NOTES ON GROUP THEORY

Abstract. These are the notes prepared for the course MTH 751 to be offered to the PhD students at IIT Kanpur.

Contents

1. Binary Structure	2
2. Group Structure	5
3. Group Actions	13
4. Fundamental Theorem of Group Actions	15
5. Applications	17
5.1. A Theorem of Lagrange	17
5.2. A Counting Principle	17
5.3. Cayley's Theorem	18
5.4. The Class Equation	18
5.5. Cauchy's Theorem	19
5.6. First Sylow Theorem	21
5.7. Second Sylow Theorem	21
5.8. Third Sylow Theorem	22
6. Structure Theorem for Finite Abelian Groups	24
References	26

1. BINARY STRUCTURE

Let S be a set. We denote by $S \times S$ the set of ordered pairs (a, b), where $a, b \in S$. Thus the ordered pairs (a, b) and (b, a) represent distinct elements of $S \times S$ unless a = b.

A binary operation \star on S is a function from $S \times S$ into S. Thus for every $(a, b) \in S \times S$, the binary operation \star assigns a unique element $a \star b$ of S. If this happens, then we say that the pair (S, \star) is a binary structure.

Let us understand the above notion through examples.

Example 1.1: We follow the standard notations to denote the set of natural numbers, integers, rationals, reals, complex numbers by $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ respectively. If S is one of the sets above, then S^* stands for $S \setminus \{0\}$.

- (1) Addition (resp. multiplication) is a binary operation on \mathbb{Z} (resp. \mathbb{Q}).
- (2) Division is *not* a binary operation on \mathbb{Z}^* .
- (3) Subtraction is a binary operation on \mathbb{Z} but not on \mathbb{N} .
- (4) Division is a binary operation on \mathbb{R}^* (resp. \mathbb{C}^*).

As seen in (3), it may happen that $a \star b \notin A$ for some $a, b \in A$.

Let (S, \star) be a binary structure. Let A be a subset of a set S. We say that \star is an *induced binary operation on* A if $a \star b \in A$ for every $a, b \in A$.

Exercise 1.2: Let \mathbb{O} denote the set of odd integers. Verify that the multiplication on \mathbb{Z} is an induced binary operation on \mathbb{O} , however, addition is not so.

Let us see some geometric examples of binary structures.

Example 1.3 : Let \mathbb{T} denote the unit circle. Consider the binary operation \cdot of multiplication from $\mathbb{T} \times \mathbb{T}$ into \mathbb{T} . Note that the action

$$(1.1) (z,w) \longrightarrow z \cdot w$$

can be interpreted as rotation of z about the origin through the angle $\arg(w)$ in the anticlockwise direction.

As an another interesting example of a binary operation, consider the binary operation \cdot of multiplication on an annulus centered at the origin. One may use the polar co-ordinates to interpret the action (0.1) as rotation of z about the origin through the angle $\arg(w)$ in the anticlockwise direction followed by a dilation of magnitude |w|.

Exercise 1.4: Let A(r, R) denote the annulus centered at the origin with inner radius r and outer radius R, where $0 \le r < R \le \infty$. Find all values of r and R for which $(A(r, R), \cdot)$ is a binary structure.

Hint. If r < 1 then r = 0 (Use: $r < \sqrt{r}$ if 0 < r < 1). If R > 1 then $R = \infty$ (Use: $\sqrt{R} < R$ if $1 < R < \infty$).

Exercise 1.5: Let L denote a line passing through the origin in the complex plane. Verify that the multiplication \cdot on the plane is not an induced binary operation on L.

A binary structure (S, \star) is associative if $x \star (y \star z) = (x \star y) \star z$ for every $x, y, z \in S$. We say that (S, \star) is abelian if $x \star y = y \star x$ for every $x, y \in S$.

Exercise 1.6: Let $M_n(\mathbb{R})$ denote the set of $n \times n$ matrices with real entries. Verify that the matrix multiplication \circ is a binary operation on $M_n(\mathbb{R})$. Verify further the following:

- (1) \circ is associative.
- (2) \circ is abelian iff n = 1.

Let (S, \star) be a binary structure. We say that $e \in S$ is identity for S if $e \star s = s = s \star e$ for every $s \in S$.

In general, (S, \star) may not have an identity. For example, the infinite interval $(1, \infty)$ with multiplication is a binary structure without identity.

Proposition 1.7. Identity of a binary structure, if exists, is unique.

Proof. The proof is a subtle usage of the definition of the binary operation. Suppose (S, \star) has two identities e and e'. By the very definition of the binary operation, the pair (e, e') assigned to a *unique* element $e \star e'$. However, $e \star e'$ equals e if e' is treated as identity, and e' if e is treated as identity. Thus we obtain e' = e as desired.

Before we discuss the isomorphism between two binary structures, it is necessary to recall the notion of isomorphism between sets. We say that two sets S and T are *isomorphic* if there exists a bijection ϕ from S onto T. Recall that \mathbb{Z} and \mathbb{Q} are isomorphic.

We say that two binary structures (S, \star) and (T, \star) are *isomorphic* if there exists a bijection $\phi: S \to T$, which preserves the binary operations:

 $\phi(a \star b) = \phi(a) \star \phi(b)$ for all $a, b \in S$.

We will refer to ϕ as the *isomorphism* between (S, \star) and (T, *).

Remark 1.8 : The set-theoretic inverse ϕ^{-1} of ϕ is an isomorphism between (T, *) and (S, \star) .

It is not always easy to decide whether or not given binary structures are isomorphic. The following two tests are quite handy for this purpose.

Exercise 1.9 : Suppose the binary structures (S, \star) and (T, \star) are isomorphic. Show that if (S, \star) is abelian (resp. associative) then so is (T, \star) .

Note that the binary structures (\mathbb{R}, \cdot) and $(M_2(\mathbb{R}), \circ)$ are not isomorphic.

Proposition 1.10. Suppose there exists an isomorphism ϕ between the binary structures (S, \star) and (T, \star) . Fix $a \in S$. Then the following is true:

NOTES ON GROUP THEORY

- (1) The equation $x \star x = b$ has a solution in S iff the equation $x \star x = \phi(b)$ has a solution in T.
- (2) There exists a bijection from the solution set S of $x \star x = b$ onto the solution set T of $x \star x = \phi(b)$.

Proof. If $x_0 \in S$ is a solution of the equation $x \star x = b$ then $\phi(x_0) \in T$ is a solution of the equation $x \star x = \phi(b)$. The converse follows from Remark 1.8. Since $\phi : S \to T$ given by $\Phi(x_0) = \phi(x_0)$ is a bijection, the remaining part follows.

Example 1.11 : Consider the binary structures $(\mathbb{Z}, +)$ and $(\mathbb{Q}, +)$. We already recorded that \mathbb{Z} and \mathbb{Q} are isomorphic. The natural question arises whether $(\mathbb{Z}, +)$ and $(\mathbb{Q}, +)$ are isomorphic ?

Let us examine the equation x + x = 1. Note that the solution set of x + x = 1 in \mathbb{Z} is empty. On the other hand, the solution set of x + x = 1 in \mathbb{Q} equals $\{1/2\}$. By Proposition 1.10, the binary structures $(\mathbb{Z}, +)$ and $(\mathbb{Q}, +)$ can never be isomorphic.

Exercise 1.12 : Whether the following binary structures are isomorphic. Justify your answer.

- (1) $(\mathbb{Z}, +)$ and $(\mathbb{N}, +)$.
- (2) (\mathbb{C}, \cdot) and (\mathbb{R}, \cdot) .

4

(3) (\mathbb{C}, \cdot) and (\mathbb{C}^*, \cdot) .

Exercise 1.13 : Consider \mathbb{C}^* and \mathbb{T} as topological spaces with the topology inherited from the complex plane. Show that there does not exist a continuous isomorphism from (\mathbb{C}^*, \cdot) onto (\mathbb{T}, \cdot) .

In view of the last exercise, one may ask: Is it true that (\mathbb{C}^*, \cdot) and (\mathbb{T}, \cdot) are isomorphic? The answer is No (refer to [2]).

Exercise 1.14 : Show that there exists no isomorphism ϕ between the binary structures $(M_2(\mathbb{R}), \circ)$ and $(M_3(\mathbb{R}), \circ)$ such that $\phi(I) = I$.

Hint. Consider the equation $A^2 = I$ for invertible solutions A.

Recall that a matrix $A \in M_n(\mathbb{R})$ is orthogonal if $A^t A = I$. Note that $A \in M_n(\mathbb{R})$ is orthogonal if and only if A preserves the euclidean distance, that is, $||AX - AY||_2 = ||X - Y||_2$ for every $X, Y \in \mathbb{R}^n$, where $|| \cdot ||_2$ denotes the euclidean norm on \mathbb{R}^n .

Exercise 1.15: Prove that any orthogonal matrix in $M_2(\mathbb{R})$ is either a rotation R_{θ} about the origin with angle of rotation θ or a reflection ρ_{θ} about the line passing through origin making an angle $\theta/2$, where

(1.2)
$$R_{\theta} = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}, \ \rho_{\theta} = \begin{pmatrix} \cos \theta & \sin \theta \\ \sin \theta & -\cos \theta \end{pmatrix}$$

Hint. Any unit vector in \mathbb{R}^2 is of the form $(\sin \theta, \cos \theta)$ for some $\theta \in \mathbb{R}$.

Here is an example of geometric nature.

Example 1.16 : Let Δ denote an equilateral triangle in the plane with origin as the centroid. For example, one may take triangle with vertices $(1,0), (-1/2, \sqrt{3}/2), (-1/2, -\sqrt{3}/2)$. By symmetry of Δ , we understand orthogonal 2×2 matrix A in $M_2(\mathbb{R})$ such that $A(\Delta) = \Delta$. Consider the set S_3 all symmetries of Δ . It is easy to see that (S_3, \circ) is a binary structure.

To understand this binary structure, we need a bit of plane geometry. By Exercise 1.15, any element of S_3 is a composition of rotations about the origin and reflections about a line passing through origin. Since Δ is an equilateral triangle with centroid 0, a rotation belongs to S if and only if the angle of rotation is either $2/3\pi, 4/3\pi, 2\pi$. Similarly, since the axes of symmetry of Δ are precisely the lines passing through the origin and mid-point of sides of Δ , a reflection belongs to S_3 if and only if the line of reflection is one of the axes of symmetry of Δ . It follows that S_3 consists exactly six elements; 3 rotations and 3 reflections.

Exercise 1.17 : Describe all symmetries of a regular polygon in the plane with origin as the centroid.

2. Group Structure

In the last section, we discussed many examples of binary structures (S, \star) . We also observed that there are some "distinguished" binary structures, namely, unital pairs (S, \star) for which the binary operation is associative. It is desirable to pay more attention to such structures. An axiomatic approach is often convenient for such studies.

Definition 2.1 : A binary structure (G, \star) is a group if

- (1) (Associativity) For all $a, b, c \in G$, we have $(a \star b) \star c = a \star (b \star c)$.
- (2) (Existence of Identity) There exists $e \in G$ such that $e \star a = a = a \star e$ for all $a \in G$.
- (3) (Existence of Inverse) For all $a \in G$, there exists $a^{-1} \in G$ (depending, of course, on a) such that $a \star a^{-1} = e = a^{-1} \star a$.

We say that a group structure (G, \star) is abelian if

(4) (Commutativity) For all $a, b \in G$, we have $a \star b = b \star a$.

Remark 2.2: Note that the inverse of the identity is the identity itself.

If there is no confusion, we will suppress the binary operation \star . Note that $(\mathbb{R}, +)$ and (\mathbb{R}^*, \cdot) are group structures.

Example 2.3 : For a positive number c, consider the open interval G = (-c, c) of real numbers. For $x, y \in G$, define

$$x \star y := \frac{x+y}{1+xy/c^2}.$$

Notice that $1 + xy/c^2 > 0$ for any $x, y \in G$, so that $x \star y \in \mathbb{R}$. To see that \star is a binary operation, we should check that $-c < x \star y < c$ if -c < x, y < c. Note that $|x \circ y| < c$ iff $c|x + y| < c^2 + xy$. If $x + y \ge 0$ then by $|x \circ y| < c$ iff (c - x)(c - y) > 0. Similarly, one can treat the case x + y < 0.

Clearly, 0 is the identity for G and the inverse of x is -x. It is easy to see that \star is associative and commutative. Thus (G, \star) is an abelian group structure. This example arises in Special Relativity.

Note that (\mathbb{C}^*, \cdot) is a group structure.

Example 2.4: For a positive integer n, let \mathbb{I}_n denote the set of n^{th} roots of unity:

(2.3)
$$\mathbb{I}_n := \{ \zeta \in \mathbb{C} : \zeta^n = 1 \}.$$

By the fundamental theorem of algebra, \mathbb{I}_n consists of exactly *n* elements including 1. Geometrically, \mathbb{I}_n consists of the vertices of the regular polygon with *n* edges and with centroid the origin.

The binary structure (\mathbb{I}_n, \cdot) is indeed a group structure. To see this, note first that $\mathbb{I}_n \subseteq \mathbb{C}^*$. Now $\zeta \in \mathbb{I}_n$ admits the inverse $1/\zeta$. Associativity and commutativity of \mathbb{I}_n follows from that of \mathbb{C}^* .

Exercise 2.5: Let $\mathbb{I} := \bigcup_{n \ge 1} \mathbb{I}_n$. Show that (\mathbb{I}, \cdot) is a group structure.

Exercise 2.6 : Fill in the blanks and justify:

- (1) Let $\mathbb{A}(r, R)$ denote the annulus of inner-radius r and outer-radius R with the assumption that $0 \leq r < R \leq \infty$. Then the binary structure $(\mathbb{A}(r, R), \cdot)$ is a group structure if and only if $r = \cdots$ and $R = \cdots$.
- (2) Let X be a subset of the group structure (\mathbb{C}^*, \cdot) . Let \mathbb{S}_X denote the set of $n \times n$ matrices $A \in M_n(\mathbb{C})$ such that the determinant det(A) of A belongs to X. Then (\mathbb{S}_X, \circ) is a \cdots structure if and only if (X, \cdot) is a \cdots structure.
- (3) Let X be a set containing at least two elements and let P(X) denote the power set of X. Define $A \star B$ (resp. $A \star B$) be the symmetric difference (resp. difference) of A and B. Then $(P(X), \star)$ (resp. $(P(X), \star)$) is a \cdots structure but not a \cdots structure.

The following summarizes some elementary properties of the group.

Proposition 2.7. Let G be a group. Every element of G has a unique inverse. More generally, for $a, b, c \in G$ the following statements hold: If ab = ac then b = c, and if ba = ca then b = c. In particular, the inverse of $a \star b$ is given by $b^{-1}a^{-1}$.

Proof. We will only prove that if ab = ac then b = c. Here inverse a^{-1} of a works as a *catalyst*. By the definition of binary operation, $a^{-1}(ab)$ and $a^{-1}(ac)$ define the same element of G. The desired conclusion now follows from the associativity of G.

Let us see a couple of applications of the last innocent result.

Exercise 2.8: Let G be a group and let $a \in G$. By a^2 , we understand aa. Inductively, we define a^n for all positive integers $n \ge 2$. Show that $(ab)^n = a^n b^n$ for all $a, b \in G$ if and only if G is abelian.

Exercise 2.9: Let G be a group. Show that if G is non-abelian then G contains at least 5 elements.

Hint. Observe that there exists $x, y \in G$ such that e, x, y, xy, yx are distinct elements of G.

Remark 2.10 : A rather extensive usage of Proposition 2.7 actually shows that a non-abelian group can not contain 5 elements. We will however deduce this fact later from a general result.

Example 2.11 : For a positive integer $n \ge 3$, consider the binary structure D_n of all symmetries of a regular *n*-gon with origin as the centroid. As in Example 1.16, it can be seen that D_n consists of rotations R_{θ} ($\theta = 0, 2\pi/n, \dots, 2\pi(n-1)/n$) and reflections ρ_{θ} ($\theta = 2\pi/n, 4\pi/n, \dots, 2\pi$)(see (1.2)). Clearly, the rotation by 0, the 2 × 2 identity matrix, plays the role of identity for D_n . Either geometrically or algebraically, observe the following:

(1)
$$R^n_{\theta} = R_0 = \rho^2_{\theta}$$
.

(2) $R_{\theta}\rho_{\eta}R_{\theta} = \rho_{\eta}.$

In particular, the inverse of R_{θ} is R_{θ}^{n-1} and the inverse of ρ_{θ} is ρ_{θ} itself. Thus (D_n, \circ) forms group structure, which is not abelian.

Remark 2.12 : (D_3, \circ) is the smallest non-abelian group structure.

Exercise 2.13 : Let A be a set and let P_A be the set of bijections $f : A \to A$. Show that (S_A, \circ) is a group structure.

Example 2.14 : For a positive integer n, let A denote the set $\{1, \dots, n\}$. Set $S_n := S_A$. The group structure (S_n, \circ) is known as the symmetric group. Note that S_n contains n! elements.

A transformation ϕ between two group structures (G, \star) and (G', \star) is said to be a group homomorphism if ϕ preserves the group operations: $\phi(a \star b) = \phi(a) \star \phi(b)$ for all $a, b \in G$. We say that (G, \star) and (G', \star) are *isomorphic* if there exists a bijective homomorphism ϕ (known as *isomorphism*) between (G, \star) and (G', \star) .

Remark 2.15: Let e and e' denote the identities of G and G' respectively. Let $\phi: G \to G'$ be a homomorphism.

(1) Then $\phi(e) = e'$. This follows from Proposition 2.7 in view of

$$\phi(e) * e' = \phi(e) = \phi(e \star e) = \phi(e) * \phi(e).$$

(2) By uniqueness of inverse, for any $a \in G$, the inverse of $\phi(a)$ is $\phi(a^{-1})$.

Again, whenever there is no confusion, we suppress the symbols \star and \star .

Example 2.16 : Let m, n be positive integers such that $m \leq n$. Define $\phi: S_m \to S_n$ by $\phi(\alpha) = \alpha(m+1)(m+2)\cdots(n)$ ($\alpha \in S_m$). Then ϕ is an injective, group homomorphism. Thus ϕ is an isomorphism iff m = n.

Let us verify that S_n is abelian if and only if $n \leq 2$. Clearly, if n = 1, 2 then S_n is abelian. Suppose $n \geq 3$. Since $\phi(S_3) \subseteq S_n$, it suffices to check that S_3 is non-abelian. To see that, consider $\alpha = (1, 2, 3)$ and $\beta = (1, 2)(3)$. Then $\alpha \circ \beta = (1, 3)(2)$ and $\beta \circ \alpha = (1)(2, 3)$.

Example 2.17 : Consider the groups (D_n, \circ) and (S_n, \circ) . Since $|D_n| = 6$ and $|S_n| = n!$, (D_n, \circ) and (S_n, \circ) can not be isomorphic for $n \ge 4$. Suppose n = 3. Define $\phi : D_3 \to S_3$ by setting

$$\phi(R_0) = (1)(2)(3), \phi(R_{2\pi/3}) = (1, 2, 3), \phi(R_{4\pi/3}) = (1, 3, 2), \phi(\rho_{\pi/3}) = (1, 2)(3), \phi(\rho_{2\pi/3}) = (1, 3)(2), \phi(\rho_{\pi}) = (1)(2, 3).$$

Clearly, ϕ is a bijection. Verify that ϕ is a group homomorphism. Likewise one can see that D_n embeds into S_n .

Exercise 2.18 : Let (G_n, \circ) denote the smallest group structure consisting the 2×2 complex matrices

$$F = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ C_k = \begin{pmatrix} e^{\frac{2\pi ki}{n}} & 0 \\ 0 & e^{-\frac{2\pi ki}{n}} \end{pmatrix} \ (k = 0, \cdots, n-1).$$

Show that $\phi: G_n \to D_n$ governed by

$$\phi(F) = \rho_{\pi/n}, \ \phi(C_k) = R_{2\pi k/n} \ (k = 0, \cdots, n-1)$$

defines an isomorphism between G_n and D_n .

Recall that a fractional linear transformation is a rational function $f_{a,b,c,d}$ of the form $\frac{az+b}{cz+d}$, where a, b, c, d are complex numbers such that cz + d is not a multiple of az + b, and $|c| + |d| \neq 0$.

Example 2.19 : Let \mathcal{F} denote the set of all fractional linear transformations. Then (\mathcal{F}, \circ) is a binary structure with identity $f_{1,0,0,1}$. Consider the transformation $\phi : \mathcal{F} \to M_2(\mathbb{C})$ given by

$$\phi(f_{a,b,c,d}) = \left(\begin{array}{cc} a & b \\ c & d \end{array}\right).$$

Verify that ϕ preserves the binary operations. In particular, the common notation \circ employed for both matrix multiplication and composition of functions is fully justified. Since ϕ is not surjective, (\mathcal{F}, \circ) and $(M_2(\mathbb{C}), \circ)$ are not isomorphic.

Let (G, \star) be a group structure and let S be a subset of G. We say that S is a subgroup of G if (S, \star) is a group structure in its own right.

Note that S is a subgroup of G iff

- (1) (Binary Structure) $ab \in S$ for every $a, b \in S$.
- (2) (Existence of Identity) There exists $e' \in S$ such that e'a = a = ae'for all $a \in S$.
- (3) (Existence of Inverse) For all $a \in S$, there exists $a^{-1} \in S$ such that $aa^{-1} = e = a^{-1}a.$

Remark 2.20 : Let *e* denote the identity of *G*. Since e'e' = e' = ee', by Proposition 2.24, we have e' = e.

Exercise 2.21: Let G be a group, $a \in G$, and let H be a subgroup of G. Verify that the following sets are subgroups of G:

- (1) (Normalizer of a) $N(a) = \{g \in G : ag = ga\}.$
- (2) (Center of G) $Z_G = \{a \in G : ag = ga \text{ for all } g \in G\}.$ (3) (Conjugate of H) $aHa^{-1} = \{aha^{-1} : h \in H\}.$

Remark 2.22 : Note that $a \in Z_G$ iff N(a) = G.

A permutation $\alpha \in S_n$ is a *transposition* if either α is the identity permutation or there exist integers i < j such that $\alpha(k) = k$ for $k \neq i, j$ and $\alpha(i) = j, \alpha(j) = i$, that is, $\alpha = (j, i)$. A permutation is said to be *even* if it is a composition of even number of transpositions.

Example 2.23 : For a positive integer $n \ge 3$, consider the set A_n of even permutations in S_n . Then (A_n, \circ) is a subgroup of S_n . Let us see that $|A_n| =$ n!/2. To see that, note that $\psi: A_n \to S_n \setminus A_n$ given by $\psi(\alpha) = (2,1) \circ \alpha$ is a bijection. The group (A_n, \circ) is known as the alternating group.

Note that $A_3 = \{(1,2,3), (2,3,1), (3,1,2)\}$. It follows that A_3 is isomorphic to the group of rotational symmetries of an equilateral triangle with centroid the origin. The elements of (A_4, \circ) can be realized as rotations of a tetrahedron.

Recall that a matrix A is *diagonalizable* if there exists a diagonal matrix D and an invertible matrix B such that $A = BDB^{-1}$. The set of invertible, diagonalizable 2×2 matrices is not a subgroup of $GL_2(\mathbb{R})$.

Proposition 2.24. Let G and G' be two group structures. If $\phi : G \to G'$ is homomorphism then ker ϕ (resp. ran ϕ) is a subgroup of G (resp. G').

Proof. We will only verify the first statement. By definition, the kernel of ϕ consists of those elements $a \in G$ for which $\phi(a) = e'$, where e' denotes the identity of G'. Now if $a, b \in \ker \phi$ then $\phi(ab) = \phi(a)\phi(b) = e'e' = e'$. That is, the binary operation on G is an induced operation on ker ϕ . If e denotes the identity of G then $\phi(e) = e'$ (Remark 2.15(1)), that is, $e \in \ker \phi$. Since $\phi(a^{-1}) = \phi(a)^{-1}$ (Remark 2.15(2)), if $a \in \ker \phi$ then so is a^{-1} . **Exercise 2.25** : Consider the group structures (\mathbb{C}^*, \cdot) and (\mathbb{T}, \cdot) . Define $\phi : \mathbb{C}^* \to \mathbb{T}$ by $\phi(z) = z/|z|$ for $z \in \mathbb{C}^*$. Show that ϕ is a surjective, group homomorphism. What is the kernel of ϕ ?

Let us examine a few instructive examples.

Example 2.26 : Consider the set C[0, 1] of real-valued continuous functions defined on the interval [0, 1]. Since addition of continuous functions is continuous, (C[0, 1], +) is a group structure. Also, consider the additive group structure $(\mathbb{R}, +)$ of real numbers.

Consider the mapping $\phi : C[0,1] \to \mathbb{R}$ given by $\phi(f) = \int_0^1 f(t)dt$, the area under the curve y = f(x) ($x \in [0,1]$). Since area is additive, ϕ is a group homomorphism. Given a real number λ , if one consider the constant function κ with constant value λ , then $\phi(\kappa) = \lambda$. Thus ϕ is surjective. The kernel of ϕ consists of those continuous functions f in C[0,1] for which the area under the curve y = f(x) is 0. We see below by explicit construction that the kernel of ϕ indeed is quite large.

Let $f \in C[0, 1/2]$ be such that the graph of f lies entirely below the X-axis and satisfies f(1/2) = 0. Consider the reflection of f along the line x = 1/2, that is, the function $g \in C[1/2, 1]$ given by

$$g(x) = f(1-x) \ (x \in [1/2, 1]).$$

Note that the area under f is same as the area under g. Now define $h \in C[0, 1]$ as follows:

$$h(x) = f(x)$$
 for $x \in [0, 1/2]$
= $-g(x)$ for $x \in [1/2, 1]$.

Obviously, $h \in C[0, 1]$ and $\phi(h) = 0$.

Exercise 2.27 : Consider the map $\phi : C[0,1] \to \mathbb{R}$ given by $\phi(f) = f(0)$. Show that ϕ is a group homomorphism from (C[0,1],+) onto $(\mathbb{R},+)$.

Example 2.28: Consider the subgroup $GL_n(\mathbb{R})$ of $(M_n(\mathbb{R}), \circ)$ of real $n \times n$ matrices with non-zero determinant. Also, consider the multiplicative group (\mathbb{R}^*, \cdot) of real numbers. Consider the mapping det : $GL_n(\mathbb{R}) \to \mathbb{R}^*$, which sends an $n \times n$ matrix to its determinant. Since determinant is multiplicative, det is a group homomorphism. If $\lambda \in \mathbb{R}^*$ then determinant of the diagonal matrix with diagonal entries $\lambda, 1, \dots, 1$ is equal to λ . Thus det is surjective. The kernel of ϕ consists of all matrices in $GL_n(\mathbb{R})$ whose determinant is 1. The kernel of ϕ is commonly denoted by $SL_n(\mathbb{R})$.

A subgroup S of a group G is said to be *normal* if for every $a \in S$ and every $b \in G$, the conjugate bab^{-1} is in S.

Trivially, any subgroup of an abelian group is normal.

Example 2.29 : The subgroup of rotations in D_n is normal in D_n . This follows from the following facts:

- (1) Any two rotations commute.
- (2) If r is a rotation and ρ is a reflection then $\rho \circ r \circ \rho^{-1} = r^{-1}$

(see Example 2.11). Let us calculate the center of D_n . If follows from (2) above that a rotation r commute with a reflection ρ iff $r^2 = 1$ iff $r = r_0, r_\pi$. It follows that $Z_{D_n} = \{r_0, r_\pi\}$ if n is even, and $Z_{D_n} = \{r_0\}$ otherwise.

Example 2.30 : The subgroup of invertible diagonal matrices is not normal in $(GL_n(\mathbb{R}), \circ)$.

Proposition 2.31. The kernel of a homomorphism is a normal subgroup.

Proof. In the notations of Proposition 2.24,

$$\phi(bab^{-1}) = \phi(b)\phi(a)\phi(b^{-1}) = \phi(b)e'\phi(b)^{-1} = e'$$

in view of Remark 2.15(2).

Remark 2.32: Note that $SL_n(\mathbb{R})$ is a normal subgroup of $(GL_n(\mathbb{R}), \circ)$.

Example 2.33 : The center of $(SL_n(\mathbb{R}), \circ)$ turns out to be the subgroup of scalar matrices. To see this, let $A \in SL_n(\mathbb{R})$. If $D \in SL_n(\mathbb{R})$ is the diagonal matrix with distinct diagonal entries then AD = DA forces that A must be diagonal. By interchanging the role of A and D, one can see that the diagonal entries A are identical.

Exercise 2.34: Show that $Z_{SL_n(\mathbb{C})}$ is isomorphic to (\mathbb{I}_n, \cdot) (see (2.3)).

Proposition 2.35. The center of a group is a normal subgroup.

Proof. Let $a \in Z_G$ and $b \in G$. For any $g \in G$, by associativity of G,

$$(bab^{-1})g = b(ab^{-1}g) = b(b^{-1}ga) = ga.$$

By a similar argument, $g(bab^{-1}) = ag$. Since $a \in Z_G$, so does bab^{-1} .

Let G be a group and let $a \in G$. If H is a subset of G, then the subset $aH = \{ah : h \in H\}$ of G is said to be a *coset* of H in G.

Remark 2.36 : Any two cosets contain same number of elements. In fact, $\phi : aH \to H$ given by $\phi(ah) = h$ is a bijection.

Let H be a subgroup of G. Note that aH = bH iff $a^{-1}b \in H$. If one defines $aH \cong bH$ if $a^{-1}b$ then \cong defines an equivalence relation on the collection of cosets of H. Define G/H to be the collection of equivalence classes corresponding to the relation \cong . In particular, the cosets of H in G are either disjoint or identical. In case G is finite, this statement becomes very interesting.

Theorem 2.37. (Lagrange) Let H be a subgroup of a finite group G. Then |G/H| = |G|/|H|.

Proof. Note that G is the disjoint union of |G/H| number of (disjoint) cosets of H. Since any coset contains |H| elements, $|G| = |H| \times |G/H|$.

Remark 2.38 : Let $a \in G$ and let k be the smallest positive integer such that $a^k = e$ (called the *order of a*). Then, since $\{e, a, \dots, a^{k-1}\}$ is a subgroup of G, order of a divides |G|. Thus the order of a is at most |G|.

Corollary 2.39. If |G| is a prime number then G is cyclic, that is, there exists $a \in G$ such that $G = \{e, a, \dots, a^{|G|-1}\}$.

Proof. Let $a \in G \setminus \{e\}$. Then the order of a divides |G|. Since |G| is prime, the order of a is |G|, and hence $G = \{e, a, \dots, a^{|G|-1}\}$.

Exercise 2.40: Let X be a finite set and let \mathcal{F} be a collection of subsets of X which is closed with respect to union and intersection. Show that there exists an integer k such that $|\mathcal{F}| = 2^k$.

Hint. \mathcal{F} endowed with the symmetric difference is a group.

If $aH, bH \in G/H$ then we define aH * bH = abH.

Proposition 2.41. (G/H, *) is a binary structure if H is normal in G.

Proof. We must check that abH is independent of representatives a and b of aH and bH respectively. Suppose that aH = a'H and bH = b'H. Then $a^{-1}a', b^{-1}b' \in H$. A simple algebra shows that

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

It follows from the normality of H that $(ab)^{-1}a'b' \in G/H$.

Remark 2.42: If *H* is normal then the binary structure (G/H, *) is actually a group with identity *H*. In particular, G/Z_G is a group.

Proposition 2.43. Let $\phi : G \to G'$ be a group homomorphism. Then $\psi: G/\ker \phi \to \operatorname{ran} \phi$ given by $\psi(a \ker \phi) = \phi(a)$ is a group isomorphism.

Proof. Note that ψ is well-defined:

 $a \ker \phi = b \ker \phi$ iff $ab^{-1} \ker \phi$ iff $\phi(a)\phi(b^{-1}) = e$ iff $\phi(a) = \phi(b)$.

By Proposition 2.31 and Remark 2.42, $G/\ker\phi$ is a group. Since ϕ is a homomorphism, so is ψ . Clearly, ψ is injective.

The following fact is analogous to rank-nullity theorem of Linear Algebra.

Corollary 2.44. Let $\phi : G \to G'$ be a group homomorphism for a finite group G. Then

$$|G| = |\ker \phi| |\operatorname{ran} \phi|.$$

Proof. By the last theorem, $G/\ker \phi$ is isomorphic to ran ϕ . In particular, $|G/\ker \phi| = |\operatorname{ran} \phi|$. The formula now follows from Lagrange's Theorem. \Box

Example 2.45: Consider the group $\mathbb{Z}_n := \mathbb{Z}/\text{mod } n$ with the binary operation addition modulo n. Define $\phi : \mathbb{Z}_6 \to \mathbb{Z}_6$ by $\phi(k) = 2k$. Then ker $\phi = \{0, 3\}$ and ran $\phi = \{0, 2, 4\}$. Obviously, we have $|\mathbb{Z}_6| = 6 = |\ker \phi| |\operatorname{ran} \phi|$.

3. Group Actions

Definition 3.1 : Let X be a set and G be a group. A group action of G on X is a map $*: G \times X \to X$ given by $(g, x) \longrightarrow g * x$ such that

- (1) (gh) * x = g * (h * x) for all $g, h \in G$ and $x \in X$.
- (2) e * x = x for all $x \in X$.

If this happens then we say that G acts on X and X is a G-set.

Definition 3.2: Let * be a group action of G on X. For $x \in X$, let Gx denote the subset $\{g * x : g \in G\}$ of X. Define an equivalence relation \sim on X by setting $x \sim y$ iff Gx = Gy. The equivalence class of x is known as the *orbit* \mathcal{O}_x of x.

Remark 3.3 : Note that

 $\mathcal{O}_x = \{y \in X : x \backsim y\} = \{y \in X : y = g * x \text{ for some } g \in G\} = Gx.$

Note that X is the disjoint union of orbits of elements of X.

For $x \in X$, consider the function $\phi_x : G \to Gx$ given by $\phi_x(g) = g * x$. Clearly, ϕ_x is surjective. Note that ϕ_x is bijective iff $\{g \in G : g * x = x\} = \{e\}$. This motivates the following definition.

Definition 3.4 : Let * be a group action of G on X. For $x \in X$, the stabiliser S_x of x is defined by $\{g \in G : g * x = x\}$.

Remark 3.5: Note that $e \in S_x$ in view of (2) of Definition 3.1. Also, if $g, h \in S_x$ then (gh) * x = g * (h * x) = g * x = x by (1) of Definition 3.1. Further, if $g \in S_x$ then by the same argument $g^{-1} * x = g^{-1} * (g * x) = x$. Thus S_x is a subgroup of G.

In view of the discussion prior to the definition, $|\mathcal{O}_x| = |G|$ if $|\mathcal{S}_x| = 1$.

We try to understand the notions of group action, orbit and stabiliser through several examples.

Exercise 3.6 : Show that \mathbb{R}^n acts on itself by translations: x * y = x + y. Find orbits and stabilisers of all points in \mathbb{R}^n .

Example 3.7 : Consider the group (\mathbb{R}^*, \cdot) and the set \mathbb{R}^n . Consider the map $\alpha * (x_1, \cdots, x_n) := (\alpha \cdot x_1, \cdots, \alpha \cdot x_n)$. By the associativity of \mathbb{R} , $(\alpha \cdot \beta) * (x_1, \cdots, x_n) = ((\alpha \cdot \beta) \cdot x_1, \cdots, (\alpha \cdot \beta) \cdot x_n) = \alpha * (\beta * (x_1, \cdots, x_n))$

for $\alpha, \beta \in \mathbb{R}^*$ and $\bar{x} = (x_1, \cdots, x_n) \in \mathbb{R}^n$. Clearly, $1 * \bar{x} = \bar{x}$ for every $\bar{x} \in \mathbb{R}^n$. Thus \mathbb{R}^* acts on \mathbb{R}^n .

Let $\bar{x} \in \mathbb{R}^n$. The orbit $\mathcal{O}_{\bar{x}}$ is the punctured line in \mathbb{R}^n passing through \bar{x} and the origin 0. Note that $\mathcal{S}_{\bar{x}} = \{1\}$ of \mathbb{R}^* if $\bar{x} \neq 0$, and $S_0 = \mathbb{R}^*$.

Example 3.8 : Consider the group structure (\mathbb{T}, \cdot) and the unit ball \mathbb{B} centered at the origin. Then $t \cdot z \in \mathbb{B}$ for every $t \in \mathbb{T}$ and $z \in \mathbb{B}$. Since

multiplication is associative and $1 \cdot z = z$, the unit circle \mathbb{T} acts on \mathbb{B} via the complex multiplication.

The orbit \mathcal{O}_z is the circle of radius |z| with origin as the center. The stabiliser of all points except the origin is $\{1\}$. Clearly, $S_0 = \mathbb{T}$.

Exercise 3.9 : Find all subsets X of the complex plane such that the complex multiplication \cdot is a group action of (\mathbb{T}, \cdot) on X.

Exercise 3.10 : Consider the power series $f(z, w) = \sum_{k,l=0}^{\infty} c_{k,l} z^k w^l$ in the complex variables z and w. The domain of convergence \mathcal{D}_f of f is given by

$$\{(z,w) \in \mathbb{C}^2 : \sum_{k,l=0}^{\infty} |c_{k,l}| |z|^k |w|^l < \infty\}.$$

Show that the multiplicative group torus $\mathbb{T} \times \mathbb{T}$ acts on \mathcal{D}_f via

$$(\lambda_1, \lambda_2) * (z, w) = (\lambda_1 z, \lambda_2 w).$$

Discuss orbits and stabilizers.

Let * be a group action of G on X. We say that * is *transitive* if there is only one (disjoint) orbit in X, and that * is *free* if every point in X has trivial stabilizer.

Exercise 3.11 : Show that the symmetric group S_n acts on $X = \{1, \dots, n\}$ via the action $* : (\sigma, j) \longrightarrow \sigma(j)$. Show that * is transitive. Find the stabiliser of j.

Exercise 3.12: Show that the symmetric group S_n acts on \mathbb{R}^n via

 $\sigma * (x_1, \cdots, x_n) = (x_{\sigma(1)}, \cdots, x_{\sigma(n)}).$

Describe orbits and stabilisers of $x \in \mathbb{R}^n$ such that $x_1 = 0, \dots, x_k = 0$ for some $1 \le k \le n$.

Exercise 3.13 : For an $n \times n$ matrix A and $\bar{x} \in \mathbb{R}^n$, define * by $A * \bar{x} = A\bar{x}$. For the group G and set X, verify that * defines a group action:

(1) $GL_n(\mathbb{R})$ and \mathbb{R}^n .

(2) $O_n(\mathbb{R})$ (group of orthogonal matrices) and \mathbb{S} (unit sphere in \mathbb{R}^n).

Find orbits and stabilisers of all points in X in both the cases.

Example 3.14 : Let us see an easy deduction of the following fact using group action: $S = \{A = (a_{ij}) \in GL_2(\mathbb{R}) : a_{i1} + a_{i2} = 1 \text{ for } i = 1, 2\}$ is a subgroup of $GL_2(\mathbb{R})$. To see that, consider the group action of $GL_2(\mathbb{R})$ on \mathbb{R}^2 as discussed in the preceding exercise, and note that S is precisely the stabilizer of the column vector $(1, 1)^T$.

Example 3.15 : For a function $f : \mathbb{R} \to \mathbb{R}$ and $x \in \mathbb{R}$, consider the map f * x = f(x). Note that * is not a group action of the group $(C(\mathbb{R}), +)$ on \mathbb{R} .

Exercise 3.16 : Consider the automorphism group $A(\mathbb{D})$ of the unit disc \mathbb{D} endowed with the composition:

$$A(\mathbb{D}) = \{ f : \mathbb{D} \to \mathbb{D} : f \text{ is a biholomorphism} \}.$$

Show that the action f * z = f(z) of $A(\mathbb{D})$ on \mathbb{D} is transitive but not free.

Hint. Schwarz Lemma from Complex Analysis.

Exercise 3.17: Let \mathcal{B} denote the set of ordered bases (e_1, e_2) of \mathbb{R}^2 . Show that $GL_2(\mathbb{R})$ acts \mathcal{B} via $A * (e_1, e_2) = (Ae_1, Ae_2)$. Describe the orbit and stabiliser of (e_1, e_2) .

Example 3.18 : Consider the group \mathbb{Z}_2 and the unit sphere \mathbb{S}_n in \mathbb{R}^n . Define * by 0 * x = x and 1 * x = -x. Verify that * is a free action of \mathbb{Z}_2 on \mathbb{S}_n .

Note that $\mathcal{O}_x = \{x, -x\}$ for any $x \in \mathbb{S}_n$. Clearly, $\mathcal{S}_x = \{0\}$. Although, we do not required this fact, note that the *real projective n-space* $\mathbb{R}P^n$ is the space of orbits \mathcal{O}_x endowed with the quotient topology.

The following example arises in the dynamics of projectile.

Exercise 3.19 : Verify that

$$t * (x, y, z, v_1, v_2, v_3) = (x + v_1t, y + v_2t, z - gt^2/2 + v_3t, v_1, v_2, v_3 - gt)$$

is a group action of the additive group \mathbb{R} on \mathbb{R}^6 , where g is a real constant. Discuss orbits and stabilizers.

4. Fundamental Theorem of Group Actions

Theorem 4.1. Let G be a finite group acting on a set X. Then:

(1) If X is finite then there exist disjoint orbits $\mathcal{O}_{x_1}, \cdots, \mathcal{O}_{x_k}$ such that

$$|X| = |\mathcal{O}_{x_1}| + \dots + |\mathcal{O}_{x_k}|.$$

- (2) The stabilizer S_x of x is a subgroup of G for every $x \in X$.
- (3) (Orbit-Stabilizer Formula) For each $x \in X$,

$$|G/\mathcal{S}_x| = |\mathcal{O}_x|$$
 and $|G| = |\mathcal{O}_x||\mathcal{S}_x|$.

- (4) If $y \in \mathcal{O}_x$ then there exists $h \in G$ such that $\mathcal{S}_x = h\mathcal{S}_y h^{-1}$.
- (5) The map $\phi: G \to S_X$ given by $\phi(g) = M_g$ is a group homomorphism, where $M_g \in S_X$ is defined by $M_g(x) = g * x$.
- (6) $\ker(\phi) = \bigcap_{x \in X} \mathcal{S}_x.$

Proof. (1) This part follows from Remark 3.3.

(2) This is already noted in Remark 3.5.

(3) By (2) and the Lagrange's Theorem, $|G| = |G/S_x||S_x|$. Thus it suffices to check that $|G/S_x| = |\mathcal{O}_x|$. To see that, we define $\psi : G/S_x \to \mathcal{O}_x$ by $\psi(gS_x) = g * x$.

 ψ is well-defined and bijective: Note that $gS_x = hS_x$ iff $h^{-1}g \in S_x$ iff $(h^{-1}g) * x = x$ iff g * x = h * x. Clearly, ψ is surjective.

(4) Let $y \in \mathcal{O}_x$. Then x = h * y for some $h \in G$, and hence by condition (1) of Definition 3.1,

$$S_x = \{g \in G : g * x = x\} = \{g \in G : g * (h * y) = h * y \text{ for some } h \in G\} \\ = \{g \in G : h^{-1}gh \in S_y\} = hS_yh^{-1}.$$

(5) First note that ϕ is well-defined since M_g is bijective with inverse $M_{g^{-1}}$. Since $M_{gh} = M_g \circ M_h$, ϕ is a group homomorphism.

 $\ker(\phi) = \{g \in G : M_g = M_e\} = \{g \in G : g * x = x \text{ for all } x \in X\} = \bigcap_{x \in X} \mathcal{S}_x.$ This completes the proof of the theorem.

Corollary 4.2. Let * be a group action of G on X. If * is transitive then $|\mathcal{S}_x| = |G|/|X|$ for every $x \in X$. If * is free then $|\mathcal{O}_x| = |G|$ for every $x \in X$.

We will refer to ϕ as the *permutation representation* of G on X. We say that ϕ is *faithful* if ker $(\phi) = \{e\}$.

Example 4.3 : Consider the square S with vertices $v_1 = (1,1), v_2 = (-1,1), v_3 = (-1,-1), v_4 = (1,-1)$. Consider the dihedral group D_4 of symmetries of S and the set $X = \{(v_1, v_3), (v_2, v_4)\}$ of unordered pairs. Then A * (u, v) = (Au, Av) defines a group action of D_4 on X.

Clearly, the orbit of any point is X, and hence * is transitive. Also, $r_{\pi} \in \mathcal{S}_{(v_1,v_3)} \cap \mathcal{S}_{(v_2,v_4)}$. In particular, the action * is not faithful.

If X is finite then S_X is isomorphic to $S_{|X|}$. Thus we have:

Corollary 4.4. Let ϕ be a permutation representation of G on X. If ϕ is faithful then G is isomorphic to a subgroup of the permutation group $S_{|X|}$.

Example 4.5 : Consider the group $GL_2(\mathbb{Z}_2)$ of invertible matrices with entries from the field \mathbb{Z}_2 . Then $|GL_2(\mathbb{Z}_2)| = 6$. Consider the set $X = \{e_1, e_2, e_1 + e_2\}$, where $e_1 = [1 \ 0]^T$ and $e_2 = [0 \ 1]^T$. Then $GL_2(\mathbb{Z}_2)$ acts on X via $A * \bar{x} = A\bar{x}$.

Let ϕ denote the permutation representation of $GL_2(\mathbb{Z}_2)$ on X. If $A \in \ker \phi$ then $A\bar{x} = \bar{x}$ for every $\bar{x} \in X$. However, Ae_i is the *i*th column of A for i = 1, 2. Therefore A is the identity matrix, and ϕ is faithful. By Corollary 4.4, $GL_2(\mathbb{Z}_2)$ isomorphic to S_3 .

Let p be a prime number. A group G is said to be a p-group if $|G| = p^k$ for some positive integer k.

Corollary 4.6. Let G be a p-group acting on X. If

 $S = \{ x \in X : \mathcal{O}_x \text{ is singleton} \},\$

then $|S| = |X| \mod p$.

Proof. Let $\mathcal{O}_{x_1}, \dots, \mathcal{O}_{x_r}$ be all disjoint orbits of X of size bigger than 1. Then $|X| = |S| + |\mathcal{O}_{x_1}| + \dots + |\mathcal{O}_{x_r}|$. By Theorem 4.1, each $|\mathcal{O}_{x_i}|$ divides |G|, and hence a multiple of p. This gives $|S| = |X| \mod p$.

5. Applications

In this section, we discuss several applications of the fundamental theorem of group actions to the group theory.

5.1. A Theorem of Lagrange.

Example 5.1 : The symmetric group S_n acts on the set $\mathbb{C}[z_1, \dots, z_n]$ of complex polynomials in n variables z_1, \dots, z_n via

$$\sigma * p(z_1, \cdots, z_n) = p(z_{\sigma(1)}, \cdots, z_{\sigma(n)}).$$

Let p be in $\mathbb{C}[z_1, \dots, z_n]$. Clearly, the identity permutation fixes p. Also,

$$(\sigma\tau) * p(z_1, \cdots, z_n) = p(z_{\sigma\tau(1)}, \cdots, z_{\sigma\tau(n)}) = p(z_{\sigma(\tau(1))}, \cdots, z_{\sigma(\tau(n)}))$$
$$= \sigma * p(z_{\tau(1)}, \cdots, z_{\tau(n)}) = \sigma * (\tau * p(z_1, \cdots, z_n)).$$

The orbit of p is $\{p(z_{\sigma(1)}, \cdots, z_{\sigma(n)}) \in \mathbb{C}[z_1, \cdots, z_n] : \sigma \in S_n\}$ and the stabilizer of p is $\{\sigma \in S_n : p(z_{\sigma(1)}, \cdots, z_{\sigma(n)}) = p(z_1, \cdots, z_n)\}$.

Theorem 5.2. For any polynomial $p \in \mathbb{C}[z_1, \dots, z_n]$, the number of different polynomials we obtain from p through permutations of the variables z_1, \dots, z_n is a factor of n!.

5.2. A Counting Principle.

Example 5.3: Let H, K be two subgroups of the group G. Then K acts on the collection $\{aH : a \in G\}$ of cosets of H by k * (aH) := (ka)H.

The orbit of aH is $\{kaH : k \in K\}$. The stabiliser of aH is the subgroup $(a^{-1}Ha) \cap K$.

Suppose H = K. Then H is normal in G iff the orbit of aH is singleton for every $a \in G$.

Theorem 5.4. For subgroups H, K of a finite group G, let $KH := \{kh : k \in K, h \in H\}$. Then

$$|KH| = \frac{|K||H|}{|K \cap H|}.$$

Proof. Consider the group action K on the cosets of H as discussed in Example 5.3. Then $\mathcal{O}_H = \{kH : k \in K\}$ and $\mathcal{S}_H = H \cap K$. By Theorem 4.1, $|K| = |\mathcal{O}_H||H \cap K|$. Also, since KH is the disjoint union of cosets in \mathcal{O}_H and since |kH| = |H|,

$$|KH| = |\mathcal{O}_H||H| = \frac{|K||H|}{|H \cap K|}.$$

This completes the proof of the corollary.

5.3. Cayley's Theorem.

Example 5.5: Consider the group action of K on $\{aH : a \in G\}$ as discussed in Example 5.3. The choice $H = \{e\}$ and K = G gives the *left multiplication action* of G on itself: $(g,h) \longrightarrow gh$. Note that $\mathcal{O}_g = G$ and $\mathcal{S}_g = \{e\}$ for any $g \in G$. In particular, the permutation representation of G on G is transitive and faithful.

Theorem 5.6. Every finite group is isomorphic to a subgroup of a symmetric group.

Proof. Consider the left multiplication action of G on itself. Let ϕ be the corresponding permutation representation of G on X. By Corollary 4.4, it suffices to check that ϕ is faithful. This is noted in the last example.

Exercise 5.7 : Let G be a group of order n. Prove:

- (1) Let $g_1, g_2, \dots, \in G$ be such that $g_1 \neq e$ and $H_i \subsetneq H_{i+1}$, where H_i is
- the subgroup generated by g_1, \dots, g_i . Then $|H_i| \ge 2^i$ for each *i*.
- (2) G can be generated by at most $\log_2 n$ elements.

Use the Cayley's Theorem to conclude that the number of non-isomorphic groups of order n does not exceed $(n!)^{\log_2 n}$.

5.4. The Class Equation. Let us discuss another important group action of G on itself.

Example 5.8 : Let G be a group. Define $*: G \times G \to G$ by $g * x = gxg^{-1}$. By Proposition 2.7 and associativity of G,

$$(gh) * x = (gh)x(gh)^{-1} = g(hxh^{-1})g^{-1} = g(h*x)g^{-1} = g*(h*x)$$

for every $g, h, x \in G$. Also, since $e * x = exe^{-1} = x$ for every $x \in G$, the map * defines a group action of G onto itself.

Note that \mathcal{O}_x is the set of all conjugate elements of x. The stabiliser \mathcal{S}_x of x is the normalizer N(x) of x.

We will refer to the group action of the last example as the *conjugate* group action of G. The orbit \mathcal{O}_x will be referred as the *conjugacy class* of G.

Exercise 5.9: Consider the conjugate group action * of G on itself. Verify:

(1) If $x, y \in Z_G$ then x = g * y for some $g \in G$ iff x = y. (2) $\mathcal{O}_a = \{a\}$ iff $a \in Z_G$.

Theorem 5.10. Let G be a p-group. Then $|Z_G|$ is divisible by p.

Proof. Apply Corollary 4.6 to the conjugate group action of G on itself. \Box

Exercise 5.11 : Let G be a p-group such that $|G| = p^2$. Show that G is abelian. Conclude that G is isomorphic either to \mathbb{Z}_{p^2} or $\mathbb{Z}_p \times \mathbb{Z}_p$.

Theorem 5.12. Let G be a finite group. Then

$$|G| = |Z_G| + \sum \frac{|G|}{|N(x)|},$$

where this sum runs over one element x from each conjugacy class with $N(x) \neq G$.

Proof. Consider the conjugate group action * of G onto itself. We observed in Example 5.8 that $S_x = N(x)$. By Theorem 4.1, there exist disjoint orbits of $\mathcal{O}_{x_1}, \dots, \mathcal{O}_{x_k}$ such that

$$|G| = |\mathcal{O}_{x_1}| + \dots + |\mathcal{O}_{x_k}| = \frac{|G|}{|\mathcal{S}_{x_1}|} + \dots + \frac{|G|}{|\mathcal{S}_{x_k}|} = \frac{|G|}{|N(x_1)|} + \dots + \frac{|G|}{|N(x_k)|}.$$

Now if $x_i \in Z_G$ then $N(x_i) = G$, and if $x_i, x_j \in Z_G$ for $i \neq j$ then the conjugacy classes of x_i and x_j are disjoint (Exercise 5.9). The desired conclusion follows immediately.

Remark 5.13 : One may derive Theorem 5.10 from the class equation: $|Z_G| = |G| - \sum |G|/|N(x)|$, where N(x) is a proper subgroup of G.

Example 5.14 : Consider the conjugate group action of the dihedral group D_4 on itself. We already noted in Example 2.29 that $Z_{D_4} = \{r_0, r_\pi\}$. In particular, $N(r_0) = D_4 = N(r_\pi)$.

Note that the normalizer of any rotation x contains exactly 4 elements (all the rotations in D_4). Note further that the normalizer of any reflection x contains exactly 4 elements (2 elements in Z_{D_4} , $x = \rho_{\theta}$ and $\rho_{\theta+\pi}$). Note also that $r_{\pi/2}$ and $r_{3\pi/2}$ are conjugate to each other, and hence belong to same conjugacy class. Note next that $\rho_{\pi/2}$ and ρ_{π} (resp. $\rho_{3\pi/2}$ and $\rho_{2\pi}$) are conjugates. Hence the class equation for D_4 is

$$(|D_4|=8) = (|Z_{D_4}|=2) + (|\mathcal{O}_{r_{\pi/2}}|=2) + (|\mathcal{O}_{\rho_{\pi/2}}|=2) + (|\mathcal{O}_{\rho_{3\pi/2}}|=2).\blacksquare$$

Exercise 5.15 : Verify that the conjugacy classes of the permutation group S_3 are $\{(1)\}, \{(1,2), (1,3), (2,3)\}, \{(1,2,3), (1,3,2)\}$. Conclude that the class equation of S_3 is

$$(|S_3| = 6) = (|Z_{S_3}| = 1) + (|\mathcal{O}_{(1,2)}| = 3) + (|\mathcal{O}_{(1,2,3)}| = 2).$$

5.5. Cauchy's Theorem.

Example 5.16 : Let G be a group and let H be the multiplicative group $\{1, -1\}$. Consider the action 1 * g = g and $(-1) * g = g^{-1}$ of H on G. It is easy to verify that * is a group action.

Let $g \in G$. The orbit of g is $\{g, g^{-1}\}$ if $g \neq e$, and $\{e\}$ otherwise. The stabiliser of g is $\{1\}$ if $g^2 \neq e$, and $\{1, -1\}$ otherwise.

Here is a particular case of the Cauchy's Theorem.

Exercise 5.17 : Prove that there exist odd number of elements of order 2 in a group of even order.

Hint. Apply Theorem 4.1 to the action discussed in Example 5.16.

Example 5.18 : Let G be a group and let p be a prime number. Let H denote the group generated by the permutation $\sigma \in S_p$ given by $\sigma(j) = j+1$ for $j = 1, \dots, p-1$ and $\sigma(p) = 1$. Note that |H| = p. Consider the set

$$X = \{ (g_1, \cdots, g_p) : g_1, \cdots, g_p \in G, g_1 \cdots g_p = e \}.$$

Since there are p parameters and 1 equation, p-1 variables are free, and hence $|X| = |G|^{p-1}$.

Suppose $(g_1, \dots, g_p) \in X$. Then g_1 commutes with $g_2 \dots g_p$, and hence $(g_{\sigma(1)}, \dots, g_{\sigma(p)}) \in X$. By finite induction, we get $(g_{\sigma^j(1)}, \dots, g_{\sigma^j(p)}) \in X$ for $j = 1, \dots, p$. This enables us to define

$$\tau * (g_1, \cdots, g_p) = (g_{\tau(1)}, \cdots, g_{\tau(p)}) \ (\tau \in H, (g_1, \cdots, g_p) \in X).$$

Then * is indeed a group action of H on X. We verify only condition (2) of Definition 3.1:

$$(\sigma\tau) * (g_1, \cdots, g_p) = (g_{\sigma\tau(1)}, \cdots, g_{\sigma\tau(p)}) = (g_{\sigma(\tau(1))}, \cdots, g_{\sigma(\tau(p))})$$
$$= \sigma * (g_{\tau(1)}, \cdots, g_{\tau(p)}) = \sigma * (\tau * (g_1, \cdots, g_p)).$$

The orbit of (e, \dots, e) is $\{(e, \dots, e)\}$. More generally, $|\mathcal{O}_{(g_1, \dots, g_p)}| = 1$ iff $g_1 = \dots = g_p$ and $g_1^p = e$. Finally, the stabiliser of any element in X consists only the identity permutation in S_p .

Theorem 5.19. Let G be a finite group and p be a prime such that p divides |G|. If P denotes the set of elements of G of order p, then $|P| \equiv -1 \mod p$.

Proof. Consider the action of H on X as discussed in Example 5.18. Recall that $|H| = p, |X| = |G|^{p-1}$, and the fact that $|\mathcal{O}_{(g_1, \dots, g_p)}| = 1$ iff $g_1 = g_2 = \dots = g_p$ and $g_1^p = e$.

By Theorem 4.1, there exist disjoint orbits of $\mathcal{O}_{x_1}, \cdots, \mathcal{O}_{x_k}$ such that

$$|X| = |\mathcal{O}_{x_1}| + \dots + |\mathcal{O}_{x_k}| = 1 + \sum_{\mathcal{O}_{x_i} \neq \mathcal{O}_{(e,\dots,e)}} |\mathcal{O}_{x_i}|.$$

Since $|X| = |G|^{p-1}$ and G is a p-group, $1 + \sum_{x_i \neq (e, \dots, e)} |\mathcal{O}_{x_i}| = lp$ for some positive integer l. Again, by Theorem 4.1, $|\mathcal{O}_{x_i}|$ divides |H| = p, and hence $|\mathcal{O}_{x_i}|$ is either 1 or p. Let $Y = \{x_i : \mathcal{O}_{x_i} \neq \mathcal{O}_{(e, \dots, e)}, |\mathcal{O}_{x_i}| = 1\}$. It follows that 1 + |Y| + (k - 1 - |Y|)p = lp. Thus we have $|Y| = -1 \mod p$.

Define $\phi : P \to Y$ by $\phi(g) = (g, \dots, g)$. Clearly, ϕ is injective. If $(g_1, \dots, g_p) \in Y$ then $|\mathcal{O}_{(g_1, \dots, g_p)}| = 1$. Then we must have $g_1 = \dots = g_p$ and $g_1^p = e$. Thus $\phi(g_1) = (g_1, \dots, g_p)$, and hence ϕ is surjective. \Box

Remark 5.20 : A group of order 6 must contain an element of order 3. In particular, there exists no group of order 6 containing identity and 5 elements of order 2.

Example 5.21 : Let G be a group of order 6. Then G contains an element x of order 3 and an element y of order 2. If i is not a multiple of 3 then

 $(x^i)^3 = (x^3)^i = e$ and $(x^i)^2 \neq e$. Similarly, the order of y^j is 3 if j is not a multiple of 2. Now if $x^i y^j = x^r y^s$ then $x^{i-r} = y^{s-j}$, and hence i = rmod 3 and $s = j \mod 2$. Thus $G = \{x^i y^j : 0 \le i \le 2, 0 \le j \le 1\}$. Now $yx \in G$, and clearly, $yx \notin \{e, x, y, x^2\}$. Hence there are only two choices of yx, namely, xy or x^2y . If xy = yx then G is the cyclic group of order 6. If $yx = x^2y$ or $yxy^{-1} = x^{-1}$ then G is isomorphic to the dihedral group D_3 .

5.6. First Sylow Theorem.

Example 5.22: Let G be a group. For a positive integer $n \leq |G|$, let \mathcal{F}_n denote the collection of all subsets A of G such that |A| = n. Note that $|\mathcal{F}_n| = \binom{|G|}{n}$. Then G acts on \mathcal{F}_n by $(g, A) \longrightarrow gA$. Indeed, |gA| = |A|, eA = A and $(g_1g_2) * A = g_1 * (g_2A)$.

The orbit \mathcal{O}_A of A equals $\{gA : g \in G\}$ and the stabilizer \mathcal{S}_A of A equals $\{g \in G : gA = A\}$. If $a \in A$ then $\mathcal{S}_A a = \{ga : gA = A\} \subseteq A$.

Suppose $|G| = p^n q$, where p is a prime not dividing q. Then a Sylow p-subgroup is a subgroup of order p^n . A subgroup is called p-subgroup if it is a p-group.

Remark 5.23: Let *a* belong to a Sylow *p*-subgroup such that $a \neq e$. By the Lagrange's Theorem, the order *a* is p^r for some positive integer *r*. Then the order of $a^{p^{r-1}}$ is precisely *p*.

The First Sylow Theorem partly generalizes the Cauchy's Theorem.

Theorem 5.24. Let G be a finite group. If p is a prime divisor of |G| then G has a Sylow p-subgroup.

Proof. Suppose $|G| = p^n q$, where q is not divisible by p. Consider the group action of G on $X := \mathcal{F}_{p^n}$ as discussed in Example 5.22. We need the fact that $|\mathcal{F}_{p^n}| = \binom{p^n q}{p^n}$ is not divisible by p. Then by Theorem 4.1(1), there exists $A \in \mathcal{F}_{p^n}$ such that $|\mathcal{O}_A|$ is not divisible by p. By the orbit-stabilizer formula, $p^n q = |\mathcal{S}_A||\mathcal{O}_A|$, and hence $|\mathcal{S}_A|$ is divisible by p^n . Also, $|\mathcal{S}_A| = |\mathcal{S}_A a|$ and $\mathcal{S}_A a \subseteq A$ for any $a \in A$. It follows that $|\mathcal{S}_A| = p^n$.

5.7. Second Sylow Theorem.

Remark 5.25: Since $|aHa^{-1}| = |H|$, if *H* is a Sylow *p*-subgroup of *G* then so is the conjugate aHa^{-1} of *H*. If *G* has only one Sylow *p*-subgroup *H* then *H* is necessarily normal in *G*.

Theorem 5.26. Let G be a finite group and let p be a prime divisor of |G|. If H is a Sylow p-subgroup of G and K is a p-subgroup of G then there exists $a \in G$ such that $K \subseteq aHa^{-1}$.

In particular, any two Sylow p-subgroups are conjugate.

Proof. Consider the group action of K on the collection $X = \{aH : a \in G\}$ of cosets of H by k * (aH) := (ka)H (see Example 5.3). Let S denote the set of

cosets aH with single-ton orbits. Since K is a p-subgroup, by Corollary 4.6, $|S| = |X| \mod p$. However, by the Lagrange's Theorem, |X| = |G|/|H| = q, where q is not divisible by p. This implies that $|S| = q \mod p$, and hence S is non-empty. Let $aH \in S$. Then kaH = aH for every $k \in K$, that is, $a^{-1}ka \in H$ for every $k \in K$. This completes the proof of the first part.

If in addition K is also a p-Sylow subgroup then $|K| = p^n = |H| = |aHa^{-1}|$. By the first part, we must have $K = aHa^{-1}$ in this case.

Remark 5.27: Let H be a Sylow p-subgroup of G. Then H is a unique Sylow p-subgroup of G iff H is normal in G.

5.8. Third Sylow Theorem.

Example 5.28 : Let G be a group and H, K be subgroups of G. Let $X := \{aHa^{-1} : a \in G\}$ be a collection of subgroups of G. Then K acts on X by $(g, L) \longrightarrow gLg^{-1}$. We just check condition (2) of Definition 3.1:

$$(gh) * L = (gh)L(gh)^{-1} = g(hLh^{-1})g^{-1} = g * (h * L)$$

for any $g, h \in K$ and $L \in X$.

Suppose K := G. Then the orbit of any element in X is the entire X. Also, the stabiliser of $K \in X$ is the subgroup $\{g \in G : gK = Kg\}$, the normalizer N(K) of K.

Theorem 5.29. Let G be a group such that $|G| = p^n q$, where p is a prime number which does not divide q. Then the number N_p of Sylow p-subgroups of G divides q. Moreover, $N_p = 1 + kp$ for some non-negative integer k.

Proof. Let H be a Sylow p-subgroup of G. Consider the group action of K := G on X as discussed in Example 5.28. By the Second Sylow Theorem, X consists of all Sylow p-subgroups of G. Thus $N_p = |X|$. Recall that $\mathcal{O}_H = X$ and $\mathcal{S}_H = N(H)$. By the orbit-stabilizer formula, |G| = |X||N(H)|. In particular, N_p divides |G|. Since $H \subseteq N(H)$, by the Lagrange's Theorem, |H| divides |N(H)|. It follows that $N_p = |G|/|N(H)|$ divides |G|/|H| = q. In particular, N_p is not divisible by p.

Consider the group action of K := H on X as described in Example 5.28. Let $S = \{L \in X : \mathcal{O}_L = \{L\}\}$. By Corollary 4.6, $|S| = |X| \mod p$. Since p does not divide $N_p = |X|$, S is non-empty. Thus there exists $L \in X$ such that $\mathcal{O}_L = \{L\}$. It follows that hL = Lh for every $h \in H$, that is, $H \subseteq N(L)$. Thus H and L are subgroups of N(L). Also, since $|N(L)| = |G|/N_p = p^nq'$ for some divisor q' of q, H and L are indeed Sylow p-subgroups of N(L). However, since L is normal in N(L), by the Second Sylow Theorem, there is only one Sylow p-subgroup of N(L). Thus H = L. This shows that S has only one element. In particular, $1 = |X| \mod p$ as desired. \Box

A group G is called *simple* if it has no normal subgroup.

Example 5.30 : Let G be a group of order 12. The possible choices for N_2 are 1 and 3. The possible choices for N_3 are 1 and 4. If $N_3 = 4$ then G must

have 8 elements of order 3. Indeed, any two Sylow 3-subgroups intersects trivially in view of the Lagrange's Theorem. In case $N_3 = 4$, there can be only one Sylow 2-group of order 4. In any case, G is not simple.

Exercise 5.31 : Show a group of order 40 has a normal, Sylow 5-subgroup.

Example 5.32 : Consider the group $GL_2(\mathbb{Z}_p)$, where \mathbb{Z}_p is the multiplicative group $\{0, 1, \dots, p-1\}$ with binary operation multiplication modulo p for a prime number p. Any element in $GL_2(\mathbb{Z}_p)$ is obviously determined by 4 elements in \mathbb{Z}_p , out of which a column can be chosen in $p^2 - 1$ ways, and then the remaining column should not be a \mathbb{Z}_p -multiple of the first column chosen in $p^2 - p$ ways. Thus $|GL_2(\mathbb{Z}_p)| = p(p-1)^2(p+1)$. By the Sylow Third Theorem, the number N_p of Sylow p-subgroups is either 1 or p+1. Produce two Sylow p-subgroups of $GL_2(\mathbb{Z}_p)$ to conclude that $N_p = p+1$.

Corollary 5.33. Let $G_{p \cdot q}$ be a group of order pq, where p and q are prime numbers such that q < p. Then:

- (1) $G_{p \cdot q}$ has only one Sylow p-subgroup H_p .
- (2) If $p \neq 1 \mod q$ then $G_{p \cdot q}$ has only one Sylow q-subgroup H_q .
- (3) If $G_{p\cdot q}$ has only one Sylow q-subgroup H_q then $G_{p\cdot q}$ is cyclic.
- (4) If $p \neq 1 \mod q$ then $G_{p \cdot q}$ is cyclic.
- (5) $G_{p\cdot 2}$ is either abelian or isomorphic to the dihedral group D_p .

Proof. (1) By the Third Sylow Theorem, N_p divides q and $N_p = 1 \mod p$. Thus $N_p \leq q < p$, and hence $N_p = 1$.

(2) Again, by the Third Sylow Theorem, N_q divides p and $N_q = 1 \mod q$. Either N_q is p or 1. If $p \neq 1 \mod q$ then N_q must be 1.

(3) Suppose $G_{p\cdot q}$ has only one Sylow q-subgroup H_q . By Remark 5.27, H_p and H_q are normal in $G_{p\cdot q}$. Clearly, H_p and H_q are cyclic of order p and q respectively. By the Lagrange's Theorem, $H_p \cap H_q$ is trivial. Let x and y denote the generators of H_p and H_q respectively. Since H_p is normal in $G_{p\cdot q}$, $(xy)(yx)^{-1} = x(yx^{-1}y^{-1}) \in H_p$. Also, since H_q is normal in $G_{p\cdot q}$, $(xy)(yx)^{-1} = (xyx^{-1})y^{-1} \in H_q$. Since $H_p \cap H_q = \{e\}$, xy = yx. It is easy to see that the order of xy is pq. In particular, $G_{p\cdot q}$ is a cyclic group generated by xy.

(4) This follows from (2) and (3).

(5) Let x and y denote the generators of H_p and H_2 respectively. Thus $x^p = e$ and $y^2 = e$. Since H_p is normal, $yxy = yxy^{-1} \in H_p$. Thus $yxy = x^j$ for some $0 \leq j < p$. But then $x = y^2xy^2 = yx^jy = x^{j^2}$, and hence $j^2 = 1$ mod p. The only possible choices of j are ± 1 . If j = 1 then $G_{p\cdot 2}$ is abelian. If i = -1 then the relations $x^p = e, y^2 = e, yxy = x^{-1}$ determines the dihedral group D_p .

Remark 5.34 : Every group of order 15 is cyclic.

Exercise 5.35 : Consider the group $G_{7.3}$. Verify the following:

- (1) $G_{7.3}$ has unique Sylow 7-subgroup, and $G_{7.3}$ has k Sylow 3-subgroups $H_{3,j}$ $(j = 1, \dots, k)$, where possible values of k are 1 and 7.
- (2) Suppose H_7 is generated by x and $H_{3,1}$ is generated by y. There exists positive integer i < 7 such that $yx = x^iy$. Further, i satisfies $i^3 = 1 \mod 7$, that is, i = 1, 2, 4.
- (3) Let G_i denote the group generated by x, y satisfying $x^7 = e, y^3 = e$, and $yx = x^i y$. Then G_1 is abelian and isomorphic to $H_7 \times H_{3,1}$.
- (4) Define $\phi: G_2 \to G_4$ by $\phi(x) = x$ and $\phi(y) = y^2$. Show that ϕ extends to an isomorphism.

Conclude that there are two isomorphism classes of groups of order 21.

Corollary 5.36. Let p, q be primes. Then every group G of order p^2q is not simple.

Proof. Let H_p, H_q denote Sylow *p*-subgroup and Sylow *q*-subgroup of *G* respectively.

Suppose $q \neq 1 \mod p$. By the Third Sylow Theorem, H_p is the only Sylow *p*-subgroup, and hence normal in *G*.

Suppose $p^2 \neq 1 \mod q$. Then $p \neq 1 \mod q$. By similar reasoning, H_q is a normal Sylow q-subgroup of G.

Suppose $q = 1 \mod p$ and $p^2 = 1 \mod q$. This implies q > p. But then q must divide p + 1 and p divides q - 1. This is possible iff p = 2 and q = 3. The desired conclusion follows from Example 5.30.

Exercise 5.37 : Let G be a group of order 56 and let N_p denote the number of Sylow p-subgroups of G. Verify the following:

(1) Either $N_7 = 1$ or $N_7 = 8$.

(2) If $N_7 = 8$ then G contains 48 elements of order 7.

(3) Either $N_7 = 1$ or $N_2 = 1$.

(4) G is not simple.

Exercise 5.38 : Show that a finite group with every normal and abelian Sylow subgroup is necessarily abelian.

6. Structure Theorem for Finite Abelian Groups

We will always assume that an abelian group G carries addition as the binary operation. We say that G is the *direct sum* $H_1 \oplus H_1 \oplus \cdots H_k$ of subgroups H_1, H_2, \cdots, H_k of G if $G = H_1 + H_2 + \cdots + H_k$ and $H_i \cap H_j = \{0\}$ for all $i \neq j$.

The most basic example of finite abelian groups is the cyclic group C_n of order n. It turns out that this forms a building block in the representation theorem for abelian groups.

Exercise 6.1: Let $m, n \in \mathbb{N}$ be coprime. Show that there exist $x, y \in C_{mn}$ of order m and n respectively such that $C_{mn} = \langle x \rangle \oplus \langle y \rangle$, where

24

 $\langle a \rangle$ denotes the cyclic group generated by $a \in C_{mn}$. Conclude that C_{mn} is isomorphic to $C_m \oplus C_n$.

Remark 6.2: Any cyclic group is isomorphic to the direct sum of finitely many cyclic groups of prime-power order. In fact, if $m = \prod_{j=1}^{l} p_{j}^{k_{j}}$, where p_{j} are distinct primes and k_{j} are positive integers then C_{m} is isomorphic to the direct sum $\bigoplus_{j=1}^{l} C_{p^{k_{j}}}$.

To understand finite abelian groups, in view of the last remark, it suffices to understand the structure of non-cyclic abelian groups.

For an $n \times n$ matrix A, the *i*th row is denoted by A_i .

Exercise 6.3: For $n \ge 2$, let a_1, \dots, a_n be integers with gcd 1. For $n \ge 2$, consider the statement P_n : Then there exists $A \in SL_n(\mathbb{Z})$ such that $A_1 = [a_1 \cdots a_n]$. Prove P_n by induction on n by verifying:

- (1) P_2 holds true.
- (2) Assume P_{n-1} . Let d be the gcd of a_1, \dots, a_{n-1} . Then there exists $B \in SL_{n-1}(\mathbb{Z})$ such that $B_1 = [b_1 \cdots b_{n-1}]$, where $b_i = a_i d^{-1}$.
- (3) Let B be as ensured by (2). Choose $s, t \in \mathbb{Z}$ such that $sa_n + td = 1$. Let A be such that $A_1 = [a_1 \cdots a_n], A_i = [B_i \ 0] \ (i = 2, \cdots, n-1),$ and $A_n = [c_1 \cdots c_{n-1} \ t]$, where $c_i = (-)^n sb_i$. Verify that $A \in SL_n(\mathbb{Z})$.

Lemma 6.4. Let G be an abelian group such that $x_1, \dots, x_n \in G$ are generators of G. If $X = [x_1 \cdots x_n]^t$ and $A \in SL_n(\mathbb{Z})$ then the entries of AX are generators of G. In particular, if $y_1 = a_1x_1 + \dots + a_nx_n$, then there exist y_2, \dots, y_n such that $y_1, \dots, y_n \in G$ are generators of G.

Proof. Note that if $A \in SL_n(\mathbb{Z})$ then $A^{-1} \in SL_n(\mathbb{Z})$. If $x \in G$ then there exists $k_1, \dots, k_n \in \mathbb{Z}$ such that $x = k_1x_1 + \dots + k_nx_n$. Now if AX = Y then $x = k_1(A^{-1}X)_1 + \dots + k_n(A^{-1}X)_n$ is a \mathbb{Z} -linear combination of y_1, \dots, y_n . This completes the proof of the first part. To see the remaining part, let $A \in SL_n(\mathbb{Z})$ with first row $[a_1 \cdots a_n]$ as ensured by the last exercise, and take $y_i = (A^{-1}X)_i$ for $i = 2, \dots, n$.

The last lemma may be interpreted as:

Proposition 6.5. Let G be a finitely generated abelian group. Let $\mathcal{F} = \{F : F \text{ is a set of generators of } G\}$. Let $n = \min_{F \in \mathcal{F}} |F|$. Let $\mathcal{F}_n = \{[g_1 \cdots g_n]^T : \{g_1, \cdots, g_n\} \in \mathcal{F}\}$. Then the group $SL_n(\mathbb{Z})$ acts on \mathcal{F}_n via A * F = AF.

Theorem 6.6. If G is a finitely generated abelian group then G is the direct sum of cyclic groups.

Proof. Let $\{x_1, \dots, x_n\} \in \mathcal{F}_n$ be such that x_n has the minimal order k, where \mathcal{F}_n is as defined in the last remark. We prove by induction that $G = \mathbb{Z}x_1 \oplus \dots \oplus \mathbb{Z}x_n$. The case n = 1 is trivial. Let H be the proper subgroup of G generated by x_1, \dots, x_{n-1} . By the induction hypothesis, $H = \mathbb{Z}x_1 \oplus \dots \oplus \mathbb{Z}x_{n-1}$. Thus it suffices to check that $G = H \oplus \mathbb{Z}x_n$.

Clearly, $G = H + \mathbb{Z}x_n$. Suppose $H \cap \mathbb{Z}x_n \neq \{0\}$. Then there there exist $a_1, \dots, a_n \in \mathbb{Z}$ such that $a_1x_1 + \dots + a_{n-1}x_{n-1} = a_nx_n \neq 0$. In particular, $a_n < k$. If gcd of a_1, \dots, a_n is d then $y_1 = \frac{a_1}{d}x_1 + \dots + \frac{a_{n-1}}{d}x_{n-1} - \frac{a_n}{d}x_n$ satisfies $dy_1 = 0$. Also, by the preceding proposition, there exist $y_2, \dots, y_n \in G$ such that $\{y_2, \dots, y_n, y_1\} \in \mathcal{F}_n$. But then the order l of y_1 must be less than or equal to the order k of x_n , that is $l \leq k$. Also, since $dy_1 = 0$, l divides $d \leq a_n < k$. This is not possible.

Remark 6.7: Any finite abelian group is isomorphic to the direct sum of finitely many cyclic groups of prime-power order. In particular, the abelian group of order 16, up to isomorphism, are

$$C_{16}, C_2 \oplus C_8, C_4 \oplus C_4, C_2 \oplus C_2 \oplus C_4, C_2 \oplus C_2 \oplus C_2 \oplus C_2$$

(see Remark 6.2).

Exercise 6.8 : List all abelian groups of order 216 up to isomorphism.

Acknowledgment. I am thankful to all the students of MTH 751 for their active participation and several valuable inputs.

References

- [1] M. Artin, Algebra, Eastern Economy Edition, 1996.
- [2] J. Clay, The Punctured Plane is Isomorphic to the Unit Circle, Journal of Number Theory, 1, 500-501, 1969.
- [3] K. Conrad, Group Actions, available online.
- [4] S. Kumaresan, *Group Actions; Sylow Theorems: Expository Articles (Level 1)*, private communication.
- [5] S. Kumaresan, Basis Theorem for Finitely Generated Abelian Groups: Expository Articles (Level 2), private communication.
- [6] P. Morandi, Group Actions, available online.

26