

Abstract Algebra

Group Theory

ALEX FENG

2023

Contents

Chapter 1	Introduction to Groups	Page 2
1.1	Basic Axioms	2
1.2	Dihedral Groups	4
1.3	Symmetric Groups	5
1.4	Matrix Groups	5
1.5	The Quaternion Group	6
1.6	Homomorphisms and Isomorphisms	6
1.7	Group Actions	7
Chapter 2	Subgroups	Page 8
2.1	Definitions	8
2.2	Centralizers, Normalizers, Stabilizers, and Kernels	9
2.3	Cyclic Groups and Cyclic Subgroups	10
Chapter 3	Quotient Groups and Homomorphisms	Page 13
3.1	Definitions	13
3.2	Lagrange's Theorem	17
3.3	The Isomorphism Theorems	19
3.4	Composition Series and The Hölder Program	20
3.5	Transpositions and the Alternating Group	21
Chapter 4	Group Actions	Page 23
4.1	Group Actions and Permutation Representations	23
4.2	Cayley's Theorem	24
4.3	The Class Equation	25
4.4	Automorphisms	27
4.5	Sylow's Theorem	30
Chapter 5	Direct Products	Page 32
5.1	Direct Products	32
5.2	The Fundamental Theorem of Finitely Generated Abelian Groups	33

Chapter 1

Introduction to Groups

1.1 Basic Axioms

Definition 1.1.1: Binary Operation

1. A binary operation $*$ on a set G is a function $*$: $G \times G \rightarrow G$. For any $a, b \in G$, we write $a * b$ for $*(a, b)$.
2. A binary operation $*$ on a set G is associative if

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

3. If $*$ is a binary operation on G , elements $a, b \in G$ commute if $a * b = b * a$. We say $*$ (or G) is commutative if

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

Example 1.1.1 (Binary Operations)

- Commutative:
- $+$, usual addition on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, or \mathbb{C}
 - \times , usual multiplication on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, or \mathbb{C}
- Noncommutative:
- $-$, usual subtraction on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, or \mathbb{C} (Not a binary operation on $\mathbb{Z}^+, \mathbb{Q}^+$, or \mathbb{R}^+)
 - Cross product of two vectors in \mathbb{R}^3 (also not associative)

Let $*$ be a binary operation on set G and $H \subseteq G$. H is said to be closed under $*$ if

$$\forall a, b \in H, a * b \in H$$

Additionally, if $*$ is associative or commutative on G , it retains the same property when it is restricted to H .

Definition 1.1.2: Group

An ordered pair $(G, *)$ is a group (for a set G under binary operation $*$) if:

1. $\forall a, b, c \in G, (a * b) * c = a * (b * c)$ ($*$ is associative),
2. $\exists e \in G, \forall a \in G, a * e = e * a = a$ (existence of identity element),
3. $\forall a \in G, \exists a^{-1} \in G, a * a^{-1} = a^{-1} * a = e$ (existence of inverse)

$(G, *)$ is called abelian if $\forall a, b \in G, a * b = b * a$

Note:-

We (informally) say G is a group under $*$ if $(G, *)$ is a group, or even just G is a group. G is a finite group if G is a finite set.

Example 1.1.2 (Groups)

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and \mathbb{C} are groups under $+$ ($e = 0, a^{-1} = -a$). $\mathbb{Q} - \{0\}, \mathbb{R} - \{0\}, \mathbb{C} - \{0\}, \mathbb{Q}^+$, and \mathbb{R}^+ are groups under \times ($e = 1, a^{-1} = \frac{1}{a}$). $\mathbb{Z} - \{0\}$ is not a group under \times because not every element has an inverse. Vector spaces are abelian groups under addition (due to their axioms).

Proposition 1.1.1

Let $(G, *)$ be a group. Then

1. the identity of G is unique
2. the inverse of each element in G is unique
3. $\forall a \in G, (a^{-1})^{-1} = a$
4. $(a * b)^{-1} = b^{-1} * a^{-1}$
5. for any $a_1, a_2, \dots, a_n \in G$, $a_1 * a_2 * \dots * a_n$ is independent of how it is bracketed (generalized associative law).

Proof: 1. Suppose f and g are both identities. By the group definition axiom, $f * g = f$ and $f * g = g$. Thus, $g = f$ and the identity is unique

2. Assume b and c are both inverses of a . By the group definition axiom, $a * b = e$ and $c * a = e$. Then,

$$\begin{aligned}
 c &= c * e \\
 &= c * (a * b) \\
 &= (c * a) * b \\
 &= e * b \\
 &= b
 \end{aligned}$$

3. Read part 2 with a and a^{-1} interchanged.

4. Let $c = (a * b)^{-1}$. Then,

$$\begin{aligned}
 (a * b) * c &= e \\
 a * (b * c) &= e \\
 a^{-1} * a * (b * c) &= a^{-1} * e \\
 (a^{-1} * a) * (b * c) &= a^{-1} \\
 e * (b * c) &= a^{-1} \\
 b * c &= a^{-1}
 \end{aligned}$$

Repeating the process for b^{-1} shows that $c = b^{-1} * a^{-1}$

**Note:-**

For simplicity, abstract groups such as G and H will be written with binary operation \cdot and $a \cdot b$ will be written as ab . Brackets will not be used if the generalized associative law applies. For an abstract group (G, \cdot) , the identity will be denoted by 1. $x \in G, n \in \mathbb{Z}^+$, the product $xx \dots x$ (with n terms) will be denoted x^n .

Proposition 1.1.2

For a group G , with $a, b \in G$,

$$au = av \implies u = v$$

and

$$ub = vb \implies u = v.$$

Definition 1.1.3: Order of Element

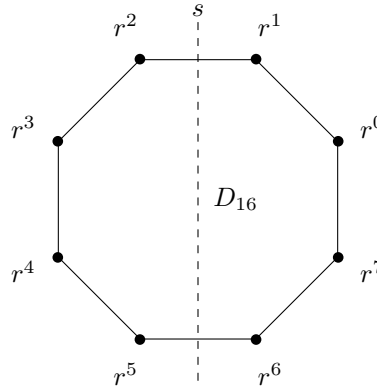
For a group G and $x \in G$, the order of x , denoted $|x|$, is the smallest positive integer n such that $x^n = 1$. x is said to be of infinite order if no such n exists.

1.2 Dihedral Groups

Definition 1.2.1: Dihedral Group

For each $n \in \mathbb{Z}^+, n \geq 3$, D_{2n} is the set of symmetries r and s of a regular n -gon (rotation by $\frac{2\pi}{n}$ and flipping over a line of symmetry).

The symmetries are represented by permutations on $\{1, 2, \dots, n\}$, and D_{2n} is a group under function composition.



Proposition 1.2.1

1. $|r| = n$
2. $|s| = 2$
3. $s \neq r^i$ for any i
4. $D_{2n} = \{1, r, r^2, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\}$
5. $rs = sr^{-1}$ (which shows that D_{2n} is not abelian)
6. $r^i = sr^{-i}$

For a group G , $S \subseteq G$ with the property that every element of G can be written as a (finite) product of elements in S and their inverses is a set of generators of G (S generates G). The equations that the generators satisfy are called relations (in G). For some collection of relations, R_1, R_2, \dots, R_m such that the relation among any element can be deduced, the presentation of G is written

$$G = \langle S \mid R_1, R_2, \dots, R_m \rangle$$

Example 1.2.1 (Presentation of Dihedral Group)

The presentation of Dihedral group of order $2n$ is

$$D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$$

1.3 Symmetric Groups

Definition 1.3.1: Set of all Permutations

Let Ω be any nonempty set. S_Ω is the set of all permutations of Ω . It is denoted S_n in the special case when $\Omega = \{1, 2, \dots, n\}$.

Under function composition, S_Ω is called the symmetric group on the nonempty set Ω . For symmetric groups, we now use cycle decomposition notation, which is much more efficient. If $a_i \mapsto a_{i+1}$ for $1 \leq i \leq m-1$ and $a_m \mapsto a_1$, with k cycles, we write

$$(a_1 \ a_2 \ \dots \ a_{m_1})(a_{m_1+1} \ a_{m_1+2} \ \dots \ a_{m_2}) \dots (a_{m_{k-1}+1} \ a_{m_{k-1}+2} \ \dots \ a_{m_k})$$

The length of a cycle is the number, t , of integers appearing in it, called a t -cycle. Two cycles are disjoint if they have no numbers in common. Elements that are mapped to themselves aren't written in cycle decomposition.

Note:-

Since the binary operation is function composition, the product of two cycles $(1 \ 2) \circ (2 \ 3)$, shortened to $(1 \ 2)(2 \ 3)$ when the context is clear, is equal to $(1 \ 2 \ 3)$ since function composition is read right to left.

1.4 Matrix Groups

Definition 1.4.1: Field

A field is a set F under two binary operations $+$ and \cdot such that $(F, +)$ and $(F - \{0\}, \cdot)$ are abelian groups following the distributive law:

$$\forall a, b, c \in F, a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

Let $F^\times = F - \{0\}$ for any field F .

Example 1.4.1 (Fields)

A few examples of fields include

- \mathbb{Q}
- \mathbb{R}
- For a prime p , $\mathbb{Z}/p\mathbb{Z}$, which will be denoted \mathbb{F}_p

Definition 1.4.2: General Linear Group of Degree n

Let $M_{n \times n}$ be the set of all $n \times n$ matrices. For any $n \in \mathbb{Z}^+$,

$$\text{GL}_n(F) = \{A \in M_{n \times n} \mid \det(A) \neq 0\}$$

The order of a finite field is equal to p^m for some prime p and integer m . Additionally, for a field F ,

$$|F| = q < \infty \implies |\text{GL}_n(F)| = \prod_{m=0}^{n-1} (q^n - q^m)$$

1.5 The Quaternion Group

Definition 1.5.1: The Quaternion Group

The quaternion group, Q_8 , is defined by

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

with product \cdot computed as follows: For all $a \in Q_8$,

$$1 \cdot a = a \cdot 1 = a$$

$$(-1) \cdot (-1) = 1$$

$$(-1) \cdot a = a, a \cdot (-1) = -a$$

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

$$i \cdot j = k,$$

$$j \cdot i = -k$$

$$j \cdot k = i,$$

$$k \cdot j = -i$$

$$k \cdot i = j,$$

$$i \cdot k = -j.$$

1.6 Homomorphisms and Isomorphisms

Definition 1.6.1: Homomorphism

Let $(G, *)$ and (H, \cdot) be groups. A homomorphism is a map $\varphi : G \rightarrow H$ such that

$$\forall x, y \in G, \varphi(x * y) = \varphi(x) \cdot \varphi(y)$$

Definition 1.6.2: Isomorphism

An isomorphism is a bijective homomorphism. Two isomorphic groups G and H can be written $G \cong H$.

Example 1.6.1 (Isomorphisms)

- The identity map is an obvious isomorphism.
- $\exp : \mathbb{R} \rightarrow \mathbb{R}^+$ is an isomorphism from $(\mathbb{R}, +)$ to (\mathbb{R}^+, \times) .

It is easy to see if two groups are not isomorphic. For an isomorphism $\varphi : G \rightarrow H$,

- $|G| = |H|$
- G is abelian if and only if H is abelian
- $\forall x \in G, |x| = |\varphi(x)|$

1.7 Group Actions

Definition 1.7.1: Group Action

A group action of a group G on a set A is a map from $G \times A$ to A , written as $g \cdot a$ for all $g \in G$ and $a \in A$, that satisfies the following properties:

1. $\forall g_1, g_2 \in G, a \in A, g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$, and
2. $\forall a \in A, 1 \cdot a = a$.

Note:-

We say that G is a group acting on a set A .

Let the group G act on the set A . For each fixed $g \in G$, we get a map $\sigma_g : A \rightarrow A$ defined by

$$\sigma_g(a) = g \cdot a.$$

Proposition 1.7.1

1. For each fixed $g \in G$, σ_g is a permutation of A , and
2. The map from G to S_A defined by $g \mapsto \sigma_g$ is a homomorphism (and it is called the permutation representation associated to the given action).

Proof: 1. σ_g is a map from A to A , and it can be shown to be a permutation if it is bijective (and has a two-sided inverse).

$$\begin{aligned}(\sigma_{g^{-1}} \circ \sigma_g)(a) &= \sigma_{g^{-1}}(\sigma_g(a)) \\ &= g^{-1} \cdot (g \cdot a) \\ &= (g^{-1}g) \cdot a \\ &= 1 \cdot a = a\end{aligned}$$

Then $\sigma_{g^{-1}} \circ \sigma_g : A \rightarrow A$ is the identity map. g was arbitrary and we can interchange the roles of g and g^{-1} to obtain $\sigma_g \circ \sigma_{g^{-1}}$ is also the identity map. Then, σ_g has a two-sided inverse, hence is a permutation of A .

2. Let $\varphi : G \rightarrow S_A$ be defined by $g \mapsto \sigma_g$ (and note that we just proved $\sigma_g \in S_A$). For all $a \in A$,

$$\begin{aligned}\varphi(g_1 g_2)(a) &= \sigma_{g_1 g_2}(a) \\ &= (g_1 g_2) \cdot a \\ &= g_1 \cdot (g_2 \cdot a) \\ &= \sigma_{g_1}(\sigma_{g_2}(a)) \\ &= (\varphi(g_1) \circ \varphi(g_2))(a)\end{aligned}$$

Thus, φ is a homomorphism.



Chapter 2

Subgroups

2.1 Definitions

Definition 2.1.1: Subgroup

Let G be a group. $H \subseteq G$ is a subgroup of G if $H \neq \emptyset$ and

$$x, y \in H \implies x^{-1} \in H, xy \in H$$

$H \leq G$ denotes that H is a subgroup of G . $H < G$ denotes proper containment.

If G is a group and $H \leq G$, H has the same binary operation on G and is a group.

Example 2.1.1 (Subgroups)

- $\mathbb{Z} \leq \mathbb{Q}$ and $\mathbb{Q} \leq \mathbb{R}$ under addition.
- All groups have trivial subgroup $\{1\}$ called the trivial subgroup, henceforth denoted by 1 .
- Let $H = \{1, r, r^2, \dots, r^{n-1}\}$. H is closed under the binary operation of D_{2n} and $H \subseteq D_{2n}$ so $H \leq D_{2n}$.
- The set of all even integers is a subgroup of \mathbb{Z} under addition.

Proposition 2.1.1 The Subgroup Criterion

Let G be a group. $H \subseteq G$ is a subgroup if and only if

1. $H \neq \emptyset$
2. $\forall x, y \in H, xy^{-1} \in H$.

Proof: 1. and 2. must obviously hold if $H \leq G$.

To show that the converse holds, let $x \in H$ (since $H \neq \emptyset$). Letting $y = x$ implies that $xx^{-1} \in H$, so $1 \in H$.

Then, H must contain the elements 1 and x , so it must also contain $1x^{-1}$ and $x^{-1} \in H$, implying that H is closed under taking inverses.

Finally, if $x, y, y^{-1} \in H \implies x(y^{-1})^{-1} \in H$. Then, $xy \in H$. Hence, H is a subgroup of G .



2.2 Centralizers, Normalizers, Stabilizers, and Kernels

Definition 2.2.1: Centralizer

The centralizer of nonempty $A \subseteq G$ in group G is the subset of G

$$C_G(A) = \{g \in G \mid \forall a \in A, gag^{-1} = a\}$$

$C_G(A)$ contains all elements of G that commute with every element in A .

To show that $C_G(A) \leq G$, we first see that $1 \in C_G(A) \implies C_G(A) \neq \emptyset$. Secondly, assume that $x, y \in C_G(A)$, or

$$\forall a \in A, xax^{-1} = a, yay^{-1} = a$$

$$\begin{aligned} (xy)a(xy)^{-1} &= (xy)a(y^{-1}x^{-1}) \\ &= x(yay^{-1})x^{-1} \\ &= xax^{-1} \\ &= a \end{aligned}$$

Then, $x, y \in C_G(A) \implies xy \in C_G(A)$. Observe that $xax^{-1} = a \implies a = x^{-1}ax$ so $\forall x \in C_G(A), x^{-1} \in C_G(A)$. Therefore, $C_G(A)$ is a subgroup.

Example 2.2.1 (Centralizers of Groups)

- If G is an abelian group, $\forall A \subseteq G, C_G(A) = G$
- $C_{Q_8}(i) = \{\pm 1, \pm i\}$

Definition 2.2.2: Center

The center of G is the subset

$$Z(G) = C_G(G) = \{g \in G \mid \forall x \in G, gx = xg\}$$

This is the set of all elements commuting with all elements of G .

Definition 2.2.3: Normalizer

Define

$$gAg^{-1} = \{gag^{-1} \mid a \in A\}.$$

The normalizer of A in G is the set

$$N_G(A) = \{g \in G \mid gAg^{-1} = A\}.$$

If G is a group acting on set S , for some fixed $s \in S$ the stabilizer of s in G is the set

$$G_s = \{g \in G \mid g \cdot s = s\}$$

The kernel of the action of G on S is defined as

$$\{g \in G \mid \forall s \in S, g \cdot s = s\}$$

2.3 Cyclic Groups and Cyclic Subgroups

Definition 2.3.1: Cyclic Group

A group H is cyclic if

$$\exists x \in H, H = \{x^n \mid n \in \mathbb{Z}\}$$

Equivalently, H is cyclic if it can be generated by a single element.

Observe that $H = \langle x \rangle \implies H = \langle x^{-1} \rangle$. Additionally, note that all cyclic groups are abelian.

Proposition 2.3.1

$$H = \langle x \rangle \implies |H| = |x|$$

(one side being infinite implies that the other is too.)

More specifically,

1. $|H| = n < \infty \implies x^n = 1$ and $1, x, x^2, \dots, x^{n-1}$ are all distinct elements in H
2. $|H| = \infty \implies (\forall n \neq 0, x^n \neq 1) \wedge (\forall a \neq b \in \mathbb{Z}, x^a \neq x^b)$

Proposition 2.3.2

Let G be an arbitrary group, $x \in G$, and $m, n \in \mathbb{Z}$.

$$x^n = 1 \wedge x^m = 1 \implies x^{(m,n)} = 1.$$

In particular,

$$x^m = 1 \implies (|x|) \mid m.$$

Proof: By the Euclidean Algorithm, $\exists r, s \in \mathbb{Z}, (m, n) = mr + ns$. Thus,

$$x^{(m,n)} = x^{mr+ns} = (x^m)^r (x^n)^s = 1^r 1^s = 1.$$



Theorem 2.3.1 Cyclic Group Isomorphism

1. If $n \in \mathbb{N}$ and $\langle x \rangle$ and $\langle y \rangle$ are both cyclic groups of order n , there exists a well defined isomorphism

$$\varphi : \langle x \rangle \rightarrow \langle y \rangle$$

$$x^k \mapsto y^k$$

2. If $\langle x \rangle$ is an infinite cyclic group, there exists a well defined isomorphism

$$\varphi : \mathbb{Z} \rightarrow \langle x \rangle$$


$$k \mapsto x^k$$

Proof: Let $\langle x \rangle$ and $\langle y \rangle$ be cyclic groups of order n and $\varphi : \langle x \rangle \rightarrow \langle y \rangle, x^k \mapsto y^k$. To prove φ is well defined

$(x^r = x^s \implies \varphi(x^r) = \varphi(x^s))$, $x^{r-s} = 1$ so, by proposition 2.3.2, $n \mid r - s$. Then,

$$\begin{aligned} r &= tn + s \\ \varphi(x^r) &= \varphi(x^{tn+s}) \\ &= y^{tn+s} \\ &= (y^n)^t y^s \\ &= y^s = \varphi(x^s) \end{aligned}$$

Thus, φ is well defined. $\varphi(x^a x^b) = \varphi(x^a) \varphi(x^b)$ so φ is a homomorphism. All elements y^k have a preimage x^k so the map is surjective. The groups have the same finite order so φ must be bijective if it is a surjection. Thus, φ is an isomorphism. If $\langle x \rangle$ has infinite order, let well defined map $\varphi : \mathbb{Z} \rightarrow \langle x \rangle, k \mapsto x^k$. $\forall a \neq b \in \mathbb{Z}, x^a \neq x^b$ so it is injective. φ is surjective by the definition of a cyclic group. Then, φ is an isomorphism.

Now, let $\langle x \rangle$ be an infinite cyclic group, and $\varphi : \mathbb{Z} \rightarrow \langle x \rangle, k \mapsto x^k$. φ is obviously well defined, and since $a \neq b \implies x^a \neq x^b$, φ is injective. φ is surjective by the definition of a cyclic group, and it can be verified to be a homomorphism. Thus, φ is an isomorphism. 

From now on, let for each $n \in \mathbb{N}$, let Z_n denote the cyclic group of order n , written multiplicatively.

Proposition 2.3.3

Let G be a group, $x \in G$, $a \in \mathbb{Z} - \{0\}$

1. $|x| = \infty \implies |x^a| = \infty$
2. $|x| = n < \infty \implies |x^a| = \frac{n}{(n,a)}$
3. $|x| = n < \infty \wedge (a \in \mathbb{Z}^+, a \mid n) \implies |x^a| = \frac{n}{a}$

Proof: Suppose that $|x| = \infty$ but $|x^a| = m < \infty$. By the definition of order,

$$\begin{aligned} 1 &= (x^a)^m = x^{am} \\ x^{-am} &= (x^{am})^{-1} = 1 \end{aligned}$$


Either am is positive or $-am$ is, so there exists a positive power of x equal to the identity, which is a contradiction.

Let $y = x^a$, $(n, a) = d$, $n = db$, $a = dc$ for $b, c \in \mathbb{Z}, b > 0$. d is the gcd of n and a so $(b, c) = 1$. To show that $|y| = b$,

$$y^b = x^{ab} = x^{dcb} = (x^n)^c = 1$$

so $(|y|) \mid b$. Then,

$$x^{a|y|} = y^{|y|} = 1$$

It follows that $n \mid (a|y|)$ so $b \mid (c|y|)$. $(b, c) = 1$ so $b \mid (|y|)$. $b \mid (|y|)$ and $(|y|) \mid b$ implies that $|y| = b$. Thus, $n = d|y|$ and $|y| = \frac{n}{d}$ 


Proposition 2.3.4

Let $H = \langle x \rangle$.

1. $|x| = \infty \implies (H = \langle x^a \rangle \iff a = \pm 1)$
2. $|x| = n < \infty \implies (H = \langle x^a \rangle \iff (a, n) = 1)$. Note that the number of generators of H is $\varphi(n)$ (where φ is Euler's φ -function)

Proof: If $|x| = n < \infty$, x^a generates a subgroup of H of order $|x^a|$. This subgroup equals H if and only if $|x^a| = |x|$.

$$|x^a| = |x| \iff \frac{n}{(a, n)} = n$$

Then $(a, n) = 1$, and by definition $\varphi(n)$ is the number of such generators. 

Theorem 2.3.2

Let $H = \langle x \rangle$ be a cyclic group.

1. $K \leq H \implies (K = \{1\}) \vee (K = \langle x^d \rangle)$, where d is the smallest positive integer such that $x^d \in K$.
2. $|H| = \infty \implies \forall a \neq b \in \mathbb{N}, \langle x^a \rangle \neq \langle x^b \rangle$. Additionally, $\forall m \in \mathbb{Z}, \langle x^m \rangle = \langle x^{|m|} \rangle$, so the nontrivial subgroups of H correspond bijectively with \mathbb{N} .
3. $|H| = n < \infty$ implies that for each $a \in \mathbb{N}, a|n$ there is a unique subgroup of H of order a , $\langle x^d \rangle, d = \frac{n}{a}$. Furthermore, for every integer m , $\langle x^m \rangle = \langle x^{(n,m)} \rangle$, so the subgroups of H correspond bijectively with the positive divisors of n .

Proof: Let $K \leq H$. The proposition is true for $K = \{1\}$, so assume $K \neq \{1\}$. Thus, $\exists a \neq 0, x^a \in K$.

$$a < 0 \implies x^{-a} = (x^a)^{-1} \in K$$

so K always contains a positive power of x . Let

$$\mathcal{P} = \{b \mid b \in \mathbb{Z}^+ \wedge x^b \in K\}$$

There must exist a minimum element $d \in \mathcal{P}$. K is a subgroup and $x^d \in K$ so $\langle x^d \rangle \leq K$. $K \leq H$ so any element in K is of the form x^a for some integer a .

$$a = qd + r, \quad 0 \leq r < d$$

$$x^r = x^a (x^d)^{-q} \in K$$

since both $x^a, x^d \in K$. By minimality of d , $r = 0$ so $x^a = (x^d)^q \in \langle x^d \rangle$. Thus, $K \leq \langle x^d \rangle$, and since $\langle x^d \rangle \leq K$, $\langle x^d \rangle = K$.

Assume $|H| = n < \infty$ and $a \mid n$. Let $d = \frac{n}{a}$ so $\langle x^d \rangle$ so is a subgroup of order a , showing its existence. To show uniqueness, suppose K is any order a subgroup of H , with

$$K = \langle x^b \rangle$$

for the minimum positive integer b such that $x^b \in K$.

$$\frac{n}{d} = a = |K| = |x^b| = \frac{n}{(n, b)}$$

so $d = (n, b)$ and $d \mid b$. Then, $x^b \in \langle x^d \rangle$, hence

$$K \leq \langle x^d \rangle$$

$|\langle x^d \rangle| = a = |K|$ so $K = \langle x^d \rangle$. $\langle x^m \rangle$ and $\langle x^{(n,m)} \rangle$ have the same order and $(n, m) \mid n$. Thus, $\langle x^m \rangle = \langle x^{(n,m)} \rangle$ 🤖

Chapter 3

Quotient Groups and Homomorphisms

3.1 Definitions

Definition 3.1.1: Kernel

The kernel of homomorphism $\varphi : G \rightarrow H$ is the set

$$\ker \varphi = \{g \in G \mid \varphi(g) = 1\}$$

Proposition 3.1.1

Let G and H be groups and $\varphi : G \rightarrow H$ be a homomorphism.

1. $\varphi(1_G) = 1_H$ (1_G and 1_H are identities of G and H , respectively)
2. $\forall g \in G, \varphi(g^{-1}) = \varphi(g)^{-1}$
3. $\forall n \in \mathbb{Z}, \varphi(g^n) = \varphi(g)^n$
4. $\ker \varphi \leq G$
5. The image of G under φ , $\text{im}(\varphi) \leq H$

Definition 3.1.2: Quotient Group

Let $\varphi : G \rightarrow H$ be a homomorphism with kernel K . The quotient group, G/K (read G modulo K) is the group whose elements are fibers (set of preimages) of φ , with group operation such that if X and Y are the fibers above a and b respectively, the product of X and Y is the fiber above the product ab .

Proposition 3.1.2

Let $\varphi : G \rightarrow H$ be a homomorphism of groups with kernel K . Let $X = \varphi^{-1}(a)$. Then,

1. $\forall u \in X, X = \{uk \mid k \in K\}$
2. $\forall u \in X, X = \{ku \mid k \in K\}$

Proof: Let $u \in X$. By definition of X , $\varphi(u) = a$. Let

$$uK = \{uk \mid k \in K\}$$

To prove $uK \subseteq X$,

$$\begin{aligned}\forall k \in K, \varphi(uk) &= \varphi(u)\varphi(k) \\ &= \varphi(u)1 \\ &= a\end{aligned}$$

so $uk \in X \implies uK \subseteq X$. To prove the reverse inclusion, let $g \in X$ and $k = u^{-1}g$.

$$\begin{aligned}\varphi(k) &= \varphi(u^{-1})\varphi(g) = \varphi(u)^{-1}\varphi(g) \\ &= a^{-1}a = 1\end{aligned}$$

So $k \in \ker \varphi$, and $g = uk \in uK$, establishing $X \subseteq uK$. Therefore, $X = uK$. 

Definition 3.1.3: Coset

For any $N \leq G$ and $g \in G$,

$$gN = \{gn \mid n \in N\} \text{ and } Ng = \{ng \mid n \in N\}$$

are the left and right cosets of N in G , respectively. Any element of a coset is called a representative for it.

Theorem 3.1.1


Let G be a group and K be the kernel of some homomorphism from G to another group. The set of left cosets of K in G with operation defined by

$$uK \circ vK = (uv)K$$

forms a group, G/K . This operation is well defined in the sense that $u_1 \in uK \wedge v_1 \in vK \implies u_1v_1 \in uvK$. Additionally, $u_1v_1K = uvK$ so the multiplication doesn't depend on choice of representatives (element in coset) for the cosets. This statement is true when "left coset" is interchanged "right coset."

Proof: Let $X, Y \in G/K$ and $Z = XY \in G/K$ (by definition). Then, X, Z , and Z are (left) cosets of K . Assume K is the kernel of some homomorphism $\varphi : G \rightarrow H$ so $X = \varphi^{-1}(a)$ and $Y = \varphi^{-1}(b)$ for some $a, b \in H$. By the definition of the G/K operation, $Z = \varphi^{-1}(ab)$. Let $u \in X$ and $v \in Y$ be arbitrary representatives their cosets, so $\varphi(u) = a, \varphi(v) = b, X = uK, Y = vK$.

$$\begin{aligned}uv \in Z &\iff uv \in \varphi^{-1}(ab) \\ &\iff \varphi(uv) = ab \\ &\iff \varphi(u)\varphi(v) = ab\end{aligned}$$

The latter equality holds so $uv \in Z \implies Z = uvK$. Thus, $XY = uvK$ for any representatives $u \in X, v \in Y$. The last statement follows since $\forall u \in G, uK = Ku$. 

It is important to note that multiplication is independent of the representative chosen. \bar{u} can be used to denote a coset uK , and \bar{G} can denote G/K . Then, $\bar{u} \cdot \bar{v} = \overline{uv}$.

Example 3.1.1

- If $\varphi : G \rightarrow H$ is an isomorphism, $K = 1$ and the fibers of φ each contain one element, so $G/1 \cong G$.
- Let G be any group and $H = 1$ be a group of order 1. $\varphi : G \rightarrow H, g \in G \mapsto 1$ is the trivial homomorphism. $\ker \varphi = G$ and $G/G \cong Z_1 = \{1\}$.
- Define $\varphi : Q_8 \rightarrow V_4$ by

$$\pm 1 \mapsto 1, \pm i \mapsto a, \pm j \mapsto b, \pm k \mapsto c$$

$\ker \varphi = \{\pm 1\}$ and $Q_8/\langle \pm 1 \rangle$ can be thought of as the "absolute value" of Q_8 .

Proposition 3.1.3

Let $N \leq G$. The set of left cosets of N in G form a partition of G . Additionally,

$$\begin{aligned}\forall u, v \in G, uN = vN &\iff v^{-1}u \in N \\ uN = vN &\iff u \in vN \wedge v \in uN\end{aligned}$$

Proof:

$$\begin{aligned}N \leq G &\implies 1 \in N \\ \forall g \in G, g &= g \cdot 1 \in gN \\ G &= \bigcup_{g \in G} gN\end{aligned}$$

To show that $uN \cap vN \neq \emptyset$, let $x \in uN \cap vN$, for some $n, m \in N$,

$$\begin{aligned}x &= un = vm \\ u &= vmn^{-1} = vm_1 \\ \forall ut \in uN, ut &= (vm_1)t = v(m_1t) \in vN.\end{aligned}$$

Thus, $uN \subseteq vN$. u and v can be interchanged to obtain that $vN \subseteq uN$. Therefore, $uN \cap vN \neq \emptyset \implies uN = vN$.

$$uN = vN \iff u \in vN \iff n \in N, u = vn \iff v^{-1}u \in N$$

**Proposition 3.1.4**

Let G be a group and $N \leq G$.

1. The operation described by

$$uN \cdot vN = (uv)N$$

is well defined if and only if $\forall g \in G, n \in N, gng^{-1} \in N$.

2. If the operation is well defined then the set of left cosets of N in G is a group. The identity is $1N$ and $(gN)^{-1} = g^{-1}N$.

Proof: First assume

$$\forall u, v \in G, u, u_1 \in uN \wedge v, v_1 \in vN \implies uvN = u_1v_1N.$$

Let $g \in G$ and $n \in N$. If $u = 1, u_1 = n, v = v_1 = g^{-1}$ then

$$\begin{aligned}1g^{-1}N &= ng^{-1}N \\ 1 \in N &\implies ng^{-1} \cdot 1 \in ng^{-1}N \\ ng^{-1} \in g^{-1}N &\implies ng^{-1} = g^{-1}n_1\end{aligned}$$

for some $n_1 \in N$. Thus, $gng^{-1} = n_1 \in N$. Now assume $\forall g \in G, n \in N, gng^{-1} \in N$. Let $u, u_1 \in uN$ and $v, v_1 \in vN$. For some $n, m \in N$,

$$\begin{aligned}u_1 &= un \\ v_1 &= vm\end{aligned}$$

To prove $u_1v_1 \in uvN$,

$$\begin{aligned}u_1v_1 &= (un)(vm) = u(vv^{-1})nvm \\ &= (uv)(v^{-1}nv)m = (uv)(n_1m)\end{aligned}$$

where $n_1 = v^{-1}nv \in N$. Now N is closed under products so $n_1m \in N$ and $u_1v_1 = (uv)n_2$ for some $n_2 \in N$. Thus, uvN and u_1v_1N contain the common element u_1v_1 .



Definition 3.1.4: Normal Subgroup

gng^{-1} is the conjugate of $n \in N$ by g . $gNg^{-1} = \{gng^{-1} \mid n \in N\}$ is the conjugate of N by g . g is said to normalize N if $gNg^{-1} = N$. A subgroup N of G is said to be normal (denoted $N \trianglelefteq G$) if $\forall g \in G, gNg^{-1} = N$.

Theorem 3.1.2

Let $N \trianglelefteq G$. The following are equivalent:

1. $N \trianglelefteq G$
2. $N_G(N) = G$
3. $\forall g \in G, gN = Ng$
4. The set of left cosets form a group under the operation described in proposition 3.1.4
5. $\forall g \in G, gNg^{-1} \subseteq N$

Proposition 3.1.5

For some $N \leq G$ and homomorphism φ ,

$$N \trianglelefteq G \iff N = \ker \varphi$$

Proof: $N = \ker \varphi \implies \forall g \in G, gN = Ng$ so N will be normal. Conversely, let $H = G/N$ and $\pi : G \rightarrow G/N$ defined by $\forall g \in G, g \mapsto gN$.

$$\pi(g_1g_2) = (g_1g_2)N = g_1Ng_2N = \pi(g_1)\pi(g_2)$$

so π must be a homomorphism.

$$\begin{aligned} \ker \pi &= \{g \in G \mid \pi(g) = 1N\} \\ &= \{g \in G \mid gN = 1N\} \\ &= \{g \in G \mid g \in N\} = N \end{aligned}$$



Definition 3.1.5: Natural Projection

Let $N \trianglelefteq G$. The homomorphism $\pi : G \rightarrow G/N$ defined by $g \mapsto gN$ is called the natural projection (homomorphism) of G onto G/N . If $\bar{H} \leq G/N$, the complete preimage of \bar{H} in G is the preimage of \bar{H} under the natural projection homomorphism.

Example 3.1.2

Let G be a group

- $G/1 \cong G, \quad G/1 \trianglelefteq G$
 $G/G \cong 1, \quad G/G \trianglelefteq G$
- If G is abelian, $\forall N \leq G, N \trianglelefteq G$, because

$$\forall g \in G, n \in N, gng^{-1} = gg^{-1}n = n \in N$$

Note that only N being abelian is not sufficient.

Suppose $G = Z_k$. Let x be a generator of G and $N \leq G$. $N = \langle x^d \rangle$, where d is the smallest power of x that lies in N .

$$G/N = \{gN \mid g \in G\} = \{x^\alpha \mid \alpha \in \mathbb{Z}\}$$

and since $x^\alpha N = \langle xN \rangle^\alpha$, $G/N = \langle xN \rangle$.

$$|xN| = d = \frac{|G|}{|N|}.$$

Thus, quotient groups of a cyclic group are cyclic.

- Generalizing the previous example, $N \leq Z(G) \implies N \trianglelefteq G$.

3.2 Lagrange's Theorem

Theorem 3.2.1 Lagrange's Theorem

If G is a finite group and $H \leq G$, $|H| \mid |G|$, and the number of left cosets of H in G equals $|G|/|H|$.

Proof: Let $|H| = n$ and let the number of left cosets of H in G equal k . The set of left cosets of H in G partition G . The map

$$H \rightarrow gH \quad \text{defined by} \quad h \mapsto gh$$

is surjective. This map is injective because $gh_1 = gh_2 \implies h_1 = h_2$. Thus,

$$|gH| = |H| = n.$$

G is partitioned into k disjoint subsets each with cardinality n , so $|G| = kn$. Thus,

$$k = \frac{|G|}{n} = \frac{|G|}{|H|}.$$



Definition 3.2.1: Index


If G is a group and $H \leq G$, the number of left cosets of H in G is called the index of H in G , denoted by $|G : H|$.

Corollary 3.2.1

If G is a finite group and $x \in G$, $|x| \mid |G|$. In particular, $\forall x \in G, x^{|G|} = 1$

Corollary 3.2.2

If $|G| = p$ for some prime p , then G is cyclic, hence $G \cong Z_p$.

Proof: Let $x \in G, x \neq 1$. Thus $|\langle x \rangle| > 1$, and $|\langle x \rangle|$ divides $|G|$. $|G|$ is prime so $|\langle x \rangle| = |G|$. Thus, $G = \langle x \rangle$. 

Theorem 3.2.2 Cauchy's Theorem

If G is a finite group and a prime p divides $|G|$, then G has an element of order p .

Theorem 3.2.3 Sylow

If G is a finite group of order $p^\alpha m$, where p is prime and $p \nmid m$, then G has a subgroup of order p^α .

Definition 3.2.2

Let H and K be subgroups and define

$$HK = \{hk \mid h \in H, k \in K\}$$

Proposition 3.2.1

If H and K are finite subgroups of a group then


$$|HK| = \frac{|H||K|}{|H \cap K|}$$

Proof:

$$HK = \bigcup_{h \in H} hK.$$

Each coset of K has $|K|$ elements. To find the number of distinct left cosets, $h_1K = h_2K \iff h_2^{-1}h_1 \in K$. Thus,

$$h_1K = h_2K \iff h_2^{-1}h_1 \in H \cap K \iff h_1(H \cap K) = h_2(H \cap K).$$

Thus the number of distinct cosets of the form hK for $h \in H$ is the number of distinct cosets $h(H \cap K)$ for $h \in H$. By Lagrange's Theorem, this is $|H|/|H \cap K|$. Thus HK consists of $|H|/|H \cap K|$ distinct cosets of K , each with $|K|$ elements. 

Proposition 3.2.2

If $H \leq G$ and $K \leq G$, $HK \leq G \iff HK = KH$

Proof: First assume $HK = KH$ and let $a, b \in HK$. To prove $ab^{-1} \in HK$ so it is a subgroup, let

$$a = h_1k_1 \quad \text{and} \quad b = h_2k_2$$

for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Thus, $b^{-1} = k_2^{-1}h_2^{-1}$, so $ab^{-1} = h_1k_1k_2^{-1}h_2^{-1}$. Let $k_3 = k_1k_2^{-1} \in K$ and $h_3 = h_2^{-1}$. Thus $ab^{-1} = h_1k_3h_3$. Since $HK = KH$,

$$k_3h_3 = h_4k_4$$

for some $h_4 \in H, k_4 \in K$. Thus $ab^{-1} = h_1h_4k_4$ and since $h_1h_4 \in H, k_4 \in K$, $ab^{-1} \in HK$.

Conversely, assume $HK \leq G$. Since $K \leq HK$ and $H \leq HK$, $KH \subseteq HK$ by the closure property of subgroups. Let $hk \in HK$. Since HK is a subgroup, if $hk = a^{-1}$ and $a = h_1k_1$,

$$hk = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH$$

so $HK \subseteq KH$, implying $KH = HK$. 


Corollary 3.2.3

If $H \leq G, K \leq G$, then $H \leq N_G(K) \implies HK \leq G$. In particular,

$$\forall H \leq G, K \trianglelefteq G \implies HK \leq G$$

Proof: To prove $HK = KH$, let $h \in H, k \in K$. $hkh^{-1} \in K$, hence

$$hk = (hkh^{-1})h \in KH$$

proving that $HK \subseteq KH$. Similarly, $kh = h(h^{-1}kh) \in HK$, so $HK = KH$. This corollary follows from the previous proposition. 

Definition 3.2.3

If $A \subseteq N_G(K)$ (or $C_G(K)$), A is said to normalize K (or centralize K , respectively).

3.3 The Isomorphism Theorems

Theorem 3.3.1 The First Isomorphism Theorem

For some homomorphism $\varphi : G \rightarrow H$,

$$\ker \varphi \trianglelefteq G \quad \text{and} \quad G / \ker \varphi \cong \varphi(G).$$

Corollary 3.3.1

Let $\varphi : G \rightarrow H$ be a homomorphism


1. φ is injective if and only if $\ker \varphi = 1$
2. $|G : \ker \varphi| = |\varphi(G)|$.

Theorem 3.3.2 The Second/Diamond Isomorphism Theorem

Let G be a group $A \leq G$, $B \leq G$, and $A \leq N_G(B)$. Then, $AB \leq G$, $B \trianglelefteq AB$, $A \cap B \trianglelefteq A$, and $AB/G \cong A/A \cap B$.

Proof: AB is a subgroup of G by corollary 3.2.3. Since $A \leq N_G(B)$ and $B \leq N_G(B)$, $AB \leq N_G(B)$ ($B \trianglelefteq AB$). B is normal in AB so AB/B is well defined. Define map $\varphi : A \rightarrow AB/B$ by $a \mapsto aB$.

$$\varphi(a_1 a_2) = (a_1 a_2)B = a_1 B \cdot a_2 B = \varphi(a_1) \varphi(a_2)$$

From the definition of AB , φ is surjective. The identity in AB/B is coset $1B$ so $\ker \varphi$ consists of elements $a \in A$ with $aB = 1B$, which are the elements $a \in B$ ($\ker \varphi = A \cap B$). By the First Isomorphism Theorem, $A \cap B \trianglelefteq A$ and $A/A \cap B \cong AB/B$. 

Theorem 3.3.3 The Third Isomorphism Theorem

Let G be a group, $H \trianglelefteq G$, $K \trianglelefteq G$, and $H \leq K$. Then, $K/H \trianglelefteq G/H$ and

$$(G/H)/(K/H) \cong G/K$$

which can be denoted

$$\overline{G}/\overline{K} \cong G/K.$$

Proof: Define

$$\begin{aligned} \varphi : G/H &\rightarrow G/K \\ (gH) &\mapsto gK. \end{aligned}$$

To show φ is well defined, suppose $g_1 H = g_2 H$. Then $g_1 = g_2 h$ for some $h \in H$. $H \leq K$ so $h \in K$, hence, $g_1 K = g_2 K$, or $\varphi(g_1 H) = \varphi(g_2 H)$. $g \in G$ can be chosen arbitrarily so φ is surjective. Finally

$$\begin{aligned} \ker \varphi &= \{gH \in G/H \mid \varphi(gH) = 1K\} \\ &= \{gH \in G/H \mid gK = 1K\} \\ &= \{gH \in G/H \mid g \in K\} = K/H. \end{aligned}$$

By the First Isomorphism Theorem, $(G/H)/(K/H) \cong G/K$. 

Theorem 3.3.4 The Fourth/Lattice Isomorphism Theorem

Let G be a group and $N \trianglelefteq G$. Then there is a bijection from the set of subgroups A of G which contain N onto the set of subgroups $\overline{A} = A/N$ of G/N . In particular, every subgroup of \overline{G} is of the form A/N for some subgroup A of G containing N (namely, its preimage in G under the natural projection homomorphism from G to G/N). This bijection have the following properties: $\forall A, B \leq G$, $N \leq A$, $N \leq B$,

1. $A \leq B \iff \overline{A} \leq \overline{B}$
2. $A \leq B \implies |B : A| = |\overline{B} : \overline{A}|$
3. $\langle \overline{A}, \overline{B} \rangle = \overline{\langle A, B \rangle}$
4. $\overline{A \cap B} = \overline{A} \cap \overline{B}$
5. $A \trianglelefteq G \iff \overline{A} \trianglelefteq \overline{G}$.

3.4 Composition Series and The Hölder Program

Proposition 3.4.1

If G is a finite abelian group and a prime p divides $|G|$, then G contains an element of order p .

Proof: We proceed by induction on $|G|$.

$$|G| > 1 \implies \exists x \in G, x \neq 1$$


By Lagrange's Theorem,

$$|G| = p \implies \exists x \in G, |x| = p$$

and we are done. We may now assume $|G| > p$. Suppose p divides $|x|$, so $|x| = pn$.

$$|x^n| = p$$

and we have an element of order p again, so we assume p does not divide $|x|$.

Let $N = \langle x \rangle$. G is abelian so $N \trianglelefteq G$. By Lagrange's Theorem, $|G/N| = \frac{|G|}{|N|}$ and $|N| > 1$ so $|G/N| < |G|$. p does not divide $|N|$ so p must divide $|G/N|$. We can now apply the induction assumption to the smaller group G/N to conclude it contains an element $\overline{y} = yN$ of order p . Since $y \notin N$ ($\overline{y} \neq \overline{1}$) but $y^p \in N$ ($\overline{y}^p = \overline{1}$), we must have $\langle y^p \rangle \neq \langle y \rangle$, or $|y^p| < |y|$. Then, p divides $|y|$. We are now in the situation described in the preceding paragraph, which again produces an element of order p . 

Definition 3.4.1: Simple

A group G is called simple if $|G| > 1$ and the only normal subgroups of G are 1 and G .

Definition 3.4.2: Composition

In a group G a sequence of subgroups

$$1 = N_0 \leq N_1 \leq N_2 \leq \cdots \leq N_{k-1} \leq N_k = G$$

is called a composition series if $N_i \trianglelefteq N_{i+1}$ and N_{i+1}/N_i is a simple group, $0 \leq i \leq k-1$. If the sequence is a composition series, the quotient groups N_{i+1}/N_i are called composition factors of G .

Theorem 3.4.1 Jordan-Hölder

Let G be a finite group with $G \neq 1$. Then

1. G has a composition series and
2. The composition factors in a composition series are unique, namely, if $1 = N_0 \leq N_1 \leq \cdots \leq N_r = G$ and $1 = M_0 \leq M_1 \leq \cdots \leq M_s = G$ are two composition series for G , then $r = s$ and there is some permutation, π , of $\{1, 2, \dots, r\}$ such that for $1 \leq i \leq r$,

$$M_{\pi(i)}/M_{\pi(i)-1} \cong N_i/N_{i-1}$$

Theorem 3.4.2

There is a list consisting of 18 (infinite) families of simple groups and 26 simple groups not belonging to these families (the sporadic simple groups) such that every finite simple group is isomorphic to one of the groups in this list.

Theorem 3.4.3 Feit-Thompson

If G is a simple group of odd order, then $G \cong Z_p$ for some prime p .

Definition 3.4.3: Solvable

A group G is solvable if there is a chain of subgroups

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_s = G$$

such that G_{i+1}/G_i is abelian for $i = 0, 1, \dots, s-1$.

Theorem 3.4.4

The finite group G is solvable if and only if for every divisor n of $|G|$ such that $(n, \frac{|G|}{n}) = 1$, G has a subgroup of order n .

3.5 Transpositions and the Alternating Group

Definition 3.5.1: Transposition

A 2-cycle is called a transposition.

Definition 3.5.2: Sign

1. $\epsilon(\sigma)$ is called the sign of σ
2. σ is called an even permutation if $\epsilon(\sigma) = 1$ and odd if $\epsilon(\sigma) = -1$.

Proposition 3.5.1

The map $\epsilon : S_n \rightarrow \{\pm 1\}$ is a homomorphism (where $\{\pm 1\}$ is a multiplicative version of Z_2).

Proof: Let

$$\Delta = \prod_{1 \leq i < j \leq n} (x_i - x_j)$$

then

$$(\tau\sigma)(\Delta) = \prod_{1 \leq i < j \leq n} (x_{\tau\sigma(i)} - x_{\tau\sigma(j)})$$

Suppose that $\sigma(\Delta)$ has exactly k factors of the form $x_j - x_i$ with $j > i$, that is $\epsilon(\sigma) = (-1)^k$. When calculating $(\tau\sigma)(\Delta)$, after first applying σ to the indices we see that $(\tau\sigma)(\Delta)$ has exactly k factors of the form $x_{\tau(j)} - x_{\tau(i)}$ with $j > i$. Interchanging the order of the terms in these k factors introduces the sign change $(-1)^k = \epsilon(\sigma)$, and now all factors of $(\tau\sigma)(\Delta)$ are of the form $x_{\tau(p)} - x_{\tau(q)}$, with $p < q$. Thus

$$(\tau\sigma)(\Delta) = \epsilon(\sigma) \prod_{1 \leq p < q \leq n} (x_{\tau(p)} - x_{\tau(q)})$$

By the definition of ϵ ,

$$\prod_{1 \leq p < q \leq n} (x_{\tau(p)} - x_{\tau(q)}) = \epsilon(\tau) \Delta$$

We have $(\tau\sigma)(\Delta) = \epsilon(\sigma)\epsilon(\tau)\Delta$. Thus, $\epsilon(\tau\sigma) = \epsilon(\sigma)\epsilon(\tau) = \epsilon(\tau)\epsilon(\sigma)$.



Proposition 3.5.2

Transpositions are all odd permutations and ϵ is surjective.

Proof: $\epsilon((1\ 2)) = -1$. Any transposition $(i\ j)$ can be represented by $\lambda(i\ j)\lambda$ for $\lambda = (1\ i)(2\ j)$. Since ϵ is a homomorphism,

$$\begin{aligned} \epsilon((i\ j)) &= \epsilon(\lambda(1\ 2)\lambda) \\ &= \epsilon(\lambda)\epsilon((1\ 2))\epsilon(\lambda) \\ &= (-1)\epsilon(\lambda)^2 \\ &= -1. \end{aligned}$$



Definition 3.5.3: Alternating Group

The alternating group of degree n , denoted by A_n , is $\ker \epsilon$ (the set of all even permutations).

Proposition 3.5.3

The permutation σ is odd if and only if the number of cycles of even length in its cycle decomposition is odd.

Chapter 4

Group Actions

4.1 Group Actions and Permutation Representations

Definition 4.1.1

1. The kernel of the action is the set of elements of G that act trivially on every element of A :

$$\{g \in G \mid \forall a \in A, g \cdot a = a\}$$

2. The stabilizer of each $a \in A$ in G is the set of elements of G that fix element a :

$$G_a = \{g \in G \mid g \cdot a = a\}$$

3. An action is faithful if its kernel is the identity.

Example 4.1.1

Let $n \in \mathbb{N}$. The group $G = S_n$ acts on the set $A = \{1, 2, \dots, n\}$ by $\forall i \in \{1, \dots, n\}, \sigma \cdot i = \sigma(i)$. The permutation representation associated with this action is the identity map $\varphi : S_n \rightarrow S_n$. This action is faithful and for each i , $G_i \cong S_{n-1}$.

Proposition 4.1.1

For any group G and nonempty set A there is a bijection between the actions of G on A and homomorphisms of G onto S_A .

Proof: Let φ be any homomorphism of G into S_A . We obtain an action of G on A by defining

$$\forall g \in G, a \in A, g \cdot a = \varphi(g)(a)$$

The permutation representation associated to this action is the given homomorphism φ .



Definition 4.1.2: Permutation Representation

If G is a group, a permutation representation of G is any homomorphism of G into S_A for some nonempty set A . We say a given action of G on A affords or induces the associated permutation representation.

Proposition 4.1.2

Let G act on nonempty set A . The relation on A defined by

$$a \sim b \iff a = g \cdot b \text{ for some } g \in G$$

is an equivalence relation. For each $a \in A$, the cardinality of the equivalence class containing a is $|G : G_a|$.

Proof: $\forall a \in A, a = 1 \cdot a$ i.e., $a \sim a$ so the relation is reflexive. If $a \sim b$ so $a = g \cdot b$ for some $b \in G$,

$$g^{-1} \cdot a = g^{-1} \cdot (g \cdot b) = (g^{-1}g) \cdot b = 1 \cdot b = b$$

that is, $b \sim a$ so the relation is symmetric. Finally, if $a \sim b$ and $b \sim c$, then $a = g \cdot b$ and $b = h \cdot c$ for some $g, h \in G$, so

$$a = g \cdot b = g \cdot (h \cdot c) = (gh) \cdot c$$

hence $a \sim c$ and the relation is transitive.

Let \mathcal{C}_a be the equivalence class of a , so


$$\mathcal{C}_a = \{g \cdot a \mid g \in G\}.$$

Suppose $b = g \cdot a \in \mathcal{C}_a$. Then gG_a is a left coset of G_a in G . The map

$$b = g \cdot a \mapsto gG_a$$

is a map from \mathcal{C}_a to the set of left cosets of G_a in G . It is surjective since $\forall g \in G, g \cdot a \in \mathcal{C}_a$. Since

$$g \cdot a = h \cdot a \iff h^{-1}g \in G_a \iff gG_a = hG_a$$

the map is also injective, hence is it a bijection. 

Definition 4.1.3: Orbit

Let G act on nonempty set A .

1. The equivalence class $\{g \cdot a \mid g \in G\}$ is called the orbit of G containing a .
2. The action of G on A is called transitive if there is only one orbit, that is, $\forall a, b \in A, \exists g \in G, a = g \cdot b$

Example 4.1.2

Let G act on A

- If G acts trivially on A then $\forall a \in A, G_a = G$ and the orbits are the elements of A . This action is transitive if and only if $|A| = 1$
- $G = S_n$ acts transitively on $A = \{1, 2, \dots, n\}$.
- The group D_8 acts transitively on the four vertices of the square and the stabilizer of any vertex is the subgroup of order 2 generated by the reflection about the line of symmetry passing through that point.

4.2 Cayley's Theorem

Theorem 4.2.1

Let G be a group, $H \leq G$. Let G act by left multiplication on A , the set of left cosets of H in G . Let π_H be the associated permutation representation afforded by this action. Then,

1. G acts transitively on A
2. the stabilizer in G of the point $1H \in A$ is the subgroup H
3. the kernel of the action ($\ker \pi_H$) is $\bigcap_{x \in G} xHx^{-1}$ and $\ker \pi_H$ is the largest normal subgroup of G contained in H .

Proof: To prove transitivity, let $aH, bH \in A$ and $g = ba^{-1}$. Then $g \cdot aH = (ba^{-1})aH = bH$, so two arbitrary elements of A lie in the same orbit.

$G_{1H} = \{g \in G \mid g \cdot 1H = 1H\}$ by definition, and $\{g \in G \mid gH = H\} = H$.

By definition of π_H ,

$$\begin{aligned} \ker \pi_H &= \{g \in G \mid \forall x \in G, gxH = xH\} \\ &= \{g \in G \mid \forall x \in G, (x^{-1}gx)H = H\} \\ &= \{g \in G \mid \forall x \in G, x^{-1}gx \in H\} \\ &= \{g \in G \mid \forall x \in G, g \in xHx^{-1}\} = \bigcap_{x \in G} xHx^{-1}. \end{aligned}$$


Observe that $\ker \pi_H \trianglelefteq G$ and $\ker \pi_H \leq H$. If $N \trianglelefteq G$ and $N \leq H$ then $\forall x \in G, N = xNx^{-1} \leq xHx^{-1}$ so that

$$N \leq \bigcap_{x \in G} xHx^{-1} = \ker \pi_H$$




Corollary 4.2.1 Cayley's Theorem

Every group is isomorphic to a subgroup of some symmetric group. If G is a group of order n , then G is isomorphic to a subgroup of S_n .

Proof: Let $H = 1$ and apply the preceding theorem to obtain a homomorphism of G into S_G . Since the kernel of this homomorphism is contained in $H = 1$, G is isomorphic to its image in S_G . 

Corollary 4.2.2

If G is a finite group of order n and p is the smallest prime dividing $|G|$, then any subgroup of index p is normal.

Proof: Suppose $H \leq G$ and $|G : H| = p$. Let π_H be the permutation representation afforded by multiplication on the set of left cosets of H in G , let $K = \ker \pi_H$ and let $|H : K| = k$. Then $|G : K| = |G : H||H : K| = pk$. Since H has p left cosets, G/K is isomorphic to a subgroup of S_p by the First Isomorphism Theorem. By Lagrange's Theorem, $pk = |G/K|$ divides $p!$. Thus $k \mid \frac{p!}{p} = (p-1)!$. But all prime divisors of $(p-1)!$ are less than p and by the minimality of p , every prime divisor of k is greater than or equal to p . This forces $k = 1$, so $H = K \trianglelefteq G$. 

4.3 The Class Equation

Definition 4.3.1: Conjugacy Classes

$a, b \in G$ are said to be conjugate in G if $\exists g \in G, b = gag^{-1}$. That is, if they are in the same orbit of G acting on itself by conjugation. The orbits of this action are called the conjugacy classes of G .

Example 4.3.1

- An abelian group G acting on itself by conjugation is equivalent to acting on itself by the trivial action: $\forall g, a \in G, a \cdot a = a$ and the conjugacy class of each $a \in G$ is $\{a\}$.
- If $|G| > 1$ then it does not act transitively on itself by conjugation because $\{1\}$ is always a conjugacy class. More generally, subset $\{a\}$ is a conjugacy class if and only if $\forall g \in G, gag^{-1} = a$ if and only if a is in the center of G .

Definition 4.3.2: Conjugate


$S, T \subseteq G$ are said to be conjugate in G if $\exists g \in G, T = gSg^{-1} = \{sgs^{-1} \mid s \in S\}$ (i.e. if and only if they are in the same orbit of G acting on its subsets by conjugation).

Proposition 4.3.1

The number of conjugates of $S \subseteq G$ in group G is $|G : N_G(S)|$. In particular, the number of conjugates of an element s of G is $|G : C_G(s)|$.

Proof: By proposition 4.1.2, the number of conjugates of S equals the index $|G : G_S|$.

$$G_S = \{g \in G \mid gSg^{-1} = S\} = N_G(S)$$

so $|G : G_S| = |G : N_G(S)|$. Observe that $N_G(\{s\}) = C_G(s)$. 

Theorem 4.3.1 The Class Equation

Let G be a finite group and let g_1, g_2, \dots, g_r be representatives of the distinct conjugacy classes of G not contained in the center $Z(G)$ of G . Then,

$$|G| = |Z(G)| + \sum_{i=1}^r |G : C_G(g_i)|$$

Proof: Any $x \in Z(G)$ will be in conjugacy class $\{x\}$. Let $\mathcal{K}_1, \mathcal{K}_2, \dots, \mathcal{K}_r$ be the conjugacy classes not contained in $Z(G)$. $Z(G) \cup (\bigcup_{i=1}^r \mathcal{K}_i)$ and $Z(G) \cap (\bigcup_{i=1}^r \mathcal{K}_i) = \emptyset$. The conjugacy classes partition G so

$$\begin{aligned} |G| &= |Z(G)| + \sum_{i=1}^r |G : C_G(g_i)| \\ &= |Z(G)| + \sum_{i=1}^r |G : C_G(g_i)| \end{aligned}$$



Example 4.3.2


- The class equation gives no information in an abelian group since conjugation is the trivial action
- In any group G we have $\langle g \rangle \leq C_G(g)$, simplifying computations of conjugacy classes.

Theorem 4.3.2

If p is prime and P is a group of order p^α for some $\alpha \geq 1$, then P has nontrivial center: $Z(P) \neq 1$.


Proof:

$$|P| = |Z(P)| + \sum_{i=1}^r |P : C_P(g_i)|$$

where g_1, \dots, g_r are representatives of the distinct non-central conjugacy classes. By definition, $C_P(g_i) \neq P$ for $i = 1, 2, \dots, r$ so p divides $|P : C_P(g_i)|$. p also divides $|P|$ so p divides $|Z(P)|$. 

Corollary 4.3.1

If $|P| = p^2$ for some prime p , then P is abelian. More precisely, P is isomorphic to either Z_{p^2} or $Z_p \times Z_p$.

Proof: Since $Z(P) \neq 1$, $P/Z(P)$ is cyclic, and P must be abelian. If P has an element of order p^2 then it is cyclic. Assume therefore that every nonidentity element of P has order p . Let $x \neq 1$ be in P and $y \in P - \langle x \rangle$. $|\langle x, y \rangle| > |\langle x \rangle| = p$ so $P = \langle x, y \rangle$. $|x| = |y| = p \implies \langle x \rangle \times \langle y \rangle = Z_p \times Z_p$. The corresponding isomorphism must be the map $(x^a, y^b) \mapsto x^a y^b$. 

Proposition 4.3.2

Let $\sigma, \tau \in S_n$ and suppose σ has cycle decomposition


$$(a_1 \ a_2 \ \dots \ a_{k_1}) (b_1 \ b_2 \ \dots \ b_{k_2}) \dots$$

Then $\tau\sigma\tau^{-1}$ has cycle decomposition

$$(\tau(a_1) \ \tau(a_2) \ \dots \ \tau(a_{k_1})) (\tau(b_1) \ \tau(b_2) \ \dots \ \tau(b_{k_2})) \dots$$

Proof: Observe that

$$\sigma(i) = j \implies \tau\sigma\tau^{-1}(\tau(i)) = \tau(j)$$

Thus, for any ordered pair i, j in the cycle decomposition of σ , ordered pair $\tau(i), \tau(j)$ appears in the cycle decomposition of $\tau\sigma\tau^{-1}$. 


Definition 4.3.3: Cycle Type

1. If $\sigma \in S_n$ is the product of disjoint cycles of lengths n_1, n_2, \dots, n_r with $n_1 \leq n_2 \leq \dots \leq n_r$ then the integers n_1, n_2, \dots, n_r are called the cycle type of σ .
2. If $n \in \mathbb{Z}^+$, a partition of n is any nondecreasing sequence of positive integers whose sum is n .

Proposition 4.3.3

Two elements of S_n are conjugate in S_n if and only if they have the same cycle type. The number of conjugacy classes of S_n equals the number of partitions of n .

Proof: By proposition 4.3.2, conjugate permutations have the same cycle type. Conversely, suppose the permutations σ_1 and σ_2 have the same cycle type. Order the cycles in nondecreasing length. Ignoring parentheses, each cycle decomposition is a list in which all the integers from 1 to n appear exactly once. Define τ to be the function which maps the i th integer in the list for σ_1 to the i th integer in the list for σ_2 . Thus, τ is a permutation since the parentheses appear in the same positions in the list. By proposition 4.3.2, $\tau\sigma_1\tau^{-1} = \sigma_2$, so that σ_1 and σ_2 are conjugate.

Since there is a bijection between the conjugacy classes of S_n and the permissible cycle types and each cycle type for a permutation in S_n is a partition of n , the second assertion of the proposition follows. 

4.4 Automorphisms

Definition 4.4.1: Automorphism

An isomorphism from group G onto itself is called an automorphism of G . The set of all automorphisms of G is denoted $\text{Aut}(G)$.

$\text{Aut}(G)$ forms a group under composition, and is a subgroup of S_G .

Proposition 4.4.1

Let $N \trianglelefteq G$. Then G acts by conjugation on H as automorphisms of H . More specifically, the action of G on H by conjugation is defined for each $g \in G$ by

$$\forall h \in H, h \mapsto ghg^{-1}$$

For each $g \in G$, conjugation by g is an automorphism of H . The permutation representation afforded by this action is a homomorphism of G into $\text{Aut}(H)$ with kernel $C_G(H)$. In particular, $G/C_G(H)$ is isomorphic to a subgroup of $\text{Aut}(H)$.

Proof: Let φ_g be conjugation by g . Observe that $\forall g \in G, gHg^{-1} = H \implies \varphi_g(H) = H$. Conjugation defines an action, so $\varphi_1 = 1$ and $\forall a, b \in G, \varphi_a \circ \varphi_b = \varphi_{ab}$. Thus, φ_g gives a bijection from H to itself because it has a 2-sided inverse $\varphi_{g^{-1}}$. Each φ_g is a homomorphism from H to H because

$$\forall h, k \in H, \varphi_g(hk) = g(hk)g^{-1} = gh(gg^{-1})kg^{-1} = (ghg^{-1})(kgg^{-1}) = \varphi_g(h)\varphi_g(k)$$

Thus, conjugation by any fixed element of G defines an automorphism of H .


The permutation representation $\psi : G \rightarrow S_H$ defined by $\psi(g) = \varphi_g$ has image contained in the subgroup $\text{Aut}(H)$ of S_H . Finally,

$$\begin{aligned} \ker \psi &= \{g \in G \mid \varphi_g = \text{id}\} \\ &= \{g \in G \mid \forall h \in H, ghg^{-1} = h\} \\ &= C_G(H) \end{aligned}$$

The First Isomorphism Theorem implies the final statement of the proposition. 


Corollary 4.4.1

If $K \leq G$ and $g \in G$, then $K \cong gKg^{-1}$. Conjugate elements and conjugate subgroups have the same order.

Proof: Letting $G = H$ in the proposition shows that the conjugation by $g \in G$ is an automorphism of G , from which the corollary follows. 

Corollary 4.4.2

For any $H \leq G$, $N_G(H)/C_G(H)$ is isomorphic to a subgroup of $\text{Aut}(H)$. In particular, $G/Z(G)$ is isomorphic to a subgroup of $\text{Aut}(G)$.

Proof: By proposition 4.4.1, $H \trianglelefteq N_G(H)$ implies the first assertion. The second assertion follows when $H = G$, in which case $N_G(G) = G$ and $C_G(G) = Z(G)$. 

Definition 4.4.2: Inner Automorphism

Let G be a group and $g \in G$. Conjugation by g is called an inner automorphism of G and the subgroup consisting of all inner automorphisms is denoted $\text{Inn}(G)$.

Example 4.4.1

- Group G is abelian if and only if every inner automorphism is trivial. If H is an abelian normal subgroup of G and H is not contained in $Z(G)$, then there is some $g \in G$ such that conjugation by g restricted to H is not an inner automorphism of H . An example of this is $G = A_4$, $H = V_4$ and g is any 3-cycle
- $Z(Q_8) = \langle -1 \rangle \implies \text{Inn}(Q_8) \cong V_4$.
- $Z(D_8) = \langle r^2 \rangle \implies \text{Inn}(D_8) \cong V_4$.
- $\forall n \geq 3, Z(S_n) = 1 \implies \text{Inn}(S_n) \cong S_n$.

Definition 4.4.3: Characteristic

A subgroup H of group G is called characteristic in G , denoted $H \text{ char } G$ if $\forall \sigma \in \text{Aut}(G), \sigma(H) = H$.

Observe that

1. characteristic subgroups are normal
2. if H is the unique subgroup of G of a given order, then H is characteristic in G .
3. $K \text{ char } H \wedge H \trianglelefteq G \implies K \trianglelefteq G$

Proposition 4.4.2


$$\begin{aligned}\text{Aut}(Z_n) &\cong (\mathbb{Z}/n\mathbb{Z})^\times \\ |(\mathbb{Z}/n\mathbb{Z})^\times| &= \varphi(n)\end{aligned}$$

Proof: Let $Z_n = \langle x \rangle$. $\psi \in \text{Aut}(Z_n) \implies \exists a \in \mathbb{Z}, \psi(x) = x^a$ and a uniquely determines ψ . Denote this automorphism ψ_a . $|x| = n$ implies that a is only defined mod n . ψ_a is an automorphism so x and x^a have the same order, implying $(a, n) = 1$. Additionally, for every a relatively prime to n , the map $x \mapsto x^a$ is an automorphism of Z_n . Hence we have a surjection

$$\begin{aligned}\Psi : \text{Aut}(Z_n) &\rightarrow (\mathbb{Z}/n\mathbb{Z})^\times \\ \psi_a &\mapsto a \pmod{n}\end{aligned}$$

The map Ψ is a homomorphism because

$$\begin{aligned}\forall \psi_a, \psi_b \in \text{Aut}(Z_n), \psi_a \circ \psi_b(x) &= \psi_a(x^b)^a = x^{ab} = \psi_{ab}(x) \\ \Psi(\psi_a \circ \psi_b) &= \Psi(\psi_{ab}) = ab \pmod{n} = \Psi(\psi_a)\Psi(\psi_b).\end{aligned}$$

Ψ is injective, hence it is an isomorphism. 

Proposition 4.4.3

1. If p is an odd prime and $n \in \mathbb{Z}^+$, $\text{Aut } Z_p$ is cyclic of order $p - 1$. More generally, $\text{Aut}(Z_{p^n})$ is cyclic of order $p^{n-1}(p - 1)$.
2. For all $n \leq 3$, $\text{Aut}(Z_{2^n}) \cong Z_2 \times Z_{2^{n-2}}$, and in particular is not cyclic but has a cyclic subgroup of index 2.
3. Let p be prime and V be an abelian group with the property that $\forall v \in V, pv = 0$. If $|V| = p^n$ then V is an n -dimensional vector space over the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. The automorphisms of V are precisely the nonsingular linear transformations from V to itself, that is

$$\text{Aut}(V) \cong GL(V) \cong GL_n(\mathbb{F}_p)$$

4. For all $n \neq 6$, $\text{Aut}(S_n) = \text{Inn}(S_n) \cong S_n$. For $n = 6$, $|\text{Aut}(S_6) : \text{Inn}(S_6)| = 2$
5. $\text{Aut}(D_8) \cong D_8$ and $\text{Aut}(Q_8) \cong S_4$.

Example 4.4.2

Suppose group G of order 45 has normal subgroup P of order 9.

$G/C_G(P)$ is isomorphic to a subgroup of $\text{Aut}(P)$ and $|\text{Aut}(P)|$ is 6 or 48. $|P|$ is the square of a prime so P is abelian, hence $P \leq C_G(P)$. $|C_G(P)|$ must be divisible by 9, implying $|G/C_G(P)|$ is 1 or 5. Thus, $|G/C_G(P)| = 1$, i.e. $C_G(P) = G$ and $P \leq Z(G)$. Then $G/Z(G)$ is cyclic and G must be abelian.

4.5 Sylow's Theorem

Definition 4.5.1: p -group

1. A group G of order p^α for some prime p $\alpha \geq 1$ is called a p -group. Subgroups of G which are p -groups are called p -subgroups.
2. If $|G| = p^\alpha m$, where $p \nmid m$, then a subgroup of order p^α is called a Sylow p -subgroup of G .
3. The set of Sylow p -subgroups of G will be denoted by $\text{Syl}_p(G)$ and the number of Sylow p -subgroups of G will be denoted by $n_p(G)$ (or n_p).

Theorem 4.5.1 Sylow's Theorem

Let G be a group of order $p^\alpha m$, for a prime p where $p \nmid m$.

1. $\text{Syl}_p(G) \neq \emptyset$
2. Any p -subgroup Q is contained in some conjugate of a Sylow p -subgroup of G , i.e.

$$P \in \text{Syl}_p(G) \wedge (Q \leq G, |Q| = p^\alpha) \implies \exists g \in G, Q \leq gPg^{-1}$$

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

3. $|\text{Syl}_p(G)|$ is of the form $1 + kp$, i.e.,

$$n_p \equiv 1 \pmod{p}$$

$$\forall P \in \text{Syl}_p(G), n_p = |G : N_G(P)|$$

$$n_p \mid m$$

Proof: Let $H = N_G(P) \cap Q$. $P \leq N_G(P) \implies P \cap Q \leq H$. To prove reverse inclusion, $H \leq Q \iff H \leq P$. $H \leq N_G(P) \implies PH \leq G$. Thus,

$$|PH| = \frac{|P||H|}{|P \cap H|}$$

All the numbers in the above quotient are powers of p so PH is a p -group. $P \leq PH \implies p^\alpha \mid |PH|$. p^α is the largest power of p dividing $|G|$, thus, $|PH| = p^\alpha = |P|$. Therefore, $P = PH$ and $H \leq P$. This establishes

Lemma 4.5.1

Let $P \in \text{Syl}_p(G)$. $\forall Q \leq G, |Q| = p^\alpha \implies Q \cap N_G(P) = Q \cap P$.

We induct on $|G|$. There is nothing to prove if $|G| = 1$. Assume inductively the existence of Sylow p -subgroups for all groups of order less than $|G|$. By Cauchy's Theorem, $p \mid |Z(G)| \implies \exists N \leq Z(G), |N| = p$. Let $\overline{G} = G/N$, so $|\overline{G}| = p^{\alpha-1}m$. By induction, \overline{G} has a subgroup \overline{P} of order $p^{\alpha-1}$. Let $P \leq G, N \subseteq P$, such that $P/N = \overline{P}$, implying $|P| = |P/N| \cdot |N| = p^\alpha$, and P is a Sylow p -subgroup of G . We are reduced to the case when $p \nmid |Z(G)|$.

Let g_1, g_2, \dots, g_r be representatives of the distinct non-central conjugacy classes of G .

$$|G| = |Z(G)| + \sum_{i=1}^r |G : C_G(g_i)|$$

$\forall i, p \mid |G : C_G(g_i)| \implies p \mid |Z(G)|$, a contradiction. Thus, $\exists i, p \nmid |G : C_G(g_i)|$. For this i , let $H = C_G(g_i)$ so

$$|H| = p^\alpha k, p \nmid k.$$

$g_i \notin Z(G) \implies |H| < |G|$. By induction, H has a Sylow p -subgroup, P , which is also a subgroup of G . $|P| = p^\alpha \implies P \in \text{Syl}_p(G)$. This completes the induction, and 1. is established. We first prove that $|\mathcal{O}_1| + (|\mathcal{O}_2| + \dots + |\mathcal{O}_s|) \equiv 1 \pmod{p}$. By 1., there exists a Sylow p -subgroup, P , of G . Let

$$\{P_1, P_2, \dots, P_r\} = \{gPg^{-1} \mid g \in G\} = \mathcal{S}$$

and Q be any p -subgroup of G . By definition, G , hence also Q , acts by conjugation on \mathcal{S} . Write \mathcal{S} as a disjoint union of orbits under this action by Q :

$$\mathcal{S} = \mathcal{O}_1 \cup \mathcal{O}_2 \cup \cdots \cup \mathcal{O}_s$$

where $r = |\mathcal{O}_1| + \cdots + |\mathcal{O}_s|$. Renumber the elements of \mathcal{S} so the first s elements of \mathcal{S} are representatives of the Q -orbits: $P_i \in \mathcal{O}_1, 1 \leq i \leq s$. It follows from proposition 4.1.2 that $|\mathcal{O}_i| = |Q : N_Q(P_i)|$. By definition, $N_Q(P_i) = N_G(P_i) \cap Q$, and by lemma 4.5.2, $N_G(P_i) \cap Q = P_i \cap Q$. Thus,

$$|\mathcal{O}_i| = |Q : P_i \cap Q|, 1 \leq i \leq s$$

Q was arbitrary so we may take $Q = P_1$ giving

$$\mathcal{O}_1 = 1$$

For all $i > 1, P_1 \neq P_i \implies P_1 \cap P_i < P_1$.

$$|\mathcal{O}_i| = |P_1 : P_1 \cap P_i| > 1, 2 \leq i \leq s$$

P_1 is a p -group so $|P_1 : P_1 \cap P_i|$ must be a power of p , hence

$$p \mid |\mathcal{O}_i|, 2 \leq i \leq s$$

$$r = |\mathcal{O}_1| + (|\mathcal{O}_2| + \cdots + |\mathcal{O}_s|) \equiv 1 \pmod{p}.$$


To prove parts 2. and 3., let Q be any p -subgroup of G . Suppose Q is not contained in P_i for any $1 \leq i \leq r$ (i.e. $\forall g \in G, Q \not\leq gPg^{-1}$). In this situation, $\forall i, Q \cap P_i < Q$, so by 1.,

$$|\mathcal{O}_i| = |Q : Q \cap P_i| > 1, 1 \leq i \leq s.$$

Thus $\forall i, p \mid |\mathcal{O}_i|$ implying $p \mid r$, contradicting $r \equiv 1 \pmod{p}$. Hence $\exists g \in G, Q \leq gPg^{-1}$.

Let $Q \in \text{Syl}_p(G)$. $\exists g \in G, Q \leq gPg^{-1}$ and $|gPg^{-1}| = |Q| = p^\alpha$ implies $gPg^{-1} = Q$, establishing 2. of the theorem. In particular, $\mathcal{S} = \text{Syl}_p(G)$ since every Sylow p -subgroup of G is conjugate to P , and so $n_p = r \equiv 1 \pmod{p}$. Finally, since all Sylow p -subgroups are conjugate,

$$\forall P \in \text{Syl}_p(G), n_p = |G : N_G(P)|$$

completing the proof of Sylow's Theorem. 

Corollary 4.5.1

Let $P \in \text{Syl}_p(G)$. Then the following are equivalent:

1. $n_p = 1$
2. $P \trianglelefteq G$
3. $P \text{ char } G$
4. $\forall X \subseteq G, x \in X, k \in \mathbb{Z}^+ \wedge |x| = p^k \implies \exists \alpha \in \mathbb{Z}^+, |\langle X \rangle| = p^\alpha$

Chapter 5

Direct Products

5.1 Direct Products

Definition 5.1.1: Direct Product

1. The direct product of $G_1 \times G_2 \times \cdots \times G_n$ of groups $(G_1, \star_1), (G_2, \star_2), \dots, (G_n, \star_n)$ is the set of n -tuples (g_1, g_2, \dots, g_n) where $g_i \in G_i$ with componentwise operation:

$$(g_1, g_2, \dots, g_n) \star (h_1, h_2, \dots, h_n) = (g_1 \star_1 h_1, g_2 \star_2 h_2, \dots, g_n \star_n h_n)$$

2. Similarly, The direct product of $G_1 \times G_2 \times \cdots$ of groups $(G_1, \star_1), (G_2, \star_2), \dots$ is the set of sequences (g_1, g_2, \dots) where $g_i \in G_i$ with componentwise operation:

$$(g_1, g_2, \dots) \star (h_1, h_2, \dots) = (g_1 \star_1 h_1, g_2 \star_2 h_2, \dots)$$

Example 5.1.1

- For \mathbb{R} under addition, $\mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R}$ (n -factors) is Euclidean n -space \mathbb{R}^n with usual vector addition.
- $\mathbb{Z} \times S_3 \times GL_2(\mathbb{R})$ is a group under operation defined by

$$(n, \sigma, \begin{bmatrix} a & b \\ c & d \end{bmatrix}) (m, \tau, \begin{bmatrix} p & q \\ r & s \end{bmatrix}) = (n + m, \sigma \circ \tau, \begin{bmatrix} ap + br & aq + bs \\ cp + dr & cq + ds \end{bmatrix})$$

Proposition 5.1.1

The order of the direct products of group G_1, \dots, G_n is $|G_1||G_2| \cdots |G_n|$ (and infinite if any G_i is infinite)

Proposition 5.1.2

Let G_1, G_2, \dots, G_n be groups and let $G = G_1 \times \cdots \times G_n$.

1. For a fixed i and g_i appearing in the i th position,

$$G_i \cong \{(1, 1, \dots, 1, g_i, 1, \dots, 1) \mid g_i \in G_i\}$$

If we identify G_i with this subgroup, then $G_i \leq G$ and

$$G/G_i \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n.$$

2. For each fixed i define $\pi_i : G \rightarrow G_i$ by

$$(g_1, g_2, \dots, g_n) \mapsto g_i$$

Then π_i is a surjective homomorphism with

$$\begin{aligned}\ker \pi_i &= \{(g_1, \dots, g_{i-1}, 1, g_{i+1}, \dots, g_n) \mid \forall j \neq i, g_j \in G_j\} \\ &\cong G_1 \times \dots \times G_{i-1} \times G_{i+1} \times \dots \times G_n\end{aligned}$$

3. Under the identifications part 1., $\forall i \neq j, x \in G_i \wedge y \in G_j \implies xy = yx$

Proof: Consider the map

$$\varphi : G \rightarrow G_1 \times \dots \times G_{i-1} \times G_{i+1} \times \dots \times G_n$$

defined by

$$(g_1, g_2, \dots, g_n) = (g_1, \dots, g_{i-1}, g_{i+1}, \dots, g_n)$$

ϕ can be easily verified to be a homomorphism. φ is surjective since j th entries are arbitrary elements of G_j for all j .

$$\ker \varphi = \{(g_1, \dots, g_n) \mid \forall j \neq i, g_j = 1\} = G_i$$

The First Isomorphism Theorem proves 1.

If $x = (1, \dots, 1, g_i, 1, \dots, 1)$ and $y = (1, \dots, 1, g_j, \dots, 1)$ where the indicated entries appear in positions i, j respectively and chosen such that $i < j$, then

$$xy = (1, \dots, 1, g_i, 1, \dots, 1, g_j, 1, \dots, 1) = yx$$



5.2 The Fundamental Theorem of Finitely Generated Abelian Groups

Definition 5.2.1: Finitely Generated

1. A group G is finitely generated if

$$\exists A \subseteq G, |A| \neq \infty, G = \langle A \rangle$$

2. For each $r \in \mathbb{Z}, r \geq 0$, let $\mathbb{Z}^r = \mathbb{Z} \times \mathbb{Z} \times \dots \times \mathbb{Z}$ be the direct product of r copies of the group \mathbb{Z} , where $\mathbb{Z}^0 = 1$. The group \mathbb{Z}^r is called the free abelian group of rank r .

Theorem 5.2.1 Fundamental Theorem of Finitely Generated Abelian Groups

Let G be a finitely generated abelian group. Then

- 1.

$$G \cong \mathbb{Z}^r \times Z_{n_1} \times Z_{n_2} \times \dots \times Z_{n_s}$$

for some integers r, n_1, n_2, \dots, n_s satisfying the following conditions,

- a. $r \geq 0$ and $\forall j, n_j \geq 2$
- b. $n_{i+1} \mid n_i$ for $1 \leq i \leq s-1$.


2. The expression in 1. is unique: if $G \cong \mathbb{Z}^t \times Z_{m_1} \times Z_{m_2} \times \dots \times Z_{m_u}$, where t and m_1, m_2, \dots, m_u satisfy a. and b.

Definition 5.2.2: Free Rank

The integer r in the previous theorem is called the free rank or Betti number of G , and the integers n_1, n_2, \dots, n_s are called the invariant factors of G . The description of G in the 1. of the previous theorem is called the invariant factor decomposition of G .

Corollary 5.2.1

If n is the product of distinct primes, then up to isomorphism the only abelian group of order n is Z_n .

Proof: Observe that all finitely generated abelian groups are finite if and only if its free rank is 0. We see that every prime divisor of n must divide n_1 , thus, $n \mid n_1$. 

Theorem 5.2.2

Let G be an abelian group of order $n > 1$ and let the unique prime factorization of n be

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

Then

1. $G \cong A_1 \times A_2 \times \cdots \times A_k$ where $|A_i| = p_i^{\alpha_i}$
2. $\forall A \in \{A_1, A_2, \dots, A_k\}, |A| = p^\alpha$,

$$A \cong Z_{p^{\beta_1}} \times Z_{p^{\beta_2}} \times \cdots \times Z_{p^{\beta_t}}$$

with $\beta_1 \geq \beta_2 \geq \cdots \geq \beta_t \geq 1$ and $\beta_1 + \beta_2 + \cdots + \beta_t = \alpha$ (where t and β_1, \dots, β_t depend on i).

3. The decomposition in 1. and 2. are unique.

Definition 5.2.3: Elementary Divisors

The integers p^{β_j} described in the preceding theorem are called the elementary divisors of G . The description of G in 1. and 2. is called the elementary divisor decomposition of G .

Proposition 5.2.1

Let $m, n \in \mathbb{Z}^+$.

1. $Z_m \times Z_n \cong Z_{mn} \iff (m, n) = 1$
2. $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \implies Z_n \cong Z_{p_1^{\alpha_1}} \times Z_{p_2^{\alpha_2}} \times \cdots \times Z_{p_k^{\alpha_k}}$

Proof: Let $Z_m = \langle x \rangle$, $Z_n = \langle y \rangle$, and $l = \text{lcm}(m, n)$. Observe that $l = mn \iff (m, n) = 1$. Let $x^a y^b \in Z_m \times Z_n$. Then,

$$\begin{aligned}
 (x^a y^b)^l &= x^{la} y^{lb} \\
 &= 1^a 1^b = 1
 \end{aligned}$$

If $(m, n) \neq 1$, every element of $Z_m \times Z_n$ has order at most l , hence $|Z_m \times Z_n| < mn$ implying $Z_m \times Z_n \not\cong Z_{mn}$. Conversely, $(m, n) = 1 \implies |xy| = \text{lcm}(|x|, |y|) = mn$. Thus, $Z_m \times Z_n = \langle xy \rangle$. 