Group Theory Notes

1 Revision of Groups

Definition 1.1.1: Definition of a Group

A **group** consists of a set G together with a function $G \times GztoG$ which maps an ordered pair $(g, h) \in G \times G$ to an element $g \star h \in G$. The following axioms must be satisfied:

1. **Associativity**: $(g \star h) \star k = g \star (h \star k)$ for each triple $(g, h, k) \in G \times G \times G$
2. **Identity**: $\exists e \in G$ such that $e \star g = g = g \star e$ for each $g \in G$
3. **Inverse**: To each element $g \in G$, there is an element $g^{-1} \in G$ such that $g \star h = e = h \star g$

Note: The closure axiom follows from the definition of a function.

Example 1.2.A: Examples of Groups

1.2.1) S_n, the n**-th symmetric group**, is the group of permutations of $\{1, 2, \dots, n\}$, with composition of functions.

1.2.2) D_n, the n**-th dihedral group**, is the group of symmetries of the n-gon. It has $2n$ elements: n rotations, and n reflections.

1.2.3) The **free group** on the letters x, y is written as $G = \langle x, y \rangle$. The elements of G are **words** in the symbols x, y, x^{-1}, y^{-1}. The group operation $\star$ is **concatenation**: so $xxx^{-1}y \star y^{-1}x = xxx^{-1}yy^{-1}x$. e is the **empty word** with 0 letters, and x^{-1} and y^{-1} is the inverse of x and y respectively. Thus $xxx^{-1}y = xy$.

1.2.4) $(\mathbb{Z}, +)$ is a group, with $e = 0$. It is a **cyclic** group, and is **generated** by 1.

1.2.5) $\mathbb{Z}/n$, the set of integers modulo n, is a group under $+$.

Definition 1.2.6: Abelian Group

A group $(G, \star)$ is **abelian** if $g \star h = h \star g$ for all $g, h \in G$.
Note: Often, when $(G, \star)$ is ablian, we write $g + h$ as the group operation.

Definition 1.3.1: Subgroup

If H is a nonempty subset of G then H is a **subgroup** provided that:

- $hk \in H$ for all $h, k \in H$.
- $h^{-1} \in H$ for all $h \in H$.

We usually just say "H is closed under the group operations". Note that $e \in H$ follows from the definition, and associativity follows from the fact that G is a group. Any subgroup H of G is a group using the same product as that of G.
We write $H \leq G$ when H is a subgroup of G (as opposed to $H \subseteq G$ which just means H is a subset of G). The notation $H < G$ means that H is a subgroup of G and $H \neq G$. A subgroup H is **proper** if $H \neq G$ and is **non-trivial** if $H \neq \{e\}$.

Example 1.3.A: Examples of Subgroups

1.3.2) The subsets $\{e\}$ and G are always subgroups of G

1.3.3) The group of rotations of an n-gon is a subgroup of D_n

1.3.4) The n**-th alternating group**, A_n is the subgroup of S_n consisting of all permutations that can be written as the product of an even number of 2-cycles.

1.3.5) Let G be a group and $g \in G$. Then $\langle g \rangle := \{g^n : n \in \mathbb{Z}\}$ is a subgroup of G, called the **subgroup generated by** g. If $G = \langle g \rangle$ for some $g \in G$, then G is **cyclic**.

Definition 1.3.6: Coset

Let $H \leq G$ and $g \in G$. Then the **left coset** of H determined by g is the set

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

Similarly, the **right coset** of H determind by g is the set

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

The set of left cosets is denoted G/H and the sets of right cosets is denoted $H \backslash G$. The number of elements in a group G is denoted by $\#G$ or $|G|$, and is known as the **order** of G. The number of left cosets of a subgroup H of G is the **index** of H in G and denoted by $|G ::|$ or $[G : H]$, that is $[G : H] = |G/H|$

Definition 1.3.7: Normal Subgroup

A subgroup $H \leq G$ is **normal**, denoted $H \lhd G$, if $gH = Hg$ for all $g \in G$

The following are equivalent:

- $H \lhd G$
- $gHg^{-1} = H$ for all $g \in G$ (where $gHg^{-1} = \{ghg^{-1} : h \in H\}$)
- $gHg^{-1} \subseteq H$ for all $g \in G$

Theorem 1.3.8: Lagrange's Theorem

Let H be a subgroup of a finite group G. Then

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

i.e. The order of a subgroup divides the order of a group

Theorem 1.3.9: Cauchy's Theorem

If G is a finite group and p is a prime that divides the order of G, then G has a subgroup of order p.

Definition 1.3.10: Order of an Element

Let $g \in G$. The **order** of g is the least positive integer such that $g^n = e$, or ∞ if n does not exist. We write the order of g as $o(g)$. Note that $o(g) = |\langle g \rangle|$.

Corollary 1.3.11: Prime Cyclic Groups

If $|G|$ is prime, then G is cyclic.

Definition 1.4.1: Group Homomorphism

Let G, H be groups. A function $\phi : G \to H$ such that $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$ is a **group homomorphism**.

Example 1.4.2: The Cyclic Group C_n

The **cyclic group or order** n, written C_n, can be thought of the set of rotations by $2\pi/n$ of an n-gon.

Definition 1.4.3: Group Isomorphism

If G and H are groups and $\psi : G \to H$ is a bijective group homomorphism, then ψ is a **group isomorphism** and G and H are isomorphic.

If p is prime, all groups of order p are isomorphic.

Definition 1.4.5: Kernel of a Homomorphism

Let $\phi : G \to H$ be a group homomorphism. The **kernel** of ϕ is

$$\{g \in G \mid \phi(g) = e\}.$$

A gropu homomorphism ϕ is injective iff $\ker \phi = \{e\}$

Definition 1.4.6: Automorphisms

Let G be a group. The set of all isomorphisms $\phi : G \to G$ is called the **automorphism group of** G, written $\mathrm{Aut}(G)$. The group oepration is composition of functions.

Definition 1.4.8: Product Group

Let G, H be groups. The **product**, or **direct product**, $G \times H$ is a group, with group operation $\star$ given by

$$(g, h) \star (g', h') = (g \star_G g', h \star_H h')$$

Note: we usually just say $(g, h) \star (g', h') = (gg', hh')$

If $\gcd(m, n) = 1$, then $C_m \times C_n \cong C_{mn}$.

Theorem 2.1.1: Normal Subgroups and Kernels

Let G be a group and $M \leq G$. Then $N \lhd G$ iff N is the kernel of a group homomorphism from G to another group H.

This implies:

1. There is a natural way to make G/N a group
2. There is a **canonical** group homomorphism $\mathbf{can} : G \to G/N$
3. $\ker(\mathbf{can}) = N$

Theorem 2.2.1: First Isomorphism Theorem for Groups

Let $\phi : G \to H$ be a group homomorphism. Then $N := \ker(\phi)$ ia a normal subgroup of G, $\Im(\phi)$ is a subgroup of H, and there is an isomorphism

$$\overline{\theta} : G/\ker(\theta) \xrightarrow{\cong} \Im(\theta)$$

defined by $\overline{\theta}(gN) = \theta(g)$. In particular, if θ is surjective, then $G/\ker(\phi) \cong H$.

Theorem 2.2.3: Universal Property of Factor Groups

Let G be a group and $N \lhd G$. Then for any homomorphism $\psi : G \to h$ with $N \subseteq \ker(\psi)$, there is a unique homomorphism $\overline{\psi} : G/N \to H$ such that $\overline{\psi} \circ \mathbf{can} = \psi$, where $\mathbf{can} : G \to G/N$ is the canonical homomorphism.

Corollary 2.2.4:

If $\phi : G \to K$ is a surjective group homomorphism, and $\phi : G \to H$ is a group homomorphism with $\ker(\phi) \subseteq \ker(\psi)$, then there is a unique group homomorphism $\overline{\psi} : K \to H$ such that $\overline{\psi}\phi = \psi$.

Proposition 2.3.1:

Let G be a group and let $N \lhd G$ Let $\mathbf{can} : G \to G/N$ be the canonical map. Let $K \leq G/N$.

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

Proposition 2.3.2: Canonical Pullback

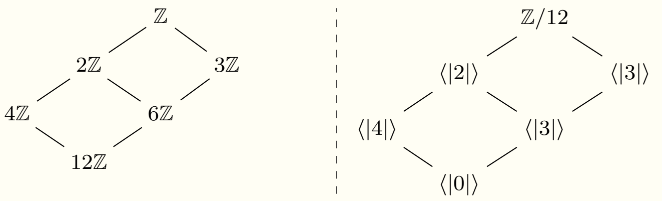
Let $N \lhd G$ and let $\mathbf{can} : G \to G/N$ be the canonical map. If $N \leq H \leq G$, then $H = \mathbf{can}^{-1}(\mathbf{can}(H))$. That is, all subgroups of G that can contain N are "pulled back" from subgroups of G/N.

Theorem 2.3.3: Correspondence Theorem

Let G be a group, $N \lhd G$, and let $\mathbf{can} : G \to GfN$ be the canonical map. The map $H \mapsto \mathbf{can}(H)$ is a bijection between subgroups of G containing N and subgroups of G/N. Under this bijection, normal subgroups match with normal subgroups. Further, if $N \subseteq A, B$ are subgroups of G, then $\mathbf{can}(A) \subseteq \mathbf{can}(B)$ iff $A \subseteq B$.

Example 2.3.4: Subgroups Example

Find all subgroups of $\mathbb{Z}/12 = \mathbb{Z}/12\mathbb{Z}$ together with their inclusions. The subgroups of $\mathbb{Z}$ that contain $12\mathbb{Z}$ are shown as:



Theorem 2.3.5: Third Isomorphism Theorem

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

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

Example 2.3.6: Example of ISO3

Consider the inclusions $10\mathbb{Z} \leq 5\mathbb{Z} \leq \mathbb{Z}$. By the Third Isomorphism Theorem,

$$(\mathbb{Z}/10\mathbb{Z})/(5\mathbb{Z}/10\mathbb{Z}) \cong \mathbb{Z}/5\mathbb{Z}$$

Thm 2.3.7: Second Isomorphism Theorem for Groups

Let N be a normal subgroup of a group G. Let H be a subgroup of G. Then

a) HN is a subgroup of G

b) $N \lhd HN$

c) $H \cap N \lhd H$

d) There is an isomorphism $HN/N \cong H(H \cap N)$

2 Group Presentations

Definition 3.1: Multiplication Table

[TODO: put one in]

Example 3.2.1: A Simple Group Presentation

Let $n \in \mathbb{Z}_{\geq 1}$. We'll define a new group A, which we write

$$A = \langle x \mid x^n = e \rangle$$

The notation means "A is the group generated by x, subject to the group axioms, the rule $x^n = e$, and all logical consequences". The elements of A are $\{x, x^2, x^3, \ldots, x^{n-1}, x^n = e\}$. i.e.e $A \cong C_n$.

Definition 3.2.2: Free Group

The **free group on generators** $x_1, x_2, \ldots, x_m$, written $\langle x_1, \ldots, x_m \rangle$, is the group whose elements are words in the symbols $x_1, \ldots, x_m, x_1^{-1}, \ldots, x_m^{-1}$ subject to the group axioms and all logical consequences. The group operation is concatenation.

Definition 3.2.3: Group Presentation

Let $r_1, \ldots, r_n \in \langle x_1, \ldots, x_m \rangle$. The group **generated** by $x_1, \ldots, x_m$ subject to the **relations** $r_1, \ldots, r_n$ is the group wiht generators $x_1, \ldots, x_m$, subject to the group axioms, the rules that $r_1 = r_2 = \cdots = r_n = e$, and all logical consequences. This group is written

$$\langle x_1, \ldots, x_m \mid r_1, \ldots, r_m \rangle$$

This notation gives a **presentation** of the group

3 E

Theorem 3.2.7: Novikov's Theorem

There is no algorithm for deciding whether or not

$$\langle x_1, \ldots, x_m \mid r_1, \ldots, r_m \rangle = \{e\}$$

Example 3.2.8: E

Let $E = \langle a, b \mid a^2, b^5, (ab)^5 \rangle$. Notice that in E, we have

$$abab = e = b^5 \implies aba = b^5 \implies ba = a^2ba = ab^4$$

Note the equation

$$ba = ab^4 \tag{1}$$

Lemma 3.2.10:

Any element $x \in E$ can be written $x = a^i b^j$, where $i \in \{0, 1\}$ and $j \in \{0, 1, 2, 3, 4\}$

Proposition 3.2.11: Universal Property of Free Groups

Let G be a group generated by a set $\{s_1, \ldots, s_n\}$. Let $F = \langle S_1, \ldots, S_n \rangle$ be the free group on the letters $\{S_1, \ldots, S_n\}$. Then there is a unique surjective homomorphism from $\pi : F \to G$ such that $\pi(S_i) = s_i$ for all i.

Example 3.2.A: Free Groups

Something something this is isomorphic to the Dihedral group.

4 Sylow Theorems

Definition 4.1.: p-subgroup

Let G be a finite group and let p be a prime. A subgroup H of G is a **p-subgroup** of G if it is a p-group, that is, it has order p^n for some n, and it is a **Sylow p-subgroup** of G if its order is the highest power of p that divides the order of G. We say that H is a **Sylow subgroup** of G if it is a Sylow p-subgroup for some prime p.

Theorem 4.1.2: Sylow I

Let $|G| = n$ and suppose that p is a prime that divides n. Write $n = p^m r$ with p not dividing r. Then there exists at least one subgroup of order p^m. That is, there is at least one Sylow p-subgroup.

Theorem 4.1.3: Sylow ii

Let $|G| = n$ and suppose that p is a prime that divides n. Write $p^m r$ with p not dividing r. Suppose that P is a Sylow p-subgroup and that $H \leq G$ is any p-subgroup of G. Then there exists $x \in G$ with $H \subseteq xPx^{-1}$. In particular, any two Sylow p-subgroups of G are conjugate in G.

Theorem 4.1.4: Sylow III

Let $|G| = n$ and suppose that p is a prime that divides n. Write $n = p^m r$ with p not dividing r. Let n_p be the number of distinct Sylow p-subgroups of G. Then $n_p \mid r$ and $n_p \equiv 1 \mod p$

Example 4.1.5: Sylow Subgroups of S_3

Consider S_3 and recall that $|S_3| = 6$ s.t. the possible nontrivial Sylow p-subgroups would be of order 2 and 3. There are three transpositions in S_3 and we get three Sylow 2-subgroups of order 2. They are all conjugate, since all transpositions in S_n are conjugate.
There is a unique subgroup of order 3, which is normal

Example 4.1.6: Sylow Subgroups of D_6

D_6 has 12 elements, so Sylow I predicts subgroups of order 3 and subgroups of order 4. Let g be a reflection and h the clockwise rotation by $\pi/3$. It's clear that h^2 generates a subgroup of order 3, and since all elements of D_6 that are not powers of h are reflections, this is the only one.
D_6 has no elements of order 4, so a Sylow 2-subgroup must be isomorphic to $C_2 \times C_2$. In D_6 we have $ah^3 = h^3 a$ for any reflection a. So $\{e, a, h^3, ah^3\}$ is a subgroup of D_6 for any reflection a. If a is a reflection, then $a = gh^i$ for some i. We see that there are 3 Sylow 2-subgroups of D_6:

$$\{e, g, h^3, gh^3\},\ \{e, gh, h^3, gh^4\},\ \{e, gh^2, h^3, gh^5\}.$$

These are all isomorphic to $C_2 \times C_2$, and are all conjugate.

Proposition 4.1.7: Normal Groups of Order 30

Any group of order 30 has a nontrivial normal subgroup.

Definition 4.1.8: Simple Subgroup

A group G is **simple** if G has no nontrivial normal subgroups: that is, the only normal subgroups are $\{e\}$ and G itself.

Motivation: If G is finite but not simple then G has a nontrivial normal subgroup N, and we can think of G being "built" from the smaller groups N and G/N. On the other hand, if G is simple it is not being built from smaller groups in any obvious way. We will see later in the term that finite groups are really built from simple groups.

Lemma 4.1.9: Sylow Subgroups and Normal Groups

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

Definition 4.2.1: Group Action

Let G be a group and X a set. An **action of** G **on** X is a function

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

satisfying the following two properties:

1. The identity acts trivially: $e \cdot x = x$ for all $x \in X$.
2. We have $g \cdot (h \cdot x) = (gh) \cdot x$ for all $g, h \in G$ and $x \in X$. (this is easiest to remember as a form of associativity.)

Note: We write our group actions as $g \cdot x$.

If $x \in X$ then the **orbit** of x is

$$G \cdot x = \{g \cdot x \mid g \in G\}$$

The **stabilizer** of x is

$$\mathrm{Stab}_G(x) = \{g \in G : g \cdot x = x\}$$

These are the elements that leave x fixed.

Lemma 4.2.2: Orbits Partitions

Let G act on X.

a) The action induces an equivalence relation $\sim$ on X defined by: $x \sim y$ iff there exists $g \in G$ with $g \cdot x = y$

b) The equivalence classes of this equivalence relation are the orbits.

c) The distinct orbits in X form a partition of X (That is, each element of x is in exactly one orbit and distinct orbits have empty intersection.)

Lemma 4.2.3: Stabilizer is a Subgroup

Let G be a group that acts on a set X. For all $x \in X$, the stabilizer $\mathrm{Stab}_G(x)$ is a subgroup of G.

Example 4.2.4: Examples of Actions

4.2.4) Let k be a field and let n be a positive integer. Let $G = GL_n(k)$ and $X = k^n$. Then G acts on X via

$$A \cdot v = Av$$

that is, by matrix multiplication

- Let n be a positive integer. Let $G = S_n$, the n-th symmetric group, and let $X = \{1, \ldots, n\}$. Then G acts on X via:

$$\sigma \cdot i = \sigma(i)$$

Theorem 4.2.6: Orbit-Stabilizer Theorem

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

$$|G| = |\mathrm{Stab}_G(x)||G \cdot x|$$

Example 4.2.A: Conjugacy Class

We will look at G ating on itself by **conjugation**

$$g \cdot a = gag^{-1}$$

Lets check this is a group action: $e \cdot a = eae^{-1} = a$, and

$$g \cdot (h \cdot a) = g \cdot (hah^{-1}) = g(hah^{-1}g^{-1}) = gha(gh)^{-1} = (gh) \cdot a$$

So conjugacy is a group action. Orbits and stabilizers of elements of G under the conjugacy action: If $a \in G$, then

$$\mathrm{Stab}_G(a) = \{g \in G \mid gag^{-1} = a\}$$

Since we can rewrite $gag^{-1} = a$ as $ga = ag$, $\mathrm{Stab}_G(a)$ is precisely the **centralizer** $C_G(a)$ (the elements of G that commute with a). The orbit of a is

$$G \cdot a = \{gag^{-1} \mid g \in G\}$$

This is the set of elements that are conjugate to a, or more concisely the **conjugacy class of** a. We will write the conjugacy class of a as $\mathrm{Cl}(a)$. Now we can apply Orbit-Stabilizer.

Lemma 4.2.7: Conjugacy Class Divides

Let G be a finite group. For any $a \in G$, we have

$$|G| = |C_G(a)||\mathrm{Cl}(a)| \tag{2}$$

Thus, $|C_G(a)|$ and $|\mathrm{Cl}(a)|$ divide $|G|$.

This can also be written with the index of $C_G(a)$ in G:

$$|Cl(a)| = [G : C_G(a)]$$

Definition 4.2.B: Class Equation

Since conjugacy classes are obits of a group action, we obtain from Lemma 4.2.2, they partition G. This gives us the **class equation**: If G is a finite group, then there are elements $a_1, \dots, a_n \in G$ s.t.

$$G = \mathrm{Cl}(a_1) \sqcup \mathrm{Cl}(a_2) \sqcup \cdots \sqcup \mathrm{Cl}(a_n)$$

It is more usual to write

$$|G| = |\mathrm{Cl}(a_1)| + |\mathrm{Cl}(a_2)| + \cdots + |\mathrm{Cl}(a_n)| \tag{3}$$

Note that this means that the class equation gives a writing $|G|$ as the sum of integers dividing $|G|$.

Definition 4.2.11: p-group

Let p be a prime. A **p-group** is a group G such that each element has an order a power of p. If $|G|$ is finite, then G is a p-group iff $|G|$ is a power of p, by Cauchy's Theorem.

Theorem 4.2.12: Nontrivial Centres of p-groups

Let G be a nontrivial finite p-group. Then the centre $Z(G) \neq |e|$

4.3 Proofs of Sylow Theorems

lol

Lemma 4.3.1: Fixed Points of a p-group

Let p be a prime and let G be a finite p-group acting ona finite set X. Then the number of fixed points in X is congruent to $|X|$ mod p

Corollary 4.3.2:

Let $|G| = p^m r$, with p not dividing r. Let P be a Sylow p-subgroup the number of conjugates of P. By definition, P is normal iff it has a unique conjugate.

Definition 4.3.3: Normalizer

Let G be a group and $H \leq G$. The **normalizer** of H is

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

Lemma 4.3.4: Conjugates Something

Let G be a finite group.

a) For any subgroup $H \leq G$, we have

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

b) Let $p \mid |G|$ and P be a Sylow p-subgroup of G. Then $n_p = [G : N_G(P)]$

Example 4.3.A: Sylows and Normalizers for S_4

Very long working

5 Finitely Generated Abelian Groups

Example 5.1.1: Isomorphisms for Groups of Order 100

Suppose A is an abelian group with $|A| = 100$. Then, since $100 = 2^2 \cdot 5^2$, there will be a (unique) Sylow 2-subgroup P, say, of order 4, and a unique Sylow 5-subgroup Q, say, of order 25. Any element in $P \cap Q$ has order dividing 4 and also dividing 25; so $P \cap Q = \{e\}$. Now, PQ is a subgroup of A that contains P, and so has order divisible by 4, and contains Q and so has order divisible by 25. Hence PQ has order at least 100 and so $PQ = A$. By Chapter 2, Ex10, $A \cong P \times Q$. Thus, the possibilities for A are:

$$\begin{gathered} C_4 \times C_{25}, \quad C_2 \times C_2 \times C_{25}, \\ C_4 \times C_5 \times C_5, \quad C_2 \times C_2 \times C_5 \times C_5 \end{gathered} \tag{5.1.2}$$

Theorem 5.1.3: Isomorphisms for Finite Groups

Suppose that A is a finite abelian group of order n, and that $n = p_1^{s_1} p_2^{s_2} \cdots p_t^{s_t}$. Let A_{p_i} be the unique Sylow p_i-subgroup of A. Then

$$A \cong A_{p_1} \times A_{p_2} \times \cdots \times A_{p_i}$$

That is, A is isomorphic to the direct product of its Sylow subgroups.

Theorem 5.1.4: Cyclic Subgroups of Abelian Groups

Let A be an abelian group with $|A| = p^n$ for some prime p. Then A is isomorphic to the direct product of cyclic subgroups of orders $p^{c_1}, p^{c_2}, \dots, p^{c_s}$, where $e_1 \geq e_2 \geq \cdots \geq e_s \geq 1$ and $e_1 + e_2 + \cdots + e_s = n$. This product is unique up to reordering the factors.

Corollary 5.1.5: FT 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 reordering the factors.

Theorem 5.1.6: Chinese Remainder Theorem

Let m, n be nonzero coprime integers, then $C_{mn} \cong C_m \times C_n$.

Example 5.1.7: Cyclic 100 via the CRT

Using the Chinese Remainder Theorem 5.0.6, we have:
$C_4 \times C_{25} \cong C_{100}$; $C_2 \times C_2 \times C_{25} \cong C_2 \times C_{50}$;
$C_4 \times C_5 \times C_5 \cong C_5 \times C_{20}$; $C_2 \times C_2 \times C_5 \times C_5 \cong C_{10} \times C_{10}$.
Therefore, an alternative list is:

$$C_{100}, \quad C_2 \times C_{50}, \quad C_5 \times C_{20}, \quad C_{10} \times C_{10}$$

Corollary 5.1.8: FT of Finite Abelian Groups II

Any finite abelian group of order n can be written as a direct product of cyclic groups

$$C_{n_1} \times C_{n_2} \times \cdots \times C_{n_s},$$

where n_i divides n_{i+1} for each $i = 1, 2, \dots, s-1$ and $n_1 n_2 \cdots n_s = n$. This product is unique up to reordering the factors.

Definition 5.1.9: Exponent of a Finite Group

The **exponent**, $e(G)$, of a finite group is the least common muliple of the orders of the elements of G. Note that $e(G) \leq |G|$ for any finite group G, by Lagrange.

Example 5.1.10: Example of an Exponent

The symmetric group S_3 has elements of order 1, 2, and 3; so $e(S_3) = 6$. However, note that S_3 has no element of order 6.

Lemma 5.1.11: Order of Exponent in FA Groups

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

Corollary 5.1.12: Cyclic Finite Abelian Groups

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

Theorem 5.1.13: Cyclicity of Field Group

Let A be a finite subgroup of the multiplicative group $K^* := K \backslash \{0\}$ of a field K. Then A is a cyclic group.

Corollary 5.1.14: The multiplicative group of nonzero elements of a finite field is cyclic.

Definition 5.2.1: Modules of a Ring

Let R be a ring. An **R-module** is an abelian group $(M, +)$ together with a mapping

$$R \times M \to M, \quad (r, a) \mapsto ra$$

that is **distributive**, **associative**, and **unital** ($1a = a \ \forall a \in M$).

Example 5.2.2: $\mathbb{Z}$-module

A $\mathbb{Z}$-module is the same as an abelian group: if $(M, +)$ is an abelian group, $n \in \mathbb{Z}$, and $a \in M$ define

$$na = \begin{cases} \underbrace{a + a + \cdots + a}_{n \text{ times}} & n > 0 \\ 0 & n = 0 \\ -(-n)a & n < 0 \end{cases}$$

Example 5.2.3: Modules and Vector Spaces

If K is a field then a K-module is the same as a K-vector space.

Definition 5.2.4: Free Module

Let R be a ring, and let $n \in \mathbb{N}$. The **free R-module of rank n** is the n-fold catesian product R^n. It is given a module structure by

$$r(a_1, a_2, \ldots, a_k) = (ra_1, ra_2, \ldots, ra_k)$$

Thm 5.2.5: FT of Finitely Generated Abelian Groups

Let A be a finitely generated abelian group. Then

$$A \cong \mathbb{Z}/r_1\mathbb{Z} \times \mathbb{Z}/r_2\mathbb{Z} \times \cdots \times \mathbb{Z}/r_k\mathbb{Z} \times \mathbb{Z}^\ell$$

for some $k, \ell \in \mathbb{N}$ and $r_1, \ldots, r_k$ nonzero elements of $\mathbb{Z}$ with $r_1 \mid r_2 \mid \cdots \mid r_k$.

Lemma 5.2.6: Basis of $\mathbb{Z}$-modules

Let α be a $\mathbb{Z}$-module automorphism of $\mathbb{Z}^s$. Then $\mathbb{Z}^s/K \cong \mathbb{Z}^s/\alpha(K)$.

Proposition 5.2.7:

Suppose that M is the $r \times s$ matrix corresponding to $K = \sum_{i=1}^r \mathbb{Z}x_i \subseteq \mathbb{Z}^s$. If we change $M \rightsquigarrow M'$ via invertible row and column operations then M' corresponds to a submodule K' of $\mathbb{Z}^s$ so that $\mathbb{Z}^s/K \cong \mathbb{Z}^s/K'$.

Useful Fact 5.3.1: Parity of Sequences

If $x_1, x_2, x_3, \ldots$ are a sequence of integers with $x_i \mid x_{i-1}$ for all i, then there is n such that $x_i = \pm x_{i+1}$ for all $i \geq n$

Proposition 5.3.2:

Let p be prime and let $a_1 \geq a_2 \geq \cdots \geq a_m$ and $b_1 \geq b_2 \geq \cdots \geq b_n$ be positive integers. If

$$A = C_{p^{a_1}} \times \cdots \times C_{p^{a_m}} \cong B = C_{p^{b_1}} \times \cdots \times C_{p^{b_n}}.$$

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

6 Alternating Groups

Recall 6.1.A: Permutations

Recall the **symmetric group** S_n is the group of permutations (or bijections) of n objects. We usually think of the n objects as being the set $\{1, 2, \ldots, n\}$. A permutation can be written as a $2 \times n$ array

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

For example, the following permutation denotes the permutation that sends $1 \mapsto 2$, $2 \mapsto 4$, $3 \mapsto 1$, and $4 \mapsto 3$.

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

Remember that $\sigma\tau$ means $\sigma \circ \tau$; that is, first apply τ and then apply σ to the result.

We usually write permutations using cycle notation. For example, the cycle (214) denotes the permutation that sends $2 \mapsto 1$, $1 \mapsto 4$ and $4 \mapsto 2$, with the convention that all other elements are fixed. Note that cycle notation does not give unique representations, e.g. $(214) = (142) = (421)$. In this notatino, the first permutation above would be written (1243). A cycle is a k-cycle if it has k entries; so (214) is a 3-cycle, while (35) is a 2-cycle.

Two cycles are **disjoint** if no integer appears in both cycles. For example $(214)(35)$ is a product of two disjoint cycles, and is the permutation

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

Note that two disjoint cycles commute; e.g. $(214)(35) = (35)(214)$. However, the product of cycles that are not disjoint is not usually commutative; e.g. $(214)(45) \neq (45)(214)$, as the first product sendsd 5 to 2 while the second product sends 5 to 4.

Lemma 6.1.1: Unique Representation of Permutations

Every permutation can be written as a product of disjoint cycles, and the product is unique up to re-ordering the factors.

e.g.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 6 & 2 & 5 & 3 \end{pmatrix}$$

is written as $(142)(36)(5)$ in cycle, but could also be written $(36)(5)(142)$. Also 1-cycles are usually omitted, and it is taken that any number not appearing is fixed by the permutation; so for example, we would usually write the above permutation as $(142)(36)$.

A 2-cycle is often called a **transposition**, and a 2-cycle of the form $(i\, i+1)$ is an **adjacent transposition**.

Lemma 6.1.2: Transposition Form of Permutations

Every permutation can be written as a product of transpositions. Thus, S_n is generated by transpositions. In fact, S_n is generated by adjacent transpositions. Think bubble sort.

Definition 6.1.3: Cycle Type of a Permutation

Suppose that $\sigma = c_1 c_2 \cdots c_k$ is a product of k disjoint cycles of length $l_1, l_2, \ldots, l_k$ with $l_1 \geq l_2 \geq \cdots \geq k_k$. Then the k-tuple $(l_1, l_2, \ldots, l_k)$ is called the **cycle type** of σ.

Example 6.1.5: Conjugate of Permutations

Let $c = (125)$ and $g = (23)(145)$ in S_5. A representation of g is shown to the right

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

The conjugate gcg^{-1} is

$$(23)(145)(125)(154)(23) = (143)(2)(5) = (431) = (g(1)g(2)g(5))$$

Lemma 6.1.7: Conjugacy Formula

Let $\sigma = (a_1\, a_2\, \cdots\, a_k) \in S_n$, and $\tau \in S_n$. Then

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

Theorem 6.1.8: Conjugacy Equals Cycle Type

Two permutations in S_n are conjugate iff they have the same cycle type.

Recall 6.2.A: Actions on Two Elements

We consider an action of S_n on a set of two elements. Let $x_1, \ldots, x_n$ be indeterminates, and set

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

Now, set $X = \{P, -P\}$. Then S_n acts on X by permuting the variables. For example, when $n = 3$ then $P = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$ and (13) sends P to $(x_3 - x_2)(x_1 - x_3)(x_2 - x_3) = -P$

Definition 6.2.1: Odd and Even Permutations

If $\sigma \in S_n$ fixes P then σ is an **even permutation**, while if $\sigma \cdot P = -P$ then σ is an **odd permutation**. The set of even permutations is denoted by A_n and is called the **alternating group**.

Lemma 6.2.2: Products of Odd and Even Permutations

The product of two even permutations is even. The product of two odd permutations is even. The product of an odd and an even permutation (in either order) is odd. A cycle of length n is even if n is odd and is odd if n is even.

Theorem 6.2.3: Even Permutations are a Subgroup

Let $n \geq 2$. Then the set of even permutations A_n is a normal subgroup of S_n of index 2; so that $|A_n| = |S_n|/2 = n!/2$ for $n \geq 2$.

Proposition 6.2.4: Properties of A_4

The alternating group A_4 has order 12. It has a unique subgroup N of order 4. The subgroup N is normal in S_4 (and so certainly $N \triangleleft A_4$) and $A_4/N \cong C_3$, while $S_4/N \cong S_3$.

Lemma 6.2.5: Closure Union

Let G be a finite group and suppose that $H \triangleleft G$. Then there are $h_1, \ldots, h_k \in H$ so that $H = \bigsqcup \mathrm{Cl}_G(h_i)$.

Theorem 6.3.A: Simple Alternating Groups

Theorem 6.3.1: The alternating group A_5 is simple.
Theorem 6.3.3: Let $n \geq 5$. Then A_n is simple.
Lemma 6.3.4: If $n \geq 5$ and σ, σ' are 3-cycles in A_n, then σ and σ' are conjugate in A_n: that is, there exists $\tau \in A_n$ with $\tau\sigma\tau^{-1} = \sigma'$
Lemma 6.3.5: If $n \geq 3$, then A_n is generated by 3-cycles.
Lemma 6.3.6: If $H \leq S_n$ and H has the property that any $\sigma \in H$ with $\sigma \neq ()$ is fixed-point-free, then $|H| \leq n$.
Lemma 6.3.7: If $n \geq 6$ and $\sigma \in A_n$ with $\sigma \neq ()$, then $|\mathrm{Cl}_{A_n}(\sigma)| \geq n$.

7 Jordan Hölder Theorem

Example 7.1.1: Composition Series

Consider the chains of normal subgroups

$$\{0\} \lhd 4\mathbb{Z}/12\mathbb{Z} \lhd 2\mathbb{Z}/12\mathbb{Z} \lhd \mathbb{Z}/12\mathbb{Z}$$
$$\{0\} \lhd 6\mathbb{Z}/12\mathbb{Z} \lhd 3\mathbb{Z}/12\mathbb{Z} \lhd \mathbb{Z}/12\mathbb{Z}$$

These are both examples of **composition series**

Definition 7.1.2: Composition Series

Let G be a group. A **composition series** for G is a chain of subgroups

$$\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_{s-1} \lhd G_s = G \qquad (*)$$

where $G_i \neq G_{i+1}$ and G_{i+1}/G_i is simple for all i.
If $(*)$ is a composition series for G, we say that s is the **length** of the composition series and the simple groups G_{i+1}/G_i are the **composition factors**.

Theorem 7.1.3: Jordan Hölder Theorem

Let G be a finite group. Then G has a composition series. Moreover, any two composition series have the same composition length, and they have the same composition factors up to isomorphism of groups and order of the factors.

Theorem 7.1.4: Classification of Finite Simple Groups

Let G be a finite simple group. Then G is isomorphic to one of:

- **Family 1**: C_p for p prime
- **Family 2**: A_n for $n \geq 5$
- 16 other infinite families
- 26 sporadic groups. These include the **Monster** and **Baby Monster**.

Proposition 7.2.1: Finite Composition Series

If G is a finite group, then G has a composition series.

Lemma 7.2.2:

Let

$$\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_{s-1} \lhd G_s = G$$

be a composition series for N, and

$$N = H_0 \lhd H_1 \lhd \cdots \lhd H_r = G/N$$

be a composition series for G/N. Then there is a composition series for G of length $s + r$, whose composition factors are, in order,

$$G_1, G_2/G_1, \ldots, G_s/G_{s-1}, H_1, H_2/H_1, \ldots, H_r/H_{r-1}$$

Theorem 7.3.1: Composition Factors of Series

Let G be a finite group. Then any two composition series have the same length and the same composition factors up to isomorphism and the order in which they are listed. More precisely, if

$$\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_{s-1} \lhd G_s = G \qquad (\dagger)$$

and

$$\{e\} = H_0 \lhd H_1 \lhd \cdots \lhd H_{r-1} \lhd H_r = G \qquad (\ddagger)$$

are two composition series for G, then $s = r$ and there is a permutation σ of $\{0, \ldots, s-1\}$ such that $H_{i+1}/H_i \cong G_{\sigma(i)+1}$, for all $i = 0, \ldots, s-1$.

Definition 8.1.1: Subnormal Series

Let G be a group. A **subnormal series** for G is a series of subgroups

$$\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_s = G$$

Warning: normality is not transitive. That is, there exists C with subgroups $A \lhd B \lhd C$ where A is not a normal subgroup of C.

Definition 8.1.2: Solvable Group

A group G is **solvable** (or **soluble**) provided that it has a subnormal series

$$\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_s = G$$

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

Example 8.1.3: Examples of Solvable Groups

a) The group S_3 is not abelian, but is solvable, as the subnormal series $\{e\} \lhd A_3 \lhd S_3$ demonstrates.

b) The group S_4 is solvable.

c) The group A_5 is not solvable: as it is a simple group, its only subnormal series is $\{e\} \lhd A_5$ and the only factor is A_5 which is not abelian.

d) Any finite p-group is solvable. Let $|G| = p^k$, where p is prime. G has a subnormal series $\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_k = G$, where $|G_i| = p^i$. Since each G_i/G_{i-1} has order p, it is abelian.

Theorem 8.1.4: Solvable Cyclic Groups

A finite group G is solvable iff all the composition factors of G are cyclic.

Lemma 8.1.5: Composition Factors for FA Groups

If A is a finite abelian group of order $p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$, then the composition factors of A are

$$\underbrace{C_{p_1}, \ldots, C_{p_1}}_{n_1}, \underbrace{C_{p_2}, \ldots, C_{p_2}}_{n_2}, \cdots, \underbrace{C_{p_k}, \ldots, C_{p_k}}_{n_k}$$

in some order.

Theorem 8.1.A: Solvable Properties

Theorem 8.1.6: Let G be a group and let $N \lhd G$. Then G is solvable iff both N and G/N are solvable.
Theorem 8.1.7: If G is solvable and $H \leq G$ then H is solvable.
Theorem 8.1.9: A general degree n polynomial $f(x)$ with rational coefficients is not solvable by radicals if $n \geq 5$, that is, there is no quintic formula.

Definition 8.2.1: Commutators and Derived Subgroups

Let G be a group. The **commutator** of two elements $a, b \in G$ is the element $aba^{-1}b^{-1}$, and is often denoted by $[a, b]$. The **derived subgroup** (or **commutator subgroup**) G' of a group G is the subgroup generated by all possible commutators in G; that is,

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

Remark: Some properties of the commutator subgroup:

a) $[a, b]^{-1} = [ba]$ and the conjugate of $[a, b]$ by z is $[zaz^{-1}, zbz^{-1}]$. Thus, inverses and conjugates of commutators are commutators

b) Every element in G' is a product of commutators

c) $G' \lhd G$

d) **Warning**: The product of two commutators is not necessarily a commutator

Theorem 8.2.2: Commutators and Abelian Groups

Let G be a group and N a normal subgroup of G. Then G/N is abelian iff $G' \subseteq N$. In particular, G/G' is abelian.

Definition 8.2.3: Derived Series

Let G be a group. Set $G^0 = 0$ and for each $i \geq$, set $G^{(i+1)} := (G^{(i)})'$. The sequence

$$G = G^{(0)} \triangleright G^{(1)} \triangleright G^{(2)} \triangleright \cdots$$

is called the **derived series** of G. (Note that $G^{(1)} = G'$)

Remark: Some properties of derived series:

a) If there is an i such that $G^{(i+1)} = G^{(i)}$ then $G^{(j)} = G^{(i)}$ for all $j \leq i$.

b) If G is a finite group, then there must be an i such that $G^{(i+1)} = G^{(i)}$. However, this may happen without it being the case that $G^{(i)} = \{e\}$

c) Let $G = A_5$. Then $G^{(1)} \triangleleft G$ and so $G^{(1)} = \{e\}$ or $G^{(1)} = G$, as G is simple. However, $G/G^{(1)}$ is abelian, and so $G^{(1)} = \{e\}$ is impossible, as $G = A_5$ is not abelian. Thus, $G^{(1)} = G$ and so $G^{(i)} = G$ for all $i \geq 1$. (this argument works for any non-abelian simple group)

d) If $G^{(n)} = \{e\}$ for some n then the series

$$G = G^{(0)} \triangleright G^{(1)} \triangleright G^{(2)} \triangleright \cdots \triangleright G^n = \{e\}$$

has abelian factors $G^{(i)}/G^{(i+1)}$, since $G^{(i)}/G^{(i+1)} = G^{(i)}/(G^{(i)})'$. Thus, G is solvable.

Theorem 8.2.4: Solvability with Derived Groups

A group G is solvable iff there is an n with $G^{(n)} = \{e\}$.

Definition 8.2.5: Derived Length

Let G be a solvable group. Then $G^{(n)} = \{e\}$ for some n. The least such n is the **derived length** of G.