MTH 301: Group Theory
Semester 1, 2023-24

November 8, 2023

Contents

1 Preliminaries

1.1 Basic definitions and examples

(i) (a) A group $(G, \cdot)$ is a nonempty set G with a binary operation $\cdot$ satisfying the properties:

(a) (Closure property) For any $a, b \in G$, we have $a \cdot b \in G$.

(b) (Associativity) For any $a, b, c \in G$, we have

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

(c) (Existence of identity) There exists an element $e \in g$ called the *identity element* such that

$$a \cdot e = a = e \cdot a,$$

for any $a \in G$.

(d) (Existence of inverse) For each $a \in G$, there exists an $a^{-1} \in G$ such that

$$a \cdot a^{-1} = e = a^{-1} \cdot a.$$

(b) In a group $(G, \cdot)$ as above, the following properties hold:

(a) (Right cancellation law) For $a, b, c \in G$, if $a \cdot c = b \cdot c$, then $a = b$.

(b) (Left cancellation law) For $a, b, c \in G$, if $c \cdot a = c \cdot b$, then $a = b$.

(c) The identity e is unique.

(d) Every element $a \in G$ has a unique inverse a^{-1}.

(ii) Let G be a group.

(a) G is a said to be *finite* if the cardinality of the set G is finite. Otherwise, G is said to be *infinite*.

(b) The *order* of a finite group (denoted by $|G|$) is the number of elements in G.

(iii) Examples of groups:

(a) Additive groups: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, and $M_n((F)$, for $F = \mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$.

(b) Multiplicative groups $(\mathbb{Q}^\times,\cdot)$, $(\mathbb{R}^\times,\cdot)$, $(\mathbb{C}^\times,\cdot)$, and $\mathrm{GL}(n,X)$, for $X=\mathbb{Q},\mathbb{R}$, and $\mathbb{C}$.

(c) The Dihedral group D_{2n} - the group of symmetries of a regular n-gon.

(iv) Let G be group and $S\subset G$. Then S is a *generating set for* G (denoted by $G=\langle S\rangle$) if every element in G can be expressed as a finite product of elements in S and their inverses.

(v) The *order of an element* $g\in G$ (denoted by $|g|$) is the smallest positive integer m such that $g^m=1$. If such an m does not exist for a given $g\in G$, then g is said to be of *infinite order* in G.

(vi) Let G be a group, let $g\in G$ with $|g|=n$. Then

$$|g^k|=\frac{n}{\gcd(k,n)}.$$

(vii) A group G is said to be *abelian* if $gh=hg$ for all $g,h\in G$.

(viii) Examples (non-examples) of abelian groups.

(a) The groups in Examples 1.1 (iii)(a) are abelian groups.

(b) The matrix groups in Examples 1.1 (iii)(b) and the group in (c) are non-abelian groups.

1.2 The cyclic group

(i) A group G is said to be *cyclic*, if there exists a $g\in G$ such that $G=\langle g\rangle$. In other words, G is cyclic, if its generated by a single element.

(ii) Let $G=\langle g\rangle$ be a cyclic group.

(a) If G is of order n (denoted by C_n), then

$$C_n=\{1,g,g^2,\dots,g^{n-1}\}.$$

(b) If G is of infinite order, then

$$G=\{1,g^{\pm1},g^{\pm2},\dots\}.$$

(iii) Realizing C_n as the multiplicative group of complex n^{th} roots unity.

(iv) The group $\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}$ of residue classes modulo n under $+$, where
$$[i] = \{nk + i \mid k \in \mathbb{Z}\}$$

(v) Using the association $[k] \leftrightarrow e^{i2\pi k/n}$, for $0 \le k \le n-1$, we can identify $\mathbb{Z}_n$ with C_n.

(vi) Let $G = \langle g \rangle$ be a cyclic group.

(a) Then G is abelian.

(b) If $H \le \langle g \rangle$, then H is also cyclic.

(c) If $|G| = n$, then it has a unique cyclic subgroup $\langle g^{n/d} \rangle$ of order d for divisor d of n.

1.3 The symmetric group

1.3.1 Basic definitions and examples

(i) Let X be a nonempty set. Then the set of permutations (or self-bijections) of X defined by
$$S(X) := \{f : X \to X : f \text{ is a bijection}\}$$
forms a group under composition called the *symmetric group of X.*

(ii) When $|X| = n$, without loss of generality, we take $X = \{1, 2, \dots, n\}$, and we denote the group $S(X)$ simply by S_n. The group S_n, of order $n!$, is called the *symmetric group (or the permutation group) on n letters.*

(iii) Examples of symmetric groups.

(a) $S_2 \cong \mathbb{Z}_2$.

(b) Since each symmetry of a regular n-gon induces a permutation of its n vertices, we have $S_3 \cong D_6$ and in general, $D_{2n} < S_n$ for $n \ge 4$.

(c) For $n \ge 4$, S_n is a non-abelian group.

(d) For any group G, $\mathrm{Aut}(G) < S(G)$, since each automorphism is a bijective map.

(e) Given any group G and fixed $g \in G$, consider $\varphi_g : G \to G$ defined by $\varphi_g(h) = gh$, for all $h \in G$ (i.e., left multiplication by the element g). Then it is apparent that $\varphi_g \in S(G)$, and consequently, the map

$$\psi : G \to S(G) : g \overset{\psi}{\longmapsto} \varphi_g$$

is a monomorphism. In particular, if $|G| = n$, then G imbeds into S_n (i.e. $G \hookrightarrow S_n$).

(iv) A typical element $\sigma \in S_n$ is a bijection $\sigma : \{1,2,\dots,n\} \to \{1,2,\dots,n\}$, so we often denote such a σ by

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

To further simplify notation for σ, we only list the values of σ on the subset $\{i \in \{1,2,\dots,n\} : \sigma(i) \neq i\}$. For example, the permutation $\sigma \in S_5$ given by

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$$

is simply written as

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

(v) A product $\sigma_1\sigma_2$ of two permutations $\sigma_1, \sigma_2 \in S_n$ is defined as the permutation

$$\begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ (\sigma_1 \circ \sigma_2)(1) & (\sigma_1 \circ \sigma_2)(2) & \dots & (\sigma_1 \circ \sigma_2)(n-1) & (\sigma_1 \circ \sigma_2)(n) \end{pmatrix}.$$

(vi) The *support* of a permutation $\sigma \in S_n$ is defined by

$$\operatorname{supp}(\sigma) := \{i \in \{1,\dots,n\} : \sigma(i) \neq i\}.$$

(vii) Two permutations $\sigma_1, \sigma_2 \in S_n$ are said to be *disjoint* if

$$\operatorname{supp}(\sigma_1) \cap \operatorname{supp}(\sigma_2) = \emptyset.$$

(viii) Any two disjoint permutations in S_n commute.

1.3.2 k-cycles

(i) A k-*cycle* in S_n is a permutation of the form

$$\begin{pmatrix} i_1 & i_2 & \dots & i_{k-1} & i_k \\ i_2 & i_3 & \dots & i_k & i_1 \end{pmatrix},$$

where $1 \leq k \leq n$. A k-cycle as above is often denoted by

$$(i_1\, i_2 \dots i_k).$$

A 2-cycle in S_n is a called a *transposition (or an inversion).*

(ii) Consider the k-cycle $\sigma = (i_1\, i_2 \dots i_k)$ in S_n. Then we have:

(a)
$$\sigma = (i_1\, \sigma(i_1)\, \sigma^2(i_1) \dots \sigma^{k-1}(i_1)), \text{ and}$$

(b) $o(\sigma) = k$.

(iii) Example of k-cycles.

(a) The permutation
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} \in S_5$$
is a 3-cycle given by $(1\,2\,3)$.

(b) The permutation
$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} \in S_4$$
is a 2-cycle (transposition) given by $(2\,3)$.

(iv) Two cycles $(i_1\, i_2 \dots i_k), (j_1\, j_2 \dots j_\ell) \in S_n$ commute if

$$\{i_1, \dots, i_k\} \cap \{j_1, \dots, j_\ell\} = \emptyset.$$

(v) Every k-cycle is a product of no less than $k-1$ transpositions. In particular, for a k-cycle $(i_1\, i_2 \dots i_k) \in S_n$, we have

$$(i_1\, i_2 \dots i_k) = (i_1\, i_k)(i_1\, i_{k-1}) \dots (i_1\, i_2).$$

(vi) Every permutation $\sigma \in S_n$ can be expressed uniquely as a product of disjoint cycles. This is called the *unique cycle decomposition* of the permutation σ.

1.3.3 Parity of a permutation

(i) Suppose that the unique cycle decomposition of a permutation $\sigma \in S_n$ is given by

$$\sigma = \sigma_1\sigma_2\ldots\sigma_{k_\sigma},$$

where each σ_i is an m_i-cycle. Then we define

$$N(\sigma) := \sum_{i=1}^{k_\sigma}(m_i - 1).$$

(ii) The *sign (or parity)* of a permutation $\sigma \in S_n$ is defined by

$$\operatorname{sgn}(\sigma) := (-1)^{N(\sigma)}.$$

(iii) A permutation $\sigma \in S_n$ is called an:

  (a) *even permutation*, if $\operatorname{sgn}(\sigma) = 1$.

  (b) *odd permutation*, if $\operatorname{sgn}(\sigma) = -1$.

(iv) Let $A_n = \{\sigma \in S_n : \operatorname{sgn} = 1\}$. For $n \geq 2$, the map

$$\tau : S_n \to \{\pm 1\}(= \mathbb{Z}_2) : \sigma \overset{\tau}{\mapsto} \operatorname{sgn}(\sigma)$$

is an epimorphism with $\ker \tau = A_n$. Thus, we have

$$S_n / A_n \cong \mathbb{Z}_2.$$

Consequently, $A_n \lhd S_n$ and $[S_n : A_n] = 2$. The group A_n consisting of the even permutations in S_n is called the *alternating group on n letters.*

1.3.4 Conjugacy classes of permutations

(i) Let G be a nontrivial group. Two elements $g, h \in G$ are said to be *conjugate in G* if there exists $x \in G$ such that $g = xhx^{-1}$.

(ii) The relation $\sim_c$ on G given by

$$g \sim_c h \iff g \text{ and } h \text{ are conjugate}$$

defines an equivalence relation on G. Each equivalence class (denoted by $[g]_c$) induced by the relation $\sim_c$ is called a *conjugacy class of G.*

(iii) A *partition of a positive integer n* is a way of writing n as a sum of positive integers, up to reordering of summands. For example, the partitions of 4 are:

(a) $1+1+1+1$,

(b) $2+1+1$,

(c) $3+1$,

(d) $2+2$, and

(e) 4.

(iv) Suppose that the unique cycle decomposition of a permutation $\sigma \in S_n$ is given by

$$\sigma = \sigma_1 \sigma_2 \ldots \sigma_{k_\sigma},$$

where each σ_i is an m_i-cycle. Then:

(a) $o(\sigma) = \operatorname{lcm}(m_1, m_2, \ldots, m_{k_\sigma})$.

(b) As $\sum_{i=1}^{k_\sigma} m_i = n$, this decomposition induces a partition P_σ of the integer n.

(c) Given two permutations $\sigma_1, \sigma_2 \in S_n$,

$$[\sigma_1]_c = [\sigma_2]_c \iff P_{\sigma_1} = P_{\sigma_2}.$$

Consequently, the number of distinct conjugacy classes of S_n is precisely the number of partitions of n.

2 Subgroups

2.1 Basic definitions and examples

(i) A subset H of a group G is called a *subgroup* of G (in symbols $H \leq G$) if H forms a group under the operation in G.

(ii) Let H be a subgroup H of a group G. Then H is said to be:

(a) *proper* subgroup of G (in symbols $H < G$) if $H \neq G$.

(b) *trivial* subgroup if $H = \{1\}$.

(c) *nontrivial* subgroup of G if $H \neq \{1\}$.

(iii) ***Subgroup Criterion.*** Let G be a group. Then $H \leq G$ if and only if for every $a, b \in H$, $ab^{-1} \in H$.

(iv) Examples of subgroups:

(a) $n\mathbb{Z} < \mathbb{Z}$, for $n \geq 2$.

(b) $D_{2n} < S_n$, for $n \geq 3$.

(c) $A_n < S_n$, for $n \geq 3$.

(d) $C_n < \mathbb{C}^\times$.

(e) For $n \geq 2$, *special linear group* $\mathrm{SL}(n, F) = \{A \in \mathrm{GL}(n, F) \mid \det(A) = 1\}$ is a subgroup of $\mathrm{GL}(n, F)$ when $F = \mathbb{R}$, $\mathbb{Q}$, or $\mathbb{C}$.

(f) For $n \geq 2$, $\mathrm{SL}(n, \mathbb{Q}) < \mathrm{SL}(n, \mathbb{R}) < \mathrm{SL}(n, \mathbb{C})$.

(g) For $n \geq 2$, $\mathrm{GL}(n, \mathbb{Q}) < \mathrm{GL}(n, \mathbb{R}) < \mathrm{GL}(n, \mathbb{C})$.

2.2 Cosets and Lagrange's Theorem

(i) Let G be a group and $H \leq G$. Then the relation $\sim_H$ on G defined by

$$x \sim_H y \iff xy^{-1} \in H$$

is an equivalence relation.

(ii) Let G be a group and $H \leq G$. Then a *left coset of H in G* is given by

$$gH = \{gh \mid h \in H\},$$

and a *right coset of H in G* is given by

$$Hg = \{hg \mid h \in H\}.$$

(iii) Let G be a group and $H \leq G$. Then

$$gH = \{g' \in G \mid g' \sim_H g\}.$$

(iv) Let G be a group and $H \leq G$. Then there exists a bijective correspondence between:

(a) g_1H and g_2H, for any $g_1, g_2 \in H$, and

(b) gH and Hg, for any $g \in G$.

(v) We define $G/H := \{gH \mid g \in G\}$ and $H \backslash G := \{Hg \mid g \in G\}$.

(vi) Let G be a group and $H \leq G$. Then there is a bijective correspondence between G/H and $H \backslash G$.

(vii) The number of distinct left (or right) cosets of subgroup H of G is called the *index of H in G*, which is denoted by $G : H]$. In other words,

$$[G : H] = |G/H| = |H \backslash G|.$$

Consequently, for a finite group G we have

$$|G| = [G : H] \cdot |H|.$$

(viii) ***Lagrange's Theorem.*** Let G be a finite group and $H \leq G$. Then $|H| \mid |G|$.

(ix) The *Euler totient function* is defined by:

$$\phi(n) = |\{k \in \mathbb{Z}^+ \mid k < n \text{ and } \gcd(k, n) = 1\}|.$$

(x) The multiplicative group $U_n = \{[k] \in \mathbb{Z}_n \mid \gcd(k, n) = 1\}$ is called the *group of units modulo n*. Note that $|U_n| = \phi(n)$.

(xi) ***Euler's Theorem.*** If a and n are positive integers such that $\gcd(a, n) = 1$, then

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

(xii) ***Fermat's Theorem.*** If p is a prime number and a is a positive integer, then

$$a^p \equiv a \pmod{p}.$$

(xiii) Let G be a group and $H, K \leq G$. Then:

(a) $HK \leq G$ iff $HK = KH$,

(b) $H \cap K \leq G$, and

(c) If $|H|, |K| < \infty$, then $|HK| = \dfrac{|H||K|}{|H \cap K|}$.

2.3 Normal subgroups

(i) Let G be a group and $H \le G$. Then H is said to be a *normal subgroup of* G (in symbols $H \trianglelefteq G$ and $H \triangleleft G$, if H is proper) if $gNg^{-1} \subset N$, for all $g \in G$.

(ii) Examples of normal subgroups:

(a) $m\mathbb{Z} \trianglelefteq \mathbb{Z}$, for all $m \in \mathbb{Z}$

(b) $A_n \triangleleft S_n$, for $n \ge 3$.

(c) For $n \ge 2$, $\mathrm{SL}(n, X) \triangleleft \mathrm{GL}(n, X)$, for $X = \mathbb{Q}, \mathbb{R}$, or $\mathbb{C}$.

(d) $C_n \triangleleft \mathbb{C}^{\times}$, for $n \ge 2$.

(iii) The G be a group, and $N \le G$. Then the following statements are equivalent

(a) $N \trianglelefteq G$.

(b) $gNg^{-1} = N$, for all $g \in G$.

(c) $gN = Ng$, for all $g \in G$.

(d) $(gN)(hN) = ghN$, for all $g, h \in G$.

(iv) Let G be a group and $N \trianglelefteq G$. Then G/N forms a group under the operation $(gN) \cdot (hN) = ghN$.

(v) Let G be a group, and $H \le G$ such that $[G : H] = 2$. Then $H \triangleleft G$.

(vi) Let G be group, $H \le G$, and $N \trianglelefteq G$. Then

(a) the *internal direct product* $NH = \{nh : n \in N, h \in H\} \le G$

(b) $N \cap H \trianglelefteq H$.

(c) $N \trianglelefteq NH$.

3 Homomorphisms and isomorphisms

3.1 Homomorphisms

(i) Let G, H be group, and $\varphi : G \to H$ be a map. Then φ is said to be a *homomorphism* if

$$\varphi(gh) = \varphi(g)\varphi(h),$$

for all $g, h \in G$.

(ii) Examples of homomorphisms:

   (a) The *trivial homomophism* $\varphi : G \to H$ given by $\varphi(x) = 1$, for all $x \in G$.
   (b) The *identity homomorphism* $i : G \to G$ given by $i(g) = g$, for all $g \in G$.
   (c) The map $\varphi : \mathbb{Z} \to \mathbb{Z}$ defined by $\varphi(x) = nx$ for any $n \in \mathbb{Z}$.
   (d) The map $\varphi_n : \mathbb{Z} \to \mathbb{Z}_n$ defined by $\varphi_n(x) = [x]$.
   (e) The determinant map $\mathrm{Det} : \mathrm{GL}(n, \mathbb{C}) \to \mathbb{C}^\times$.
   (f) The sign map $\tau : S_n \to \{\pm 1\}$ defined by $\tau(\sigma) = (-1)^{n(\sigma)}$, where if σ is expressed as product of transpositions, $n(\sigma)$ is the number of transpositions appearing in the product. In other words,

$$\tau(\sigma) = \begin{cases} 1, & \text{if } \sigma \in A_n, and \\ -1, & \text{otherwise.} \end{cases}$$

(iii) Let $\varphi : G \to H$ be a homomorphism.

   (a) If φ is injective, then it is called a *monomorphism.*
   (b) If φ is surjective, then it is called an *epimorphism.*

(iv) Of the examples in (vii) above, (b) and (c) are isomorphisms, while (d) and (f) are epimorphisms.

(v) Let $\varphi : G \to H$ be a homomorphism. Then:

   (a) $\varphi(1) = 1$ and
   (b) $\varphi(g^{-1}) = \varphi(g)^{-1}$, for all $g \in G$.

(vi) Let $\varphi : G \to H$ be a homomorphism. Then:

   (a) The set $\ker \varphi = \{g \in G : \varphi(g) = 1\}$ is called the *kernel of* φ.
   (b) The set $\mathrm{Im}\,\varphi = \{\varphi(g) : g \in G\}$ is called the *image of* φ.

(vii) Let $\varphi : G \to H$ be a homomorphism. Then:

   (a) $\ker \varphi \trianglelefteq G$.
   (b) $\mathrm{Im}\,\varphi \leq H$.

(viii) A homomorphism $\varphi : G \to H$ is said to be *order-preserving* if $|g| = |\varphi(g)|$, for every $g \in G$ of finite order.

(ix) Let $\varphi : G \to H$ be a homomorphism. Then the following statements are equivalent.

(a) φ is a monomorphism.

(b) $G \cong \operatorname{Im}\varphi$.

(c) $\ker\varphi = \{1\}$.

(d) φ is order-preserving

3.2 The Isomorphism Theorems

(i) Let G be a group, and $N \lhd G$. Then the quotient map $q : G \to G/N$ given by $q(g) = gN$ is an epimorphism.

(ii) ***First Isomorphism Theorem:*** Let G, H be groups, and $\varphi : G \to H$ is a homomorphism. Then

$$G/\ker\varphi \cong \operatorname{Im}\varphi.$$

In particular, if φ is onto, then

$$G/\ker\varphi \cong H.$$

(iii) Applications of the First isomorphism theorem.

(a) The map $\operatorname{Det} : \operatorname{GL}(n,F) \to F^\times$ is an epimorphism whose kernel is given by

$$\ker(\operatorname{Det}) = \{A \in \operatorname{GL}(n,F) : \operatorname{Det}(A) = 1\} = \operatorname{SL}(n,F).$$

Therefore, the First isomorphism theorem implies that

$$\operatorname{GL}(n,F)/\operatorname{SL}(n,F) \cong F^\times.$$

(b) For $n \geq 2$, the map $\beta_n : \mathbb{Z} \to \mathbb{Z}_n$ is an epimorphism whose kernel is given by

$$\ker\beta_n = \{x \in \mathbb{Z} : \beta_n(x) = [x] = [0]\} = n\mathbb{Z}.$$

Therefore, the First isomorphism Theorem implies that

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n.$$

(c) The map

$$\varphi : \mathbb{R} \to S^1 = \{z \in \mathbb{C} : |z| = 1\} : x \overset{\varphi}{\longmapsto} e^{i2\pi x}$$

is an epimorphism whose kernel is given by

$$\ker \varphi = \{x \in \mathbb{R} : \varphi(x) = \cos(2\pi x) + i\sin(2\pi x) = 1\} = \mathbb{Z}.$$

Therefore, the First isomorphism theorem implies that

$$\mathbb{R}/\mathbb{Z} \cong S^1.$$

(iv) Let G be a group, $H < G$, and $N \lhd G$. Then

(a) $H \cap N \lhd H$.

(b) $N \lhd HN$.

(v) ***Second Isomorphism Theorem:*** Let G be a group, $H < G$, and $N \lhd G$. Then

$$H/H \cap N \cong HN/N.$$

(vi) ***Third Isomorphism Theorem:*** Let G be group, and $H, K \lhd G$ such that $H < K$. Then

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

(vii) Some applications of the Third isomorphism theorem.

(a) For positive integers ℓ, m, n such that $m \mid \ell$ and $n \mid m$, we know that

$$\ell\mathbb{Z} \lhd n\mathbb{Z}, m\mathbb{Z} \lhd n\mathbb{Z} \text{ and } \ell\mathbb{Z} < m\mathbb{Z}.$$

Therefore, the Third Isomorphism Theorem implies that

$$(n\mathbb{Z}/\ell\mathbb{Z})/(m\mathbb{Z}/\ell\mathbb{Z}) \cong n\mathbb{Z}/m\mathbb{Z},$$

or equivalently, we have

$$\mathbb{Z}_{\ell/n}/\mathbb{Z}_{\ell/m} \cong \mathbb{Z}_{m/n}.$$

(b) Consider the group D_{2n}, when n is even and $n \geq 4$. Then we know that

$$\langle r^{n/2} \rangle \lhd D_{2n}, \langle r \rangle \lhd D_{2n}, \text{ and } \langle r^{n/2} \rangle < \langle r \rangle.$$

Therefore, the Third isomorphism Theorem implies that

$$(D_{2n}/\langle r^{n/2} \rangle)/(\langle r \rangle/\langle r^{n/2} \rangle) \cong D_{2n}/\langle r \rangle.$$

(viii) ***Fourth (or Lattice) Isomorphism Theorem:*** Let G be a group and let $N \trianglelefteq G$. Then there is a one-to-one correspondence between the set of subgroups of G containing N and the set of subgroups of G/N. In particular, every subgroup of G/N is of the form H/N for some subgroup H of G containing N.

4 Group actions

4.1 Basic definitions and examples

(i) Let G be a group and A be nonempty say. Then *an action of G on A*, written as $G \curvearrowright A$ is a map

$$G \times A \to A : (g, a) \mapsto g \cdot a$$

satisfying the following conditions

(a) $1 \cdot a = a$, for all $a \in a$, and

(b) $g \cdot (h \cdot a) = (gh) \cdot a$, for all $g, h \in G$ and $a \in A$.

(ii) Examples of group actions:

(a) There is a natural action (denoted by $G \curvearrowright G$) of a group G on itself by left multiplication given by

$$(g, h) \mapsto gh, \text{ for all } g, h \in G.$$

The permutation representation $\psi_{G \curvearrowright G} : G \to S(G)$ afforded by this action given by

$$\psi_{G \curvearrowright G}(g) = \varphi_g, \text{ where } \varphi_g(h) = gh, \text{ for all } h \in G,$$

is called the *left regular representation*.

(b) A group G also acts on itself by conjugation (denoted by $G \curvearrowright^c G$), which is defined in the following manner

$$(g, h) \mapsto ghg^{-1}, \text{ for all } g, h \in G,$$

and this yields the permutation representation

$$\psi_{G \curvearrowright^c G}(g) = \varphi^c_g, \text{ where } \varphi^c_g(h) = ghg^{-1}, \text{ for all } h \in G.$$

(c) Let P_n be the regular n-gon imbedded within the closed disk $\{z \in \mathbb{C} : |z| \leq 1\} \subset \mathbb{C}$ so that its vertices coincide with the roots of unity. Then $D_{2n} = \langle r, s \rangle \curvearrowright P_n$ and this action if defined as follows for each $z \in P_n$:

   i. $r \cdot z = e^{i2\pi/n} \cdot z$ and

   ii. $s \cdot z = \bar{z}$.

(d) The group $\mathbb{Z} \curvearrowright \mathbb{R}$ via translation by an integer, which is formally defined as:

$$\mathbb{Z} \times \mathbb{R} \to \mathbb{R} : (z, x) \mapsto x + z.$$

In a similar manner, we can define the action $\mathbb{Z}^2 \curvearrowright \mathbb{R}^2$.

(iii) For a group G, the set $S(G) = \{f : G \to G \mid f \text{ is a bijection}\}$ forms a group under composition.

(iv) Every action $G \curvearrowright A$ induces a homomorphism

$$\psi_{G \curvearrowright A} : G \to S(A),$$

defined by

$$\psi(g) = \varphi_g, \text{ where } \varphi_g(a) = g \cdot a, \text{ for all } a \in A,$$

which is called the *permutation representation* induced (or afforded) by the action.

(v) Conversely, given a homomorphism $\psi : G \to S(A)$, the map

$$G \times A \to A : (g, a) \mapsto \psi(g)(a)$$

defines an action of G on A.

(vi) A group action $G \curvearrowright A$ is said to be *faithful* if the permutation representation $\psi_{G \curvearrowright A}$ it affords, is a monomorphism.

(vii) Examples (and non-examples) of faithful actions.

(a) The actions in 4 (ii) (a), (c), and (d) above are faithful actions.

(b) The conjugation action $G \curvearrowright^c G$ is not in general a faithful action.

4.2 The Orbit-Stabilizer Theorem

(i) Consider an action $G \curvearrowright A$. Then

(a) for each $a \in A$, the set $G_a = \{g \in G \,|\, g \cdot a = a\}$ is called the *stabilizer* of a under the action.

(b) or each $a \in A$, the set $\mathcal{O}_a = \{g \cdot a \,|\, g \in G\}$ is called the *orbit* of a under the action.

(c) ker $\psi_{G \curvearrowright A}$ is called *kernel of the action*, and is also denoted by $\operatorname{Ker}(G \curvearrowright A)$.

(ii) Consider an action $G \curvearrowright A$. Then

(a) $\operatorname{Ker}(G \curvearrowright A) \trianglelefteq G$, and

(b) for each $a \in A$, $G_a \leq G$.

(iii) Consider an action $G \curvearrowright A$.

(a) Then the relation $\sim$ on A defined by

$$a \sim b \iff \text{there exists some } g \in G \text{ such that } g \cdot a = b$$

defines an equivalence relation on A.

(b) Moreover, the equivalence classes under $\sim$ are precisely the distinct orbits $\mathcal{O}_a$ under the action. Consequently, for any two orbits $\mathcal{O}_a$ and $\mathcal{O}_b$, we have that either

$$\mathcal{O}_a = \mathcal{O}_b \text{ or } \mathcal{O}_a \cap \mathcal{O}_b = \emptyset.$$

(iv) An action $G \curvearrowright A$ is said to be *transitive* if there exists some $a \in A$ for which $\mathcal{O}_a = A$. This is equivalent to requiring that for an action to be transitive, $\mathcal{O}_a = A$, for all $a \in A$.

(v) ***Orbit-Stabilizer Theorem:*** Consider an action $G \curvearrowright A$, where $|A| < \infty$. Then for each $a \in A$, we have that

$$[G : G_a] = |\mathcal{O}_a|.$$

4.3 Applications of the Orbit-Stabilizer Theorem

4.3.1 The Burnside Lemma

(i) Consider an action $G \curvearrowright A$, where $|G|, |A| < \infty$. Then

$$|\mathscr{O}_a| \mid |G|, \text{for each } a \in A.$$

(ii) The collection of distinct orbits under an action $G \curvearrowright A$ is defined by:

$$A/G = \{\mathscr{O}_a : a \in A\}.$$

(iii) ***Burnside Lemma:*** Consider an action $G \curvearrowright A$, where $|G|, |A| < \infty$. Then the number of distinct orbits under the action (denoted by $|A/G|$) is given by

$$|A/G| = \frac{1}{|G|} \sum_{g \in G} |A_g|,$$

where $A_g = \mathrm{Fix}_g(A) = \{a \in A \mid g \cdot a = a\}$.

4.3.2 The action $G \curvearrowright G$

(i) For a group G, consider the self-action $G \curvearrowright G$ by left-multiplication.

(a) $G \curvearrowright G$ is a transitive action,

(b) $\mathrm{Ker}(G \curvearrowright G) = 1$, and consequently

(c) $G \xhookrightarrow{\psi_{G \curvearrowright G}} S(G)$.

(ii) ***Cayley's Thorem:*** Every group G is isomorphic to a subgroup of $S(G)$. In particular, if $|G| = n$, then G isomorphic to a subgroup of S_n.

(iii) Given a group G and $H \leq G$, the self-action $G \curvearrowright G$ induces an action $G \curvearrowright G/H$, which is defined by $(g, g'H) \mapsto (gg')H$, and this action has the following properties:

(a) It is a transitive action.

(b) Its kernel is the largest normal subgroup of G that is also a subgroup of H, which is given by

$$\mathrm{Ker}(G \curvearrowright G/H) = \bigcap_{g \in G} gHg^{-1}.$$

(c) $G_H = H$ and $\mathscr{O}_H = G/H$.

(d) Hence, when $|G/H| < \infty$ and $|G| < \infty$, the Orbit-Stabilizer Theorem yields

$$[G:H] = |G|/|H|,$$

which is the Lagrange's Theorem.

4.3.3 The action $G \curvearrowright^c G$ and the Class Equation

(i) For a group G, the set

$$Z(G) = \{g \in G \mid gh = hg, \text{ for all } h \in G\}$$

is called the *center of G*.

(ii) Let G be a group and $S \subseteq G$.

(a) The set

$$C_G(S) = \{g \in G \mid gs = sg, \text{ for all } s \in S\}$$

is called the *centralizer of S in G*.

(b) The set

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

is called the the *normalizer of H in G*.

(iii) Let G be a group and $S \subseteq G$. Then $C_G(S) \leq G$ and $N_G(S) \leq G$. Furthermore, when $S = \{h\}$, we have that $C_G(h) = N_G(h)$.

(iv) For a group G, consider the self-action $G \curvearrowright^c G$ by conjugation.

(a) Since $\mathscr{O}_1 = \{1\}$, $G \curvearrowright^c G$ is a non-transitive action.

(b) $\mathrm{Ker}(G \curvearrowright^c G) = Z(G)$, and hence $Z(G) \trianglelefteq G$.

(c) For each $h \in G$, $G_h = C_G(h)$.

(d) For each $h \in G$, the orbit $\mathscr{O}_h = \{ghg^{-1} \mid g \in G\}$ is called the *conjugacy class of h in G* (also denoted by $\mathscr{C}_h$).

(v) Let $P(G)$ denote the power set of G. The action $G \curvearrowright^c G$ extends to an action $G \curvearrowright^c P(G)$ defined by $(g, S) \mapsto gSg^{-1}$. This action has the following properties.

(a) For each $S \in P(G)$, we have

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

(b) For each $S \in P(G)$, we have

$$\mathcal{O}_S = \{gSg^{-1} \mid g \in G\} = \mathscr{C}_S,$$

the conjugacy class of the set S.

(c) When $|G| < \infty$, we have that $|P(G)| < \infty$, and hence the Orbit-Stabilizer Theorem, yields

$$|\mathscr{C}_S| = [G : N_G(S)].$$

(vi) ***Class Equation:*** Let G be a finite group, and let $g_1, g_2, \ldots, g_r$ be representatives of the distinct classes of G not contained in $Z(G)$. Then

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

(vii) Let G be a finite group, and p is the smallest prime such that $p \mid |G|$. Then every index p subgroup of G is normal is G.

4.4 Sylow's Theorems

(i) Let p be a prime number. A group G is said to be a p-*group* if $|G| = p^k$ for some postive integer k.

(ii) Example of p groups.

(a) Abelian: $\mathbb{Z}_{p^k}$ and $\mathbb{Z}_p^k$.

(b) Non-abelian: Q_8, A_3, and $D_{2 \cdot 2^k}$.

(iii) Consider an action $G \curvearrowright A$, where $|G| = p^n$ and $|A| < \infty$. Then

$$|A| \equiv |A_G| \pmod{p}$$

(iv) Let H be a p-subgroup of a finite group G. Then

$$[N_G(H) : H] \equiv [G : H] \pmod{p}$$

(v) ***Cauchy Theorem:*** Let G be a finite group, and let p be a prime number such that $p \mid |G|$. Then G has an element of order p.

(vi) ***First Sylow Theorem:*** Let G be a finite group with $|G| = p^n m$, where p is a prime number, and m is a positive integer such that $p \nmid m$. Then

  (a) for $1 \leq i \leq n$, G contains a subgroup of order p^i, and

  (b) for $1 \leq i < n$, every subgroup of G of order p^i is a normal subgroup of a subgroup of G of order p^{i+1}.

(vii) If $|G| = p^n m$, where p is a prime number, and m is a positive integer such that $p \nmid m$, then a subgroup of order p^n is called a *Sylow p-subgroup* of G.

(viii) If $|G| = pq$, where p and q are primes, then G has a Sylow p-subgroup H of order p and a Sylow q-subgroup K of order q, and so $G = HK$.

(ix) ***Second Sylow Theorem:*** Any two Sylow p-subgroups of a group G are conjugate in G.

(x) If P is a unique Sylow p-subgroup of a group G, then $P \trianglelefteq G$.

(xi) Let P be a Sylow p-subgroup, and Q, a p-subgroup of a group G. Then

$$N_G(P) \cap Q = P \cap Q$$

(xii) ***Third Sylow Theorem:*** Let n_p denote the number of Sylow p-subgroups of a group G. Then:

  (a) $n_p \equiv 1 \pmod{p}$ and

  (b) for each Sylow p-subgroup P of G, we have $[G : N_G(P)] = n_p$. Consequently, $n_p \mid |G|$.

4.5 Simple groups

(i) A group G is said to be *simple* if it has no proper normal subgroups.

(ii) Examples of simple/non-simple groups:

  (a) If $|G| = p$, where p is a prime, then G has no proper subgroups, and so G has to be simple.

(b) Let $|G| = p^k$, where p is a prime and $k > 1$. Then by the First Sylow Theorem, G has a subgroup H of order p^{k-1}. Since $[G : H] = p$, we have that $H \trianglelefteq G$, and so G is non-simple.

(c) Let $|G| = 2p^k$, where p is a prime. Then by the First Sylow Theorem, G has a subgroup H of order p^{k-1}. Since $[G : H] = 2$, we have that $H \trianglelefteq G$, and so G is non-simple.

(d) If $|G| = pq$, where $p < q$ are distinct primes, then G is not simple, as it has a subgroup of order q that has index p in G.

(iii) Let G be any group that has non-prime order less than 60. Then G is non-simple.

(iv) The group A_5 (of order 60) is the simple group of smallest non-prime order.

5 Semi-direct products and group extensions

5.1 Direct products

(i) Given two groups G and H, consider the cartesian product $G \times H$ with a binary operation given by

$$(g_1, h_2)(g_2, h_2) = (g_1 g_2, h_1 h_2), \text{ for all } g_1, g_2 \in G \text{ and } h_1, h_2 \in H.$$

Under this operation, the set $G \times H$ forms a group called the *external direct product (or the direct product)* of the groups G and H, and is denoted simply as $G \times H$.

(ii) The identity element in $G \times H$ is $(1, 1)$ and the inverse of an element $(g, h) \in G \times H$ is given by (g^{-1}, h^{-1}).

(iii) The notion of a direct of two groups can be extended to define the direct product of n groups G_i, $1 \le i \le n$, denoted by

$$\prod_{i=1}^{n} G_i = G_1 \times G_2 \times \ldots \times G_n.$$

(iv) The groups G and H inject into the $G \times H$, via the natural monomorphisms

$$G \hookrightarrow G \times H : g \mapsto (g, 1)$$
$$H \hookrightarrow G \times H : h \mapsto (1, h)$$

(v) For any two groups G and H, the natural homomorphism

$$G \times H \to H \times G : (g,h) \mapsto (h,g)$$

is an isomorphism, and hence we have that

$$G \times H \cong H \times G.$$

In other words, up to isomorphism, the direct product of two groups is commutative.

(vi) For any three groups G, H, and K, the natural homomorphism

$$(G \times H) \times K \to (G \times H) \times K : ((g,h),k) \mapsto (g,(h,k))$$

is an isomorphism, and hence we have that

$$G \times (H \times K) \cong (G \times H) \times K.$$

In other words, up to isomorphism, the direct product of three groups is associative.

(vii) A direct product $\prod_{i=1}^{n} G_i$ of groups is abelian, if and only if, each component group G_i is abelian.

(viii) Let $m, n \geq 2$ be positive integers. Then

$$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$$

if and only is $\gcd(m,n) = 1$.

(ix) **Classification of finitely generated abelian groups:** Every finitely generated abelian group is isomorphic to a group of the form

$$\mathbb{Z}^r \times \mathbb{Z}_{r_1} \times \ldots \times \mathbb{Z}_{r_k}, \tag{*}$$

where n and the $r_i \geq 1$ are positive integers such that $r_i \mid r_{i+1}$, for $1 \leq i \leq k-1$.

(x) Let G be a finitely generated abelian group that has a direct product decomposition of the form (*) above.

(a) The component $\mathbb{Z}^r$ is the called *free part*, and the component $\mathbb{Z}_{r_1} \times \ldots \times \mathbb{Z}_{r_k}$ is called the *torsion* part of the direct product decomposition of G.

(b) The integer r is called *rank* of G.

5.2 Semi-direct products

(i) For a group G, the set

$$\mathrm{Aut}(G) = \{\varphi : G \to G \,|\, \varphi \text{ is a isomorphism}\}$$

forms a group under composition (with identity element id_G) called the *automorphism group of G*.

(ii) For a group G, $\mathrm{Aut}(G) \leq S(G)$.

(iii) Examples of automorphism groups.

(a) $\mathrm{Aut}(\mathbb{Z}_n) \cong U_n$, the multiplicative group of units modulo n.

(b) $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$.

(c) $\mathrm{Aut}(D_8) \cong D_8$.

(iv) Let G, H be groups, and $\psi : G \to \mathrm{Aut}(H)$ be a homomorphism.

(a) Consider the binary operation $\cdot$ on the set $G \times H$ defined by

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 \psi(g_1)(h_2))$$

Then $(G \times H, \cdot)$ forms a group called the *semi-direct product of the groups G and H with respect to* ψ, and is denoted by $G \ltimes_\psi H$.

(b) The identity element in $G \ltimes_\psi H$ is $(1,1)$ and the inverse of an element $(g, h) \in G \times H$ is given by (g^{-1}, h^{-1}).

(c) By definition, it follows that $H \lhd G \ltimes_\psi H$.

(v) A semi-direct product $G \ltimes_\psi H$ is abelian if and only if both G and H are abelian, and ψ is trivial.

(vi) Examples of semi-direct products:

(a) If ψ is taken to be the trivial homomorphism (that maps all elements of G to the identity isomorphism $1 \in \mathrm{Aut}(H)$), then

$$G \ltimes_\psi H = G \times H.$$

Hence, the semi-direct product of groups is a generalization of the direct product.

(b) Let $G = \mathbb{Z}_m$ and $H = \mathbb{Z}_n$

- Then a non-trivial homomorphism $\psi : G \to \mathrm{Aut}(H) \cong U_n$ exists if and only if

$$\gcd(m, \phi(n)) > 1.$$

- Moreover, ψ is completely determined by $\psi(1)$, and so if $\psi(1) = k \in U_n$, then k has to satisfy

$$k^m \equiv 1 \pmod{n}.$$

- Hence, $\mathbb{Z}_m \ltimes_\psi \mathbb{Z}_n$ is often abbreviated as $\mathbb{Z}_n \ltimes_k \mathbb{Z}_n$.
- In particular, consider the case when $m = 2$ in example (a) above with the homomorphism ψ determined by $\psi(1) = -1 \in \mathrm{Aut}(H)$. (Note that -1 here denotes the isomoprhism $h \xmapsto{-1} h^{-1} = -h$, for each $h \in H$.) Representing the dihedral group as before, that is,

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

we have that

$$\mathbb{Z}_2 \ltimes_{-1} \mathbb{Z}_n \cong D_{2n}$$

via the isomorphism

$$(i, j) \mapsto s^i r^j.$$

(c) If $G = H = \mathbb{Z}$, there exists only non-trivial semi-direct product $\mathbb{Z} \ltimes_\psi \mathbb{Z}$, which occurs when

$$\psi : \mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2 : 1 \xmapsto{\psi} [1].$$

(d) Consider group $S(\mathbb{R}^2)$ of symmetries (or isometries) of the plane $\mathbb{R}^2$. Then subgroup of translations by a vector (in $\mathbb{R}^2$) is a normal subgroup of $S(\mathbb{R}^2)$ that is isomorphic to $\mathbb{R}^2$. Thus, we have

$$S(\mathbb{R}^2) \cong \mathrm{O}(2, \mathbb{R}) \ltimes_\psi \mathbb{R}^2,$$

where $\psi : \mathrm{O}(2, \mathbb{R}) \to \mathrm{Aut}(\mathbb{R}^2)$ is defined by $\psi(A)(v) = Av$.

(e) The special real orthogonal group $H = \mathrm{SO}(n, \mathbb{R})$ is a normal subgroup of the real orthogonal group $G = \mathrm{O}(n, \mathbb{R})$ since $[G : H] = 2$. Consider a subgroup $\{1, R\} < \mathrm{O}(n, \mathbb{R})$, where R is a reflection that preserves the origin. Then it follows that

$$\mathrm{O}(n, \mathbb{R}) \cong \{1, R\} \ltimes_\psi \mathrm{SO}(n, \mathbb{R}) \cong \mathbb{Z}_2 \ltimes_\psi \mathrm{SO}(n, \mathbb{R}),$$

where $\Psi : \{1, R\} \to \mathrm{Aut}(\mathrm{SO}(n, \mathbb{R}))$ is defined by $\psi(R)(A) = RAR^{-1})$.

(f) For $n \geq 3$, the alternating group $H = A_n$ is a normal subgroup of the symmetric group $G = S_n$ since $[G : H] = 2$. Consider a subgroup $\{1, \tau\} < S_n$, where $\tau \in S_n \setminus A_n$ and $|\tau| = 2$. Then it follows that

$$S_n \cong \{1, \tau\} \ltimes_\psi A_n \cong \mathbb{Z}_2 \ltimes_\psi A_n,$$

where $\Psi : \{1, \tau\} \to A_n$ is defined by $\psi(\tau)(\sigma) = \tau\sigma\tau^{-1}$.

5.3 Group Extensions

(i) A sequence of groups G_i and homomorphisms φ_i of the form

$$\ldots \to G_{n-1} \xrightarrow{\varphi_{n-1}} G_n \xrightarrow{\varphi_n} G_{n+1} \to \ldots$$

is called an *exact sequence* if $\ker \varphi_{i+1} = \operatorname{Im} \varphi_i$, for all i.

(ii) (a) A *short exact sequence* is an exact sequence of the form

$$1 \xrightarrow{\varphi_0} N \xrightarrow{\varphi_1} G \xrightarrow{\varphi_2} H \xrightarrow{\varphi_4} 1,$$

where 1 denotes the trivial group, and φ_0, φ_4 are trivial homomorhisms.

(b) The exactness of the sequence above implies that φ_1 is injective and and φ_2 is surjective.

(iii) If G, N and H are group, then G is called an *extension of H by N* if there exists a short exact sequence of the form

$$1 \to N \to G \to H \to 1.$$

(iv) Examples of group extensions:

(a) For any group G, and $N \trianglelefteq G$, there is a natural short exact sequence given by

$$1 \to N \hookrightarrow G \xrightarrow{g \mapsto gN} G/N \to 1.$$

Hence, G is an extension of G/N by N.

(b) A semi-direct product $H \ltimes_\psi N$ of groups N and H is an extension of H by N by virtue of the short exact sequence:

$$1 \to N \xhookrightarrow{n \mapsto (n,0)} H \ltimes_\psi N \xrightarrow{(h,n) \mapsto h} H \to 1.$$

(c) A group G that is an extension of $\mathbb{Z}_m$ by $\mathbb{Z}_n$ is called a *metacyclic group.*

- D_{2n} is a metacyclic group, which is an extension of $\mathbb{Z}_2$ by $\mathbb{Z}_n$ via the short exact sequence

$$1 \to \langle r \rangle \hookrightarrow D_{2n} \to D_{2n}/\langle r \rangle \to 1.$$

- Q_8 is a metacyclic group that is an extension of $\mathbb{Z}_2$ by $\mathbb{Z}_4$ via the short exact sequence

$$1 \to \langle x \rangle \hookrightarrow Q_8 \to Q_8/\langle x \rangle \to 1,$$

where $x \in \{i, j, k\}$. In fact, Q_8 is also an extension of the Klein 4-group $\mathbb{Z}_2 \times \mathbb{Z}_2$ by $\mathbb{Z}_2$ via the short exact sequence

$$1 \to Z(Q_8) \hookrightarrow Q_8 \to Q_8/Z(Q_8) \to 1.$$

(v) A short exact sequence

$$1 \to N \xrightarrow{\varphi_1} G \xrightarrow{\varphi_2} H \to 1$$

splits if there exists a homomorphism $\bar{\varphi}_2 : H \to G$ such that $\varphi_2 \circ \bar{\varphi}_2 = id_H$.

(vi) A short exact sequence

$$1 \to N \xrightarrow{\varphi_1} G \xrightarrow{\varphi_2} H \to 1$$

splits if and only if $G \cong H \ltimes_\psi N$.

(vii) Examples of split and non-split short exact sequences.

(a) The short exact sequence

$$1 \to N \xhookrightarrow{n \mapsto (n,0)} H \ltimes_\psi N \xrightarrow{(h,n) \overset{\varphi_2}{\longmapsto} h} H \to 1$$

splits as the homomorphism $\bar{\varphi}_2 : H \to H \ltimes_\psi N : h \overset{\bar{\varphi}_2}{\longmapsto} (h, 0)$ satisfies $\varphi_2 \circ \bar{\varphi}_2 = id_H$. In particular, the short exact sequence

$$1 \to \langle r \rangle \hookrightarrow D_{2n} \to D_{2n}/\langle r \rangle \to 1$$

splits.

(b) The short exact sequence

$$1 \to \langle x \rangle \hookrightarrow Q_8 \to Q_8/\langle x \rangle \to 1,$$

where $x \in \{i, j, k\}$, does not split, whereas the short exact sequence

$$1 \to Z(Q_8) \hookrightarrow Q_8 \to Q_8/Z(Q_8) \to 1$$

splits.

6 Classification of groups up to order 15

Below is a table describing the abelian and non-abelian groups (up to isomorphism) of orders ≤ 15.

Order	Abelian groups	Non-abelian groups
1	$\mathbb{Z}_1$	None
2	$\mathbb{Z}_2$	None
3	$\mathbb{Z}_3$	None
4	$\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$	None
5	$\mathbb{Z}_5$	None
6	$\mathbb{Z}_6$	S_3
7	$\mathbb{Z}_7$	None
8	$\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	D_8, Q_8
9	$\mathbb{Z}_9$, $\mathbb{Z}_3 \times \mathbb{Z}_3$	None
10	$\mathbb{Z}_{10}$	D_{10}
11	$\mathbb{Z}_{11}$	None
12	$\mathbb{Z}_{12}$, $\mathbb{Z}_6 \times \mathbb{Z}_2$	A_4, D_{12}, $\mathbb{Z}_4 \ltimes \mathbb{Z}_3$
13	$\mathbb{Z}_{13}$	None
14	$\mathbb{Z}_{14}$	D_{14}
15	$\mathbb{Z}_{15}$	None

7 Solvable groups

7.1 Normal and composition series

(i) Let G be a group.

(a) A series of subgroups N_i, for $1 \le i \le k$ satisfying

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_{k-1} \trianglelefteq N_k = G$$

is called a *subnormal series* of G.

(b) A subnormal series as above in which each $N_i \trianglelefteq G$ is called a *normal series* of G.

(c) If in a subnormal series

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_{k-1} \trianglelefteq N_k = G,$$

the quotient groups N_{i+1}/N_i are simple for $1 \le i \le k-1$, then the normal series is called a *composition series* of G. The quotient groups N_{i+1}/N_i are called *composition factors.*

(ii) Examples of composition and normal series.

(a) The following series of D_{2n}

$$1 \triangleleft \langle r \rangle \triangleleft D_{2n}$$

is a normal series for all n, and is a composition series when n is prime.

(b) The series of S_n

$$1 \trianglelefteq A_n \trianglelefteq S_n$$

is a composition series of S_n for $n = 3$ and for $n \ge 5$ (since A_n is simple.) However, for $n = 4$ it is simply a normal series of S_4.

(c) Every group G of order p^k, for p prime and $k > 1$ admits a composition series of the form

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \ldots \trianglelefteq H_{k-1} \trianglelefteq H_k = G,$$

where H_i is a group of order p^i whose existence and normality in H_{i+1} are guaranteed by the Sylow's Theorems.

(iii) Let G be a group and $A, B \triangleleft G$ with $A \ne B$ such that both G/A and G/B are simple. Then $G/A \cong B/A \cap B$ and $G/B \cong A/A \cap B$.

(iv) **Jordan-Holder Theorem.** Let G be a finite non-trivial group. Then:

(a) G has a composition series, and

(b) if

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_{r-1} \trianglelefteq N_r = G$$
and
$$1 = M_0 \trianglelefteq M_1 \trianglelefteq \ldots \trianglelefteq M_{s-1} \trianglelefteq M_s = G$$

are two composition series' for G, then $r = s$, and there exists a permutation π of $\{1, 2, \ldots, r\}$ such that

$$M_{\pi(i)+1}/M_{\pi(i)} \cong N_{i+1}/N_i, \text{ for } 1 \leq i \leq r-1.$$

7.2 Derived series and solvable groups

(i) The subgroup $[G, G] = \langle S \rangle$ of a group G generated by elements in the set

$$S = \{ghg^{-1}h^{-1} \mid g, h \in G\}$$

is called the *commutator subgroup or the derived subgroup of* G. It is also denoted by G' or $G^{(1)}$.

(ii) Let G be a group. Then:

(a) $G^{(1)} \trianglelefteq G$.

(b) $G/G^{(1)}$ is an abelian group called the abelianization of G.

(c) G is abelain if and only if $G^{(1)} = 1$.

(d) Given $N \trianglelefteq G$, G/N is abelian if and only if $[G, G] \leq N$.

(iii) For $i \geq 0$, the i^{th} *commutator subgroup (or the* i^{th} *derived group)* $G^{(i)}$ of a group G is defined as follows:

(a) $G^{(0)} := G$, and

(b) $G^{(i)} := [G^{(i-1)}, G^{(i-1)}]$, for $i \geq 1$.

(iv) The *derived series (or the commutator series)* of a group G is the series

$$\ldots G^{(i+1)} \trianglelefteq G^{(i)} \trianglelefteq \ldots \trianglelefteq G^{(1)} \trianglelefteq G^{(0)} = G.$$

(v) A group G is said to be *solvable* if it has a subnormal series

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_{k-1} \trianglelefteq N_k = G$$

such that N_{i+1}/N_i is abelian, for $1 \leq i \leq k-1$.

(vi) Examples of solvable and non-solvable groups.

(a) The group S_3 is solvable, as it has a normal series

$$1 \trianglelefteq A_3 \trianglelefteq S_3,$$

where $A_3 \cong \mathbb{Z}_3$ and $S_3/A_3 \cong \mathbb{Z}_2$.

(b) The Jordan-Holder Theorem asserts that S_5 has a composition series given by

$$1 \trianglelefteq A_5 \trianglelefteq S_5$$

that is unique up to permutation of its composition factors, and these factors are isomorphic to A_5 and $\mathbb{Z}_2$. Since A_5 is a non-abelian simple group and $[S_5 : A_5] = 2$, S_5 is not solvable.

(c) Abelian groups are solvable, as all of their subgroups are normal and all quotient groups formed using these subgroups will also be abelian.

(d) A group G of order p^k, for p prime and $k > 1$ admits a normal series of the form

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \ldots \trianglelefteq H_{k-1} \trianglelefteq H_k = G,$$

where H_i is a group of order p^i whose existence and normality in H_{i+1} are guaranteed by the Sylow's Theorems. Since $H_{i+1}/H_i \cong \mathbb{Z}_p$, G is solvable.

(e) Consider a group G such that $|G| = pq$, where p and q are distinct primes with $p > q$. Then by the Sylow's theorems, G has a unique Sylow p-subgroup P of order p, which implies that $P \triangleleft G$. Furthermore, as $|G/P| = q$, G/P is abelian, and so we have subnormal series of G with abelian factors given by:

$$1 \triangleleft P \triangleleft G.$$

Therefore, G is solvable.

(vii) A subgroup of a solvable group is solvable.

(viii) A group G is solvable if and only if there exists $N \trianglelefteq G$ such that both N and G/N are solvable.

(ix) A group G is solvable if and only if there exists and integer $k \geq 0$ such that $G^{(k)} = 1$.

(x) For a solvable group G, smallest integer $k \geq 0$ such that $G^{(k)} = 1$ is called the *derived length or the solvable length* of G.

(xi) Properties of the derived length.

  (a) A group G has derived length 0 if and only if G is trivial.

  (b) A group G has derived length 1 if and only if G is abelian.

  (c) A group has derived length at most two if and only it has an abelian normal subgroup such that the quotient group is also an abelian group.

(xii) Let G be a finite group. Here are some known non-trivial results on solvable groups.

  (a) (Philip-Hall) G is solvable if and only if for every divisor d of $|G|$ such that $\gcd(d, |G|/d) = 1$, G has a subgroup of order d.

  (b) (Burnside) If $|G| = p^a q^b$, where p and q are primes, then G is solvable.

  (c) (Feit-Thompson Theorem) If $|G|$ is odd, then G is solvable.

  (d) (Thompson) If for for every pair of elements $x, y \in G$, $\langle x, y\rangle$ is a solvable group, then G is solvable.