Syllabus

B.Sc. I Year Second Semester

(First Week) Groups, Subgroups and their examples, the group $\mathbb{Z}_n$ of integers under addition modulo n, The group $U(n)$ of units under multiplication modulo n,
(Second Week)Cyclic groups, complex roots of unity, circle group, the general linear group $GL_n(n, R)$, Dihedral group. The commutator subgroup, Examples of subgroups including the center of a group, Cosets, Index of subgroup, Lagrange Theorem, order of an element. Normal subgroups: their definition, examples, and characterizations, Quotient groups, Class equations.

Books Recommended

1. John B. Fraleigh, A First Course in Abstract Algebra, 7th Ed., Pearson, 2002.
2. M. Artin, Abstract Algebra, 2nd Ed., Pearson, 2011.
3. Joseph A Gallian, Contemporary Abstract Algebra, 4th Ed., Narosa, 1999.
4. I. Herrnstein, Topics in Algebra, 2nd ed., John Wiley, 1999

M.Sc. First Year Second Semester

Review: Group, Subgroups, Normal subgroups, Lagrange Theorem, Isomorphism Theorems, Cayleys Theorem, Class Equation, Sylow's Theorems. (15 Lectures)

Ring Theory: Rings, Examples (including formal power series ring and matrix ring), Sub-ring, Ideals, Prime and Maximal Ideals, Rings of Fractions, Integral domains, Homomorphism of Rings and its basic theorems. Polynomial Rings, Gaussian Rings, Euclidean Domains, Principal Ideal Domains and Unique Factorizations, Gauss Lemma, Irreducibility Criteria. (25 Lectures)

Field Theory: Field, Field extension, Algebraic extension, Finite fields. (15 Lectures)

Books Recommended

[1] I. Herrnstein, Topics in Algebra, 2nd ed., John Wiley, 1999

[2] D. S. Dummit, R. M. Foote, Abstract Algebra, 3rd edition, Wiley India. 2014.

[3] J. B. Fralieigh, A first course in abstract algebra, 5th ed., Addison-Wesley, 1994.

[4] Michael Artin, Algebra, Prentice Hall of India (1991).

[5] Serge Lang, Algebra, revised 3 rd edition, Springer (2004).

[6] J. A. Gallian, Contemporary Abstract Algebra, Narosa.

Contents

Syllabus i

B.Sc. I Year Second Semester i

M.Sc. First Year Second Semester i

Chapter 1. Some Preliminaries 1

1. Intoduction to Set Thoery 1
2. Algebra of Sets 1
3. The integers modulo n 1
4. Algebra of $\mathbb{Z}/n\mathbb{Z}$ 3
5. A subset of $\mathbb{Z}/n\mathbb{Z}$ 3

Chapter 2. Introduction to Groups 5

1. Basics 5
2. Group 6

Exercises 6

3. Properties 7
4. More Examples 8

Exercises 9

5. Properties of Groups 12

Exercises 12

12

Chapter 3. Finite Groups 13

1. Subgroups 13
2. Cyclic Groups 13
3. Cosets 13

Chapter 4. Normal subgroups 15

1. Normal subgroups 15
2. Quotient groups 15

Chapter 5. Class equations 17

Chapter 1

Some Preliminaries

1. Intoduction to Set Thoery

Definition 1.1. A well defined collection of objects is called set.

Here 'Well defined' removes any ambiguity in process of selection of objects to make a set.

2. Algebra of Sets

.

Union
Intersection
Complement with respect to a set (Difference)
Complement with respect to universe
Cross Product
Relations
Equivalence Relations

3. The integers modulo n

Let n be a fixed integer. Define a relation on $\mathbb{Z}$ by

$$a \sim b \iff n|(b-a)$$

This relation is called as *congruence relation*. We read it as: a is congruent to b modulo n. We also write this as

$$a \equiv b \pmod{n}$$

Example 3.1. $5 \sim 15$ *for* $n = 5$ *as* $5|(15-5)$. *So, 5 is congruent to 15 modulo 5. Think when* $n = 3$. *5 is not congruent to 15 modulo 3.*

Example 3.2. $42 = 30 \pmod{6}$ *because 42 30 = 12, which is a multiple of 6.*

Theorem 3.3. *Congruence relation is equivalence relation.*

Proof. (1) $a \sim a$ because $n|(a-a)$.

(2)

$$\begin{aligned} a \sim b &\iff n|(b-a) \\ &\iff n|(a-b) \\ &\iff b \sim a \end{aligned}$$

(3)

$$\begin{aligned} a \sim b, b \sim c &\implies n|(b-a) \text{ and } n|(c-b) \\ &\implies n|(a-b)+(c-b) \\ &\implies n|(c-a) \\ &\implies a \sim c \end{aligned}$$

Since all above three properties are satisfied, the relation $\sim$ is an equivalence relation.

□

3.1. Reminders. Finding the remainder is referred to as the modulo operation, and denoted with "mod" .

Example 3.4. *The remainder of the division of 14 by 12 is denoted by* $14 \mod 9$*; as this remainder is 5, so we have*

$$14 \mod 12 = 2.$$

The congruence, indicated by $\equiv$ followed by "(mod)", means that the operator "mod", applied to both side, gives the same result. That is

$$a \equiv b \pmod{n}$$

is equivalent to

$$a \mod n = b \mod n.$$

3.2. Congruence classes. Consider the following set

$$\bar{a} = \{a + kn | k \in \mathbb{Z}\} = \{\dots, a-2n, a-n, a, a+n, a+2n, \dots\}$$

$\bar{a}$ is called equivalence class of a. This set, consisting of the integers congruent to a modulo n, is also called the congruence class or residue class or simply residue of the integer a, modulo n. When the modulus n is known from the context, that residue may also be denoted $[a]$.

Any one of its members may represent each residue class modulo n. Usually, We denote each residue class by the smallest nonnegative integer of that class.

Think about any two integers of different residue classes modulo n. Is there any possibility of being these congruent modulo n to each other? No, never. These are incongruent modulo n. That means, every integer belongs to one and only one residue class modulo n.

Now, think! how many congruence classes are? This depends on n. Think when $n = 2$.

When remainder is 0;

$$\bar{0} = \{\dots, -4, -2, 0, 2, 4, \dots\}$$

When remainder is 1;

$$\bar{1} = \{\dots, -3, -1, 1, 3, \dots\}$$

Note that no other classes are possible. Look carefully that $\bar{2}$ is same as $\bar{0}$ and so on.

In general, There are exactly n distinct equivalence classes modulo n, namely,

$$\bar{0}, \bar{1}, \dots, (n \bar{-} 1)$$

This can be determined by possible remainders after division by n. These residue classes partition the set of integers $\mathbb{Z}$. Here look in above discussion, $\mathbb{Z}$ is partitioned in two parts, the set $\bar{0}$ and $\bar{1}$.

3.3. Integers modulo n.

Definition 3.1. The set of all residue classes of integers for modulo n is called the set of integer modulo n and is denoted by $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}_n$.

The set is defined as follows.

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{a}_n | a \in \mathbb{Z}\}.$$

When $n = 0$, it is same as $\mathbb{Z}$, since $\bar{a_0} = \{a\}$. When $n \neq 0$, it has n elements, and can be written as:

$$\mathbb{Z}/n\mathbb{Z} = \left\{\overline{1}_n, \overline{2}_n, \ldots, \overline{(n-1)}_n\right\}$$

4. Algebra of $\mathbb{Z}/n\mathbb{Z}$

Addition, subtraction, and multiplication on $\mathbb{Z}/n\mathbb{Z}$ are defined by the following rules:

$$\overline{a}_n + \overline{b}_n = \overline{(a+b)}_n \qquad \overline{a}_n - \overline{b}_n = \overline{(a-b)}_n \qquad \overline{a}_n\overline{b}_n = \overline{(ab)}_n.$$

Example 4.1. *Let $n = 12$.*

$$\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$$

Let $\overline{a} = 3$, $\overline{b} = 9$, then $a + b = 3 + 9 = 12$. Take $\mod 12$, that gives $12 \mod 12 = 0 = \overline{a+b}$, i.e.,

$$3 + 9 \equiv 0 \pmod{12}$$

Example 4.2. *From previous example, $3.9 = 27$. On reducing to modulo 12, we get 3, i.e.,*

$$3.9 \equiv 3 \pmod{12}$$

5. A subset of $\mathbb{Z}/n\mathbb{Z}$

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} | \gcd(a, n) = 1\}$$

Tn other words, a has inverse in the set.

Example 5.1.

$$(\mathbb{Z}/n\mathbb{Z})^\times = \left\{ \right\}$$

Introduction to Groups

1. Basics

1.1. Ordered Pair. The ordered collection of n objects denoted as $(a_1, a_2, ..., a_n)$ and is called ordered n-tuple. When we talk about only two objects, we call it ordered pair. i.e. (a, b) is an ordered pair.

Two ordered pair (a, b) and (c, d) are said to equal if and only if $a = c$ and $b = d$. Therefore $(a, b) \neq (b, a)$ unless $a = b$.

1.2. Cartesian Product. Let A and B sets. The cartesian product[1] of A and B, denoted by $A \times B$, is the set of all ordered pairs (a, b) where $a \in A$ and $b \in B$. Mathematically,

$$A \times B = \{(a, b) | a \in A \text{ and } b \in B\}$$

Example 1.1. *The cartesian product of $A = \{1, 2, 3\}$ and $B = \{a, b\}$ is*

$$A \times B = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b), \}$$

1.3. Relation. Let A and B be two nonempty sets. A relation R from A to B is subset of $A \times B$. That is, if $R \subset A \times B$ and $(a, b) \in R$, we say that a is related to b by relation R. We write it as aRb.

Frequently A and B are equal. In this case, we often say that $R \subseteq A \times A$ is a relation on A. (Instead of saying relation from A to A).

1.4. Binary Operations.

Definition 1.1 (Binary Operation)**.** A binary operation on a set G is a rule which assigns each order pair of G an element of G. This rule is well defined, that is, exactly one element is assigned to each possible ordered pair of G. This rule is closed, i.e., for each ordered pair in G, the element assigned is again in G.

The map $* : G \times G \to G$ is a binary operation on G. It is conventional to write $a * b$ in place of $*(a, b)$.

Example 1.2. *Usual addition $+$ is a binary operation on the set $\mathbb{R}$. e.g. consider an ordered pair (2,2.5), addition assigns 4.5 to this ordered pair.*

Example 1.3. *On $\mathbb{Q}^+$, let $a * b := a/b$. Check, here $*$ is a binary operation on $\mathbb{Q}^+$*

[1] Named after Rene Descartes, a Mathematician.

Example 1.4. *On $\mathbb{Q}$, let $a * b := a/b$. Check, here $*$ is not a binary operation on $\mathbb{Q}$. Note that here it is not well defined as there is no number assigned to the ordered pair $(2, 0)$.*

Example 1.5. *On $\mathbb{Z}^+$, let $a * b := a/b$. Check, here $*$ is not a binary operation on $\mathbb{Z}$. Note that here $\mathbb{Z}^+$ is not closed under $*$.*

1.5. Some properties of binary operations.

Definition 1.2. A binary operation $*$ on set G is commutative if $a * b = b * a$ for all $a, b \in G$.

Definition 1.3. A binary operation $*$ on set G is associative if $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$.

2. Group

Definition 2.1. Let G be a set closed under a binary operation $*$. We denote this algebraic structure as $(G, *)$. The algebraic structure $(G, *)$ is a group if the following properties are satisfied.

(1) The operation is associative; that is $\forall a, b, c \in G$, we have
$$a * (b * c) = (a * b) * c$$
(2) There is an element e (called the identity) in G such that $\forall a \in G$
$$e * a = a * e = a$$
(3) There is an element a' corresponding to each element $a \in G$ (called an inverse of a) such that
$$aa' = a'a = e$$

Example 2.1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ *are groups under addition* $(+)$.

Example 2.2. $\mathbb{Z} - \{0\}, \mathbb{Q}^+, \mathbb{R}^+, \mathbb{R} - \{0\}, \mathbb{C} - \{0\}$ *are groups under product* $(\times)$.

Definition 2.2. A group $(G, *)$ is *Abelian* if binary operation $*$ is commutative. That is, if group has the property $ab = ba$ for every pair of elements a and b .

Exercise 2.1. Check previous two examples. Recognize, which are Abelian?

Example 2.3. *Is $(G, *)$ a Abelian group? Where $G := \left\{(x, y, z) \in \mathbb{R}^3\right\}$ Binary operation $*$ is defined as*
$$(x_1, y_1, z_1) + (x_2, y_2, z_2) = (x_1 + x_2, y_1 + y_2, z_1 + z_2)$$

Proof. To Do (Yes! It is Abelian group.) □

Exercises

1. Decide which of the following binary operations are associative and commutative.
   (a) The algebraic structure $(\mathbb{Z}, *)$ where binary operation is defined by $a * b = a - b$
   (b) The algebraic structure $(\mathbb{R}, *)$ where binary operation is defined by $a * b = a + b + ab$
   (c) The algebraic structure $(\mathbb{Q}, *)$ where binary operation is defined by $a * b = \dfrac{a + b}{3}$
   (d) The algebraic structure $(\mathbb{Z} \times \mathbb{Z}, *)$ where binary operation is defined by
   $$(a, b) * (c, d) = (ad + bc, bd)$$
   (e) The algebraic structure $(\mathbb{Z}, *)$ where binary operation is defined by $a * b = a - b$
2. Prove $\forall\, n \in \mathbb{N} > 1$ that $\mathbb{Z}/n\mathbb{Z}$ is not a group under multiplication of residue classes.
3. Verify that each of the following examples are groups under the proposed operation, and calculate the identity and the inverse of a general element.
   (a) The integers $\mathbb{Z}$ under $+$.
   (b) The set $\mathbb{R}^n$ under component-wise addition.

(c) The set of 2×2 matrices with real entries and nonzero determinant under matrix multiplication. This is called the *general linear group in dimension* 2 *over* $\mathbb{R}$ and denoted as $GL_2(\mathbb{R})$ or $GL(2, \mathbb{R})$.

(d) The set of 2×2 matrices of the form $\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$ where a is nonzero and b is arbitrary under matrix multiplication.

3. Properties

Here we denote $a * b$ as ab. If context of binary operation is obvious we will omit the symbol $*$ for convenience

Theorem 3.1. *The identity element of the group is unique.*

Proof. Let e, e' be the two identities in G. Now, if $a \in G$, then

$$a \in G \quad \Rightarrow \quad ae = a \qquad \text{(as } e \text{ is identity)} \tag{1}$$
$$a \in G \quad \Rightarrow \quad ae' = a \qquad \text{(as } e' \text{is identity)} \tag{2}$$

From 1 and 2, we get

$$\begin{aligned} ae &= ae' \\ e &= e' \end{aligned}$$

Hence the identity element in a group is unique. □

Theorem 3.2. *The inverse of each element of the group is unique.*

Proof. Let b, and c be the two inverses of $a \in G$. e is the identity element of the group, then

$$a \in G, b \in G \quad \Rightarrow \quad ab = e \qquad \text{(as } b \text{ is inverse of } a\text{)} \tag{3}$$
$$a \in G, c \in G \quad \Rightarrow \quad ac = e \qquad \text{(as } c \text{is inverse of } a\text{)} \tag{4}$$

From 3 and 4, we get

$$\begin{aligned} ab &= ac \\ b &= c \end{aligned}$$

Hence the inverse element in a group is unique. □

Theorem 3.3. *In group, $(a^{-1})^{-1} = a$.*

Proof. Here, $(a^{-1})^{-1}$ is inverse of a^{-1}, and by definition of inverse, we have

$$a^{-1}(a^{-1})^{-1} = e$$

Multiply both sides by a, we get

$$\begin{aligned} a(a^{-1}(a^{-1})^{-1}) &= ae \\ (aa^{-1})(a^{-1})^{-1} &= a \\ e(a^{-1})^{-1} &= a \\ (a^{-1})^{-1} &= a \end{aligned}$$

Hence. □

Theorem 3.4. *The inverse of the product of two elements of a group G is the product of the inverses tken in reverse order. i.e. $(ab)^{-1} = b^{-1}a^{-1}$.*

Proof. Here $(ab)^{-1}$ is inverse of ab. By definition of inverse, we have

$$\begin{aligned}
\Rightarrow \quad (ab)(ab)^{-1} &= e \\
\Rightarrow \quad a^{-1}(ab)(ab)^{-1} &= a^{-1}e \\
\Rightarrow \quad (a^{-1}a)b(ab)^{-1} &= a^{-1} \\
\Rightarrow \quad eb(ab)^{-1} &= a^{-1} \\
\Rightarrow \quad b(ab)^{-1} &= a^{-1} \\
\Rightarrow \quad b^{-1}b(ab)^{-1} &= b^{-1}a^{-1} \\
\Rightarrow \quad e(ab)^{-1} &= b^{-1}a^{-1} \\
\Rightarrow \quad (ab)^{-1} &= b^{-1}a^{-1}
\end{aligned}$$

Hence $(ab)^{-1} = b^{-1}a^{-1}$. □

Theorem 3.5. *In a group left and right cancellation laws hold.*
Left cancellation law: if $au = av \implies u = v$
Right cancellation law: if $ub = vb \implies u = v$

Proof. Suppose $au = av$. Then Apply a^{-1} on both side in left. Then check every step. Each step is based on some axiom of group.

$$a^{-1}(au) = a^{-1}(av)$$
$$(a^{-1}a)u = (a^{-1}a)v$$
$$(e)u = (e)v$$
$$u = v$$

Do other part yourself. □

Theorem 3.6. *Let G be a group then the equations $ax = b$ and $ya = b$ have unique solutions, x, y, where $a, b, x, y \in G$.*

Proof. Left as an exercise. □

Example 3.7 (The group Z_n of integers under addition modulo n)**.** *For each integer $n \geq 2$ define the set*

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}.$$

For all $a, b \in \mathbb{Z}_n$ let

$a + b =$ remainder when the ordinary sum of a and b is divided by n, and

$a \cdot b =$ remainder when the ordinary product of a and b is divided by n.

The binary operations defined in Example 3.7 are usually referred to as **addition modulo** n and **multiplication modulo** n. The integer n in $\mathbb{Z}_n$ is called the **modulus**. The plural of modulus is **moduli**.

4. More Examples

4.1. The group U(n) of units under multiplication modulo n.

Definition 4.1. Let $n \geq 2$. An element $a \in \mathbb{Z}_n$ is said to be a *unit* if there is an element $b \in \mathbb{Z}_n$ such that $ab = 1$. Here the product is multiplication modulo n. We denote the set of all units in $\mathbb{Z}_n$ by U_n.

Theorem 4.1. *U_n is a group under multiplication modulo n.*

We call U_n the **group of units of** $\mathbb{Z}_n$.

Theorem 4.2. *For $n \geq 2$, $U_n = \{a \in \mathbb{Z}_n : \gcd(a, n) = 1\}$.* [2]

Theorem 4.3. *If p is a prime then there is an element $a \in U_p$ such that $U_p = \langle a \rangle$.*

Exercises

1. Prove the easy part of Theorem 4.2; namely, show that if $a \in \mathbb{Z}_n$ and $\gcd(a, n) = d > 1$, then a is not a unit. [Hint: Show (1) that if $a \in \mathbb{Z}_n$ and $\gcd(a, n) = d > 1$ there is an element $b \in \mathbb{Z}_n - \{0\}$ such that $ab = 0$. (2) If $b \in \mathbb{Z}_n - \{0\}$ and $ab = 0$ then a is not a unit.]
2. Demonstrate Theorem 4.3 for all primes $p < 12$.

4.2. Dihedral Groups.

The dihedral group D_n is the symmetry group of a regular n-sided polygon. Generated by a rotation r of $2\pi/n$ radians and by a mirroring operation s, there are $2n$ elements in the group D_n:

$$D_n = \{e, r, r^2, ..., r^{n-1}, s, rs, ..., r^{n-1}s\} \tag{5}$$

The largest (proper) subgroup of a dihedral group D_n is of course the group generated by just r, the cyclic group C_n, of index 2 inside D_n.

Example 4.4. Let T be an equilateral triangle with sides A, B, C opposite vertices a, b, c in anticlockwise order. The symmetries of T are the reflections in the lines running from the corners to the midpoints of opposite sides, and the rotations. There are three possible rotations, through anticlockwise angles $0, 2\pi/3, 4\pi/3$ which can be thought of as e, ω, ω^2. Observe that $\omega^{-1} = \omega^2$. Let r_a be a reflection through the line from the vertex a to the midpoint of A. Then $r_a = r_a^{-1}$ and similarly for r_b, r_c. Then $\omega^{-1} r_a \omega = r_c$ but $r_a \omega^{-1} \omega = r_a$ so this group is *not commutative.* It is callec the *dihedral group* D_3 and has 6 elements.

Figure 1. The composition $\omega^{-1} r_a \omega = r_c$, but $r_a \omega^{-1} \omega = r_a$, so D_3 is not commutative.

Example 4.5. If P is an equilateral n–gon, the symmetries are reflections as above and rotations. This is called the *dihedral group* D_n and has $2n$ elements. The elements are $e, \omega, \omega^2, \ldots, \omega^{n-1} = \omega^{-1}$ and $r_1, r_2, \ldots, r_n$ where $r_i^2 = e$ for all i, $r_i r_j = \omega^{2(i-j)}$ and $\omega^{-1} r_i \omega = r_{i-1}$.

Example 4.6. The symmetries of an "equilateral ∞–gon" (i.e. the unique infinite 2–valent tree) defines a group D_∞, the *infinite dihedral group.*

4.3. Generators and Relations*.

4.4. Permutation Groups*.

Definition 4.2. A function $f : X \to Y$ is *injective* if for every $x_1, x_2 \in X$, when $f(x_1) = f(x_2)$, $x_1 = x_2$. A function $f : X \to Y$ is *surjective* if for every $y \in Y$, there exists an $x \in X$ such that $f(x) = y$. A function $f : \to Y$ is *bijective* if it is both injective and surjective.

Definition 4.3. A function is a *permutation* if it is a bijection onto itself $f : X \to X$. Notation: $X = \{1, 2, ...n\}$. $\alpha = \begin{pmatrix} 1 & 2 & ... & n \\ \alpha(1) & \alpha(2) & ... & \alpha(n) \end{pmatrix}$.

[2] (Number Thoery) The order of the group U_n is denoted by $\phi(n)$, is called the *Euler totient function* and is pronounced *fee of n*. If a and b are positive integers such that $\gcd(a, b) = 1$ then $\phi(ab) = \phi(a)\phi(b)$ and if p is prime and $n \in \mathbb{N}$ then $\phi(p^n) = p^n - p^{n-1}$. These facts make it easy to compute $\phi(n)$ if one can write n as a product of primes. But there is no known easy way to compute $\phi(n)$ if the factorization of n is unknown.

Definition 4.4. S_n is the group of permutations called the *symmetric group.*

Example 4.7. *Suppose* $X = \{1, 2, 3, 4\}$ *and* $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$.

$\alpha \in S_4$*, the set of permutations on* X*, and* $\alpha(1) = 3, \alpha(2) = 1, \alpha(3) = 4, \alpha(4) = 2$.

Suppose $X = \{1, 2, 3, 4\}$ *and* $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$.

$\beta \in S_4$ *as well.*

Composing $\alpha \circ \beta(1)$*, we get* $\alpha(2) = 1$.

Example 4.8. *Let* $X = \{1, 2, 3\}$*. We list the elements of* S_3*:*

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

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

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

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

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

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

Example 4.9. *Consider the Dihedral Group,* D_4.

The identity is $I = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$

A rotation of 90-degrees would be: $R_{90} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$

We can do this for the other rotations and flips about various axes too: $R_{180}, R_{270}, H, V, D_1, D_2$.

Definition 4.5. If $\alpha \in S_n$ and $i \in \{1, 2, ..., n\}$, then α *fixes* i if $\alpha(i) = i$. α *moves* i if $\alpha(i) \neq i$.

Definition 4.6. Let $i_1, i_2, ..., i_r$ be elements in $X = \{1, 2, ..., n\}$. If $\alpha \in S_n$ fixes the other integers, and if $\alpha(i_1) = i_2, \alpha(i_2) = i_3, ..., \alpha(i_{r-1}) = i_n$ and $\alpha(i_r) = i_1$, then α is called an *r-cycle.* A 2-cycle is called a *transposition.* A 1-cycle is just the *identity.*

Example 4.10. $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 4 & 5 & 2 & 3 \end{pmatrix}$

Example 4.11. $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 4 \end{pmatrix} \begin{pmatrix} 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$

Example 4.12. *Write as a product of disjoint cycles.* $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 4 & 7 & 2 & 5 & 1 & 8 & 9 & 3 \end{pmatrix}$

$= \begin{pmatrix} 1 & 6 \end{pmatrix} \begin{pmatrix} 2 & 4 \end{pmatrix} \begin{pmatrix} 3 & 7 & 8 & 9 \end{pmatrix} \begin{pmatrix} 5 \end{pmatrix}$

Example 4.13. *Product of Permutations.* $\alpha = \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 3 & 4 & 2 & 5 \end{pmatrix} \begin{pmatrix} 2 & 5 & 1 & 3 \end{pmatrix}$

We see that:

$1 \to 3 \to 4$

$2 \to 5 \to 1 \to 2$

$3 \to 2 \to 5$

$4 \to 2 \to 1$

$5 \to 1 \to 3$

So we have: $= \begin{pmatrix} 1 & 4 \end{pmatrix} \begin{pmatrix} 2 \end{pmatrix} \begin{pmatrix} 3 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 4 \end{pmatrix} \begin{pmatrix} 3 & 5 \end{pmatrix}$

Definition 4.7. Two cycles $\alpha = (a_1 a_2 ... a_m)$ and $\beta = (b_1 b_2 ... b_m)$ are disjoint if $a_i \neq b_j$ for all i, j.[3]

Lemma 4.14. *Disjoint cycles* $\alpha, \beta \in S_n$ *commute.*

Notation 4.15. Every permutation is a product of disjoint cycles.

Theorem 4.16. (1) *The inverse of* $(i_1, i_2, ..., i_r)$ *is the r-cycle* $(i_r, i_{r-1}, ..., 1)$.
(2) *If* $\alpha = \beta_1 \beta_2 ... \beta_t$ *is a product of disjoint cycles, then* $\alpha^{-1} = \beta_1^{-1} \beta_2^{-1} ... \beta_t^{-1}$.

Proof. (1) Consider

$$(i_1, i_2, ..., i_r)(i_r, i_{r-1}, ..., 1).$$

We see that:
$i_1 \to i_r \to i_1$
$i_2 \to i_1 \to i_2$
...
$i_{r-1} \to i_{r-2} \to i_{r-1}$
$i_r \to i_{r-1} \to i_r$
So $(i_1, i_2, ..., i_r)(i_r, i_{r-1}, ..., 1) = (1)$
Similarly, $(i_r, i_{r-1}, ..., 1)(i_1, i_2, ..., i_r) = (1)$.

(2) Consider $(\beta_1 \beta_2 ... \beta_t)(\beta_t^{-1} \beta_{t-1}^{-1} ... \beta_1^{-1})$.
We see that $\beta_t \beta_t^{-1} = 1, \beta_{t-1} \beta_{t-1}^{-1} = 1$ and so on. Thus we have 1.
Similarly, $(\beta_t^{-1} \beta_{t-1}^{-1} ... \beta_1^{-1})(\beta_1 \beta_2 ... \beta_t) = 1$.
Since $\alpha = \beta_1 \beta_2 ... \beta_t$, then $\alpha^{-1} = \beta_t^{-1} \beta_{t-1}^{-1} ... \beta_1^{-1}$. From the Lemma, we know that $\alpha^{-1} = \beta_1^{-1} \beta_2^{-1} ... \beta_t^{-1}$.

□

Notation 4.17. If $n \geq 2$, then every $\alpha \in S_n$ is a product of transpositions. To check this, consider:

$\begin{pmatrix} 1 & 2 & ... & r \end{pmatrix} = \begin{pmatrix} 1 & r \end{pmatrix} \begin{pmatrix} 1 & r-1 \end{pmatrix} ... \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 \end{pmatrix}$

We see that:

$1 \to 2$

$2 \to 1 \to 3$

$3 \to 1 \to 4$

...

$r - 1 \to 1 \to r$

Definition 4.8. A permutation is *even* if it can be factored into a product of an even number of transpositions; otherwise, it is *odd*. The *parity* of a permutation is whether it is even or odd.

Example 4.18. $\alpha = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 \end{pmatrix}$ *So it is even.*

4.5. The general linear group GLn (n,R).

[3] Due to some confusion during the lecture, this definition was later added to these notes and is from Durbin's *Modern Algebra*, Fifth Edition.

4.6. Quaternion Group*.

The *quaternion group* is defined by

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

with product computed as following group table.

$\cdot$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	1	-1	k	$-k$	$-j$	j
$-i$	$-i$	i	-1	1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	1	-1	i	$-i$
$-j$	$-j$	j	k	$-k$	-1	1	$-i$	i
k	k	$-k$	j	$-j$	$-j$	j	1	-1
$-k$	$-k$	k	$-j$	j	j	$-j$	-1	1

5. Properties of Groups

Exercises

1. Compute the order of each elements in Q_8.
2. Find generators and relations for Q_8.

Verify that each of the following examples are groups under the proposed operation, and calculate the identity and the inverse of a general element.

1. The group of *integers modulo* n under $+$. These are the sets of equivalence classes of integers, where $a \sim b$ if and only if $a - b$ is divisible by n. This group is denoted $\mathbb{Z}/n\mathbb{Z}$.
2. The set of 2×2 matrices with entries in $\mathbb{Z}/2\mathbb{Z}$ (i.e. "even" and "odd") with the usual rules of multiplication and addition for even and odd numbers, with odd determinant, under matrix multiplication. This group is denoted $GL_2(\mathbb{Z}/2\mathbb{Z})$.
3. The group of permutations of n objects (which might as well be the set $\{1, \ldots, n\}$) under composition. This group is called the *symmetric group* S_n.
4. The group of symmetries of a regular n–gon under composition. This group is called the *dihedral group* D_n.
5. For an arbitrary set X, the group of 1–1 and invertible maps $X \to X$ under composition is a group. This group is called the *symmetric group of* X and denoted S_X.
6. For all integers $n \geq 1$, the set of complex nth roots of unity
$$\left\{\cos\frac{2k\pi}{n} + \sin\frac{2k\pi}{n} | k = 0, 1, 2, \ldots, n-1\right\}$$
is a group under multiplication.

   MORE: Gallian ex 17-21/p47 (Assignment M.Sc.)

Chapter 3

Finite Groups

1. Subgroups

2. Cyclic Groups

–complex roots of unity, circle group The commutator subgroup, Center of a group,

3. Cosets

Index of subgroup, Lagranges theorem, order of an element.

Chapter 4

Normal subgroups

1. Normal subgroups

?characterizations

2. Quotient groups

,

Chapter 5

Class equations