MATH 325: Group Theory I

Brief lecture notes

Rashid M. Talha

School of Natural Sciences, NUST

(Date: March 15, 2024)

Textbook: Contemporary Abstract Algebra, Joseph Gallian

1 Introduction

Definition 1.1. A binary operation is a map $*: X \times X \to X$, $(a, b) \mapsto a * b$.

By definition, a binary operation ensure that $a * b \in X$ for all $a, b \in X$. This property is called closure.

Definition 1.2. A binary operation $*: X \times X \to X$ is called commutative if

$$\forall a, b \in X, \quad a * b = b * a$$

Definition 1.3. Let G be a non-empty set, and $*: G \times G \to G$ be a binary operation. The pair $(G, *)$ is called a group if it satisfies all of the following

1. $\forall a, b, c \in G$, $(a * b) * c = a * (b * c)$ (Associativity)
2. $\exists e \in G$ such that $\forall a \in G$, $a * e = e * a = a$ (Identity)
3. $\forall a \in G$, $\exists a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$ (Inverse)

Definition 1.4. A group $(G, *)$ is called Abelian if the binary operation $*$ is commutative. That is

$$\forall a, b \in G, \quad a * b = b * a$$

Typically we write $a * b$ simply as ab and call the binary operation a multiplication. In the case where the binary operation is the usual addition, we write $a + b$ instead.

Similarly, we often refer to G as the group and don't explicitly mention the pair $(G, *)$.

Theorem 1.5. *Each group has a unique identity element.*

Proof. Let $e, f \in G$ be identity elements. Then, for all $a \in G$

$$ea = ae = a \qquad \text{and} \qquad fa = af = a.$$

In particular, (taking $a = f$ in the first case and $a = e$ in the second)

$$ef = fe = f \qquad \text{and} \qquad fe = ef = e.$$

As a result, $e = ef = f$. □

Theorem 1.6. *Each $a \in G$ has a unique inverse element.*

Proof. Take any $a \in G$. Let $a^{-1}, b \in G$ be inverse elements of a. That means

$$aa^{-1} = a^{-1}a = e \qquad \text{and} \qquad ab = ba = e.$$

As a result, $b = be = b(aa^{-1}) = (ba)a^{-1} = ea^{-1} = a^{-1}$. □

Theorem 1.7. *Let G be a group. Then, for all $a \in G$, $(a^{-1})^{-1} = a$.*

Proof. Take any $a \in G$. Then, it has an inverse $a^{-1} \in G$ such that $aa^{-1} = e$. Since, $a^{-1} \in G$ it also has an inverse $(a^{-1})^{-1}$ such that $a^{-1}(a^{-1})^{-1} = e$.

Therefore, $a = ae = a(a^{-1}(a^{-1})^{-1}) = (aa^{-1})(a^{-1})^{-1} = e(a^{-1})^{-1} = (a^{-1})^{-1}$. □

Theorem 1.8. *Let G be a group. Then, for all $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.*

Proof. Note that $(ab)^{-1}(ab) = (ab)(ab)^{-1} = e$ by definition of the inverse of ab.

Now,

$$(b^{-1}a^{-1})(ab) = b^{-1}((a^{-1}a)b) = b^{-1}(eb) = b^{-1}b = e.$$

And,

$$(ab)(b^{-1}a^{-1}) = a((bb^{-1})a^{-1}) = a(ea^{-1}) = aa^{-1} = e.$$

So, $b^{-1}a^{-1}$ is also an inverse of ab. By uniqueness of inverse, $b^{-1}a^{-1} = (ab)^{-1}$. □

Theorem 1.9. *Take $a, b, c \in G$. Then,*

1. $ab = ac \implies b = c$.
2. $ba = ca \implies b = c$.

Proof. Since $a \in G$, we have $a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = e$. Therefore,

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

Similarly,

$$ba = ca \implies (ba)a^{-1} = (ca)a^{-1} \implies b(aa^{-1}) = c(aa^{-1}) \implies be = ce \implies b = c$$

□

Theorem 1.10. *Let G be a group. Take $a, b \in G$. Then, the equation $ax = b$ has a unique solution. Likewise, the equation $ya = b$ has a unique solution.*

Proof. (Existence.) Since $a \in G$, we have $a^{-1} \in G$ such that $a^{-1}a = e$. So,

$$ax = b \implies a^{-1}(ax) = a^{-1}b \implies (a^{-1}a)x = a^{-1}b \implies ex = a^{-1}b \implies x = a^{-1}b.$$

And $ab^{-1} \in H$ due to the closure property. So, $x = ab^{-1} \in H$.

(Uniqueness.) Suppose there are $x_1, x_2 \in H$ that satisfy $ax = b$. Then, $ax_1 = b$ and $ax_2 = b$. So, by the cancellation property

$$ax_1 = ax_2 \implies x_1 = x_2$$

The proof for $ya = b$ is analogous, with multiplications on the right hand side. □

Definition 1.11. The order of a group G, denoted $|G|$ or $O(G)$, is the number of elements in G. If G has infinitely many elements then $|G| = \infty$.

Example. Some examples of groups are

1. $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^+, \cdot)$. Here $\mathbb{R}^* = \mathbb{R} - \{0\}$, and $\mathbb{R}^+ = \{r \in \mathbb{R} \mid r > 0\}$.
2. The set of nth roots of unity $U_n = \{\exp(\frac{2\pi i}{n}) \in C | n = 0, 1, \ldots, n-1\}$ forms a group under the multiplication of complex numbers.
3. The set of $n \times n$ matrices with entries in $\mathbb{R}$ is denoted as $M_n(\mathbb{R})$. This forms a group under the usual additional of matrices.
4. $\mathrm{GL}_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det A \neq 0\}$ with the usual matrix multiplication is called the general linear group of order n.
5. The usual matrix multiplication makes $\mathrm{SL}_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det A = 1\}$ into a group, called the the special linear group of order n.

Example 1.12. Consider the set with a single element $G = \{e\}$ and the binary operation $e * e = e$. This forms a group, called the trivial group. Note that for the trivial group $|G| = 1$.

Definition 1.13. A non-empty subset $H \subseteq G$ is called a subgroup of G if it is a group under the same binary operation. We denote this as $H \leq G$.

Definition 1.14. $H \leq G$ is called a proper subgroup if $H \neq G$. This is sometimes emphasised by writing $H < G$. A proper subgroup is called non-trivial if $H \neq \{e\}$.

Example. Some examples of subgroups are

1. $\mathbb{Z} \leq \mathbb{R}$.
2. $\mathbb{R}^+ \leq \mathbb{R}^*$.
3. $2\mathbb{Z} \leq \mathbb{Z}$, with $2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$.
4. $\mathrm{SL}_n(\mathbb{R}) \leq \mathrm{GL}_n(\mathbb{R})$.

Theorem 1.15. *Let G be a group. A non-empty subset $H \subseteq G$ is a subgroup of G if and only if*

1. $a, b \in H \implies ab \in H$.
2. $a \in H \implies a^{-1} \in H$.

Proof. Suppose $H \leq G$. Then, H is a group under the same binary operation. In particular, both the closure property and the existence of inverse property holds in H.

Conversely, the closure property is explicitly given. Associativity is inherited from the binary operation on G. Also, the existence of inverse property is explicitly given. Finally, since H is non-empty, take $a \in H$. Then, $a^{-1} \in H$. By the closure property, $aa^{-1} = e \in H$. Therefore, H also contains the identity element. As a result, H is a group with respect to the same binary operation. That is, $H \leq G$. $\square$

Theorem 1.16. *Let G be a group. A non-empty subset $H \subseteq G$ is a subgroup of G if and only if $a, b \in H \implies ab^{-1} \in H$.*

Proof. Suppose $H \leq G$. Then, H is a group under the same binary operation. Take $a, b \in H$. Then, by the previous subgroup test $b^{-1} \in H$. Again, by the previous subgroup test, $ab^{-1} \in H$.

For the converse, we check that H satisfies all the group axioms.

Firstly, H has the same binary operation as G, so associativity is inherited from G.

Next, since H is non-empty, take any $a \in H$. Then, $aa^{-1} \in H$ implies $e \in H$. So, H contains the identity element.

Similarly, take $e, a \in H$. Then, $ea^{-1} \in H$ implies $a^{-1} \in H$. Therefore, each element of H has an inverse within H.

Lastly, take $a, b \in H$. Then, $b^{-1} \in H$. So, $a\left(b^{-1}\right)^{-1} \in H$ implies $ab \in H$, since $\left(b^{-1}\right)^{-1} = b$.

Therefore, H is a group under the same binary operation as G. So, $H \leq G$. $\square$

Theorem 1.17. *Let $H_i \leq G$, for all $i \in I$. Then, $H = \cap_{i \in I} H_i$ is a subgroup of G.*

Proof. Firstly, $e \in H_i$ for all $i \in I$ because each H_i is a subgroup of G. As a result, $e \in H$. So, H is non-empty.

Take $a, b \in H$. Then, $a, b \in H_i$ for all $i \in I$. As H_i are subgroups, $ab^{-1} \in H_i$ for all $i \in I$. Therefore, $ab^{-1} \in H$. By the subgroup criteria, this shows that $H \leq G$. $\square$

Theorem 1.18. *Let G be a group and take $a \in G$. The set $H = \{a^n \mid n \in \mathbb{Z}\}$ is a subgroup of G. Here, $a^0 = e$ and $a^{-n} = \left(a^{-1}\right)^n$.*

Proof. Firstly, H is non-empty because $a^0 = e \in H$.

Next, take any $a^n, a^m \in H$. Then, $(a^m)^{-1} = a^{-m}$. So,

$$a^n (a^m)^{-1} = a^n a^{-m} = a^{n-m} \in H,$$

since $n - m \in \mathbb{Z}$.

By the subgroup criteria, this shows that $H \leq G$. $\square$

Definition 1.19. The order of an element $a \in G$ is the least positive integer k such that $a^k = e$. We denote this as $O(a)$ or $|a|$.

Theorem 1.20. *$H_1, H_2 \leq G$. Then, $H_1 \cup H_2$ is a subgroup of G if and only if $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$.*

Proof. Suppose (WLOG) $H_1 \subseteq H_2$. Then, $H_1 \cup H_2 = H_2$. And $H_2 \leq G$. Therefore, $H_1 \cup H_2 \leq G$.

Conversely, suppose $H_1 \subsetneq H_2$ and $H_2 \subsetneq H_1$ but $H_1 \cup H_2$ is a subgroup of G. Then, ... $\square$

2 Modular Addition

Definition 2.1. Let a, b be integers and fix a positive integer n. We say that a is congruent to b modulo n if n divide $a - b$. That is $n|(a - b)$. This is denoted as $a \equiv b \mod n$.

Definition 2.2. Take $a \in \mathbb{Z}$, and fix some integer $n \geq 2$. The set of all the integers that are equivalent to a modulo n is called the residue class of a modulo n. We write this as

$$[a]_n = \{b \in \mathbb{Z} \,|\, a \equiv b \mod n\}. \tag{1}$$

Remark. $[a]_n$ and $[b]_n$ are either equal of disjoint. (This was skipped.)

3 $\mathbb{Z}_3$

Definition 3.1. Fix some integer $n \geq 2$. The set of all the residue classes modulo n in $\mathbb{Z}$ is denoted as

$$\mathbb{Z}_n = \{[a]_n \,|\, a \in \mathbb{Z}\}. \tag{2}$$

We can define a binary operation $+_n$, called modular addition (mod n) on this set,

$$[a]_n +_n [b]_n := [a + b]_n. \tag{3}$$

It needs to be shown that this is well-defined; that is if $[a]_n = [c]_n$ and $[b]_n = [d]_n$, then, $[a]_n +_n [b]_n = [c]_n +_n [d]_n$. (This was skipped.)

Theorem 3.2. *The set $\mathbb{Z}_n$ forms a group with respect to $+_n$.*

Proof. TBC. □

When it is clear from the context, we drop the subscript and simply write $[a]_n$ as a and $+_n$ as $+$.

4 Klein 4-Group

Consider a set $G = \{e, a, b, c\}$ with a binary operation that satisfies $a^2 = b^2 = c^2 = e$, $xy = yx$ for all $x, y \in G$. It can easily be checked that this forms a group. We also find that some of the conditions imposed on the binary operation are redundant, and instead this group can be expressed more compactly. The following theorem states this observation.

Theorem 4.1. *The set $K_4 = \{1, a, b, ab\}$, where the order of each non-identity element is 2 forms a group.*

Proof. TBC. □

This group K_4 is called the Klein 4-group. It is a group of order 4. Its multiplication rule can be represented as table, called a Cayley table.

	1	a	b	ab
1	1	a	b	ab
a	a	1	ab	b
b	b	ab	1	a
ab	ab	b	a	1

Multiplication table for K_4.

Here, the entry in the the (i, j)-th entry is the result of multiplying the element in the jth column with the element in the ith row in the 'column-on-the-left' order.

$$(\mathrm{col}_j) * (\mathrm{row}_i) = (i, j)\text{-th entry}$$

There are precisely three non-trivial subgroups of K_4: $\{1, a\}$, $\{1, b\}$ and $\{1, ab\}$.

Consider the set

$$G = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\} \tag{4}$$

of matrices with the usual matrix multiplication. We find that it forms a group. Clearly, this is a group of order 4. Moreover, each non-identity element in this group has order 2. This coincides exactly with the group structure of K_4. We say that this group is the same as K_4 (this notion will be made precise when we define isomorphisms later), and that it is simply a matrix representation of K_4.

Another group of order 4 that we have already seen in $\mathbb{Z}_4$. This group has an element of order 4, namely $[1]_4$. Therefore, it cannot be the 'same' as K_4. (Again, this observation will be made precise through the use of isomorphisms.) This shows that not all groups of order 4 are the same as k_4.

5 Group of Quaternions

Consider the group $\mathrm{GL}_2(\mathbb{C})$ of 2×2 invertible matrices with complex entries. Consider its subset

$$H = \left\{ \pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \pm \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \pm \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \pm \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \right\}. \tag{5}$$

It is easy to check that this is a subgroup of $\mathrm{GL}_2(\mathbb{C})$, and therefore a group. We note that this is a group of order 8.

Using the multiplication of H as a template, we can define an abstract group of order 8 as follows.

Theorem 5.1. *The set $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ forms a group with the multiplication rule*

$$i^2 = j^2 = k^2 = 1 \tag{6}$$
$$ij = k, jk = i, ki = j \tag{7}$$
$$ji = -k, kj = -i, ik = -j. \tag{8}$$

This group is called the group of quaternions.

	1	i	j	k	-1	$-i$	$-j$	$-k$
1	1	i	j	k	-1	$-i$	$-j$	$-k$
i	i	1	$-k$	j	$-i$	-1	k	$-j$
j	j	k	1	$-$	$-$	$-$	$-$	$-$
k	k	$-j$	$-$	1	$-$	$-$	$-$	$-$
-1	-1	$-i$	$-$	$-$	1	$-$	$-$	$-$
$-i$	$-i$	-1	$-$	$-$	$-$	1	$-$	$-$
$-j$	$-j$	$-k$	$-$	$-$	$-$	$-$	1	$-$
$-k$	$-k$	j	$-$	$-$	$-$	$-$	$-$	1

Multiplication table for Q_4.

6 Dihedral Group (of Order 3)

Consider the set $D_3 = \{1, a, a^2, b, ba, ba^2\}$ with the conditions $a^3 = 1$, $b^2 = 1$ and $ab = ba^2$. We can check that this forms a non-abelian group. This is called the dihedral group of order 6

THE CAYLEY TABLE

7 Cyclic Group

Definition 7.1. A group G is called cyclic if there is an element $a \in G$ such that all elements of G can be written as powers of a. More precisely, $\forall g \in G$, $\exists m \in \mathbb{Z}$ such that $g = a^m$.

Such as element a is called a generator of G, and we say that G is the group generated by a and denote this as $G = \langle a \rangle$. Cyclic group of order n is sometimes denoted as C_n.

Generators are not unique. Indeed if $a \in G$ is a generator then so is a^{-1}.

Notation. For $m > 0$, a^m means $a * \cdots * a$, where m factors of a are multiplied together. Similarly, $a^0 \equiv 1$, the identity element. And, a^{-m} means $\left(a^{-1}\right)^m$.

Theorem 7.2. *Let $G = \langle a \rangle$ be a cyclic group. Then, $O(G) = O(a)$.*

Proof. If $O(a)$ is infinite then a^n and a^m are distinct for all $n \neq m$; because otherwise,

$$a^n = a^m \implies a^{n-m} = 1 \implies O(a) \leq |n - m| \tag{9}$$

which is a contradiction. Now, since each a^n is different from a^{n+1}, we have infinitely many elements in the set

$$\langle a \rangle = \{a^n \,|\, n \in \mathbb{Z}\}. \tag{10}$$

Consequently, $G = \langle a \rangle$ has infinitely many elements; i.e. $O(G)$ is also infinite.

Next, consider the case when $O(a) = n$ is finite.

If $O(a) = 1$, then $G = \langle a \rangle = \{a^n \,|\, n \in \mathbb{Z}\} = \{1\}$ and $O(G) = 1$.

Otherwise $O(a) = n \geq 2$. SOMETHING SOMETHING. $\square$

Theorem 7.3. *Let G be a group, and take $a \in G$ such that $a^n = 1$. Then, the cyclic group $\langle a \rangle$ has the form $\{1, a, a^2, \ldots, a^{n-1}\}$.*

Theorem 7.4. *Let G be a group and $a \in G$ with $O(a) = n$. If $a^m = 1$ then $n \mid m$.*

Proof. By the division algorithm, we have $m = qn + r$ for $q, r \in \mathbb{Z}$ and $0 \leq r < n$. So,

$$a^m = a^{nq+r} = (a^{nq})(a^r) = (1^q)(a^r) = (1)(a^r) = a^r. \tag{11}$$

Now, $a^m = 1 \implies a^r = 1$. However, $r < n$ and n is the least positive integer for which $a^n = 1$. Therefore, r must be zero (if it was positive then it would contradict the minimality of n). Therefore, $m = qn$, or $n \mid m$ $\square$

Theorem 7.5. *Every cyclic group is abelian.*

Proof. Let $G = \langle g \rangle$ be a cyclic group. Take $a, b \in G$. Then, $a = g^m$, $b = g^n$ for some $m, n \in \mathbb{Z}$. As a result, $ab = g^m g^n = g^{m+n} = g^{n+m} = g^n g^m = ba$. $\square$

Theorem 7.6. *Every subgroup of a cyclic group is cyclic.*

Theorem 7.7. *Let $G = \langle a \rangle$ be a finite cyclic group of order n. Then an element a^k is a generator of G if and only if $\gcd(k, n) = 1$.*

Proof. Suppose a^k is a generator of G. Then, we can write a as a power of a^k, say

$$a = \left(a^k\right)^m = a^{km} \tag{12}$$

for some $m \in \mathbb{Z}$. Then,

$$a = \left(a^k\right)^m \implies aa^{-km} = e \implies a^{1-km} = e. \tag{13}$$

So, $n \mid 1 - km$. That is $\exists q \in \mathbb{Z}$ such that $1 - km = qn$. We can re-arrange this to get $qn + km = 1$. From number theory (Bezout's lemma) we know that this implies $\gcd(n, k) = 1$.

Conversely, suppose $\gcd(n, k) = 1$. Then, there exist integers x, y such that $xk + yn = 1$. So,

$$a = a^{xk+yn} \implies a = \left(a^k\right)^x (a^n)^y \implies a = \left(a^k\right)^x e^y \implies a = \left(a^k\right)^x. \tag{14}$$

Now for all $b \in \langle a \rangle$, we have $b = a^r$ for some $r \in Z$. Therefore, we can write it as a power of a^k as

$$b = a^r = \left(\left(a^k\right)^x\right)^r = \left(a^k\right)^{xr}. \tag{15}$$

So, a^k also generates $\langle a \rangle$. $\square$

Remark. The number of generators for a finite cyclic group of order n is $\varphi(n)$, the Euler's φ function.

Theorem 7.8. *An infinite cyclic group $G = \langle a \rangle$ has exactly two generators.*

Proof. Let $b \in G$ be another generator of G. Firstly, we have $b = a^n$ for some $n \in \mathbb{Z}$. SOMETHING. $\square$

8 Equivalence Relations

Definition 8.1. A partition of a non-empty set S is a collection of non-empty disjoint subsets $S_i \subseteq S$ such that $\cup_{i \in I} S_i = S$.

Definition 8.2. A relation R on a set S is a subset of $S \times S$. We say that x is related to y if $(x, y) \in R$. This is denoted as xRy.

Definition 8.3. A relation R on S is called an equivalence relation if it satisfies

(i) For all $x \in S$, xRx. (reflexive)

(ii) For all $x, y \in S$, $xRy \implies yRx$. (symmetric)

(iii) For all $x, y, z \in S$, if xRy and yRz then xRz. (transitive)

An equivalence relation is typically denoted by the symbol $\sim$ instead of R.

Example 8.4. $a \sim b$ if $n \mid (a - b)$. This is an equivalence relation.

Example 8.5. $a \sim b$ if $a \leq b$ is not an equivalence relation because it is not symmetric.

Definition 8.6. Let $\sim$ be an equivalence relation on S. The equivalence class of $a \in S$ is the set

$$[a] = \{b \in S \,|\, b \sim a\}. \tag{16}$$

Some authors use the notation $\bar{a}$ or $cl(a)$ to denote the equivalence class of a.

Theorem 8.7. *Let $\sim$ be an equivalence relation on S. Then, the collection of equivalence classes $\{[a] \,|\, a \in S\}$ partitions S. More precisely, each $[a]$ is non-empty, and $S = \cup_{a \in S} [a]$, and if $[a] \neq [b]$ then $[a] \cap [b] = \emptyset$.*

Proof. Exercise. $\square$