MATH 325: Group Theory I

Brief lecture notes

Rashid M. Talha

School of Natural Sciences, NUST

(Date: April 15, 2024)

Textbook: Contemporary Abstract Algebra, Joseph Gallian.

Disclaimer: This document most likely contains some errors — use with caution. I have rephrased or paraphrased the content in most of the sections. Some examples may be missing. The numbering that I have used for sections, definitions, theorems, etc will not match the numbering given in the lectures.

1 Introduction

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

By definition of $*$, $a * b \in X$ 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

(i) $\forall a, b, c \in G$, $(a * b) * c = a * (b * c)$ (Associativity)

(ii) $\exists e \in G$ such that $\forall a \in G$, $a * e = e * a = a$ (Identity)

(iii) $\forall a \in G$, $\exists a^{-1} \in G$ 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, for all $a, b \in G$, $a * b = b * a$.

Remark. Typically we write $a * b$ simply as ab and call the binary operation 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 $(G, *)$. Moreover, we sometimes denote the identity element by 1 for multiplicative binary operations, and by 0 for additive binary operations.

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, $b = be = b(aa^{-1}) = (ba)a^{-1} = ea^{-1} = a^{-1}$. $\square$

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, $a = ae = a(a^{-1}(a^{-1})^{-1}) = (aa^{-1})(a^{-1})^{-1} = e(a^{-1})^{-1} = (a^{-1})^{-1}$. $\square$

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 the uniqueness of inverse, $b^{-1}a^{-1} = (ab)^{-1}$. $\square$

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,

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

$\square$

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

Proof. Consider the equation $ax = b$.

(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 $a^{-1}b \in G$ due to the closure property. So, $x = a^{-1}b \in G$.

(Uniqueness.) Suppose there are $x_1, x_2 \in G$ 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. $\square$

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 $U_n = \{\exp(\frac{2\pi i}{n}) \in C \mid n = 0, 1, \ldots, n-1\}$ forms a group under the multiplication of complex numbers.
3. The set of $n \times n$ matrices with entries in $\mathbb{R}$ is denoted by $M_n(\mathbb{R})$. 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, $H \leq G$. □

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 $H \leq G$. □

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 $a^n, a^m \in H$.. So, $a^n(a^m)^{-1} = a^n a^{-m} = a^{n-m} \in H$ since $n - m \in \mathbb{Z}$ and $(a^m)^{-1} = a^{-m}$.

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

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. *Let $H, K \leq G$. Then, $H \cup K$ is a subgroup of G if and only if $H \subseteq K$ or $K \subseteq H$.*

Proof. If $H \subseteq K$ then, $H \cup K = H \leq G$. Instead, if $K \subseteq H$ then, $H \cup K = K \leq G$. In either case, $H \cup K \leq G$.

Conversely, suppose $H \cup K \leq G$. For a contradiction assume $H \nsubseteq K$ and $K \nsubseteq H$. Then we can pick $h \in H - K$ and $k \in K - H$. So, $h, k \in H \cup K$. Since $H \cup K$ is a group of G, we have $hk \in H \cup K$. So, either $hk \in H$ or $hk \in K$ (or both).

If $hk \in H$, then $k \in H$ because $h \in H$ (and so, $h^{-1} \in H$). Alternatively, if $hk \in K$, then $h \in K$ because $k \in K$ (and so, $k^{-1} \in K$). Both of these are contradictions. Therefore the assumption $H \nsubseteq K$ and $K \nsubseteq H$ is wrong, and either $H \subseteq K$ or $K \subseteq H$. □

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

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

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

Definition 2.3. Fix some integer $n \geq 2$. The set of all the residue classes modulo n in $\mathbb{Z}$ is denoted as

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

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

$$[a]_n +_n [b]_n := [a+b]_n.$$

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

We sometimes drop the subscript and simply write $[a]_n$ as a and $+_n$ as $+$.

3 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 3.1. *The set $K_4 = \{1, a, b, ab\}$ where the order of each non-identity element is 2 forms a group.*

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.

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

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

Consider the set

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

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 is $\mathbb{Z}_4$. 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.

4 Group of Quaternions

Consider the subset

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

of the group $\mathrm{GL}_2(\mathbb{C})$ of 2×2 invertible matrices with complex entries. It is easy to check that this is a subgroup of $\mathrm{GL}_2(\mathbb{C})$ and therefore a group in its own right. We note that this is a group of order 8.

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

Theorem 4.1. *The set $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ forms a group with the multiplication rule $i^2 = j^2 = k^2 = ijk = -1, (-1)^2 = 1$.*

This is called the group of quaternions. Its full multiplication table is given below.

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

Multiplication table for Q_8.

5 Dihedral Group (of Order 6)

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.

	1	a	a^2	b	ba	ba^2
1	1	a	a^2	b	ba	ba^2
a	a	a^2	1	ba	ba^2	b
a^2	a^2	1	a	ba^2	b	ba
b	b	ba^2	ba	1	a^2	a^2
ba	ba	b	ba^2	a	1	a
ba^2	ba^2	ba	b	a^2	a	1

Multiplication table for D_3.

6 Cyclic Group

Definition 6.1. 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, $a^0 \equiv e$, the identity element. And, a^{-m} means $\left(a^{-1}\right)^m$.

Theorem 6.2. *Let G be a group, and take $a \in G$ such that $a^n = e$. Then, the cyclic group $\langle a \rangle$ has the form $\{e, a, a^2, \dots, a^{n-1}\}$.*

Proof. By definition $\langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$. We can write $k = qn + r$ for $q, r \in \mathbb{Z}$ and $0 \le r < n$. So, for all $k \in \mathbb{Z}$, $a^k = a^{qn+r} = a^{qn}a^r = (a^n)^q = ea^r = a^r$.

Therefore, $\langle a \rangle = \{a^r \mid 0 \le r < n\} = \{e, a, a^2, \dots, a^{n-1}\}$. ☐

Theorem 6.3. *Let $G = \langle a \rangle$ be a cyclic group. Then, $|G| = O(a)$.*

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

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

which is a contradiction. Now, since each a^n is different from a^{n+1}, we have infinitely many elements in the set $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$. Consequently, $G = \langle a \rangle$ has infinitely many elements; i.e. $|G|$ is also infinite.

Next, consider the case when $O(a) = n$ is finite. Then, $G = \langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$ by theorem (6.2). So, $|G| = n$ also. ☐

Theorem 6.4. *Let G be a group and $a \in G$ with $O(a) = n$. If $a^m = e$ then $n \mid m$.*

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

$$a^m = a^{nq+r} = (a^{nq})(a^r) = (e^q)(a^r) = e(a^r) = a^r.$$

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

Theorem 6.5. *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, $ab = g^m g^n = g^{m+n} = g^{n+m} = g^n g^m = ba$. □

Theorem 6.6. *Every subgroup of a cyclic group is cyclic.*

Proof. Consider the cyclic group $G = \langle a \rangle$. Let H be a subgroup of G. If $H = \{e\}$ then it is generated by e. So, suppose H is not the trivial subgroup. Then, every element in H can be written as a^k for some $k \in \mathbb{Z}$. Let m be the least positive integer such that $a^m \in H$. Therefore, $a^{-m} \in H$ also.

Take any $a^t \in H$. Then, we can write $t = mq + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < m$. Equivalently, $r = t - mq$. So,

$$a^r = a^{t-mq} = a^t a^{-mq} = a^t (a^{-m})^q \in H$$

by closure. If $r \neq 0$, then this contradicts the requirement that m is the least positive integer with $a^m \in H$. Therefore, $r = 0$. So, $t = mq$, and every arbitrary element of H has the form $a^t = a^{mq} = (a^m)^q$. Therefore, $H = \langle a^m \rangle$. □

Theorem 6.7. *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 $a = (a^k)^m = a^{km}$ for some $m \in \mathbb{Z}$.

Then, $a = a^{km} \implies aa^{-km} = e \implies a^{1-km} = e$.

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, $a = a^{xk+yn} \implies a = (a^k)^x (a^n)^y \implies a = (a^k)^x e^y \implies a = (a^k)^x$.

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 $b = a^r = ((a^k)^x)^r = (a^k)^{xr}$. So, a^k also generates $\langle a \rangle$. □

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

Theorem 6.8. *An infinite cyclic group $G = \langle a \rangle$ has exactly two generators.*

Proof. Firstly, since $|\langle a \rangle| = \infty$, the order of a is infinite. And $a^n = e$ is only possible when $n = 0$.

Let $b \in G$ be another generator of G. Then, we can write $b = a^s$ and $a = b^t$ for some $s, t \in \mathbb{Z}$. Therefore, $a = (a^s)^t = a^{st} \implies a^{st-1} = e \implies st - 1 = 0$.

The only solutions to this Diophantine equation are $s = t = 1$ and $s = t = -1$. So, $b = a$ or $b = a^{-1}$. □

7 Equivalence Relations

Definition 7.1. 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 7.2. 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 7.3. 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 7.4. $a \sim b$ if $n \mid (a - b)$. This is an equivalence relation.

Example 7.5. $a \sim b$ if $a \leq b$ is not an equivalence relation because it is not symmetric.

Definition 7.6. Let $\sim$ be an equivalence relation on S. The equivalence class of $a \in S$ is the set

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

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

Theorem 7.7. *Let $\sim$ be an equivalence relation on S. The collection of equivalence classes $\{[a] \,|\, a \in S\}$ partitions S. More precisely, each $[a]$ is non-empty, and $S = \bigcup_{a \in S} [a]$, and if $[a] \neq [b]$ then $[a] \cap [b] = \emptyset$.*

Proof.

1. By reflexivity, $a \sim a$ we have $a \in [a]$. Therefore, $[a] \neq \emptyset$.

2. By definition $[a] \subseteq S$, so $\bigcup_{a \in S} [a] \subseteq S$.

   Take any $a \in S$. Then, $a \in [a] \subseteq \bigcup_{a \in S} [a]$. So, $S = \bigcup_{a \in S} [a]$.

3. We prove the contrapositive statement.

   Suppose $[a] \cap [b] \neq \emptyset$. So, there is some $c \in [a] \cap [b]$. By definition, this means $c \sim a$ and $c \sim b$. Then, by symmetry, $a \sim c$. So, the transitivity of $\sim$ gives

   $$a \sim c \quad \text{and} \quad c \sim b \implies a \sim b.$$

   Also, by symmetry, $b \sim a$.

   Now, if $x \in [a]$, then $x \sim a$. By transitivity, $x \sim a$ and $a \sim b$ implies $x \sim b$. That is, $x \in [b]$. So, $[a] \subseteq [b]$.

   Similarly, if $y \in [b]$, then $y \sim b$. Again, by transitivity, $y \sim b$ and $b \sim a$ implies $y \sim a$. That is, $y \in [a]$. So, $[b] \subseteq [a]$. Overall, $[a] = [b]$. □

Theorem 7.8. *Let $H \leq G$ and $\sim$ be a relation on G such that $a \sim b := a^{-1}b \in H$. Then, $\sim$ is an equivalence relation.*

Proof. We check that $\sim$ satisfies the three conditions of being an equivalence relation.

(Reflexive.) Take $a \in G$. Then, $a^{-1}a = e$ and $e \in H$ because $H \leq G$. So, $a \sim a$.

(Symmetric.) Suppose $a \sim b$. That means $a^{-1}b \in H$. As $H \leq G$, the element $(a^{-1}b)^{-1} \in H$. And $(a^{-1}b)^{-1} = b^{-1}a$. That is, $b^{-1}a \in H$. So, $b \sim a$.

(Transitive.) Suppose $a \sim b$ and $b \sim c$. That is $a^{-1}b \in H$ and $b^{-1}c \in H$. As H is a subgroup, closure and associativity gives $(a^{-1}b)(b^{-1}c) = a^{-1}c \in H$. So, $a \sim c$. $\square$

Theorem 7.9. *Let $H \leq G$ and $\sim$ be a relation on G such that $a \sim b := ab^{-1} \in H$. Then, $\sim$ is an equivalence relation.*

8 Cosets

Definition 8.1. Let $H \leq G$. Take some $a \in G$. The subsets

$$aH = \{ah \mid h \in H\} \quad \text{and} \quad Ha = \{ha \mid h \in H\}$$

are called the left and right cosets of H containing $a \in G$, respectively.

For the coset aH, the element a is called a representative of the coset. We note that any element of aH can act as its representative. A coset always contains its representative element; because $a = ae = ea$ and $e \in H$ for every subgroup.

Theorem 8.2. *Let $H \leq G$ and $\sim$ be an equivalence relation on G such that $a \sim b$ if $a^{-1}b \in H$. Then, $[a] = aH$.*

Proof. We know that $[a] = \{b \in G \mid b \sim a\} = \{b \in G \mid a \sim b\} = \{b \in G \mid a^{-1}b \in H\}$.

Take any $x \in aH$. Then, $x = ah$ for some $h \in H$. So, $a^{-1}x = h \in H$. Therefore, $x \in [a]$. So, $aH \subseteq [a]$.

Likewise, take any $x \in [a]$. Then, $a^{-1}x \in H$. So, there is some $h \in H$ such that $a^{-1}x = h$. Therefore, $x = ah \in aH$. So, $[a] \subseteq aH$. Overall, $[a] = aH$. $\square$

We have an analogous result for the right cosets.

Theorem 8.3. *Let $H \leq G$ and $\sim$ be an equivalence relation on G such that $a \sim b$ if $ab^{-1} \in H$. Then, $[a] = Ha$.*

Theorem 8.4. *Let $H \leq G$ and $a \in G$.*

(i) $a \in aH$

(ii) $aH = bH \iff a \in bH$

(iii) $aH = bH$ *or* $aH \cap bH = \emptyset$

Proof. (i) Since $H \leq G$, $e \in H$. So, $a = ae \in aH$.

(ii) Suppose $aH = bH$. By part (i) $a \in aH$. So, $a \in aH = bH$. Therefore, $a \in bH$.

For the converse, suppose $a \in bH$. Then, $a = bh_0$ for some $h_0 \in H$. So,

$$aH = \{ah \,|\, h \in H\} = \{(bh_0)h \,|\, h \in H\} = \{b(h_0h) \,|\, h \in H\} = \{bk \,|\, k \in H\} = bH$$

(iii) Suppose $aH \cap bH \neq \emptyset$. Then, $\exists c \in G$ such that $c \in aH \cap bH$. By part (ii),

$$c \in aH \implies cH = aH \quad \text{and} \quad c \in bH \implies cH = bH.$$

So, $aH = cH = bH$.

Therefore, either $aH \cap bH = \emptyset$ or $aH = bH$. □

Theorem 8.5. *Let H be a subgroup of G and let $a, b \in G$. Then,*

(i) $aH = H$ *if and only if* $a \in H$.

(ii) $|aH| = |bH|$

(iii) $aH = bH$ *if and only if* $a^{-1}b \in H$.

Proof. (i) This is a special case of part (ii) from theorem (8.4) with $b = e$. Here, we need to note that $eH = \{eh \,|\, h \in H\} = \{h \,|\, h \in H\} = H$.

(ii) Consider the map $\varphi : aH \to bH$ with $\varphi(ah) = bh$. This is injective because

$$\varphi(ah_1) = \varphi(ah_2) \implies bh_1 = bh_2 \implies h_1 = h_2 \implies ah_1 = ah_2.$$

It is also surjective by construction. Therefore, φ is a bijection between the sets aH and bH. So, $|aH| = |bH|$.

(iii) By theorem (8.4) part(ii),

$$aH = bH \iff b \in aH \iff b = ah \text{ for some } h \in H \iff a^{-1}b = h \in H. \quad \square$$

Again, we have an analogous version of the previous two theorems for right cosets.

Remark. Since $|aH| = |bH|$ for all $a, b \in G$, we have that $|aH| = |H|$ for all $a \in G$. Therefore, the cardinality of each coset of H is the same as the order of H.

Theorem 8.6 (Lagrange)**.** *Let G be a finite group and H be its subgroup. Then $|H|$ divides $|G|$. Moreover, the number of distinct left (right) cosets of H in G is $|G|/|H|$.*

Proof. Let $a_1H, \ldots, a_kH$ be all the distinct cosets of H in G. Then, $G = \bigcup_{j=1}^{k} a_jH$ because for all $g \in G$, $g \in a_jH$ for some j.

Moreover, $|aH| = |bH|$, for all $a, b \in G$. In particular, $|a_jH| = |eH| = |H|$ for all j.

Now, since G is written as a union of distinct sets, we have

$$|G| = |a_1H| \cup \cdots \cup |a_kH| = |H| \cup \cdots \cup |H| = k|H|.$$

So, $|H|$ divides $|G|$ and the number of distinct left (right) cosets is $k = |G|/|H|$. □

This proof shows that number of distinct left cosets is the same as the number of distinct right cosets. Therefore, the following statement is well-defined.

Definition 8.7. Let $H \leq G$. The number of distinct left (right) cosets of H in G is called the index of H in G. It is denoted as $[G : H]$.

When G is a finite group, Lagrange's theorem states that $[G : H] = |G|/|H|$.

Corollary 8.8. *Let G be a finite group and $a \in G$. Then $O(a)$ divides the order of G.*

Proof. Consider the subgroup $\langle a \rangle$ generated by $a \in G$. By theorem (6.3) we know that $|\langle a \rangle| = O(a)$. By Lagrange's theorem, $|\langle a \rangle|$ divides $|G|$. Therefore, $O(a)$ divides the order of $|G|$. □

Corollary 8.9. *If G is a finite group and $a \in G$, then $a^{|G|} = e$.*

Proof. Suppose $|G| = n$ and $O(a) = m$. By corollary (8.8), $m \mid n$. Therefore, $n = mk$ for some $k \in \mathbb{Z}$. So, $a^{|G|} = a^n = a^{mk} = (a^m)^k = e^k = e$. □

Corollary 8.10. *Every group of prime order is cyclic.*

Proof. Let $|G| = p$, where p is prime. Take $a \in G - \{e\}$, with $O(a) = m$. Since, $O(a) \mid p$, we have either $O(a) = 1$ or $O(a) = p$. Since, $a \neq e$, we have $O(a) \neq 1$. Therefore, $O(a) = p$.

Let $H = \langle a \rangle$. Then $|H| = O(a) = p$. Now, $H \subseteq G$ and $|H| = |G|$ (finite). Therefore, $G = H = \langle a \rangle$. □

Remark. If $|G|$ is infinite then $[G : H]$ may or may not be finite. Therefore, we cannot write $[G : H] = |G|/|H|$ when $|G|$ is infinite. For example, $[\mathbb{Z} : n\mathbb{Z}] = n$, while $[\mathbb{R} : \mathbb{Z}] = \infty$.

9 Symmetric Groups

Definition 9.1. A permutation of a non-empty set A is a bijective function $\varphi : A \to A$.

Notation. Let A be a non-empty set. The set of all the permutations of A is denoted by $S_A = \{\varphi : A \to A \mid \varphi \text{ is bijective}\}$.

Lemma 9.2. *Let A be a non-empty set. The the composition of functions is a binary operation on S_A. More precisely, if $\varphi, \psi \in S_A$, then $\varphi \circ \psi \in S_A$.*

Proof. Take $\varphi, \psi \in S_A$. So, φ, ψ are bijective.

Consider the map $\varphi \circ \psi : A \to A$ with $(\varphi \circ \psi)(a) = \varphi(\psi(a))$.

Let $a, b \in A$. Then, $\varphi(\psi(a)) = \varphi(\psi(b)) \implies \psi(a) = \psi(b) \implies a = b$. Therefore, $\varphi \circ \psi$ is injective.

Next, for all $a \in A$, there exists $b \in A$ such that $\varphi(b) = a$. And for all $b \in A$, there exists $c \in A$ such that $\psi(c) = b$. So, for all $a \in A$, we have $c \in A$ such that $(\varphi \circ \psi)(c) = \varphi(\psi(c)) = \varphi(b) = a$. Therefore, $\varphi \circ \psi$ is surjective.

Consequently, $\varphi \circ \psi$ is bijective. □

Notation. The operation of composition of functions in S_A is also called permutation multiplication.

Theorem 9.3. *Let A be a non-empty set. Then, S_A is a group under permutation multiplication.*

Proof. (Closure.) By lemma (9.2), S_A is closed under permutation multiplication.

(Associativity.) Let $\varphi_1, \varphi_2, \varphi_3 \in S_A$. Then, for all $a \in A$,

$$(\varphi_1 \circ (\varphi_2 \circ \varphi_3))(a) = \varphi_1 \circ (\varphi_2(\varphi_3(a))) = \varphi_1(\varphi_2(\varphi_3(a)))$$

and

$$((\varphi_1 \circ \varphi_2) \circ \varphi_3)(a) = (\varphi_1 \circ \varphi_2)(\varphi_3(a)) = \varphi_1(\varphi_2(\varphi_3(a)))$$

So, $\varphi_1 \circ (\varphi_2 \circ \varphi_3) = (\varphi_1 \circ \varphi_2) \circ \varphi_3$.

(Identity.) The map $I : A \to A$ with $I(a) = a$ is the identity element because I is bijective and for all $\varphi \in S_A$,

$$(I \circ \varphi)(a) = I(\varphi(a)) = \varphi(a) \quad \text{and} \quad (\varphi \circ I)(a) = \varphi(I(a)) = \varphi(a)$$

(Inverse.) For each $\varphi \in S_A$ consider the map $\varphi^{-1} : A \to A$ with SOMETHING. $\square$

Definition 9.4. When $A = \{1, \dots, n\}$ with $n \geq 1$, the set S_A is denoted by S_n. This is called the symmetric group of n elements.

9.1 Cycle Notation for Permutations

A permutation $\sigma : A \to A$ is a bijection, so it can be viewed simply as a relabelling of the elements in A. This suggests a more compact notation, called the cycle notation,

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

where the top row is the input and the bottom row contains its corresponding output; each column should be read as $a \mapsto \sigma(a)$. By convention, we keep the elements of the top row (input) sorted in ascending order.

Composition of permutations can also be carried out in this notation. We present this with an example.

Example 9.5. Consider $\sigma, \rho \in S_4$ given as

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}, \quad \rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}.$$

Then,

$$\sigma\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}.$$

We compute this by starting at 1 in the input row of the matrix for ρ (recall that the permutation on the right is applied first). We read $\rho(1)$, in this case it is 3. We then locate 3 in the input row of the next permutation (that is σ), and read the corresponding output. In this case, $\sigma(3) = 3$. So, we write 1 under 3 in the final matrix. This process basically computed $\sigma(\rho(1)) = 3$. Next, we focus on 2 in the input row of the matrix for ρ and repeat the full process, obtaining $\sigma(\rho(2)) = 1$.

This process is continued until all entries in the output row of $\sigma\rho$ have been assigned.

The same method can be extended to longer chains of permutations, $\sigma_1\sigma_2\ldots\sigma_k$.

The inverse of a permutation can also be calculated easily in this cycle notation. Given a permutation σ, we simply swap its two rows and then re-arrange the columns so that the top row is in ascending order.

Example 9.6. In order to calculate the inverse of

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

we, firstly, swap the input and output rows

$$\sigma^{-1} = \begin{pmatrix} 2 & 4 & 3 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix},$$

and then sort the columns to get the conventional order for the top row

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}.$$

An even more compact notation can be achieved by omitting the top row (since it is always in the ascending order by convention). The permutation $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{smallmatrix}\right)$ is then written as $\sigma = (2, 4, 3, 1)$. We shall not this notation.

9.2 Symmetric Group S_3

The symmetric groups S_n are non-abelian for $n \geq 3$; we shall later show that S_2 is the same as C_2, the cyclic group of order 2. The order of S_n is $n!$, the number of possible permutations of n distinct elements.

In particular, $|S_3| = 6$. The six elements of S_3 are

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$
$$\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

A simple calculation shows that their orders are

$$O(\sigma_1) = 1, \quad O(\sigma_2) = 3, \quad O(\sigma_3) = 3, \quad O(\sigma_4) = 2, \quad O(\sigma_5) = 2, \quad O(\sigma_6) = 2.$$

Since, S_3 is not abelian, its Cayley table is not symmetric.