted by ord(a). If there is no such positive integer n such that $a^n = e$, then a is said to have an ***infinite order***.

[10] Examples.

In $(\mathbf{Z}^*_5, \cdot)$, ord(3) = 4 since $3^4 = 1$, and ord(4) = 2 since $4^2 = 1$.
In $(\mathbf{Z}_{10}, +)$, ord(5) = 2 since 5+5 = 0, and ord(4) = 5, since 4+4+4+4+4 = 0.

[11] Definition. Let G be a group, and let H be a subset of G. Then H is called a ***subgroup*** of G if H is itself a group, under the operation induced by G.

[12] Example. $\{0, 2, 4, 6, 8\}$ is a subgroup of $(\mathbf{Z}_{10}, +)$.

[13] Proposition. Let G be a group with identity element e, and let H be a subset of G. Then H is a subgroup of G if and only if the following conditions hold:

(i) $ab \in H \;\; \forall a, b \in H$
(ii) $e \in H$
(iii) $a^{-1} \in H \;\; \forall a \in H$

[14] Theorem. (Lagrange theorem) If H is a subgroup of the finite group G, then the order of H divides the order of G.

[15] Proposition. Let G be a finite group of order n. For all $a \in G$,

(a) $\text{ord}(a) \mid n$
(b) $a^n = e$

[16] Definition. (the Euler's Phi function) The ***totient*** of a positive integer n, denoted by $\phi(n)$, is the number of nonnegative integers less than n which are relatively prime to n.

i.e. $\phi(n) = | \mathbf{Z}^*_n |$, where $\mathbf{Z}^*_n = \{x \mid 0 \le x < n \text{ and } \gcd(x, n) = 1\}$

[17] Algorithm. The ϕ-function can be computed recursively by the following theorems:

1. $\phi(1) = 1$
2. if n is prime or a power of a prime, $n = p^e$, then $\phi(n) = (p - 1)\, p^{(e-1)}$
3. if $\gcd(m, n) = 1$, then $\phi(mn) = \phi(m) \cdot \phi(n)$

[18] Examples.

$\phi(17) = 16$

$\phi(25) = (5 - 1) \cdot 5 = 20$

$\phi(16) = (2 - 1) \,.\, 2^3 = 8$

$\phi(105) = \phi(\,3 \,.\, (5 \,.\, 7)\,) = 2 \,.\, (4 \,.\, 6) = 48$

$\phi(200) = \phi(2^3 \cdot 5^2) = ((2-1) \cdot 2^2)\,((5-1) \cdot 5) = 4 \cdot 20 = 80$

[19] Theorem. (Euler's theorem) In the multiplicative group $\mathbf{Z}^*_m$, the order of the group is $\phi(m)$. Therefore, for all $a \in \mathbf{Z}^*_m$, we have $a^{\phi(m)} = 1$ (by Proposition [15-b]). Hence,

$$\text{if } \; k \equiv j \pmod{\phi(m)} \; \text{ then } \; a^k \equiv a^j \pmod{m}$$

[20] Example. In $(\mathbf{Z}^*_5, \cdot)$, we have $2^{46} = 2^2$, since $46 \equiv 2 \pmod{\phi(5)}$. Is $2^{73} = 2^3 \pmod 5$?

[21] Examples. Compute the following:

(a) $14^{52} \pmod{11}$
$14^{52} \equiv 3^{52} \pmod{11}$. Since $\phi(11) = 10$, we have $52 \equiv 2 \pmod{10}$.
So, $3^{52} \equiv 3^2 \equiv 9 \pmod{11}$

(b) $463^{91} \pmod{15}$
$463^{91} \equiv 13^{91} \equiv (-2)^{91} \pmod{15}$. Since $\phi(15) = 2 \cdot 4 = 8$, we have
$91 \equiv 3 \pmod 8$. So, $(-2)^{91} \equiv (-2)^3 \equiv -8 \equiv 7 \pmod{15}$

Exercises:

1. Let G = {0, 2, 4, 6, 8}. Show that (G, #) is a group, where # is a binary operator defined as $x \# y = (x + y) \bmod 10$. Determine the identity and the inverse of each element.

2. Consider the group G in Exercise 1. Prove or disprove that G has a subgroup of order 2.

3. Let A = {1, 5, 7, 11}. Show that (A, *) is a group, where * is a binary operator defined as $x * y = (x \cdot y) \bmod 24$. Determine the identity and the inverse of each element.

4. Consider the group A in Exercise 3,
    a. Prove or disprove that A has a subgroup of order 2.
    b. Prove or disprove that A has a subgroup of order 3.

5. Let $G = \{a, b, c, d, e, f\}$.
    a. Define a binary operator * on G such that (G, *) is an abelian group.
    b. Determine the identity element and the inverse of every element in G.
    c. Find the order of every element in G.
    d. If possible, find two subgroups of G of orders 2 and 3.

6. Compute the following:
    a. $\phi(17)$
    b. $\phi(72)$
    c. $\phi(81)$
    d. $\phi(1200)$

7. Apply Euler's theorem to compute the following:
    a. $(14^{53} + 28^{61}) \bmod 11$
    b. $((33^{71} + 285^{43})(143^{20} + 150^{61})) \bmod 7$
    c. $(15^{1234500} \cdot 14^{1234520}) \bmod 19$ (Hint: $(-4)(-5) \equiv 1 \pmod{19}$)

§ 2. Cyclic Groups

[1] Notation. Let G be a group, and let $a \in G$. The set of all elements generated by a is denoted by:

$$<a> = \{ x \in G \mid x = a^n \text{ for some } n\}$$

[2] Definition. Let G be a group, and let $\alpha \in G$. Then α is a ***generator*** of G if $<\alpha> = G$.

[3] Definition. The group G is ***cyclic*** if G has a generator, i.e. $\exists\ \alpha \in G, <\alpha> = G$.

[4] Proposition. Any group of a prime order is cyclic.

[5] Lemma. Let $(G, *)$ be a group, and let $a, b \in G$ be elements such that $a*b = b*a$. If the orders of a and b are relatively prime, then $\text{ord}(a*b) = \text{ord}(a) \cdot \text{ord}(b)$.

[6] Proposition. Let a be an element of the group G.

- **(a)** If a has infinite order, and $a^k = a^m$ for integers $k, m,$ then $k = m$.
- **(b)** If a has finite order and k is any integer, then $a^k = e$ if and only if $\text{ord}(a) \mid k$.
- **(c)** If a has finite order, then for all integers k and m, we have

$$a^k = a^m \text{ if and only if } k \equiv m \pmod{\text{ord}(a)}.$$

[7] Proposition. Let G be a group, and let $a \in G$. Then,

- **(a)** The set $<a>$ is a cyclic subgroup of G.
- **(b)** $\mid <a> \mid = \text{ord}(a)$ in G.
- **(c)** If K is any subgroup of G such that $a \in K$, then $<a> \subseteq K$.
- **(d)** $\forall n \in Z^+$, $\text{ord}(a^n) = \text{ord}(a) / \gcd(\text{ord}(a), n)$

[8] Proposition. Let $G = <\alpha>$ be a cyclic group, then

- **(a)** the element α^k generates G if and only if $\gcd(k, |G|) = 1$.
- **(b)** for every positive divisor d of $|G|$, G has exactly one subgroup of order d.
- **(c)** if d divides $|G|$, then G has exactly $\phi(d)$ elements of order d.
- **(d)** G has exactly $\phi(|G|)$ generators.

[9] Theorem. Every subgroup of a cyclic group is cyclic.

[10] Definition. The generators of the multiplicative group $\mathbf{Z}^*_n$ are called ***primitive*** elements of $\mathbf{Z}^*_n$ or ***primitive roots*** of n.

[11] Theorem. A positive integer n has a primitive root if and only if $n = 2, 4, p^k$ or $2p^k$, where p is an odd prime and $k \geq 1$.

[12] Definition. Let G_1 and G_2 be groups, and let $\theta: G_1 \to G_2$ be a function. Then θ is said to be a ***group isomorphism*** if

(i) θ is a bijection (i.e. a one-to-one and onto function) and
(ii) $\theta(ab) = \theta(a)\,\theta(b)$ for all $a, b \in G_1$.

In this case, G_1 is said to be ***isomorphic*** to G_2, and this is denoted by $G_1 \cong G_2$.
Note: θ is called a ***group homomorphism*** if (ii) holds.

[13] Example. $(\mathbf{Z}_4, +)$ and $(\mathbf{Z}^*_5, \cdot)$ are isomorphic, where θ defined as follows:

$$\theta(0) = 1,\ \theta(1) = 2,\ \theta(2) = 4, \text{ and } \theta(3) = 3.$$

[14] Example. (Exponential functions for groups) Let G be any group, and let $a \in G$. Define $\theta: \mathbf{Z} \to G$ by $\theta(n) = a^n$, for all $n \in \mathbf{Z}$. This is a group homomorphism from $\mathbf{Z}$ to G. If G is abelian, with its operation denoted additively, then we define $\theta: \mathbf{Z} \to G$ by $\theta(n) = n \cdot a$.

[15] Proposition. If $\theta: G_1 \to G_2$ is a group homomorphism, then

(a) $\theta(e_1) = e_2$
(b) $(\theta(a))^{-1} = \theta(a^{-1})$ for all $a \in G_1$
(c) for any integer n and any $a \in G_1$, we have $\theta(a^n) = (\theta(a))^n$

[16] Proposition. Let $\theta: G_1 \to G_2$ be a group isomorphism. Then,

(a) $\forall\, a \in G_1$, $\text{ord}(a) = \text{ord}(\theta(a))$
(b) If G_1 is abelian, then so is G_2.
(c) If G_1 is cyclic, then so is G_2.

Exercises:

1. Consider the group $(\mathbf{Z}^*_{21}, \cdot)$
   a. Find < 2 >
   b. Find < 5 >
   c. Find < 11 >
2. Consider the group *A* in Exercise 3 of Section §1. Is *A* a cyclic group? Why?
3. Let $(\mathbf{Z}^*_{38}, \cdot)$ be the multiplicative group modulo 38.
   a. Find a generator of $\mathbf{Z}^*_{38}$
   b. Find a subgroup that has 6 elements?
   c. How many subgroups are there with 6 elements?
   d. Find a subgroup that has 3 elements?
   e. How many subgroups are there with 3 elements?
   f. How many subgroups are there with 4 elements?
   g. How many elements of order 9 are there in $\mathbf{Z}^*_{38}$? List them.
   h. How many elements of order 3 are there in $\mathbf{Z}^*_{38}$? List them.
4. Let G be a group of order 17.
   a. Prove that *G* is cyclic.
   b. Prove or disprove that every element in *G* (except the identity) is a generator of *G*.
5. For each value of *n*, determine whether the multiplicative group $(\mathbf{Z}^*_n, \cdot)$ is cyclic. Briefly justify your answer in each case.
   a. $n = 6$ b. $n = 30$
   c. $n = 32$ d. $n = 75$
   e. $n = 50$ f. $n = 100$
6. Let $(\mathbf{Z}^*_{54}, \cdot)$ be the multiplicative group modulo 54.
   a. Is this group cyclic? How many generators does it have?
   b. How many subgroups of $\mathbf{Z}^*_{54}$ are there of order 3? and of order 27?
   c. Find a subgroup of $\mathbf{Z}^*_{54}$, if any, that has exactly 9 elements.
7. How many elements of order 6 in each of the following groups.
   a. $\mathbf{Z}^*_{13}$ b. $\mathbf{Z}^*_{54}$
   c. $\mathbf{Z}^*_{24}$ d. $\mathbf{Z}_6$
   e. $\mathbf{Z}_{17}$ f. $\mathbf{Z}_{18}$
8. Consider the group *G* in Exercise 1 of Section §1.
   a. Let $(\mathbf{Z}, +)$ be an infinite additive group where $\mathbf{Z}$ is the set of all integers. Give an example of a group homomorphism $\theta: \mathbf{Z} \to G$.
   b. Show that *G* is isomorphic to the additive group $(\mathbf{Z}_5, +)$.
9. Prove or disprove that the multiplicative groups $\mathbf{Z}^*_{125}$ and $\mathbf{Z}^*_{250}$ are isomorphic.
10. Let $(G, *)$ be a group of order *n*. Prove that if *n* is prime, then $(G, *)$ and $(\mathbf{Z}_n, +)$ are isomorphic.

§ 3. Permutation Groups

[1] Definition. Let $A = \{1, 2, \ldots, n\}$ be a set of n elements. A ***permutation*** π of A is a bijection from A to A. i.e. π: A → A, where π is one-to-one and onto. Here, π can be considered as an ordered list of the elements of A.

[2] Notations.
The set of all permutations of a set A is denoted by $S(A)$.
If the size of the set A is $|A| = n$, then S_n denotes $S(A)$ for short.
So, the set of all permutations of the set $\{1, 2, ..., n\}$ is denoted by S_n, i.e.

$$S_n = \{\pi \mid \pi \text{ is a permutation of set of } n \text{ elements}\}$$

[3] Example. For $n = 3$, we have $A = \{1, 2, 3\}$, and $S_3 = \{[1\ 2\ 3], [1\ 3\ 2], [2\ 1\ 3], [2\ 3\ 1], [3\ 1\ 2], [3\ 2\ 1]\}$. Consider the permutation $\pi = [2\ 1\ 3]$. Notice that the function $\pi: A \rightarrow A$ is a bijection, and it maps the elements of A as follows: $\pi(1) = 2$, $\pi(2) = 1$, and $\pi(3) = 3$. The permutation [1 2 3] is called *neutral*, and it maps every element of A to itself.

[4] Proposition. Let A be a set of n elements, then $(S_n, \circ)$ is a group with the operation of composition of functions, $\pi_1 \circ \pi_2$, defined by: $\pi_1 \circ \pi_2\,(x) = \pi_1\,(\,\pi_2\,(x)\,)$
Here, S_n is called the ***permutation group*** of A, also known as the ***symmetric group*** on A.

[5] Note. In $(S_n, \circ)$, the operation $\pi_1 \circ \pi_2$ is read as π_1 after π_2. The identity is the *neutral* permutation, e, where $e(x) = x$, $\forall x \in A$. Like the additive and multiplicative groups, the permutation group is important in cryptography. However, the permutation groups are non-abelian for $n > 2$.

[6] Example. $(S_3, \circ)$ is the symmetric group on $A = \{1, 2, 3\}$. The group is closed under the composition operation since the composition of any two permutations gives a permutation of the set A. For example, $[1\ 3\ 2] \circ [3\ 2\ 1] = [2\ 3\ 1] \in S_3$. The identity is the neutral permutation, $e = [1\ 2\ 3]$. The inverse of [3 1 2] is [2 3 1], and so on.

[7] Theorem. Every permutation in S_n can be written as a product of disjoint cycles. The cycles that appear in the product are unique.

[8] Example. Let S_6 be the set of all permutations of 6 elements on $A = \{1, 2, 3, 4, 5, 6\}$, and let the permutation $\pi = [1\ 4\ 6\ 5\ 2\ 3]$ be an element in S_6. Using arrows, we can identify three disjoint cycles: the first cycle is the unit cycle c_1: $1 \rightarrow 1$ (i.e. a cycle of length one), the second cycle is c_2: $2 \rightarrow 4 \rightarrow 5 \rightarrow 2$, and the third cycle is c_3: $3 \rightarrow 6 \rightarrow 3$. So, we can write π as a product (or composition) of disjoint cycles.

$$\pi = c_1 \circ c_2 \circ c_3 = (1) \circ (2\ 4\ 5) \circ (3\ 6)$$

This expression means that we apply c_1 after c_2 after c_3. Let us take a couple of examples:
$\pi(2) = c_1 \circ c_2 \circ c_3\,(2) = c_1\,(\,c_2\,(\,c_3\,(2)\,)\,) = c_1\,(\,c_2\,(2)\,) = c_1\,(4) = 4$, and
$\pi(6) = c_1 \circ c_2 \circ c_3\,(6) = c_1\,(\,c_2\,(\,c_3\,(6)\,)\,) = c_1\,(\,c_2\,(3)\,) = c_1\,(3) = 3$.

[9] Notation. For compactness, we usually denote the product of cycles in juxtaposition and omit the unit cycles. Therefore: $\pi = c_1 \circ c_2 \circ c_3 = (1) \circ (2\ 4\ 5) \circ (3\ 6)$ can be written in a compact notation as:

$$\pi = (2\ 4\ 5)\ (3\ 6).$$

By convention, the identity element is denoted by a single unit cycle (1). For example:

$$[1\ 2\ 3\ 4\ 5\ 6] = (1)\ (2)\ (3)\ (4)\ (5)\ (6) = (1)$$

[10] Proposition. If a permutation in S_n is written as a product of disjoint cycles, then its order is the *least common multiple* of the lengths of its cycles.

[11] Example. In Example [8], the lengths of disjoint cycles of $\pi = [1\ 4\ 6\ 5\ 2\ 3]$ are:
$| c_1 | = 1$, $| c_2 | = 3$, and $| c_3 | = 2$. Therefore, $\text{ord}(\pi) = \text{lcm}(1, 3, 2) = 6$.
Hence, $\pi^6 = \pi \circ \pi \circ \pi \circ \pi \circ \pi \circ \pi = [1, 2, 3, 4, 5, 6] = e$ (the identity permutation).

[12] Examples. Using Proposition [10], find two subgroups of S_7 of orders 3 and 10.
For order 3, we take any cycle of length 3, like (2 3 1). Then we have:

H = {[2 3 1 4 5 6 7], [3 1 2 4 5 6 7], [1 2 3 4 5 6 7]} is a subgroup of order 3.

For order 10, we take two cycles of lengths 5 and 2, like (2 3 4 5 1) and (7 6). Then we have:

H = {[2 3 4 5 1 7 6], [3 4 5 1 2 7 6], [4 5 1 2 3 7 6], [5 1 2 3 4 7 6], [1 2 3 4 5 7 6],
[2 3 4 5 1 6 7], [3 4 5 1 2 6 7], [4 5 1 2 3 6 7], [5 1 2 3 4 6 7], [1 2 3 4 5 6 7]}

[13] Theorem. (Cayley Theorem) Every group is isomorphic to a subgroup of some permutation group.

[14] Examples.

(a) The additive group $\mathbf{Z}_2$ is isomorphic to the permutation group S_2, with the trivial isomorphism mapping of $\theta(0) = [1\ 2]$ and $\theta(1) = [2\ 1]$.

(b) The additive group $\mathbf{Z}_3$ is isomorphic to a subgroup of S_3, with the isomorphism mapping of $\theta(0) = [1\ 2\ 3]$, $\theta(1) = [2\ 3\ 1]$, and $\theta(2) = [3\ 1\ 2]$.

(c) The multiplicative group $\mathbf{Z}^*_5$ is isomorphic to a subgroup of S_4. Here, we notice that $\text{ord}(2) = 4$. So we need a permutation of order 4 to generate a subgroup of 4 elements. Taking the permutation [2 3 4 1], we obtain a possible mapping as follows: $\theta(1) = [1\ 2\ 3\ 4]$, $\theta(2) = [2\ 3\ 4\ 1]$, $\theta(3) = [4\ 1\ 2\ 3]$, and $\theta(4) = [3\ 4\ 1\ 2]$.

Exercises:

1. Show the complete inverse table of the elements in $(S_3, \circ)$.

2. Consider the permutation group $(S_4, \circ)$
   a. Compute: [2 3 1 4] $\circ$ [4 3 2 1]
   b. Compute: [1 2 4 3] $\circ$ [2 1 3 4]
   c. Compute: $[4\ 3\ 2\ 1]^2$

3. Write the following permutations as a product of cycles in a compact notation.
   a. [1 2 3 4 6 5]
   b. [5 4 6 1 2 3]
   c. [1 2 3 4 5 6 7]
   d. [7 6 5 4 3 2 1]
   e. [2 1 3 6 5 4 7 8]
   f. [1 8 2 7 3 6 4 5]

4. Find the order of each permutation in Exercise 3.

5. Consider the permutation group $(S_5, \circ)$, and let $\pi = [2\ 1\ 4\ 5\ 3]$.
   a. Find π^{-1}
   b. Find π^{-2}
   c. Find π^2
   d. Find $(\pi^2)^{-1}$ and verify whether it equals to π^{-2} in (b) or not.
   e. Find ord(π)
   f. Find $< \pi >$
   g. Is S_5 cyclic? Briefly justify your answer.
   h. Show that the group S_5 is non-abelian by a counterexample.

6. Consider the symmetric group S_{12}.
   a. Find a permutation in S_{12} of order 3.
   b. Find a subgroup of order 3.
   c. Find a permutation in S_{12} of order 20.
   d. Find a permutation in S_{12} of order 24.
   e. Find a permutation in S_{12} of a maximum order.

7. Let π be a permutation of order p in some symmetric group S_n, where p is a large prime. Find the order of the permutation (π^4).

8. Find a subgroup of a permutation group isomorphic to $\mathbf{Z}^*_9$, and show the isomorphism mapping.

9. Prove Proposition [4], i.e. show that $(S_n, \circ)$ is a group.