Group Theory

William Bevington — s1610318

Contents

Isomorphism Theorems

Theorem 1

Let G be a group and $N \leq G$. Then $N \triangleleft G$ if and only if N is the kernel of some group homomorphism $\varphi : G \to H$.

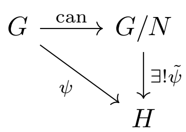
Theorem 2: First Isomorphism Theorem

Let $\theta : G \to H$ be a group homomorphism, then $N = \ker\theta$ is a normal subgroup of G, imθ is a subgroup of H and there is an isomorphism

$$\tilde{\theta} : G/\ker\theta \xrightarrow{\sim} \text{im}\theta, \qquad \tilde{\theta}(gN) := \theta(g).$$

Theorem 3: Universal Property of Factor Groups

Let G be a group with normal subgroup $N \triangleleft G$. For any homomorphism $\psi : G \to H$ with $N \subseteq \ker\psi$ there is a unique homomorphism $\tilde{\psi} : G/N \to H$ so that $\tilde{\psi} \circ \text{can} = \psi$ where $\text{can} : G \to G/N$ is the **canonical homomorphism** $\text{can}(g) = g + N$, making the following commute



Corollary 4

If $\phi : G \to K$ is a surjective group homomorphism and $\psi : G \to H$ is a group homomorphism with $\ker\phi \subseteq \ker\psi$ then there exists a unique group homomorphism $\tilde{\psi} : K \to H$ so that $\tilde{\psi}\phi = \psi$.

Theorem 5

Let G be a group with normal subgroup $N \triangleleft G$ and $K \leq G/N$, then:

1. $\text{can}^{-1}(K) \leq G$ with $N \subseteq \text{can}^{-1}(K)$, and
2. $\text{can}^{-1}(K) \triangleleft G$ if and only if $K \triangleleft G/N$.

Theorem 6

Let G be a group with normal subgroup $N \triangleleft G$, if $N \leq H \leq G$ then $H = \text{can}^{-1}(\text{can}(H))$.

Theorem 7: Correspondence Theorem

Let G be a group with normal subgroup $N \triangleleft G$. The map $H \mapsto \text{can}(H)$ is a bijection between the set of subgroups of G containing N and subgroups of G/N:

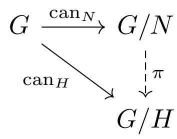
$$\{H : N \leq H \leq G\} \xleftrightarrow{\sim} \{J : J \leq G/N\}.$$

Theorem 8: Third Isomorphism Theorem

If $N \leq H \leq G$ with $N, H \triangleleft G$ then

$$\frac{G/N}{H/N} \cong \frac{G}{H},$$

as seen by the diagram



Theorem 9: Second Isomorphism Theorem

Let $N \triangleleft G$ and $H \leq G$, then

1. HN is a subgroup of G,
2. $N \triangleleft HN$,
3. $H \cap N \triangleleft H$, and
4. there is an isomorphism

$$\frac{HN}{N} \cong \frac{H}{H \cap N}.$$

Sylow Theorems

Theorem 1: Cauchy's Theorem

If p is a prime that divides the order of G then G has a subgroup of order p.

Definition 1: Sylow p-Subgroup

Let G be a finite group and p a prime. A subgroup $H \leq G$ is a **Sylow p-subgroup** of G if its order is the highest power of p that divides G; $\#H = p^k$ where $p^k | \#G$ but $p^{k+1} \not| \#G$.

Theorem 2: Sylow I

Let $\#G = n = p^m r$ for some prime p and $r \in \mathbb{N}$ with $p \not| r$, then there exists at least one Sylow p-subgroup (of order p^m).

Theorem 3: Sylow II

Let $\#G = n = p^m r$ for some prime p and $r \in \mathbb{N}$ with $p \not| r$, and suppose that P is a Sylow p-subgroup and that $H \leq G$ is any p-subgroup of G, then there exists some $g \in G$ with $H \subseteq gPg^{-1}$; *any two Sylow p-subgroups are conjugate.*

Theorem 4: Sylow III

Let $\#G = n = p^m r$ for some prime p and $r \in \mathbb{N}$ with $p \not| r$, Let n_p be the number of distinct Sylow p-subgroups of G, then $n_p | r$ and $n_p = 1 \mod p$.

Definition 2: Simple Group

A group G is **simple** if it has no non-trivial normal subgroups, i.e. if $N \lhd G$ given that $N = \{e_G\}$ or $N = G$.

Theorem 5

If a group G has a unique Sylow p-subgroup P then $P \lhd G$.

Definition 3: Group Action

Let G be a group and X a set, an **action of G on X** is a map

$$G \times X \to X, \qquad (g, x) \mapsto g \cdot x$$

so that for all $x \in X$ and $g, h \in G$ we have that $e_G \cdot x = x$ and $g \cdot (h \cdot x) = (gh) \cdot x$. The **orbit** of $x \in X$ is

$$G \cdot x = \{g \cdot x \, : \, g \in G\},$$

and the **stabiliser** is

$$\text{Stab}_G(x) = \{g \in G \, : \, g \cdot x = x\}.$$

Theorem 6

Let G act on some set X:

1. the action of G induces an equivalence relation $x \sim y \Leftrightarrow \exists g \in G : y = g \cdot x$,
2. the equivalence classes of this action are the orbits,
3. the distinct orbits in X form a partition of X,

Theorem 7

Let G be a group acting on some set X, then for all $x \in X$ we have that $\text{Stab}_G(x) \leq G$.

Theorem 8: Orbit Stabiliser

Let G be a finite group acting on a set X and $x \in X$, then

$$\#G = \#\text{Stab}_G(x)\#(G \cdot x).$$

Theorem 9

Let p be a prime and G a p-group so that each element of G has order of p^n for some $n \in \mathbb{N}$. If G acts on a set X, then the number of fixed points of X (i.e. the $x \in X$ such that $\forall g \in G : g \cdot x = x$) is congruent to $\#X \mod p$.

Corollary 10

Let p be a prime and G a p-group so that each element of G has order of p^n for some $n \in \mathbb{N}$. If G acts on a set X and $\#G = p^m r$ then if P is a Sylow p-subgroup of G we have that

$$P \lhd G \Leftrightarrow P \textit{ is the unique Sylow } p\textit{-subgroup of } G.$$

Definition 4: Normalizer

Let $H \leq G$ for some group G, the **normalizer** of H in G is

$$N_G(H) = \{g \in G : gHg^{-1} = H\}.$$

Theorem 11

Let G be a finite group,

1. for any $H \leq G$ we have that

$$[G : N_G(H)] = \textit{the number of conjugates of } H,$$

2. let $p|\#G$ and P be a Sylow p-subgroup of G, then $n_p = [G : N_G(H)]$.

Finitely Generated Abelian Groups

Theorem 1

Suppose that A is a finite abelian group of order $n = \prod_{i=1}^{t} p_i^{s_i}$ for primes p_i and $s_i \in \mathbb{N}$. Let A_{p_i} be the unique Sylow p_i-subgroup of A, then

$$A \cong A_{p_1} \times \cdots \times A_{p_t},$$

that is, A is isomorphic to the product of its Sylow p-subgroups.

Theorem 2

Let A be an abelian group with $\#A = p^n$ for some prime p. Then A is isomorphic to a direct product of cyclic subgroups of order $p^{e_1}, p^{e_2}, \ldots, p^{e_s}$ where $e_1 + \cdots + e_s = n$ and for all $i > j$ we have $e_i \geq e_j$. This product is unique up to re-ordering factors.

Corollary 3: Fundamental Theorem of Finite Abelian Groups I

Let A be a finite abelian group, then A is a direct product of cyclic groups of prime power order. This product is unique up to re-ordering factors.

Theorem 4: Chinese Remainder Theorem

Let $m, n \in \mathbb{Z}$ be coprime, then $C_{mn} \cong C_m \times C_n$.

Definition 1: Exponent

The **exponent** $e(G)$ of a finite group G is the least common multiple of the orders of the elements of G.

Theorem 5

Let A be a finite abelian group, then A contains an element of order $e(A)$.

Corollary 6

If A is a finite abelian group with $e(A) = \#A$ then A is cyclic.

Linear Algebra Over the Integers

Theorem 7: Fundamental Theorem of Finite Abelian Groups II

Let A be a finitely generated abelian group, then

$$A \cong \mathbb{Z}/r_1\mathbb{Z} \times \cdots \times \mathbb{Z}/r_K\mathbb{Z} \times \mathbb{Z}^l$$

for some $k, l \in \mathbb{Z}$ and where for $i < j$ we have $r_i | r_j$.

Theorem 8

Let p be prime and $a_1 \geq a_2 \geq \cdots \geq a_m$ and $b_1 \geq \cdots \geq b_n$ be positive integers, if

$$C_{p^{a_1}} \times \cdots \times C_{p^{a_m}} \cong C_{p^{b_1}} \times \cdots \times C_{p^{b_n}},$$

then $m = n$ and $a_i = b_i$ for all $i = 1, \ldots, m$.

Symmetric and Alternating Groups

Theorem 1

Every permutation $\sigma \in S_n$ can be written as a product of disjoint cycles which is unique up to re-ordering.

Theorem 2

Every permutation $\sigma \in S_n$ can be written as a product of transposition, thus the transpositions generate S_n.

Definition 1: Cycle Type

Suppose that $\sigma = c_1 \dots c_k \in S_n$ is the product of k disjoint cycles of lengths $l_1, \dots, l_k$, then the **cycle type** of σ is the k-tuple $(l_1, \dots, l_k)$

Theorem 3

Let $\sigma = (a_1\, a_2\, \dots\, a_k) \in S_n$ and $\tau \in S_n$ then

$$\tau\sigma\tau^{-1} = (\tau(a_1)\, \tau(a_2)\, \dots\, \tau(a_k)).$$

Theorem 4

Two permutations of S_n are conjugate if and only if they are of the same cycle type.

Definition 2: Even Permutations

Let S_n act on $\{x_1, \dots, x_n\}$ and $P = \prod_{1 \leq i \leq j \leq n}(x_i - x_j)$, letting $X = \{P, -P\}$ we have that this action reduces to an action on X. If $\sigma \in S_n$ fixes P then σ is an **even permutation**. The set of even permutations is the **alternating group** A_n.

Theorem 5

The product of two even or two odd permutations is even, the product of an odd and an even permutations is odd. A cycle in S_n is even if and only if its length l is odd.

Theorem 6

Let $n \geq 2$, then $A_n \triangleleft S_n$ with index two so that $\#A_n = \frac{\#S_n}{2}$.

Theorem 7

The alternating group A_4 has order 12, and has a unique subgroup $N \triangleleft A_4$ of order $\#N = 4$ so that $A_4/N \cong C_3$ and $S_4/N \cong S_3$.

Theorem 8

Let G be a finite group with $H \triangleleft G$ and denote by $cl_G(h) = \{h' \in G : \exists g \in G,\ h' = ghg^{-1}\}$ the conjugacy class of $h \in H$ in G. Then there exists $h_1, \dots, h_k \in H$ such that $H = \bigsqcup_{i=1}^{k} cl_G(h_i)$.

Theorem 9: Alternating Groups and Simplicity

The alternating group A_n is simple for $n \geq 5$.

Theorem 10

If $n \geq 3$ then A_n is generated by three-cycles.

Theorem 11

If $n \geq 6$ and $\sigma \in A_n$ is a non-identity element then $\#cl_{A_n}(\sigma) \geq n$.

Jordan-Hölder Theorem

Definition 1: Composition Series

Let G be group, a **composition series** for G is a chain

$$\{e\} = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_{s-1} \triangleleft G_s = G$$

where for all i, $G_i \neq G_{i+1}$ and the **composition factors** G_{i+1}/G_i are simple.

WARNING: normality of subgroups is not transitive; $A \triangleleft B \triangleleft C$ does not give that $A \triangleleft C$.

Theorem 1: Jordan-Hölder

Let G be a finite group, then G has a composition series. Moreover any two composition series for G have the same length and composition factors up to isomorphism and ordering.

Theorem 2: Classification of Finite Simple Groups

Let G be a finite simple group, then G is isomorphic to one of

- C_p for some prime p,
- A_n for some $n \geq 5$,
- a group of 'Lie type' (non-examinable), of which there are 16 types, or
- one of the 26 'sporadic' groups (non-examinable).

Solvable Groups

Definition 1: Sub-normal Series

Let G be a group, a **subnormal series** for G is a series

$$\{e\} = G_0 \triangleleft G_1 \triangleleft \ldots \triangleleft G_s = G.$$

Definition 2: Solvable

A group G is **solvable** (or 'soluable') if it has a subnormal series

$$\{e\} = G_0 \triangleleft G_1 \triangleleft \ldots \triangleleft G_s = G.$$

such that each G_{i+1}/G_i is abelian.

Theorem 1

A finite group G is solvable if and only if all of the composition facts of G are cyclic.

Theorem 2

Let G be a group and $N \triangleleft G$, then G is solvable if and only if both N and G/N are solvable.

Theorem 3

A general degree n polynomial $f(x)$ with rational coefficients is not solvable by radicals if $n \geq 5$.

Definition 3: Derived Subgroup

Let G be a group, the **commutator** of $a, b \in G$ is $[a, b] = aba^{-1}b^{-1}$. The **derived subgroup** G' of G is the subgroup generated by all commutators

$$G' = \langle aba^{-1}b^{-1} \,:\, a, b \in G \rangle.$$

Theorem 4

Let G be a group and $N \triangleleft G$, then G/N is abelian if and only if the derived subgroup $G' \subseteq N$, in particular G/G' is abelian.

Definition 4: Derived Series

Let G be a group, set $G^{(0)} = G$ and $G^{(i+1)} = (G^{(i)})'$ is the derived subgroup of $G^{(i)}$. The sequence

$$G = G^{(0)} \triangleleft G^{(1)} \triangleleft \ldots$$

is the **derived series** for G

Theorem 5

A group G is solvable if and only if there exists some $n \in \mathbb{N}$ in which $G^{(n)} = \{e\}$. The smallest such n is called the **derived length** of the derived series.

Group Presentations

Definition 1: Free Group

The **free group** $\langle x_1, \dots, x_n \rangle$ on n generators $x_1, \dots, x_n$ is the group whose elements are the *words* whose letters are in the *alphabet* $\{x_1, \dots, x_n\}$. The group operation is concatenation $(x, y) \mapsto xy$.

More abstractly we have the following universal property. Let $X = \{x_1, \dots, x_n\}$, then the free group $F(X)$ on X is the unique group (up to isomorphism) such that for any group G and any map $f : X \to G$ there is a unique homomorphism $\varphi : F(X) \to G$ such that the following commutes

$$\begin{array}{ccc} X & \xrightarrow{\iota} & F(X) \\ & \searrow^{f} & \downarrow{\scriptstyle \varphi} \\ & & G \end{array}$$

where $\iota : X \hookrightarrow F(X)$ is inclusion.

Definition 2: Generators and Relations

Let $r_1, \dots, r_m \in \langle x_1, \dots, x_n \rangle$, the group

$$G = \langle x_1, \dots, x_n \,:\, r_1, \dots, r_m \rangle$$

generated by $x_1, \dots, x_n$ with **relations** $r_1, \dots, r_m$ is given by the the group with generators $x_1, \dots, x_n$ such that $r_1 = \cdots = r_n = e$, we call this a **presentation** of the group.

Explicitly we can set $X = \{x_1, \dots, x_n\}$ and $R = \{r_1, \dots, r_m\}$ and then $G = F(X)/N$ where N is the smallest normal subgroup of $F(X)$ containing R.

Theorem 1: Novikov

There is no algorithm for deciding whether or not

$$\langle x_1, \dots, x_n \,:\, r_1, \dots, r_m \rangle = \{e\}.$$