MTH 301: Group Theory
Semester 1, 2016-17

Contents

1 Preliminaries

1.1 Basic definitions and examples

(i) Definition of a group.

(ii) The *order of a group* G (denoted by $|G|$) is the number of elements in it (or its cardinality).

(iii) Examples of groups:

  (a) Additive groups: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, and $M_n((X)$, for $X = \mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, 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 powers of elements in S.

(v) The *order of an element* $g \in G$ (denoted by $o(g)$) is the smallest positive integer m such that $g^m = 1$.

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

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

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

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

(b) If G is of infinite order, then

$$G = \{1, g^{\pm 1}, g^{\pm 2}, \ldots\}.$$

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

(iv) The group $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$ 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 $0 \leq k \leq n-1$, we can realize C_n as $\mathbb{Z}_n$.

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

(a) If $H \leq g$, then H is also cyclic.

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

1.3 The symmetric group S_n

(i) The *symmetric group* S_n is the group all bijections from a set of size n onto itself.

(ii) $|S_n| = n!$.

(iii) A *k-cycle* $\sigma = (i_1\, i_2\, \ldots\, i_k)$ in S_n is a permutation of the form

$$\begin{pmatrix} i_1 & i_2 & \ldots & i_{n-1} & i_n \\ i_2 & i_3 & \ldots & i_n & i_1 \end{pmatrix}$$

(iv) A 2-cycle in S_n is a called a *transposition.*

(v) Every permutation $\sigma \in S_n$ can be expressed as a product of disjoint cycles.

(vi) Suppose that the 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 $\sum_{i=1}^{k_\sigma} m_i = n$, or in other words, the decomposition induces a partition of the integer n as follows

$$n = m_1 + m_2 + \ldots + m_{k_\sigma}.$$

(vii) Two permutations of S_n lie in the same conjugacy class if, and only if they induce the same partition of the integer n. Consequently, the cycle decomposition of a permutation is unique.

(viii) Every k-cycle $(i_1\, i_2\, \ldots\, i_k)$ (for $k \geq 2$) is a product of $k-1$ transpositions, namely

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

(ix) The order of an element in S_n is the least common multiple of the lengths of the cycles in its unique cycle decomposition.

(x) Every normal subgroup of S_n is a disjoint union of conjugacy classes.

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

(a) *even permutation*, if it can be expressed as the product of an even number of transpositions.

(b) *odd permutation*, if it can be expressed as the product of an odd number of transpositions.

2 Subgroups

2.1 Basic definitions and examples

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

(ii) A subgroup H of a group G is said to *proper* if $H \neq \{1\}$ or G.

(iii) 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) $n\mathbb{Z} \leq \mathbb{Z}$.
   (b) $C_n \leq D_{2n} \leq S_n$.
   (c) The *alternating group* $A_n = \{\sigma \in S_n \,|\, \sigma \text{ is even.}\}$
   (d) The group of complex n^{th} roots of unity is a subgroup of $\mathbb{C}^\times$.
   (e) $\mathrm{SL}(n, \mathbb{C}) = \{A \in \mathrm{GL}(n, \mathbb{C}) \,|\, \det(A) = 1\}$ is a subgroup of $\mathrm{GL}(n, \mathbb{C})$.
   (f) $\mathrm{SL}(n, \mathbb{Q}) \leq \mathrm{SL}(n, \mathbb{R}) \leq \mathrm{SL}(n, \mathbb{C})$.
   (g) $\mathrm{GL}(n, \mathbb{Q}) \leq \mathrm{GL}(n, \mathbb{R}) \leq \mathrm{GL}(n, \mathbb{C})$.

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

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

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

$$Hg = \{hg \,|\, h \in H\}.$$

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

$$Hg = \{g' \in G \,|\, g' \sim_H g\}.$$

(iv) Let G be a group and $H \leq G$. Then for any $g \in G$, there is a bijective correspondence between gH and Hg.

(v) Let G be a group and $H \leq G$. Then for any $g_1, g_2 \in G$, there is a bijective correspondence between g_1H and g_2H.

(vi) The sets $G/H = \{gH \,|\, g \in G\}$ and $H \backslash G = \{Hg \,|\, g \in G\}$.

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

(viii) 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,

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

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

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

(xi) The multiplicative group $U_n = \{[k] \in \mathbb{Z}_n \mid \gcd(k, n) = 1\}$ of integers modulo n.

(xii) $|U_n| = \phi(n)$.

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

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

(xiv) Fermat's Theorem: If p is a prime number and a is a positive integer, then

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

(xv) Let G be a group and $H, K \leq G$. Then $HK \leq G$ if, and only if $HK = KH$.

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

(xvii) Let G be a group and H, K be finite subgroups of G. Then

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

2.3 Normal subgroups

(i) Let G be a group and $H \leq G$. Then H is said to be a *normal subgroup of* G (denoted by $H \trianglelefteq G$) 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) $A_n \trianglelefteq S_n$, for $n \geq 3$.
  (c) $\mathrm{SL}(n, \mathbb{C}) \trianglelefteq \mathrm{GL}(n, \mathbb{C})$, for $n \geq 2$.
  (d) $C_n \trianglelefteq \mathbb{C}^\times$, for $n \geq 2$.

(iii) The G be a group, and $N \leq G$. 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 $(gN, hN) \mapsto ghN$.

(v) Let G be a group, and $H \leq G$ such that $|G/H| = 2$. Then $H \trianglelefteq G$.

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

  (a) $NH \leq G$ i.e. NH is the internal direct product of N and H.
  (b) $N \cap H \trianglelefteq H$.
  (c) $H \trianglelefteq NH$.

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 $\varphi(x) = nx$.

(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,

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

(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) $\varphi(1) = 1$.

(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 $\mathrm{Ker}\,\varphi = \{g \in G \,:\, \varphi(g) = 1\}$ 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) $\mathrm{Ker}\,\varphi \trianglelefteq G$.

(b) $\mathrm{Im}\,\varphi \leq H$.

(c) φ is a monomorphism if and only if $\mathrm{Ker}\,\varphi = \{1\}$.

3.2 The Isomorphism Theorems

(i) A homomoprhism $\varphi : G \to H$ is called an *isomorphism* if φ is bijective.

(ii) Let G be a group, and $N \trianglelefteq G$. Then the quotient map $q : G \to G/N$ given by $q(g) = gN$ is a homomorphism.

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

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

In particular, if φ is onto, then

$$G/\operatorname{Ker}\varphi \cong H.$$

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

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

(b) $H \trianglelefteq NH$.

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

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

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

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

4 Group actions

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

(iii) 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.

(iv) 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.

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

(vi) Examples of group actions:

(a) There is a natural faithful 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

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

(c) Let P_n be the regular n-gon. Then $D_{2n} \curvearrowright P_n$ by permuting its vertices $\{P_1, P_2, \dots, P_n\}$ as follows

$$\sigma \cdot (P_1, P_2, \dots, P_n) = (P_{\sigma(1)}, P_{\sigma(2)}, \dots, P_{\sigma(n)}),$$

and this permutation extends to a faithful action on the entire polygon P_n.

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

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

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

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

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

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

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

(ix) 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

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

(x) 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 $a \in A$.

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

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

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

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

(xiii) Burnside Lemma: Consider an action $G \curvearrowright A$, where $|G|, |A| < \infty$. Then the number of distinct orbits under the action (denoted by $|\mathcal{O}(G \curvearrowright A)|$) is given by

$$|\mathcal{O}(G \curvearrowright A)| = \frac{1}{|G|} \sum_{g \in G} |A_g|,$$

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

(xiv) 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, and consequently, a cyclic subgroup of order p.

4.1 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 $G \curvearrowright G$ extends to 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 smallest normal subgroup of G containing H, which is given by

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

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

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

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

which is the Lagrange's Theorem.

4.2 The action $G \curvearrowright^c G$

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

(b) $\operatorname{Ker}(G \curvearrowright^c G) = Z(G)$, 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 $\mathcal{O}_h = \{ghg^{-1} \,|\, g \in G\}$ is called the *conjugacy class of h in G* (also denoted by $\mathcal{C}_h$).

(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

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

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

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

the conjugacy class of the set S.

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

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

(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.

4.3 Sylow's Theorems and simple groups

(i) Let p be a prime number. A group G is said to be a *p-group* if each element in G has order a power of the p.

(ii) A subgroup H of a group G is a called a *p-subgroup* if H itself is a p-group.

(iii) Example: For a prime p, the group $\mathbb{Z}_{p^k}$ is a p-group for every $k \in \mathbb{N}$.

(iv) A finite group is a p-group if, and only if $|G| = p^k$, for some $k \in \mathbb{N}$.

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

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

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

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

(vii) 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}.

(viii) 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.

(ix) 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 $G = HK$.

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

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

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

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

(xiii) Third Sylow Theorem: Let n_p denote the number of Sylow p-subgroups of a group G. Then for each Sylow p-subgroup P of G, we have

$$[G : N_G(P)] = n_p$$

Moreover,

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

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

(xv) 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 H of p^{k-1}. Since $[G : H] = p$, we have that $H \trianglelefteq G$, and so G is non-simple.

(c) 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.

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

(xvii) The group A_5 that has order 60 is smallest simple group of 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, $1 \leq i \leq n$, 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 $\displaystyle\prod_{i=1}^{n} G_i$ 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

$$\mathbb{Z}^r \times \mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \ldots \times \mathbb{Z}_{p_k^{r_k}}, \qquad (*)$$

where n and the $r_i \geq 1$ are positive integers, and the p_i are prime numbers.

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

  (a) The component $\mathbb{Z}^r$ is the called *free part*, and the component $\mathbb{Z}_{p_1^{r_1}} \times \ldots \times \mathbb{Z}_{p_k^{r_k}}$ 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) The set $\{[k] \in \mathbb{Z}_n \,|\, \gcd(k, n) = 1\}$ under multiplication modulo n is called the *multiplicative group of units modulo n*, and is denoted by U_n.

(iv) The group U_n is cyclic if and only if

$$n = 1, 2, 4, p^k, \text{ or } 2p^k,$$

where p is an odd prime.

(v) Examples of automorphism groups:

  (a) When $G = \mathbb{Z}$, $\mathrm{Aut}(G) \cong \mathbb{Z}_2$, as it comprises only 1 (i.e. id_G) and -1 (i.e. $-id_G$).

  (b) For $G = \mathbb{Z}_n$, $\mathrm{Aut}(G) \cong U_n$, as any such isomorphism has to map 1 to a generator of G.

(vi) Let G, H be groups, and $\psi : G \to \mathrm{Aut}(H)$ be a homomorphism. 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 under ψ, and is denoted by $G \ltimes_\psi H$.

(vii) 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}).

(viii) 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.

(ix) For a semi-direct product $G \ltimes_\psi H$, the homomorphism $\psi : G \to \mathrm{Aut}(H) \leq S(G)$ is indeed the permutation representation of an action $G \curvearrowright H$.

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

(xi) Examples of semi-direct products:

(a)
- When $G = \mathbb{Z}_m$ and $H = \mathbb{Z}_n$, 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 $\mathbb{Z}_n \ltimes_k \mathbb{Z}_n$.

(b) 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,

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

we have that

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

via the isomorphism

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

5.3 Group Extensions

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

$$G_0 \xrightarrow{\varphi_1} G_1 \xrightarrow{\varphi_2} \dots \xrightarrow{\varphi_{n-1}} G_n$$

is called an *exact sequence* if $\operatorname{Ker}\varphi_{i+1} = \operatorname{Im}\varphi_i$, for $1 \le i \le n-2$.

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

$$1 \xrightarrow{\varphi_0} G_1 \xrightarrow{\varphi_1} G_2 \xrightarrow{\varphi_2} G_3 \xrightarrow{\varphi_4} 1,$$

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

(iii) The exactness of the sequence

$$1 \xrightarrow{\varphi_0} G_1 \xrightarrow{\varphi_1} G_2 \xrightarrow{\varphi_2} G_3 \xrightarrow{\varphi_4} 1,$$

implies that φ_1 is injective and and φ_2 is surjective.

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

$$1 \to N \to G \to Q \to 1.$$

(v) Examples of group extensions:

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

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

is a short exact sequence. Hence, G is an extension of N by G/N.

(b) For any two groups G and H, and a semi-direct product $G \ltimes_\psi H$,

$$1 \to G \xhookrightarrow{g \mapsto (g,0)} H \ltimes_\psi G \xrightarrow{(g,h) \mapsto h} H \to 1$$

is a short exact sequence. Hence, $G \ltimes_\psi H$ is an extension of G by H.

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

(d) The group D_{2n} is a metacyclic group, which is an extension of $\mathbb{Z}_2$ by $\mathbb{Z}_n$.

(e) Consider the set $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ having 8 elements with an operation $\cdot$ satisfying the following relations

$$i \cdot i = j \cdot j = k \cdot k = -1$$
$$i \cdot j = k,\ j \cdot k = i,\ k \cdot i = j$$
$$(-1) \cdot (-1) = +1$$

Then $(Q_8, \cdot)$ is a group with $+1$ as its identity element called the group of *quaternions*. The group Q_8 is a metacyclic group that is an extension of $\mathbb{Z}_4$ by $\mathbb{Z}_2$.

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) In a group G, a series of subgroups N_i, for $1 \leq i \leq k$ satisfying

$$1 = N_0 \trianglelefteq N_2 \trianglelefteq \ldots \trianglelefteq N_{k-1} \trianglelefteq N_k = G$$

are said to form a *normal series.*

(ii) If in a normal series

$$1 = N_0 \trianglelefteq N_2 \trianglelefteq \ldots \trianglelefteq N_{k-1} \trianglelefteq N_k = G,$$

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

(iii) Examples of composition series.

(a) The following are composition series' associated with the group $D_8 = \langle s, r \rangle$

$$1 \trianglelefteq \langle s \rangle \trianglelefteq \langle s, r^2 \rangle \trianglelefteq D_8$$
$$1 \trianglelefteq \langle r^2 \rangle \trianglelefteq \langle r \rangle \trianglelefteq D_8$$

(b) The group S_3 has a composition series

$$1 \trianglelefteq A_3 \trianglelefteq S_3$$

(c) Since A_5 is a simple group, the group S_5 has a composition series

$$1 \trianglelefteq A_5 \trianglelefteq S_5$$

(d) 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.

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

(a) G has a composition series, and furthermore

(b) the composition factors in the composition series are unique up to permutation of its composition factors. More precisely, 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 $G^{(1)} = 1$.

(iii) For $i \geq 1$, the i^{th} *commutator subgroup* $G^{(i)}$ of a group G is defined by

$$G^{(i)} = [G^{(i-1)}, G^{(i-1)}] \text{ with } G^{(0)} = G.$$

(iv) Let G be a group. Then for any $i \geq 0$,

(a) $G^{(i+1)} \trianglelefteq G^{(i)}$, and hence G has a chain of normal subgroups

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

and furthermore,

(b) $G^{(i)}/G^{(i+1)}$.

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

$$1 = N_0 \trianglelefteq N_2 \trianglelefteq \ldots \trianglelefteq N_{k-1} \trianglelefteq N_k = G$$

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

(vi) Examples of solvable/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.

(vii) Every 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) Let G be a finite group.

(a) (Philip Hall) G is solvable if, and only if for every divisor d of n such that $\gcd(d, n/d) = 1$, 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 of odd order, then it is solvable.

(d) (Feit-Thompson) If G is simple, then $G \cong \mathbb{Z}_p$, for some prime number p.

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

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

(xi) 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.

(xii) 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.