Abstract

These notes follow MATH 6111—Abstract Algebra 1 in the Fall 2023 semester at The Ohio State University, and largely follow lectures by Professor Stefan Patrikis (MWF) and recitation sessions (TR) by Dr. Ariel Weiss. These notes cover group theory, group actions, composition series of groups, ring theory, unique factorization domains and principal ideal domains, polynomial and Noetherian rings, modules over rings, and linear and multilinear algebra.

Contents

1 Groups

1.1 Groups, Monoids, and Semigroups

Definition 1.1.1. A **group** is a set G equipped with a function $m : G \times G \to G$ satisfying

(i) (associativity) For all $x, y, z \in G$, $m(m(x, y), z) = m(x, m(y, z))$,

(ii) (identity) There exists $e \in G$ such that for all $x \in G$, $m(x, e) = m(e, x) = x$.

(iii) (inverses) For all $x \in G$, there exists $y \in G$ such that $m(x, y) = m(y, x) = e$.

Less formally, we may write $*$ for the operation, so that $x * y = m(x, y)$. For even shorter hand and much more common, we write $x \cdot y$, or even simply as xy (no symbol at all). In some contexts we will use addition signs, and this is usually when G is **abelian**, that is, when m is a symmetric function. We will write x^{-1} for the element y provided in item (iii), and often 1 for the e in item (ii). In abelian contexts, we tend to write the element y in item (ii) as 0 and the e in item (ii) as 0.

Example 1.1.2. We will provide a list of examples of groups, and write them as $(G, *)$, where G is the underlying set and $*$ denotes the group operation.

(i) $(\mathbb{Z}, +)$, that is, $m(x, y) = x + y$.

(ii) $(\mathbb{Q}, +)$.

(iii) $(\mathbb{R} \smallsetminus \{0\}, \cdot)$.

Examples (i)-(iii) are abelian groups.

(iv) Fix an integer $n \geqslant 1$ and define the **symmetric group on n elements** as

$$S_n = \{\text{bijections } f \colon \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}\},$$

where the group operation is composition of functions, that is, $m(f, g) = f \circ g$ for $f, g \in S_n$. Informally, S_n is called the **group of permutations of $1, \ldots, n$**. This group is non-abelian for $n \geqslant 3$. //

Definition 1.1.3. A **monoid** is a set M with an operation $*$ satisfying (i) and (ii) in the definition of a group (**??**).

Definition 1.1.4. A **semigroup** is a set S with operation $*$ satisfying (i) in the definition of a group (**??**), that is, $x * (y * z) = (x * y) * z$.

Example 1.1.5. (1) $(\mathbb{Z}_{\geqslant 0}, +)$ is a monoid, not a group.

(2) $(\mathbb{Z}_{\geqslant 2}, +)$ is a semigroup, not a monoid.

(3) For any set S, let $\mathcal{P}(S) = \{\text{subsets } A \subset S\}$, and for all $A, B \in \mathcal{P}(S)$, let $A * B \coloneqq A \cup B$. The identity is $\varnothing \subset S$. When $S \neq \varnothing$, we do not have inverses for all $A \in \mathcal{P}(S)$ (for example, not for $A = S$). So, when $S \neq \varnothing$, $(\mathcal{P}(S), \cup)$ is a monoid, but not a group.

(4) Denote by $M_n(\mathbb{R})$ the set of $n \times n$ matrices with entries in $\mathbb{R}$. Then $(M_n(\mathbb{R}), +)$ is a group with identity element the zero matrix.

(5) $(M_n(\mathbb{R}), \cdot)$ is a monoid, with identity the identity matrix.

(6) $\mathrm{GL}_n(\mathbb{R})$, the collection of invertible matrices with matrix multiplication as its group operation is a group. Note that we can replace $\mathbb{R}$ with any field or indeed with any ring. //

Lemma 1.1.6. (1) In any monoid $(M, *)$, the identity is unique.

(2) In any group $(G, *)$, inverses are unique.

Proof. (1) If $e, e' \in M$ are identities, then

$$e = e * e' = e',$$

where the first equality uses e is an identity, and the second uses that e' is an identity.

(2) Suppose y and z are inverses of some $x \in G$. Then

$$y = y * e = y * (x * z) = (y * x) * z = e * z = z.$$ □

1.2 Subgroups

Henceforth, if an arbitrary group G is introduced, then the group operation will usually be left implicit, and the identity will be denoted 1 in general.

Definition 1.2.1. Let G be a group. A **subgroup** of G is a subset $H \subset G$ such that

(i) For all $x, y \in H$, $xy \in H$.

(ii) $1 \in H$.

(iii) For all $x \in H$, $x^{-1} \in H$.

We typically write $H < G$ to indicate H is a subgroup of G.

Example 1.2.2. Let S be the square in the plane with vertices $\{(1, \pm 1), (-1, \pm 1)\}$, and define

$$G = \{f \colon \mathbb{R}^2 \to \mathbb{R}^2 \mid |p - q| = |f(p) - f(q)| \text{ for all } p, q \in \mathbb{R}^2 \text{ and } f(S) = S\}.$$

Then G is a group under composition. The only non-obvious thing that must be checked to justify this is that G contains inverses. Homework 1 addresses this. A sample element of G is the element $\rho \in G$ that is a rotation through $\pi/2$. Then $\rho^4 = 1$, $\rho^{-1} = \rho^3$, and the subset $\{1, \rho, \rho^2, \rho^3\}$ is a subgroup of G. But it is not all of G, since G also contains reflections: let τ be reflection in the x-axis. Then $\{1, \tau\}$ is a subgroup of G.

Question: Suppose $L < G$ is a subgroup containing ρ and τ. What can we say about L? Obviously L contains $1, \rho, \rho^2, \rho^3, \tau, \tau\rho, \tau\rho^2, \tau\rho^3, \tau\rho\tau, \tau\rho\tau\rho^2\tau\rho^3, \ldots$, but there may be repeats. How do we only

write one representation, preferably the simplest one, for elements of L? To demonstrate, let us analyze $\tau\rho\tau$:

Observe: An element $f \in G$ is determined by its effect on the vertices. (Check!). We have $\tau\rho\tau$ acts as

$$v_1 \mapsto v_4$$
$$v_2 \mapsto v_1$$
$$v_3 \mapsto v_2$$
$$v_4 \mapsto v_3$$

Hence $\tau\rho\tau = \rho^3 = \rho^{-1}$. This implies

$$L = \{1, \rho, \rho^2, \rho^3, \tau, \tau\rho, \tau\rho^2, \tau\rho^3\}.$$

, Notice that L must in fact be G because G has at most 8 elements. Indeed, any $f \in G$ is determined by $f(v_1)$, of which there are 4 possibilities, and its neighbor must be $f(v_2)$, of which there are two possibilities, since this must be connected to $f(v_1)$ via an edge. Then $f(v_3)$ is uniquely determined since it is the unique vertex other than $f(v_2)$ adjacent to $f(v_1)$, and $f(v_4)$ is uniquely determined by being the only remaining vertex.

Conclusion: $L = G$ is a non-abelian group with 8 elements. It is called the **dihedral group of order 8**, and we will denote this group by D_8. (Note however that some people call this D_4, which is just a different convention.) //

1.3 Group Homomorphisms

Definition 1.3.1. Let $(G, *)$ and $(G', *')$ be groups. A **group homomorphism** from $(G, *)$ to $(G', *')$ is a map $\varphi\colon G \to G'$ such that for all $x, y \in G$, $\varphi(x * y) = \varphi(x) *' \varphi(y)$.

Lemma 1.3.2. Let $\varphi\colon G \to G'$ be a group homomorphism. Then

(1) $\varphi(1_G) = 1_{G'}$, where 1_G is the identity of G and $1_{G'}$ is the identity of G';

(2) For all $x \in G$, $\varphi(x^{-1}) = \varphi(x)^{-1}$.

Proof. (1) $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1)$. Multiplying both sides by $\varphi(1)^{-1}$ (on the left, say), we obtain $1 = \varphi(1)$. (2) $1 = \varphi(1) = \varphi(x \cdot x^{-1}) = \varphi(x) \cdot \varphi(x^{-1})$. Multiply both sides on the left by $\varphi(x)^{-1}$ to get $\varphi(x)^{-1} = \varphi(x^{-1})$. □

Remark 1.3.3. We can define a **monoid homomorphism** in the same way as a group homomorphism. However, only part (1) of **??** is now false, and part (2) makes no sense. For example, let S be a nonempty set and consider the monoid $(\mathcal{P}(S), \cup)$. Then the map $\varphi\colon \mathcal{P}(S) \to \mathcal{P}(S)$ given by $\varphi(A) = S$ for all $A \in \mathcal{P}(S)$ is a monoid homomorphism, since

$$\varphi(A \cup B) = S = \varphi(A) \cup \varphi(B),$$

but $\varphi(\varnothing) = S \neq \varnothing$, which shows (1) of **??** fails.

Example 1.3.4. (1) Define $\varphi\colon (\mathbb{R}, +) \to (\mathbb{R}, \cdot)$ by $\varphi(x) = e^x$. Then

$$\varphi(x + y) = e^{x+y} = e^x \cdot e^y = \varphi(x) \cdot \varphi(y).$$

Likewise, $\log\colon (\mathbb{R}_{\geqslant 0}, \cdot) \to (\mathbb{R}, +)$ is also a group homomorphism.

(2) $(\mathbb{Z}, +) \to (\mathbb{Q}, +)$,

(3) $(\mathbb{Z}, +) \xrightarrow{\varphi} (\mathbb{Z}/n\mathbb{Z}, +)$ given by $\varphi(a) = a \pmod n$. By $\mathbb{Z}/n\mathbb{Z}$ we mean the integers modulo n for some $n \in \mathbb{Z}$, which we will elaborate on soon.

(4) $\det\colon \mathrm{GL}_n(K) \to K^\times$, where $K^\times \coloneqq (K \smallsetminus \{0\}, \cdot)$ and K is any field.

(5) Recall $D_8 = \{1, \rho, \rho^2, \rho^3, \tau, \tau\rho, \tau\rho^2, \tau\rho^3\}$ as a set. Then consider the map $\varepsilon\colon D_8 \to (\{\pm 1\}, \cdot)$ given by $\varepsilon(\rho^j) = 1$ for all j, and $\varepsilon(\tau \cdot \rho^j) = -1$ for all j. This is a homomorphism, and showing this is left as an exercise. We can relate examples (4) and (5) as follows. The elements of D_8 are invertible linear transformations of $\mathbb{R}^2$, and hence forms a subgroup of $\mathrm{GL}_2(\mathbb{R})$. Then we have the following diagram.

$$\begin{array}{ccccccc} D_8 & < & \mathrm{GL}_2(\mathbb{R}) & \xrightarrow{\det} & \mathbb{R}^\times & \subset & \{\pm 1\} \\ \text{rotations} & & \longmapsto & & +1 & & \\ \text{reflections} & & \longmapsto & & -1 & & \end{array} \qquad //$$

Every group homomorphism $\varphi\colon G \to G'$ gives a subgroup $\ker\varphi < G$ and $\mathrm{im}(\varphi) < G'$.

Definition 1.3.5. The **kernel** $\ker\varphi$ of φ is $\{x \in G \mid \varphi(x) = 1\}$. The **image** $\mathrm{im}\,\varphi$ is $\{y \in G' \mid$ there exists $x \in G$ such that $\varphi(x) = y\}$.

Lemma 1.3.6. If $\varphi\colon G \to G'$ is any group homomorphism, then $\ker\varphi < G$ and $\mathrm{im}\,\varphi < G'$.

Proof. For all $x, y \in \ker\varphi$, we have $\varphi(xy) = \varphi(x) \cdot \varphi(y) = 1 \cdot 1 = 1$, so $xy \in \ker\varphi$. $\varphi(1) = 1$ by **??**, so $1 \in \ker\varphi$. For $x \in \ker\varphi$, $\varphi(x^{-1}) = \varphi(x)^{-1} = 1^{-1} = 1$, so $x^{-1} \in \ker\varphi$. Thus $\ker\varphi < G$.

The proof that $\mathrm{im}\,\varphi < G'$ is similar, and is left as an exercise. □

Example 1.3.7. The kernel of the map $\varepsilon\colon D_8 \to \{\pm 1\}$ given in **??** is $\ker\varepsilon = \{1, \rho, \rho^2, \rho^3\}$, which by **??** is a subgroup of D_8. //

1.4 Group Isomorphisms

A group isomorphism encapsulates the notion of two groups having the "same" group structure.

Definition 1.4.1. Let G, G' be groups. Set

$$\mathrm{Hom}(G, G') \coloneqq \{\text{group homomorphisms } G \to G'\}.$$

We say $\varphi \in \mathrm{Hom}(G, G')$ is an **isomorphism** if there exists $\psi \in \mathrm{Hom}(G', G)$ such that

$$\varphi \circ \psi = \mathrm{id}_{G'} \qquad \text{and} \qquad \psi \circ \varphi = \mathrm{id}_G,$$

where the maps on the right-hand side of these equations are the identity maps for G and G', respectively sending elements to themselves. We call G and G' **isomorphic** if there exists an isomorphism between them.

Example 1.4.2. Consider the map

$$\begin{aligned} \varphi\colon \{1, \rho, \rho^2, \rho^3\}(< D_8) &\longrightarrow \{\pm 1, \pm i\}(< \mathbb{C}^\times), \\ \rho^n &\longmapsto \varphi(\rho^n) = i^n. \end{aligned}$$

Then φ is an isomorphism with inverse $\psi(i^n) = \rho^n$. //

Lemma 1.4.3. A group homomorphism $\varphi\colon G \to G'$ is

(1) injective if and only if $\ker\varphi = \{1\}$, and

(2) an isomorphism if and only if φ is a bijection of the underlying sets of G and G'.

Proof. (1) Suppose φ is injective. For all $x \in \ker\varphi$, $\varphi(x) = 1 = \varphi(1)$, so since φ is injective we know $x = 1$. Conversely, suppose $\ker\varphi = \{1\}$, and let $x, y \in G$ be such that $\varphi(x) = \varphi(y)$. Multiply by $\varphi(y)^{-1} = \varphi(y^{-1})$ on the right to get

$$\varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1}) = \varphi(x)\varphi(y)^{-1} = \varphi(y)\varphi(y)^{-1} = 1$$

Thus $xy^{-1} \in \ker\varphi = \{1\}$, so $x = y$. Hence φ is injective.

(2) We need to check that a set-theoretic inverse $\psi\colon G' \to G$ of $\varphi\colon G \to G'$ is automatically a group homomorphism. Observe that

$$\psi(\varphi(x)\cdot\varphi(y)) = \psi(\varphi(xy)) = \mathrm{id}_{G'}(xy) = xy = \psi(\varphi(x))\cdot\psi(\varphi(y)),$$

and we win since any $a, b \in G'$ have the form $a = \varphi(x), b = \varphi(y)$ for some $x, y \in G$ (since φ is onto). □

Warning 1.4.4. ?? is just a nice feature of the structure of groups. This does not hold in all generality, however. Indeed, in topological spaces, there exist continuous bijections that are not homeomorphisms.

1.5 Automorphisms

An automorphism of a group G is a group isomorphism $G \to G$.

Definition 1.5.1. Define the **automorphism group** of G as

$$\mathrm{Aut}(G) \coloneqq \{\text{isomorphisms } G \xrightarrow{\cong} G\}.$$

We call elements of $\mathrm{Aut}(G)$ **automorphisms** of G.

Lemma 1.5.2. $\mathrm{Aut}(G)$ is a group under composition.

Proof. The identity of $\mathrm{Aut}(G)$ is the identity map $\mathrm{id}_G\colon G \to G$. Inverses of automorphisms exist by **??**. Lastly, composition of functions is associative. □

Warning 1.5.3. $\mathrm{End}(G) \coloneqq \mathrm{Hom}(G, G)$ under composition is a monoid, but *not* a group.

1.6 Automorphism Group of Cyclic Groups

Definition 1.6.1. For any group G and any element $g \in G$, define

$$\langle g\rangle = \{g^n \mid n \in \mathbb{Z}\},$$

where

$$g^n = \begin{cases} \overbrace{g\cdots g}^{n \text{ copies of } g} & \text{if } n > 0, \\ \overbrace{g^{-1}\cdots g^{-1}}^{n \text{ copies of } g^{-1}} & \text{if } n < 0, \\ 1 & \text{if } n = 0. \end{cases}$$

Then $|\langle g\rangle|$ is called the **order** of g in G. A group such that $G = \langle g\rangle$ for some $g \in G$ is called a **cyclic group**. If G is cyclic, the element $g \in G$ such that $G = \langle g\rangle$ is called a **generator** of G. The cyclic group G generated by an element g of order $n \in \mathbb{Z}$ is called the **cyclic group of order n**, and is denoted C_n.

Example 1.6.2. Let G be a cyclic group with generator g. Then g^i is a generator of G if and only if $\gcd(i, n) = 1$. //

Proof. Let g be a generator for the cyclic group G. For the forward direction we prove the contrapositive, that is, suppose $\gcd(i, n) > 1$. Then the elements $1, g^i, g^{2i}, \ldots, g^{(n-1)i}$ are distinct elements of G (Why?). But

$$g^{(n/d)i} = (g^n)^{i/d} = 1^{i/d} = 1,$$

so we are done. (Why?)

Now the converse. By Bézout's identity, there exist $a, b \in \mathbb{Z}$ such that $1 = ai + bn$. Then

$$g = g^{ai+bn} = g^{ai}(g^n b) = g^{ai}.$$

This completes the proof. (Why?) □

Remark 1.6.3. There are no cyclic groups G of uncountable order, since otherwise $G = \{g^n \mid n \in \mathbb{Z}\}$ is an uncountable list. But $\mathbb{Z}$ is countable, so the number of distinct elements is at most countable.

We summarize our above discussion with teh following statement.

Corollary 1.6.4. If G is an arbitrary cyclic group, then

$$\mathrm{Aut}(G) \cong \begin{cases} (\mathbb{Z}/n\mathbb{Z})^\times & \text{if } |G| = n < \infty, \\ \{\pm 1\} & \text{if } |G| = \infty. \end{cases}$$

2 Normal Subgroups and Quotient Groups

2.1 Normal Subgroups

For any group homomorphism $\varphi\colon G \to G'$, $\ker\varphi < G$ is a subgroup satisfying the following definition:

Definition 2.1.1. For any group G and subgroup $H < G$, we say H is a **normal subgroup** of G if for all $g \in G$ and for all $h \in H$, $ghg^{-1} \in H$. We write this as $H \lhd G$.

Example 2.1.2. (1) We have $\ker\varphi \lhd G$ because for all $h \in \ker\varphi$ and for all $g \in G$,

$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1} = \varphi(g) \cdot 1 \cdot \varphi(g^{-1}) = 1. \qquad //$$

(2) Recall the dihedral group of order 8, D_8, with its generators ρ and τ. The subgroup $\langle\tau\rangle$ is *not* a normal subgroup of D_8, because

$$\rho\tau\rho^{-1} = \tau(\tau\rho\tau)\rho^{-1} = \tau\rho^{-2} \notin \langle\tau\rangle.$$

On the other hand, $\{1, \rho, \rho^2, \rho^3\} < D_8$ is a normal subgroup of D_8.

2.2 Quotient Groups

We will now example a "converse" to the fact that the kernel of a group homomorphism is a normal subgroup.

Definition 2.2.1. If G is a group and $H < G$, a **left coset** of H in G is a subset of G of the form

$$aH = \{ah \mid h \in H\} \subset G$$

for some $a \in G$. A **right coset** of H in G is a subset

$$Ha = \{ha \mid h \in H\} \subset G$$

for some $a \in G$.

Example 2.2.2. If $a \in H$, then $aH = Ha = H$. //

Lemma 2.2.3. The left (resp. right) cosets of a group partition the group. More precisely, if $H < G$, $a, b \in G$, and $aH \cap bH \neq \varnothing$ (resp. $Ha \cap Hb \neq \varnothing$), then $aH = bH$ (resp. $Ha = Hb$).

Proof. If there exist $x, y \in H$ such that $ax = by$, then

$$a = b \underbrace{yx^{-1}}_{\in H \text{ since } H<G}.$$

Thus $aH \subset bH$; likewise $bH \subset aH$, so $aH = bH$. The case of right cosets is similar. □

Remark 2.2.4. If $H < G$, then $H \lhd G$ if and only if $\forall g \in G$, $gH \subset Hg$ (equivalently, $gH = Hg$, or $gH \supset Hg$ or $gHg^{-1} \subset H$). This can be justified as follows: If $H \lhd G$, then $\forall g \in G$, $gHg^{-1} \subset H$, so $gH \subset Hg$. If $\forall g \in G$, $gH \subset Hg$, then $gHg^{-1} \subset H$. Apply this to g^{-1} instead of g to get $g^{-1}Hg \subset H$, that is, $Hg \subset gH$. Hence $Hg = gH$. The other statements can be checked similarly.

Proposition 2.2.5. Suppose $N, H < G$, $N \lhd G$ and $N < H$. Then $N \lhd H$.

Proof. Consider an arbitrary element $h \in H$. Then $h \in G$, so $hNh^{-1} = N$ by normality of N in G. But h was an arbitrary element of H, so $N \lhd H$. □

Remark 2.2.6. Suppose $N \lhd H \lhd G$, that is, $N \lhd H$ and $H \lhd G$. Does then $N \lhd G$? Unfortunately, the answer is *not in general*. Indeed, in D_8 we have

$$\underbrace{\langle \tau \rangle}_{\coloneqq N} \lhd \underbrace{\langle \tau, \rho^2 \rangle}_{\coloneqq H} \lhd \underbrace{D_8}_{\coloneqq G}.$$

Then by Lagrange's theorem, $[G : H] = [H : N] = 2$, so $N \lhd H$ and $H \lhd G$ by **??**. But $\langle \tau \rangle$ is not normal in D_8 as we have already shown in **??**, so this is a counterexample to our question.

Definition 2.2.7. For any $H < G$, define sets

$$G/H = \{\text{left cosets of } H \text{ in } G\},$$
$$H\backslash G = \{\text{right cosets of } H \text{ in } G\}.$$

So, **??** can be interpreted as the following corollary.

Corollary 2.2.8. If G is a group and $H < G$, then

$$G = \coprod_{aH \in G/H} aH.$$

Goal: We aim to show that when $H \lhd G$, there is a group structure on G/H.

Theorem 2.2.9 (Construction of the Quotient Group)**.** Suppose $H \lhd G$. Then with the operation

$$aH \cdot bH \coloneqq (ab)H,$$

$(G/H, \cdot)$ is a group, called the **quotient group** of G by H, with identity $1 \cdot H = H$, and with inverses $(aH)^{-1} = a^{-1}H$.

Moreover, the canonical quotient map $\pi \colon G \to G/H$ given by $\pi(a) = aH$ is a (surjective) group homomorphism with kernel $\ker \pi = H$.

Proof. Since $H \lhd G$, the set

$$aHbH = \{ah_1bh_2 \mid h_1, h_2 \in H\} \subset G$$

is equal to the set

$$a(Hb)H = a(bH)H = abH \cdot H = (ab)H,$$

so $aH \cdot bH$ can instead be expressed as $aHbH$, so evidently this group operation is well-defined.

Once we know the group operation is well-defined, the properties of associativity, that $(1 \cdot H)$ is the identity, and that inverses are $(aH)^{-1} = a^{-1}H$, are inherited from the corresponding properties of $(G, \cdot)$.

$\pi \colon G \to G/H$ is a group homomorphism: $\forall a, b \in G$, by definition of π we have $\pi(ab) = abH =: (aH) \cdot (bH) = \pi(a) \cdot \pi(b)$. Its kernel is $\ker \pi = \{a \in G \mid aH = H\}$, and $aH = H$ if and only if $a \in H$. Hence $\ker \pi = H$. □

Example 2.2.10. Again consider D_8 with its generators ρ and τ. **??** gives us another way to show the subgroup $\langle \tau \rangle$ is not normal. Indeed,

$$\text{right cosets: } \langle \tau \rangle \backslash D_8 = \{\langle \rho, \tau \rangle, \langle \rho, \tau\rho \rangle, \langle \rho^2, \tau\rho^2 \rangle, \langle \rho^3, \tau\rho^3 \rangle\},$$
$$\text{left cosets: } D_8 / \langle \tau \rangle = \{\langle \rho, \tau \rangle, \langle \rho, \tau\rho^3 \rangle, \langle \rho^2, \tau\rho^2 \rangle, \langle \rho^3, \tau\rho \rangle\}.$$

But notice that $(\rho H)(\rho H) = \rho^2 H$ and $(\rho\tau H)(\rho\tau H) = (\rho\tau)^2 H = H \neq (\rho H)(\rho H)$, contrary to $\rho, \rho\tau$ being elements of the same coset of $\langle \tau \rangle$. Thus $\langle \tau \rangle$ is not a normal subgroup of D_8. //

2.3 An Example: Integers Modulo n

The classical example of a quotient groups is the group of integers modulo n, where n is a fixed integer. Using **??**, we will construct this group. First note that $(\mathbb{Z}, +)$ is an abelian group, so any of its subgroups are normal. What are the subgroups of $(\mathbb{Z}, +)$?

Lemma 2.3.1. Every subgroup $H < (\mathbb{Z}, +)$ has the form $H = N \cdot \mathbb{Z} = \{Nx \mid x \in \mathbb{Z}\}$ (*not* the coset $N + \mathbb{Z} = \mathbb{Z}$) for some $N \in \mathbb{Z}$. Moreover, each subgroup corresponds to a unique positive integer N.

Proof. If $H = \{0\}$ then take $N = 0$, which affirms the claim. Now suppose $H \neq \{0\}$. Then H must have a positive element, since $h \in H \iff -h \in H$. Then by well-ordering of $\mathbb{Z}$, there is some smallest positive element of H. Call that element N. We claim $H = N\mathbb{Z}$. Indeed, suppose not, so there exists $a \in H$ such that $a \neq N\mathbb{Z}$. We can assume a is positive, since otherwise we can take $-a \in H$. Then by division with remainder (a consequence of well-ordering), there exists $q \in \mathbb{Z}$ and $0 \leqslant r < N$ such that $a = Nq + r$. Since $a \notin N\mathbb{Z}$, we must have $r > 0$, which implies $0 < r = a - Nq < N$. Hence r is a positive integer that is smaller than N. But H is closed under addition since H is a subgroup, so

$$r = \underbrace{a}_{\in H} - \underbrace{Nq}_{\in H} \implies r \in H,$$

so r is a positive integer in H that is strictly less than N, which by assumption is the least positive integer in H, which is absurd. Thus $H = N\mathbb{Z}$. □

Definition 2.3.2. Let N be an integer. The **integers modulo n** is the group $(\mathbb{Z}/N\mathbb{Z}, +)$ in **??**, together with the canonical homomorphism $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/N\mathbb{Z}$ giving it its group operation, also denoted $+$.

2.4 Applications of Quotient Groups: Counting and Lagrange's Theorem

We already saw that for all $H < G$,

$$G = \coprod_{aH \in G/H} aH.$$

This has an immediate counting consequence, since all of these cosets have the same size.

Corollary 2.4.1 (Lagrange's theorem)**.** Suppose $H < G$ and G is a finite group. Then

$$|G| = |H| \cdot |G/H|.$$

In particular, $|H|$ divides $|G|$.

Proof. For all $a \in G$, the map $H \mapsto aH$ given by $a \mapsto aH$ is a bijection, so $|H| = |aH|$. Thus

$$|G| = \sum_{aH \in G/H} |aH| = \sum_{G/H} |H| \cdot |G/H|. \qquad \square$$

Definition 2.4.2. The quantity $|G/H|$ is called the **index** of H in G, often written $[G : H]$. When $[G : H] < \infty$, we say H has **finite index**.

Example 2.4.3. $[\mathbb{Z} : 13\mathbb{Z}] = 13 < \infty$, so $13\mathbb{Z}$ is a subgroup of $(\mathbb{Z}, +)$ of finite index. //

We can now formulate and prove the following surprisingly useful result:

Proposition 2.4.4. If $H < G$ and $[G : H] = 2$, then $H \lhd G$.

Proof. By **??**, the elements of G/H partition the group. Thus we can write

$$G = \coprod_{aH \in G/H} aH = H \amalg aH, \tag{2.4.4.1}$$

where $aH \in G\backslash H$. But **??** also applies to the elements of $H\backslash G$, so

$$G = \coprod_{Ha \in H\backslash G} Ha = H \amalg Ha. \tag{2.4.4.2}$$

Combining **????**, we obtain

$$H \amalg aH = G = H \amalg Ha.$$

Thus $aH = Ha$. Since a was an arbitrary element of $G\backslash H$, we conclude $H \lhd G$. $\square$

By applying Lagrange's theorem to the cyclic subgroups of G generated by the element $g \in G$, we can say the following about the order of any element of a group:

Corollary 2.4.5. If g is an element of a finite group G, then the order of g divides $|G|$.

2.5 Normalizers and Centralizers

Definition 2.5.1. Let G be a group, $H < G$. Then the **normalizer** of H in G, denoted $N_G(H)$, is the collection of elements $g \in G$ such that the left coset and right coset of H by g agree. In other words,

$$N_G(H) = \{g \in G \mid gH = Hg\}.$$

The **centralizer** of H in G, denoted $C_G(H)$, is the collection of elements $g \in G$ that commute with all elements of H. In other words,

$$C_G(H) = \{g \in G \mid gh = hg \text{ for all } h \in H\}.$$

Example 2.5.2. Let G be a group.

- $C_G(G) = Z(G)$.
- $N_G(G) = G$.
- If $H < G$, then $C_G(H) \subset N_G(H)$.
- If $H = \langle g \rangle$ for some $g \in G$, then $C_G(H) = N_G(H)$.
- $G = D_8$. $H = \langle \tau \rangle$. Then by looking at our computations in **??** and finding left cosets that are equal to their corresponding right coset, we find $N_G(H) = \{1, \tau, \rho^2, \tau\rho^2\}$. //

Exercise 2.5.3. Let $G = \mathrm{GL}_n(\mathbb{R})$. Then the subgroup H is the subgroup of matrices of the form

$$\begin{pmatrix} 1 & * & & & * \\ & 1 & * & & * \\ & & & & \\ & & & & * \\ & & & & 1 \end{pmatrix},$$

show that $N_G(H)$ is the set of upper triangular matrices, that is, matrices of the form

$$\begin{pmatrix} * & * & & & * \\ & * & * & & * \\ & & & & \\ & & & & * \\ & & & & * \end{pmatrix}.$$

Proposition 2.5.4. The normalizer of H in G is the largest subgroup of G having H as a normal subgroup in the sense that if $H \lhd K < G$, then $K \subset N_G(H)$.

Proof. We first need to show $H \lhd N_G(H)$. $H \subset N_G(H)$ because $hHh^{-1} = H$ for all $h \in H$. Since $H < G$ and $H \subset N_G(H) < G$, we must have $H < G$. Lastly, $N_G(H)$ is precisely the set of elements $g \in G$ such that $gHg^{-1} = H$, so $H \lhd N_G(H)$.

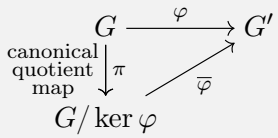
Now suppose $H \lhd K < G$. We claim $K \subset N_G(H)$. Indeed, since $H \lhd K$, we have $kHk^{-1} = H$ for all $k \in K$. But by definition of being elements of $N_G(H)$, this means $k \in N_G(H)$ for all $k \in K$, that is, that $K \subset N_G(H)$. This completes the proof. □

2.6 The Isomorphism Theorems

We now give results about quotient groups. Many call these results the *isomorphism theorems*.

Theorem 2.6.1 (First Isomorphism Theorem)**.** Let $\varphi\colon G \to G'$ be a group homomorphism. Then

- there exists a unique group homomorphism $\overline{\varphi}\colon G/\ker\varphi \to G'$ such that the diagram



  commutes, that is, $\varphi = \overline{\varphi} \circ \pi$, and

- $\overline{\varphi}$ induces an isomorphism $\overline{\varphi}\colon G/\ker\varphi \xrightarrow{\cong} \operatorname{im}\varphi$.

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ {\scriptstyle \text{canonical quotient map}}\downarrow{\scriptstyle \pi} & & \uparrow \\ G/\ker\varphi & \xrightarrow[\cong]{\overline{\varphi}} & \operatorname{im}\varphi \end{array}$$

Proof. Set $H = \ker\varphi$. Define $\overline{\varphi}(gH) = \varphi(g)$.

(i) $\overline{\varphi}$ is well-defined: if $g_1H = g_2H$ for $g_1, g_2 \in G$, then, $g_2 = g_1 \cdot h$ for some $h \in H$, so
$$\overline{\varphi}(g_2H) = \varphi(g_2) = \varphi(g_1h) = \varphi(g_1)\cdot\varphi(h) = \varphi(g_1)\cdot 1 = \varphi(g_1) = \overline{\varphi}(g_1H).$$

(ii) $\overline{\varphi}$ is a homomorphism: $\overline{\varphi}(g_1H\cdot g_2H) = \overline{\varphi}(g_1g_2H) \coloneqq \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \overline{\varphi}(g_1H)\overline{\varphi}(g_2H)$.

(iii) $\ker\overline{\varphi} = \{gH \in G/H \mid \varphi(g) = 1\} = 1\cdot H = H$, so $\overline{\varphi}$ is injective. $\operatorname{im}\overline{\varphi} = \operatorname{im}\varphi$, so $\overline{\varphi}$ gives a bijective group homomorphism, and is hence a group isomorphism $G/\ker\varphi \xrightarrow{\cong} \operatorname{im}\varphi$.

(iv) φ is unique subject to $\varphi = \overline{\varphi}\circ\pi$ for all $g \in G$, this relation forces $\varphi(g) = \overline{\varphi}(\pi(g)) = \overline{\varphi}(gH)$. □

Example 2.6.2. Consider the map $\varepsilon\colon D_8 \to \{\pm 1\}$, where rotations $\rho^j \mapsto +1$ and reflections $\tau\rho^j \mapsto -1$. Then ε has kernel $\{\rho^j\} = \langle\rho\rangle$, so ε induces an isomorphism
$$D_8/\langle\rho\rangle \xrightarrow{\cong} \{\pm 1\} = \operatorname{im}\varepsilon. \qquad //$$

Theorem 2.6.3 (Correspondence Theorem)**.** Let G be a group and $K \lhd G$. There is a bijection
$$\left\{\begin{smallmatrix}\text{subgroups of } G \\ \text{containing } K\end{smallmatrix}\right\} \longleftrightarrow \left\{\begin{smallmatrix}\text{subgroups of} \\ G/H\end{smallmatrix}\right\}.$$
$$H \xmapsto{\Phi} H/K \coloneqq \pi(H), \qquad (*)$$
$$\pi^{-1}(\overline{H}) \xmapsto{\Psi} \overline{H},$$
where $\pi\colon G \to G/K$ is the canonical projection map $g \mapsto gK$. Moreover, under this bijection, $H \lhd G$ if and only if $H/K \lhd G/K$.

Proof.

- For $K < H < G$, $K \lhd H$ since $K \lhd G$, so H/K is a group, clearly a subgroup of G/K. If moreover $H \lhd G$, then $H/K \lhd G/H$ because for all $gK \in G/H, hK \in H/K$, we have
$$(gK)(hK)(gK)^{-1} = (gK)(hK)(g^{-1}K) = (ghg^{-1})K \in H/K,$$
since $ghg^{-1} \in H$. So, there really is a map from the left-hand side to the right-hand side of $(*)$, and it really maps normal subgroups to normal subgroups.

- Conversely, given $\overline{H} < G/K$, $\pi^{-1}(\overline{H})$ is indeed a subgroup of G (Check $\pi^{-1}(\overline{H})$ is closed under group multiplication, contains 1, and contains inverses. For multiplication, if $a, b \in \pi^{-1}(\overline{H})$, then $aK, bK \in \overline{H}$, so $aK\cdot bK = abK \in \overline{H}$. But $\overline{H} < G/K$, so $a\cdot b \in \pi^{-1}(\overline{H})$. The other two checks are left as exercises.) And also $\pi^{-1}(\overline{H})$ contains K.

- If moreover $\overline{H} \lhd G/K$, then $\pi^{-1}(\overline{H}) \lhd G$: indeed, for all $g \in G$, $h \in \pi^{-1}(\overline{H})$, we need to show $ghg^{-1} \in \pi^{-1}(\overline{H})$, that is, $ghg^{-1}K = gKhK(gK)^{-1} \in \overline{H}$, which it does since $\overline{H} \lhd G/K$. The remaining part of the proof of (i) is to show that our map is a bijection. That is, that $\Phi\circ\Psi = \mathrm{id}$ and $\Psi\circ\Phi = \mathrm{id}$. For $\Phi\circ\Psi = \mathrm{id}$: Let $\overline{H} < G/K$. Then $\Phi\circ\Psi(\overline{H}) = \Phi(\pi^{-1}(\overline{H}) = \pi^{-1}(\overline{H}/K) = \{gK \mid gK \in \overline{H}\} = \overline{H})$, so $\Phi\circ\Psi = \mathrm{id}$. On the other hand, for $\Psi\circ\Phi$, let $K < H < G$. Then $\Psi\circ\Phi(H) = \Psi(H/K) = \pi^{-1}(H/K) = \{g \in G \mid gK \in H/K\} = H$, where checking the last equality is an exercise. This completes the proof. □

Theorem 2.6.4 (Second Isomorphism Theorem)**.** Let G be a group and $K, H \lhd G$, and $K \subset H$. Then the surjective group homomorphism $G/K \to G/H$ sending $gK \mapsto gH$ induces, by the first isomorphism theorem, an isomorphism

$$\frac{G/K}{H/K} \xrightarrow{\cong} G/H.$$

Proof. Define $\varphi\colon G/K \to G/H$ by $\varphi(gK) = gH$. φ is well-defined: if $g_1K = g_2K$, then $g_2 = g_1k$ for some $k \in K$. So $\varphi(g_2k) = g_2H = g_1kH$. But $k \in H$, so $kH = H$, which means $\varphi(g_2k) = g_1H = \varphi(g_1K)$, so φ is well-defined. And φ is a homomorphism by definition of the group operation of the quotient groups G/K and G/H. Then $\ker\varphi = \{gK \in G/K \mid gH = H\} = H/K$. That φ is surjective, so by the first isomorphism theorem we know φ induces an isomorphism

$$\frac{G/K}{H/K} \xrightarrow[\overline{\varphi}]{\cong} G/H.$$

□

Theorem 2.6.5 (Third Isomomorphism Theorem)**.** Let G be a group, let $K \lhd G$ and $H < G$. Then

(i) $H \cap K \lhd H$, $HK = \{hk \mid h \in H, k \in K\}$ is a subgroup, and $HK = KH = \{kh \mid k \in K, h \in H\}$.

(iii) The group homomorphisms

$$H \hookrightarrow HK \twoheadrightarrow HK/K$$
$$h \longmapsto h \cdot 1 \longmapsto hK$$

by the first isomorphism theorem, induces an isomorphism

$$\frac{H}{H \cap K} \xrightarrow{\cong} \frac{HK}{K}.$$

Proof. (i) If $h \in H$, $k \in H \cap K$, then $hkh^{-1} \in K (\lhd G)$ and $mkhkh^{-1} \in H (< G)$, as desired.

(ii) We first show $HK = KH$. For $h \in H, k \in K$,

$$hk = \underbrace{(hkh^{-1})}_{\in K}\underbrace{h}_{\in H} \in KH,$$

so $HK \subset KH$ and likewise $KH \subset HK$, so $KH = HK$. To show HK is a subgroup, we have $1 = 1 \cdot 1 \in HK$. If $hk \in HK$, then $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$. If $h_1, h_2 \in H$, $k_1, k_2 \in K$, then

$$h_1k_1 \cdot h_2k_2 = \underbrace{h_1h_2}_{\in H} \cdot \underbrace{h_2^{-1}k_1h_2k_2}_{\in K} \in HK.$$

□

Let G be a group, $H \lhd G$. So, if $g, g' \in G$ differ by an element of H in the sense that there exists $h \in H$ such that $g' = gh$, then $g = g'$ in G/H (or, more precisely, $[g] = [g'] \in G/H$).

Another way of thinking about quotient groups: By the first isomorphism theorem, there exists a bijection

$$\left\{\begin{smallmatrix}\text{normal}\\ \text{subgroups}\\ N \lhd G\end{smallmatrix}\right\} \longleftrightarrow \left\{\begin{smallmatrix}\text{group}\\ \text{homomorphisms}\\ G \to G'\end{smallmatrix}\right\}.$$
$$N \longmapsto (G \xrightarrow{\pi} G/N),$$
$$\ker\theta \longleftarrow\!\shortmid (G \xrightarrow{\theta} G'),$$

where π is the canonical quotient map. Similarly, there is a bijection

$$\left\{\begin{smallmatrix}\text{quotients}\\ \text{of } G\end{smallmatrix}\right\} \longleftrightarrow \left\{\begin{smallmatrix}\text{images of}\\ G \xrightarrow{\theta} G'\end{smallmatrix}\right\},$$

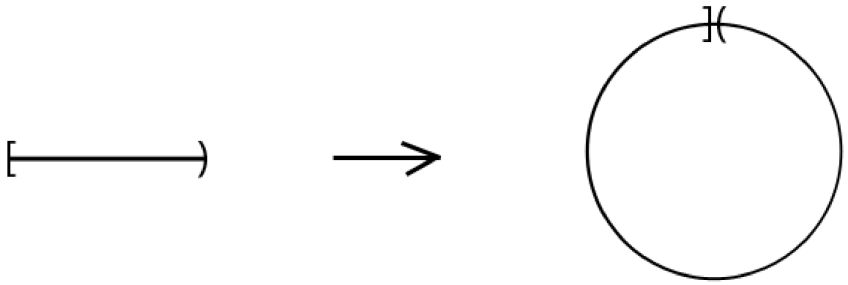
that is, $G/\ker\theta \cong \operatorname{im}\theta$.

So, we can think about quotient groups as images of group homomorphisms.

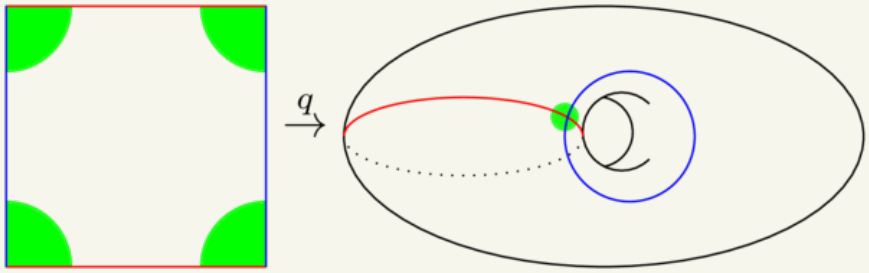
2.7 Examples of Quotient Groups

Exercise 2.7.1. $G = (\mathbb{R}^\times, \times)$, $H = \{\pm 1\}$. What is G/H? We have $|-|\colon \mathbb{R}^\times \to \mathbb{R}_{>0}$. This map is surjective with kernel $\{\pm 1\}$. So $\mathbb{R}^\times/\{\pm 1\} \cong \mathbb{R}_{>0}$.

Example 2.7.2. $G = \mathbb{R}$, $H = \mathbb{Z}$. What is G/H? By our rule of thumb, G/H is the real numbers but where we only care about what is after the decimal point, that is, a circle. To make this precise, consider the group homomorphism $\mathbb{R} \to \mathbb{C}^\times$, $x \mapsto e^{2\pi i x}$. This is a group homomorphism because $x + y \mapsto e^{2\pi i(x+y)} = e^{2\pi i x} e^{2\pi i y}$. Its kernel is $\mathbb{Z}$, and its image is $\{z \in \mathbb{C}^\times \mid |z| = 1\}$. //

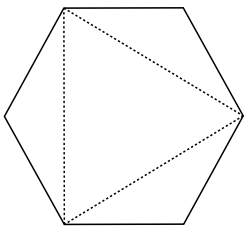


Exercise 2.7.3. $G = \mathbb{R} \times \mathbb{R}$, $H = \mathbb{Z} \times \mathbb{Z}$. What is G/H? Again by the rule of thumb, it is the torus. Prove this with an argument similar to that of the previous example.



Example 2.7.4. $\mathbb{Z} < \mathbb{Q} < \mathbb{R}$, so by the second isomorphism theorem, $\mathbb{Q}/\mathbb{Z} < \mathbb{R}/\mathbb{Z}$. Then $x \in \mathbb{R}$ has finite order in $\mathbb{R}/\mathbb{Z}$ if and only if there exist n, m such that $nx = m$ if and only if $x \in \mathbb{Q}$ (Why?). //

Example 2.7.5. Let $G = D_{12}$ and $H = D_6$. Then by one of our rules of thumb, think of D_{12}/D_6 as D_{12} but with two elements of D_{12} being the same if they differ by an element of D_6. Equivalently, D_{12}/D_8 consists of the symmetries of the hexagon, but where two elements g, g' are the same if $g^{-1}g'$ fixes the triangle.



Example 2.7.6. Let $G = \mathrm{GL}_n(\mathbb{R})$, $H = \mathrm{SL}_n(\mathbb{R})$. Is $H \lhd G$? Well, H is the kernel of determinant $\det\colon G \to \mathbb{R}^\times$, so not only is H a subgroup of G, but it is normal in G. //

Example 2.7.7. Show that the group G of upper triangular matrices has the group H of matrices of the form

$$\begin{pmatrix} 1 & * & & & * \\ & 1 & * & & * \\ & & & & \\ & & & & * \\ & & & & 1 \end{pmatrix}_{\ddots}$$

as a normal subgroup. We want to do this in a manner similar to the previous example above. Observe that

$$\begin{pmatrix} a & * \\ & b \end{pmatrix}\begin{pmatrix} c & * \\ & d \end{pmatrix} = \begin{pmatrix} ac & * \\ 0 & bd \end{pmatrix}.$$

This hints that we should consider the map $G \to (\mathbb{R}^\times)^n$ given by

$$\begin{pmatrix} a_{11} & * & & & * \\ & a_{22} & * & & * \\ & & & & \\ & & & & * \\ & & & & a_{nn} \end{pmatrix}_{\ddots} \longmapsto (a_{11}, a_{22}, \ldots, a_{nn})$$

Its kernel is H, so $H \lhd G$. //

Example 2.7.8. Let G be a group, $H < G$, and $K \lhd G$. By the third isomorphism theorem,

$$\frac{H}{H \cap K} \cong \frac{HK}{K}.$$

As an example, let us apply the third isomorphism theorem to the groups $G = \mathbb{Z}$, $H = a\mathbb{Z}$, and $K = b\mathbb{Z}$. First we need to compute $H \cap K$ and HK. Firstly, $H \cap K = \mathrm{lcm}(a,b)\mathbb{Z}$. As for HK, note that $n \in HK$ if and only if $(ax) + (by) = n$. But by Bézout's identity, this is true if and only if $\gcd(a,b) \mid n$. Hence

$$\frac{a\mathbb{Z}}{\mathrm{lcm}(a,b)\mathbb{Z}} \cong \frac{\gcd(a,b)\mathbb{Z}}{b\mathbb{Z}}.$$

Then applying Lagrange's theorem, this proves that

$$|ab| = \gcd(a,b)\,\mathrm{lcm}(a,b). \qquad //$$

Example 2.7.9. Let m, n be relatively prime integers, $G = \mathbb{Z} \times \mathbb{Z}$, and $H = \{(am, an) \mid a \in \mathbb{Z}\}$, where $\gcd(m,n) = 1$. What is

$$\frac{\mathbb{Z} \times \mathbb{Z}}{\{(am, an) \mid a \in \mathbb{Z}\}}?$$

The group G is a product of countable sets and the bottom map is as well but offset from the numerator, so our intuition should say the quotient may be $\mathbb{Z}$. Our goal now is to show this. We want a surjective group homomorphism $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ with kernel $\{(am, an) \mid a \in \mathbb{Z}\}$. Let us try the map

$$(x, y) \mapsto nx - my,$$

Is it surjective? Yes, by Bézout's identity, since $\gcd(m,n) = 1$. Its kernel is H. (Check!) //

2.8 Homework 1

Exercise 2.8.1. Show that every group of order at most 5 is abelian. Show that for all $n \geqslant 3$ the symmetric group S_n is non-abelian.

Solution. Suppose G is a finite non-abelian group. Then there exist non-identity $a, b \in G$ such that $ab \neq ba$. Notice that $ab \neq 1$ (resp. $ba \neq 1$), since otherwise $a = b^{-1}$ (resp. $b = a^{-1}$), which forces $ba = a^{-1}a = 1 = ab$ (resp. $ab = b^{-1}b = 1 = ba$), contradicting our assumption $ab \neq ba$. Notice $ab = a$ (resp. $ab = b$) implies $b = 1$ (resp. $a = 1$), so $ab \notin \{1, a, b\}$. Similarly, $ba = a$ (resp. $ba = b$) implies $b = 1$ (resp. $a = 1$). It follows that $1, a, b, ab, ba$ are five distinct elements of G. Hence any group of order 4 or less is abelian.

Now suppose G is a non-abelian group of order 5. Then, as argued in the previous paragraph, the underlying set of G is $G = \{1, a, b, ab, ba\}$. $a^2 \neq a$, since otherwise $a = 1$. Also notice $a^2 \neq ab$ (resp. $a^2 \neq ba$), since otherwise left (resp. right) multiplication by a^{-1} yields $a = b$, a contradiction. This forces $a^2 = 1$. Next notice that $aba \neq 1$, since otherwise we can write

$$[a, b] = aba^{-1}b^{-1} = ab(ab)b^{-1} = aba = 1,$$

contrary to a and b not commuting. But $aba \neq a$ (resp. $aba \neq b$) since otherwise $ab = 1$ (resp. otherwise $ab = ba^{-1} = ba$, where the third equality is because $a^2 = 1$). Similarly, $aba \neq ab$ (resp. $aba \neq ba$) since otherwise $a = 1$ (resp. $b = 1$). This forces $aba = 1$, contradicting our observation $aba \neq 1$. It follows that all groups of order 5 are abelian.

Now let n be an integer such that $n \geqslant 3$. Let $\tau \in S_n$ be the transposition (12) and let $\sigma \in S_n$ the cycle $(123) \in S_n$. (The pair τ, σ exist in S_n since $n \geqslant 3$.) Then τ and σ do not commute, since

$$\tau\sigma = \sigma\tau \iff \tau\sigma\tau^{-1} = \sigma \iff \tau(123)\tau^{-1} = (\tau(1)\tau(2)\tau(3)) = (213) \neq \sigma = (312).$$

Hence S_n is a non-abelian group for all $n \geqslant 3$. □

Exercise 2.8.2. Consider the subset

$$Q_8 = \{\pm\mathbf{1}, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\} \subset \mathrm{GL}_2(\mathbb{C}),$$

where

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},\ \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ \text{and } \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

(a) Verify that Q_8 is a subgroup of $\mathrm{GL}_2(\mathbb{C})$ (for the usual operation of matrix multiplication).

(b) Prove that Q_8 is not isomorphic to D_8.

Solution. We will abuse notation and write $\pm\mathbf{1}$, $\pm\mathbf{i}$, $\pm\mathbf{j}$, and $\pm\mathbf{k}$ as ±1, $\pm i$, $\pm j$, and $\pm k$, respectively.

(a) Q_8 contains the identity 1 of $\mathrm{GL}_n(\mathbb{C})$. Q_8 is closed under inverses, since direct computation reveals

$$(\pm i)^{-1} = \mp i, \qquad (\pm j)^{-1} = \mp j, \qquad \text{and} \qquad (\pm k)^{-1} = \mp k.$$

It remains to show Q_8 is closed under multiplication. Again by direct computation, we have

$$ij = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = k,$$

$$ik = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = -j,$$

$$jk = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} = -i.$$

On the left-hand side we omitted any sign parity because the corresponding computations are similar, *mutatis mutandis*. This determines the multiplication table of Q_8, because

$$ji = (-j)^{-1}(-i)^{-1} = ((-i)(-j))^{-1} = (ij)^{-1} = k^{-1} = -k,$$
$$ki = (-k)^{-1}(-i)^{-1} = ((-i)(-k))^{-1} = (ik)^{-1} = (-j)^{-1} = j,$$
$$kj = (-k)^{-1}(-j)^{-1} = ((-j)(-k))^{-1} = (jk)^{-1} = (-i)^{-1} = i.$$

It follows that Q_8 is closed under matrix multiplication. It follows that Q_8 is a subgroup of $\mathrm{GL}_2(\mathbb{C})$. The multiplication table of Q_8, up to sign, is shown in **??**.

Q_8	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	$-i$
k	k	j	i	-1

Table 1: Multiplication table for the subgroup Q_8 of $\mathrm{GL}_2(\mathbb{C})$, up to sign

(b) Using **??**, we observe that the only non-identity element $\alpha \in Q_8$ such that $\alpha^2 = 1$ is -1. On the other hand, consider the generators τ and ρ of D_8, which satisfy $\rho^4 = \tau^2 = 1$. Then both τ and ρ^2 square to 1. But $\tau \neq \rho^2$, since otheriwse

$$\tau\rho\tau^{-1} = \rho \implies \rho^2\rho(\rho^{-1})^2 = \rho^{-1} \implies \rho = \rho^{-1} \implies \rho^2 = 1,$$

which contradicts that $\rho^k \neq 1$ for all $k = 1, 2, 3$. Hence D_8 has at least two elements of order 2, but Q_8 has exactly one. Therefore, Q_8 and D_8 are not isomorphic. (Indeed, if $\Phi : D_8 \to Q_8$ were an isomorphism, then

$$\Phi(\rho^2)^2 = \Phi((\rho^2)^2) = 1 = \Phi(\tau^2) = \Phi(\tau)^2,$$

so the elements $\Phi(\rho^2)$ and $\Phi(\tau)$ of Q_8, which must be distinct by injectivity of Φ, both square to 1. Both $\Phi(\tau)$ and $\Phi(\rho^2)$ are not equal to 1 also by injectivity, so we have found two non-identity elements of Q_8 of order 2, contradicting our observation above that there is only one such element.)

□

Exercise 2.8.3. Let G be a group. For any $g \in G$, consider the conjugation map $c_g : G \to G$ given by

$$c_g(x) = gxg^{-1} \text{ for all } x \in G.$$

(a) Prove that for each $g \in G$, c_g is an automorphism of G.

(b) Prove that the map $c : G \to \mathrm{Aut}_{\mathrm{Grp}}(G)$ given by $g \mapsto c_g$ is a group homomorphism.

(c) Prove that the image $\mathrm{im}(c) \subset \mathrm{Aut}_{\mathrm{Grp}}(G)$ is a normal subgroup (called the group of **inner automorphisms** of G).

Solution.

(a) Let $g \in G$ be fixed. We claim $c_g : G \to G$ is a group automorphism. We show this in three steps:

– *Step 1: Show c_g is a group homomorphism.* Conjugation by g is well-defined, and for all $x_1, x_2 \in G$, we have
$$c_g(x_1x_2) = gx_1x_2g^{-1} = gx_11x_2g^{-1} = gx_1g^{-1}gx_2g^{-1} = c_g(x_1)c_g(x_2),$$
so c_g is a group homomorphism.

– *Step 2: Show c_g is injective.* Given $x_1, x_2 \in G$, we have
$$c_g(x_1) = c_g(x_2) \implies gx_1g^{-1} = gx_2g^{-1} \implies x_1 = x_2,$$
where for the last implication we left multiplied and right multiplied both sides by g and g^{-1}, respectively. Thus c_g is injective.

– *Step 3: Show c_g is surjective.* Given $y \in G$, choose $x = g^{-1}yg \in G$. Then
$$c_g(x) = gxg^{-1} = gg^{-1}ygg^{-1} = 1y1 = y,$$
so c_g is surjective.

We conclude that c_g is an automorphism of G.

(b) We first show c is well-defined. This requires us to show two things:

– $g \mapsto c_g$ maps into $\mathrm{Aut}(G)$: We showed in part (a) that c_g is an automorphism of G for all $g \in G$, so $g \mapsto c_g$ is indeed a map into $\mathrm{Aut}_{\mathrm{Grp}}(G)$.

– If g, h are elements of G and $g = h$, then conjugation by g is the same map as conjugation by h. Thus $g = h \implies c_g = c_h$.

It follows that $g \mapsto c_g$ is a well-defined map. Next, if g, h, a are elements of G, then
$$c_{gh}(a) = (gh)a(gh)^{-1} = ghah^{-1}g^{-1} = (c_g \circ c_h)(a).$$
Hence $g \mapsto c_g$ is a group homomorphism.

(c) Denote the image of c in $\mathrm{Aut}(G)$ by $\mathrm{Inn}(G)$. We claim $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$. $\mathrm{Inn}(G)$ is a subgroup of $\mathrm{Aut}(G)$ as the image of the group homomorphism $c : G \to \mathrm{Aut}(G)$. Now let $\sigma \in \mathrm{Aut}(G)$, $c_g \in \mathrm{Inn}(G)$, and $a \in G$. Write
$$(\sigma \circ c_g \circ \sigma^{-1})(a) = \sigma(g\sigma^{-1}(a)g^{-1}) = \sigma(g)\sigma(\sigma^{-1}(a))\sigma(g^{-1}) = c_{\sigma(g)}(a)$$
where the second-to-last equality uses that σ is a group homomorphism. Since this holds for all $a \in G$, we conclude $(\sigma \circ c_g \circ \sigma^{-1}) \in \mathrm{Inn}(G)$. Hence $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$.

□

Exercise 2.8.4. Let G be any group. The **center** of G, denoted $Z(G)$, is defined by
$$Z(G) = \{g \in G : gx = xg \text{ for all } x \in G\}.$$

(a) Prove that $Z(G)$ is a normal subgroup of G. (You can do this by direct verification, but also think about the relationship to the previous problem.)

(b) Assume there is a subgroup $H \subset Z(G)$ such that G/H is cyclic. Prove that G is then abelian. Give an example where $H \subset Z(G)$ and G/H is *abelian*, but G is not abelian.

Solution.

(a) It suffices to show $\ker c = Z(G)$, the center of G, because $\ker c$ is a normal subgroup of G. To see this, write
$$g \in \ker c \iff c_g = \mathrm{id} \iff \text{for all } a \in G,\ gag^{-1} = a \iff ga = ag,$$

so $g \in \ker c$ if and only if $g \in Z(G)$, which means $\ker c = Z(G)$.

(b) Suppose H is a subgroup of G contained in the center $Z(G)$ such that G/H is a cyclic subgroup generated by the left coset xH. (Note that this question is valid because in this case G/H is indeed a group: $H \leqslant Z(G) \implies ghg^{-1} = hgg^{-1}$ because $h \in Z(G)$, which shows H is a normal subgroup of G; thus the quotient G/H is indeed a group.) We claim G is abelian. To that end, let $a, b \in G$ be arbitrary. The elements of G/H partition the group G, so we can write $a \in x^m H$, $b \in x^n H$ for some integers m, n. Hence there exists $h_1, h_2 \in H$ such that $a = x^m h_1$ and $b = x^n h_2$. But then

$$ab = x^m h_1 x^n h_2 = x^{m+n} h_1 h_2 = x^n h_2 x^m h_1 = ba,$$

where the third and fourth equalities hold because $h_1, h_2 \in H \subset Z(G)$. Since a and b were arbitrary, G is abelian.

We now present an example of a group G and a subgroup H of $Z(G)$ such that G/H is *abelian* but G is non-abelian. The group Q_8 is a non-abelian group of order 8 (*cf.* **??**) and $\{\pm 1\}$ is an order 2 subgroup of $Z(Q_8)$, so the quotient $Q_8/Z(Q_8)$ is a group of order 4. Then by **??**, $Q_8/Z(Q_8)$ is abelian. (Notice that this implies $Q_8/Z(Q_8)$ is a (the) non-cyclic group of order 4, since otherwise Q_8 would be abelian by the argument in the previous paragraph.)

□

Exercise 2.8.5 (Construction of D_{2n}, the Dihedral Group of Order $2n$)**.** For an integer $n \geqslant 3$, consider a regular n-gon P_n in $\mathbb{R}^2$ centered at the origin. Let M be the group of all mappings $f : \mathbb{R}^2 \to \mathbb{R}^2$ that preserve the Euclidean distance ($\|p - q\| = \|f(p) - f(q)\|$ for all $p, q \in \mathbb{R}^2$), and let $G = \{f \in M : f(P_n) = P_n\}$.

(a) Show that any $f \in M$ maps the line segment between points $p, q \in \mathbb{R}^2$ to the line segment between points $f(p), f(q) \in \mathbb{R}^2$, and that f maps angles to congruent angles. Use this to justify more carefully the claim made in class that any $f \in G$ maps vertices of P_n to vertices of P_n, and likewise for edges of P_n.

(b) Show that $|G| = 2n$, and that the elements of G can be listed as

$$\{1, \rho, \rho^2, \ldots, \rho^{n-1}, \tau, \tau\rho, \ldots, \tau\rho^{n-1}\},$$

where ρ is the rotation by $2\pi/n$ (counterclockwise) about the origin, and where τ is reflection in the perpendicular bisector of a fixed edge of P_n (it does not matter which edge you choose). Verify the relations $\rho^n = 1, \tau^2 = 1, \tau\rho\tau = \rho^{-1} = \rho^{n-1}$.

Solution. Let n be an integer with $n \geqslant 3$, and suppose P_n is the regular n-gon centered at the origin.

(a) Suppose $f \in M$ and let $p, q \in \mathbb{R}^2$.

– *Step 1: Show f maps the line segment between two points to the line segments between their images.* Given points $a, c \in \mathbb{R}^2$, we denote by $[a, c]$ the line segment connecting p and q. By the characterization of the case of equality in the triangle inequality, we can write

$$c \in \mathbb{R}^2 \text{ lies on } [a, b] \iff \|b - a\| + \|b - c\| = \|a - c\|. \tag{$*$}$$

Now fix $v \in [v_1, v_2]$, so that

$$\|v - v_1\| + \|v - v_2\| = \|v_1 - v_2\|. \tag{2.8.5.1}$$

Since f preserves Euclidean distances, we can write

$$\begin{aligned}\|f(v)-f(v_1)\|+\|f(v)-f(v_2)\| &= \|v-v_1\|+\|v-v_2\| \\ &= \|v_1-v_2\| \qquad \text{(by ??)} \\ &= \|f(v_1)-f(v_2)\|.\end{aligned}$$

Thus $(*)$ implies $f(v)\in[f(v_1),f(v_2)]$. Hence $f([v_1,v_2])\subset[f(v_1),f(v_2)]$. We now argue f is a bijection.

* *f is injective*: Suppose points $v,w\in[v_1,v_2]$ satisfy $f(v)=f(w)$. Then since f preserves Euclidean distance,
$$\|v-w\|=\|f(v)-f(w)\|=0,$$
which holds if and only if $v=w$. Thus f is injective.

* *f is surjective*: Suppose $w\in[f(v_1),f(v_2)]$. Then
$$\begin{aligned}\|w-f(v_1)\|+\|w-f(v_2)\| &= \|f(v_1)-f(v_2)\| \\ &= \|v_1-v_2\|.\end{aligned}$$
Consider the continuous map $r:[v_1,v_2]\to[0,\infty)$ defined as $r(v)=\|v-v_1\|$. Notice that $r(v_1)=0$ and $r(v_2)=\|v_1-v_2\|$. On the other hand, because $w\in[f(v_1),f(v_2)]$, the quantity $\|w-f(v_1)\|$ lies in the interval $[0,\|f(v_1)-f(v_2)\|]=[0,\|v_1-v_2\|]$. Then by the Intermediate Value Theorem, there exists some $v'\in[v_1,v_2]$ such that $\|v'-v_1\|=\|w-f(v_1)\|$. Then using that f preserves Euclidean distance once more, we conclude
$$\big\|f(v')-f(v_1)\big\|=\|w-f(v_1)\|.$$
Thus, the distance from v' to $f(v_1)$ equals the distance from w to v_1. There exists a unique point on $[f(v_1),f(v_2)]$ with any given distance to $f(v_1)$, so because both $f(v')$ and w are contained in the segment $[f(v_1),f(v_2)]$, we conclude $f(v')=w$. It follows that f is surjective.

Thus f maps segments $[v_1,v_2]$ bijectively onto the segment $[f(v_1),f(v_2)]$, and moreover f maps the endpoints v_1, v_2 of the domain segment to the endpoints $f(v_1)$, $f(v_2)$ of the image segment.

– *Step 2: Show f maps angles to congruent angles.* Let θ be an angle between two line segments. Intersecting segments form two angles with each other, so without loss of generality we will assume $\theta\in[0,\pi]$. Translation preserves angles, so without loss of generality we may assume the angle θ is formed by an intersection of lines at the origin, which can be described by vectors v_1 and v_2. It follows that
$$\cos\theta=\frac{\langle v_1,v_2\rangle}{\|v_1\|\cdot\|v_2\|},$$
where $\langle-,-\rangle$ denotes the standard Euclidean inner product, and $\|-\|$ denotes the norm induced by $\langle-,-\rangle$. Then, where $\theta'\in[0,\pi]$ is the angle between $f(v_1)$ and $f(v_2)$, we have
$$\begin{aligned}\cos\theta' &= \frac{\langle f(v_1),f(v_2)\rangle}{\|f(v_1)\|\cdot\|f(v_2)\|} \\ &= \frac{\frac{1}{2}(\|f(v_1)\|^2+\|f(v_2)\|^2-\|f(v_1)-f(v_2)\|^2)}{\|f(v_1)\|\cdot\|f(v_2)\|} \qquad \text{(by the polarization identity)} \\ &= \frac{1}{2}\left(\frac{\|v_1\|^2+\|v_2\|^2+\|v_1-v_2\|^2}{\|v_1\|\cdot\|v_2\|}\right)\end{aligned}$$

$$= \frac{1}{2}\left(\frac{\langle v_1, v_1\rangle + \langle v_2, v_2\rangle - \langle v_1, v_1 - v_2\rangle + \langle v_2, v_1 - v_2\rangle}{\|v_1\| \cdot \|v_2\|}\right)$$
$$= \frac{1}{2}\left(\frac{\cancel{\langle v_1, v_1\rangle} + \cancel{\langle v_2, v_2\rangle} - \cancel{\langle v_1, v_1\rangle} + \langle v_1, v_2\rangle + \langle v_2, v_1\rangle - \cancel{\langle v_2, v_2\rangle}}{\|v_1\| \cdot \|v_2\|}\right)$$
$$= \frac{1}{2}\left(\frac{2\langle v_1, v_2\rangle}{\|v_1\| \cdot \|v_2\|}\right) = \frac{\langle v_1, v_2\rangle}{\|v_1\| \cdot \|v_2\|} = \cos\theta.$$

Since cos is injective on $[0, \pi]$, we conclude $\theta' = \theta$. Hence f maps angles to congruent angles.

- *Step 3: Show that if $f \in G$, then f maps vertices (resp. edges) of P_n to vertices (resp. edges) of P_n.* Suppose $f \in G$, so that $f(P_n) = P_n$. Let $p_0, p_1, p_2, \ldots, p_{n-1}$ be a counterclockwise enumeration of the vertices of P_n in the sense that for each $j = 0, \ldots, n-1$, the vertex p_j satisfies $\rho(p_j) = p_{(j+1) \pmod n}$, where ρ denotes the counterclockwise rotation of $\mathbb{R}^2$ through the angle $2\pi/n$ about the origin. We know from Steps 1 and 2 that f maps the segment $[p_j, p_{(j+1) \pmod n}]$ bijectively onto the segment $[f(p_j), f(p_{(j+1) \pmod n})]$ in P_n. But $f(P_n) = P_n$, so the image segment, that is, the line segment in $\mathbb{R}^2$ connecting $f(p_j)$ to $f(p_{(j+1) \pmod n})$, is also an edge of P_n. It follows that $f(p_j)$ and $f(p_{(j+1) \pmod n})$ are (distinct) adjacent vertices in P_n. We conclude that f maps vertices (resp. edges) of P_n to vertices (resp. edges) of P_n.

(b) Let $\rho : \mathbb{R}^2 \to \mathbb{R}^2$ be a counterclockwise rotation by $2\pi/n$ (about the origin) and let $\tau : \mathbb{R}^2 \to \mathbb{R}^2$ be the map reflecting points about the perpendicular bisector of some fixed edge of P_n.

- *Step 1: Show $\rho, \tau \in G$.* We will again argue in steps:
  - *Step 1(a): Show $\rho, \tau \in M$.* Rotations and reflections are isometries, and hence preserve Euclidean distance, so ρ and τ are elements of M.
  - *Step 1(b): Show that to show $\rho, \tau \in G$, it suffices to show each maps the vertex set of P_n bijectively onto itself.* Suppose we are given that ρ and τ each map the vertex set $\{p_0, \ldots, p_{n-1}\}$ of P_n bijectively onto itself. Then ρ and τ map the edge set of P_n bijectively onto itself, because two vertices of P_n are adjacent if and only if the distance between them equals the edge length of P_n, and this is the case for the endpoints of the images of edges in P_n because ρ and τ preserves lengths.

    This would then imply that both ρ and τ are elements of G, since otherwise there exists some edge missed by our mapping, which is to say f is not injective as a map from the edge set of P_n to itself. But this means some two segments in P_n map to the same edge in P_n, which forces at least three vertices contained in those two edges to map onto the two vertices in the image edge, which contradicts our assumption that f maps the vertex set of P_n bijectively onto itself. We conclude $\rho(P_n) = \tau(P_n) = P_n$, so $\rho, \tau \in G$.
  - *Step 1(c): Show that ρ, τ map the vertex set of P_n bijectively onto itself.* This is clear for the rotation ρ, since $\rho p_j = p_{(j+1) \pmod n}$ for each $j = 1, \ldots, n-1$, so $\rho : \{p_0, \ldots, p_{n-1}\} \to \{p_0, \ldots, p_{n-1}\}$ shifts the indices of the vertices by 1, which is a bijection of sets. If a vertex of P_n lies on the axis of reflection for τ, then τ fixes that vertex. Otherwise, τ is an involution between points and their mirror image across the axis of reflection. Hence τ maps the vertex set of P_n onto the vertex set of P_n. We can now conclude $\rho, \tau \in G$.

– *Step 2: Show $\rho^n = 1$, $\tau^2 = 1$, and $\tau\rho\tau = \rho^{-1} = \rho^{n-1}$.* The first two relations are immediate by definition of ρ and τ. This is equivalent to showing $(\tau\rho)^2 = 1$. Let p_j be any fixed vertex of P_n. Without loss of generality, we may assume $j = p_1$ (since we can always shift the indices). Then $\rho p_1 = p_2$. Then, where p_2' denotes τp_2, we have $\rho\tau\rho p_1 = \rho p_2' = p_1'$. Applying τ once more yields p_1. Hence $\tau\rho\tau\rho(p_1) = p_1$, so we are done. Note we can write this relation as $\tau\rho\tau = \tau^{n-1}$ because $\rho^n = 1 \implies \rho^{n-1} = \rho^{-1}$.

– *Step 3: Show $|G| = 2n$.* Let $f \in G$. By part (a), f maps vertices (resp. edges) of P_n to vertices (resp. edges) of P_n. Then since f maps endpoints to endpoints, it follows that $f(p_j) = p_k$ for some $k = 0, \dots, n-1$. Since $f(p_{(j+1) \pmod n})$ is connected to $f(p_j) = p_k$ by a segment, it follows that $f(p_{(j+1) \pmod n}) \in \{p_{(k-1) \pmod n}, p_{(k+1) \pmod n}\}$. But then $p_{(j+2) \pmod n}$ is determined, since it is the unique vertex adjacent to $f(p_{(k+1) \pmod n})$, and in turn $f(p_{(k+3) \pmod n})$ is determined because it is the unique vertex adjacent to $f(p_{(k+2) \pmod n})$ different from $f(p_{(k+1) \pmod n})$, and so on. It follows that the image of the pair $p_j, p_{(j+1) \pmod n}$ determines f. We just argued that there are n possible images for p_j under f, and for each of these there are 2 possible images for $p_{(j+1) \pmod n}$. We conclude there exist precisely $2n$ elements $f \in G$. Using the relations from Step 2, we can list them all: $\{1, \rho, \rho^2, \dots, \rho^{n-1}, \tau, \tau\rho, \dots, \tau\rho^{n-1}\}$. Since the generators ρ, τ (and thus any of their products with each other) are invertible, function composition is associative, and the identity map $1 = \mathrm{id}_{\mathbb{R}^2} : \mathbb{R}^2 \to \mathbb{R}^2$ is an element of G, we conclude that G is the group $\{1, \rho, \rho^2, \dots, \rho^{n-1}, \tau\rho, \dots, \tau\rho^{n-1}\}$ under function composition.

□

3 Free Groups and Presentations of Groups

3.1 The Subgroup and Normal Subgroup Generated by a Set

Definition 3.1.1. Let G be a group and let X be any subset of G. The **subgroup generated by X**, denoted $\langle X \rangle$ is defined by

$$\langle X \rangle = \bigcap_{X \subset H < G} H.$$

Similarly, define the **normal subgroup generated by X** by

$$\langle X \rangle^{\text{normal}} = \bigcap_{X \subset N \lhd G} N.$$

The following lemma shows the terms used in the above definition, are accurate, and that informally we can say that $\langle X \rangle$ (resp. $\langle X \rangle^{\text{normal}}$) is the smallest subgroup (resp. the smallest normal subgroup) of G containing X.

Lemma 3.1.2. Let G be a group and let X be any subset of G. Then $\langle X \rangle$ (resp. $\langle X \rangle^{\text{normal}}$) is a subgroup (resp. normal subgroup) of G, and if H is a subgroup (resp. normal subgroup) of G containing X, then H contains $\langle X \rangle$ (resp. $\langle X \rangle^{\text{normal}}$).

Proof. The intersection $\langle X \rangle = \bigcap_{X \subset H < G} H$ is a subgroup, since any intersection of subgroups is a subgroup. For the "equivalently," temporarily let H be the subset of all finite products of elements of $X \cup X^{-1}$, where $X^{-1} = \{x^{-1} \mid x \in X\}$. For any $H < G$ containing X, we have $Y \subset H$, so $Y \subset \langle X \rangle = \bigcap_{H < G, X \subset H} H = \langle X \rangle$. So, it is enough to show Y is a subgroup, and this is clear from the definition.

The proof of the statements about $\langle X \rangle^{\text{normal}}$ are similar. □

Remark 3.1.3. An equivalent definition for the subgroup generated by X in G is that $\langle X \rangle$ is all finite products of elements of $X \cup X^{-1}$, where $X^{-1} = \{x^{-1} \mid x \in X\}$.

Exercise 3.1.4. Think through the normal analog of the "equivalently" in the last lemma.

Definition 3.1.5. Let G be a group and $x, y \in G$. A **commutator** of x and y in G, denoted $[x, y]$, is defined by

$$[x, y] = xyx^{-1}y^{-1}.$$

So, $[x, y] = 1$ if and only if x and y commute in G. The **commutator subgroup** $[G, G]$ of G is defined by

$$[G, G] = \langle \{[x, y] \mid x, y \in G\} \rangle.$$

The commutator subgroup $[G, G]$ is also typically called the **derived subgroup** of G.

Remark 3.1.6. The commutator subgroup $[G, G]$ is the smallest thing one can quotient by to get an abelian group. In other words, $G/[G, G]$ is the "closest" abelian group related to G that is abelian. (See the homework). That said, the group $G/[G, G]$ is called the **abelianization** of G, and is denoted G^{ab}.

Observation: $[G, G] \lhd G$. (See homework).

3.2 Construction of the Free Group by Relations on Abstract Generators

Let S be any set, and let S^{-1} be any set disjoint from S such that there exists a bijection of sets $S \to S^{-1}$. Given an element $s \in S$, we will write s^{-1} to mean the image of s in S^{-1} under this bijection. Let

$$W = \{1\} \cup \bigcup_{n \geqslant 1} (S \cup S^{-1})^n.$$

Elements of W are called **words**, and $\{1\}$ is sometimes called the **empty word**. For example, if $S = \{s_1, s_2, s_3\}$, then $s_1 s_1 s_2 s_2^{-1} s_3 s_1 s_2 s_2^{-1} s_3^{-1} \in W$. Given any two words in W, we can define **word composition** by their concatenation, that is, by their image under the map

$$W \times W \longrightarrow W$$

$$x_1 \cdots x_m \times y_1 \cdots y_n \longmapsto x_1 \cdots x_m y_1 \cdots y_n,$$

and if the empty word 1 is in either slot, then the image is the word in the other slot. To obtain a group out of this construction, we need that any given word has an inverse under composition. To do this, we introduce an equivalence relation $\sim$ on W as follows. Set

$$x_1 \cdots x_{i-1} x_i x_{i+1} \cdots x_n \qquad \sim \qquad x_1, \cdots x_{i-1} x_{i+2} \cdots x_n$$

if $x_i = x_{i+1}^{-1}$ or $x_i^{-1} = x_{i+1}$. We call this a **cancellation**, and we let $\sim$ be the equivalence relation on W generated by cancellation. We can reformulate $\sim$ using the following lemma.

Lemma 3.2.1. For each word $w \in W$, there exists a unique $w_0 \in W$ such that w_0 is obtained from w by a series of cancellations, such that no cancellations can be done in w_0. We call w_0 the **reduced word** of w.

For example, by applying cancellations to the word $w = s_1 s_1 \cancel{s_2 s_2^{-1}} s_3 s_1 \cancel{s_2 s_2^{-1}} s_3^{-1}$, we obtain the reduced word $w_0 = s_1 s_1 s_3 s_1 s_3^{-1}$.

Proof of **??**. We induct on the length ℓ of w. If $\ell = 0$ or $\ell = 1$, then the result is clear. Now let $n \geqslant 2$ and suppose the claim is true for all lengths $\ell < n$, and let w be a word of length n. If w is

reduced, then $w = w_0$ and there is nothing to show. Otherwise,

$$w = y_1 \cdots y_i x \cdot x^{-1} y_{i+1} \cdots y_{n-2}$$

for some $x \in S \cup S^{-1}$. (For all $a \in S$, write $(a^{-1})^{-1} = a$.)

We claim that *any* reduced form of w can be obtained by cancelling $x \cdot x^{-1}$ *first*. The claim completes the proof, since by induction $y_1 \cdots y_i y_{i+1} \cdots y_{n-2}$ has a *unique* reduced form, and hence the same is true for w.

We now prove the above claim.

- *Case (i): The cancellations leading from w to w_0 include the $x \cdot x^{-1}$ cancellation.* Then we can rearrange te cancellations to do this first, so we are done.
- *Case (ii): We get from w to w_0 without the $x \cdot x^{-1}$ cancellation.* But the individual symbols x and x^{-1} must still be canceled, since otherwise w_0 is not reduced; the first cancellation including one of these terms is either

$$\underbrace{x^{-1}}_{\in\{y_1,\ldots,y_i\}} \cdot x \cdot x^{-1} \qquad \text{or} \qquad x \cdot x^{-1} \cdot \underbrace{x}_{\in\{y_{i+1},\ldots,y_{n-2}\}},$$

  and the result is no different from if we cancelled the original pair instead—so we may as well do that, and then we win by case (i). This completes the proof. □

As a consequence of **??**, $W/\!\sim \cong \{\text{reduced words in } W\}$.

Lemma 3.2.2. If $w \sim w'$ and $v \sim v'$, then $wv \sim w'v'$.

Proof. Write $(-)_0$ for the reduced form of $(-)$. Then

$$wv \sim w_0 v_0 \sim w'v',$$

where the first $\sim$ is by cancelling individually in w and v, and the second $\sim$ is by individually cancelling in w' and v'. □

Lemma 3.2.3. $W/\!\sim$ is a group under concatenation. That is, $W/\!\sim$ is a group under composition of the word composition map with the natural quotient map $W \twoheadrightarrow W/\!\sim$.

Proof. The previous lemma shows concatenation is well-defined on the quotient $W/\!\sim$. Concatenation is associative since it is on W ,and has identity the empty word 1. $W/\!\sim$ has inverses, since if $x_1 \cdots x_n$ is a word in W, then

$$(x_1 \cdots x_n)(x_n^{-1} x_{n-1}^{-1} \cdots x_1^{-1}) \sim 1 \sim (x_n^{-1} x_{n-1}^{-1} \cdots x_1^{-1})(x_1 \cdots x_n),$$

(Note that here we are observing the convention that for $s \in S$, $(s^{-1})^{-1} = s$.) Thus $W/\!\sim$ is a group. □

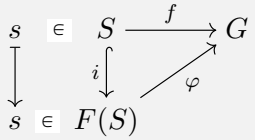
Definition 3.2.4. For any set S, we define the **free group** on S, denoted $F(S)$, as the group $W/\!\sim$ under concatenation, where $W/\!\sim$ is in the notation of **??**.

3.3 Universal Mapping Property of Free Groups

Freeness has to do with a certain universal mapping property.

Theorem 3.3.1 (Universal Mapping Property of Free Groups)**.** If G is a group, S is a set, and $f\colon S \to G$ is a map of sets, then there exists a unique group homomorphism $F(S) \to G$ such that

the diagram



commutes. The association $f \mapsto \varphi$ induces a bijection

$$\mathrm{Hom}_{\mathrm{Set}}(S, G) \xrightarrow{\cong} \mathrm{Hom}_{\mathrm{Grp}}(F(S), G).$$

Proof. Given a set map $f\colon S \to G$, extend f to $f\colon S \cup S^{-1} \to G$ by $f(s^{-1}) = f(s)^{-1}$ for all $s \in S$. Define a function $\widetilde{\varphi}\colon W \to G$ by $\widetilde{\varphi}(X_1 \cdots x_n) = f(x_1)f(x_2)\cdots f(x_n)$, where $x_i \in S \cup S^{-1}$ for each i. Then $\widetilde{\varphi}$ descends to a group homomorphism $\varphi\colon W/\!\sim \to G$ because

$$\widetilde{\varphi}(x_1 \cdots x_{i-1}x_i x_i^{-1} x_{i+1} \cdots x_n) = \widetilde{\varphi}(x_1)\underbrace{\widetilde{\varphi}(x_i)\widetilde{\varphi}(x_i^{-1})}_{=f(x_i)f(x_i)^{-1}}\widetilde{\varphi}(x_{i+1})\cdots\widetilde{\varphi}(x_n).$$

This shows φ is well-defined on $W/\!\sim$. Because $F(S)$ is generated by S, φ is the unique homomorphism making the given diagram commute.

The fact that this is a bijection between hom sets follows from showing it has an inverse: $f \mapsto \varphi$ gives a map

$$\mathrm{Hom}_{\mathrm{Set}}(S, G) \xrightarrow{\cong} \mathrm{Hom}_{\mathrm{Grp}}(F(S), G)$$

with inverse $\varphi \mapsto \varphi|_S$, the restriction along the inclusion map $S \xhookrightarrow{i} F(S)$. Checking this is indeed an inverse is almost immediate by definition, but can be checked as an exercise. □

Definition 3.3.2. Let S be a set and let R be a subset of the free group $F(S)$. The **group with generators S and relations R**, denoted $\langle S \mid R\rangle$, is defined by

$$\langle S \mid R\rangle \coloneqq F(S)/\langle R\rangle^{\mathrm{normal}}.$$

Given a group G, an isomorphism $G \cong \langle S \mid R\rangle$ for some S, R above is called a **presentation** of G.

Remark 3.3.3. It is straightforward that every group can be written as a presentation. On the other hand, there cannot exist an algorithm that, when given an arbitrary group presentation , can determine if the group being presented is even the trivial group.

3.4 Free Abelian Groups

We want to define an abelian analog to the free group generated by a set S. We can consider doing this in several ways, and two such ways are as follows.

- Define $F(S)$ by the usual free group, but with the additional relations $xy \sim yx$ for all $x, y \in S$, and similarly for strings of larger length.
- $F(S)$ is the abelian group of all finite $\mathbb{Z}$-linear combinations of elements of S.

Showing these definitions are equivalent is left as an exercise. We will opt for the first definition:

Definition 3.4.1. Let S be any set. The **free abelian group** generated by S is the abelianization of the free group $F(S)$, that is,

$$F(S)^{\mathrm{ab}} = F(S)/[F(S), F(S)] = F(S)/\langle S \mid R\rangle,$$

where $R = \{[x, y] \mid x, y \in S\}$.

Let us make this more formal using the universal property of free groups, which we recall is the following: If $S \xrightarrow{f} G$ is a set map, then there exists a unique group map $F(S) \xrightarrow{\varphi} G$ such that the diagram

$$\begin{array}{ccc} S & \xrightarrow{\quad f \quad} & G \\ \downarrow & \nearrow_{\varphi} & \\ F(S) & & \end{array}$$

commutes. We will show the free abelian group enjoys a mapping property similar to the one for the usual free group:

Theorem 3.4.2 (Universal Mapping Property of Free Abelian Groups)**.** Let A be any abelian group. If $f\colon S \to A$ is a set map, then there exists a unique group map $\varphi\colon F(S)^{\mathrm{ab}} \to G$ such that the diagram

$$\begin{array}{ccc} S & \xrightarrow{\quad f \quad} & A \\ \downarrow & \nearrow_{\varphi} & \\ F(S)^{\mathrm{ab}} & & \end{array}$$

commutes.

Proof Sketch. Let A be any abelian group, so that there exists a unique $\widetilde{\varphi}$ such that $\widetilde{\varphi}$ is the top map in the above diagram. Certainly, if $x, y \in S$ then $\widetilde{\varphi}([x,y]) = \widetilde{\varphi}(xyx^{-1}y^{-1}) = \widetilde{\varphi}(x)\widetilde{\varphi}(y)\widetilde{\varphi}(x)^{-1}\widetilde{\varphi}(y)^{-1} = 1$. Hence $[x,y] \in \ker\widetilde{\varphi}$. So, $\widetilde{\varphi}$ factors through a map

$$\begin{array}{ccc} & & F(S) \\ & & \downarrow \\ F(S)^{\mathrm{ab}} & = & F(S)/\langle [x,y] \mid x,y \in S\rangle \xrightarrow[\widetilde{\varphi}]{} A \end{array} \qquad \text{with } \widetilde{\varphi} \text{ on the diagonal}$$

and φ is unique. □

We now show that if $|S| = n$ is a positive integer, then $F(S)^{\mathrm{ab}}$ is isomorphic to $\mathbb{Z}^n$. We exhibit an explicit isomorphism. Given $S = \{x_1, \ldots, x_n\}$, then consider the map

$$\begin{aligned} S &\longrightarrow \mathbb{Z}^n, \\ x_i &\longmapsto (0, \ldots, 0, 1, 0, \ldots, 0). \end{aligned}$$

This is a well-defined group homomorphism, so by **??** we get a group map $F(S)^{\mathrm{ab}} \xrightarrow{\varphi} \mathbb{Z}^n$.

Remark 3.4.3 (Aside). The group $G = \langle x \mid x^n\rangle$ is the cyclic group of order n. Indeed, the map

$$\begin{aligned} \{x\} &\longrightarrow \mathbb{Z}/n\mathbb{Z}, \\ x &\longmapsto 1, \end{aligned}$$

is a set map, so by the universal property of $F(\{x\})^{\mathrm{ab}}$ we get a group map

$$\begin{aligned} F(\{x\})^{\mathrm{ab}} &\twoheadrightarrow \mathbb{Z}/n\mathbb{Z}, \\ x^n &\to 0, \\ G &\longrightarrow \mathbb{Z}/n\mathbb{Z}, \end{aligned}$$

so $G \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$, and $G = \{1, x, x^2, \ldots, x^{n-1}\}$, and $|G| \leqslant n$.

Example 3.4.4 (Group Presentation)**.** Consider $G = \langle x, y \mid xy = y^2x, yx = x^2y\rangle$. It turns out G

is just the trivial group. Indeed,

$$xy = y^2x = y(yx) = y(x^2y),$$

and multiplying by x^{-1} on the left gives $x = yx^2$, so $yx = 1$. From this it is straightforward that G is the trivial group. //

Note that if $|S| = \infty$, then

$$\mathbb{Z}^{|S|} \neq \prod_{s\in S} \mathbb{Z}.$$

We will show that if this were true, then the universal property fails. Indeed, suppose $F(S)^{\text{ab}} = \prod_{s\in S} \mathbb{Z}$ and $|S| = \infty$. Then consider the set map

$$\begin{aligned} \{x_1, x_2, \dots\} &\longrightarrow \bigoplus_{n=1}^{\infty} \mathbb{Z}, \\ x_i &\longmapsto (0, \dots 0, 1, 0, \dots, 0). \end{aligned}$$

If the universal property were to hold, then there should be a map

$$\prod_{n=1}^{\infty} \mathbb{Z} \longrightarrow \bigoplus_{n=1}^{\infty} \mathbb{Z}$$

But then the elements $(1, 1, 1, 1, \dots,)$, $(0, 1, 1, 1, \dots,)$, $(0, 0, 1, 1, \dots)$, $(0, 0, 0, 1, 1, \dots)$, and so on, must all map 0. This contradicts the universal property (Why?).

The correct answer for what the free abelian group generated by an infinite set S is

$$\bigoplus_{s\in S} \mathbb{Z} = \{(x_s)_{s\in S} \in \prod_S \mathbb{Z} \text{ such that for all but finitely many } s \in S,\ x_j = 1\}.$$

Example 3.4.5. Are the following groups free abelian groups?

(1) $(\mathbb{Q}, +)$: For all $x \in \mathbb{Q}$, for all $n \in \mathbb{N}$, there exists $y \in \mathbb{Q}$ such that $ny = x$. Thus this is a free group. Indeed, $(\mathbb{Q}, +) = \langle x_n \mid x_n^n = x_{n-1}\rangle$, and in fact $x_n = 1/n!$ works.

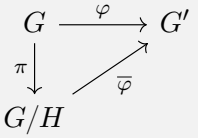
(2) $(\mathbb{Q}^\times, \times)$: Here we have $(-1)^2 = 1$. How does this answer whether this is a free group?

(3) $(\mathbb{Q}^\times_{>0}, \times)$: This is a free group, since this is isomorphic to $\bigoplus_{n=1}^{\infty} \mathbb{Z}$, given by the map $p_\iota \longleftrightarrow (0, \dots, 0, 1, 0, \dots)$, where p_i is the ith prime. //

Note for Homework 2, Exercise 3: Use the universal property of free groups. Show the induced homomorphism maps relations to the identity of D_{2n} (under the induced map $F(S) \to D_{2n}$), which by universal property of quotients induces a quotient map $F(S)/R \to D_{2n}$. Then to show that map it is isomorphism, we need to show it is surjective and injective. One of these should be straightforward, and to obtain the other you must use an argument using the fact D_{2n} has $2n$ elements.

3.5 Universal Mapping Property of Quotient Groups

Theorem 3.5.1 (Universal Mapping Property of Quotient Groups)**.** Suppose $H \lhd G$ and $H \subset \ker\varphi$ for a group homomorphism $\varphi\colon G \to G'$. Then there exists a unique homomorphism $\overline{\varphi} : G/H \to G'$ such that the diagram



commutes. Moreover, the assignment $\varphi \mapsto \overline{\varphi}$ induces a bijection

$$\text{Hom}_{\text{Grp}}(G/H, G') \longleftrightarrow \left\{\varphi \in \text{Hom}_{\text{Grp}}(G, G') \,\middle|\, H \subset \ker\varphi\right\}.$$

Proof. Define

$$\begin{aligned}\overline{\varphi}\colon G/H &\longrightarrow G',\\ gH &\longmapsto \varphi(g).\end{aligned}$$

- *φ is well-defined*: if $g_1H = g_2H$ then there exists $h \in H$ such that $g_1 = g_2h$. Then
$$\overline{\varphi}(g_1H) = \varphi(g_1) = \varphi(g_2h) = \varphi(g_2)\varphi(h) = \varphi(g_2) = \overline{\varphi}(g_2).$$
- *$\overline{\varphi}$ is a homomorphism*: since
$$\overline{\varphi}(g_1g_2H) = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \overline{\varphi}(g_1H)\overline{\varphi}(g_2H)$$
- *$\overline{\varphi}$ is the unique map with these properties*: $\overline{\varphi}$ is unique by considering the commuting diagram
$$\begin{array}{ccc} G & \xrightarrow{\quad\varphi\quad} & G' \\ {\scriptstyle\pi_H}\downarrow & \searrow^{\pi_{\ker\varphi}} & \uparrow{\scriptstyle\widetilde{\varphi}} \\ G/H & \xrightarrow[\pi_{\ker\varphi/H}]{} & G/\ker\varphi \end{array}$$
since $\ker\varphi/H \lhd G/H$ by the correspondence theorem and $\frac{G/H}{\ker\varphi/H} \cong G/\ker\varphi$ by the second isomorphism theorem.
- *The assignment $\varphi \mapsto \overline{\varphi}$ induces a bijection* $\mathrm{Hom}(G/H, G') \leftrightarrow \{\varphi \in \mathrm{Hom}(G, G') \mid H \subset \ker\varphi\}$: $\overline{\varphi} \hookleftarrow \varphi$ by the theorem. Given $\psi \in \mathrm{Hom}(G/H, G')$, let $\widetilde{\psi} = \pi_H \circ \psi$. Then
$$\begin{array}{ccc} h & & G \\ \downarrow & & {\scriptstyle\pi_H}\downarrow \searrow^{\widetilde{\psi}} \\ H & & G/H \xrightarrow[\psi]{} G' \end{array}$$
commutes. Then $\varphi = \widetilde{\psi}$ makes the diagram
$$\begin{array}{ccc} G & & \\ {\scriptstyle\pi_H}\downarrow & \searrow^{\varphi=\widetilde{\psi}} & \\ G/H & \xrightarrow[\overline{\varphi}]{} & G' \end{array}$$
commute. Lastly, by the uniqueness clause of the theorem, $\overline{\varphi} = \psi$. □

Example 3.5.2. There are bijections

$$\begin{aligned}\mathrm{Hom}(D_{2n}, G) &\longleftrightarrow \{\varphi \in \mathrm{Hom}(F(\{x,y\}), G) \mid \langle x^n, y^2, xyxy\rangle^{\text{normal}} \subset \ker\varphi\}\\ &\longleftrightarrow \{\varphi \in \mathrm{Hom}(F(\{x,y\}), G) \mid \varphi(x^n) = \varphi(y^2) = \varphi(xyxy) = 1\}\\ &\longleftrightarrow \{f\colon \{x,y\} \to G \mid f(x)^n = f(y)^2 = f(x)f(y)f(x)f(y) = 1\}\end{aligned}$$

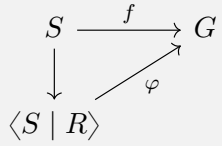
$D_{2n} \longrightarrow \mathrm{GL}_2(\mathbb{R})$, $x \xrightarrow{f} \begin{pmatrix}\cos\theta & \sin\theta\\ -\sin\theta & \cos\theta\end{pmatrix}, y \xrightarrow{f} \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$.

Then check $\begin{pmatrix}\cos\theta & \sin\theta\\ -\sin\theta & \cos\theta\end{pmatrix}^n \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ and $\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}^2 = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$. Indeed,

$$\begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}\cos\theta & \sin\theta\\ -\sin\theta & \cos\theta\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}. \qquad //$$

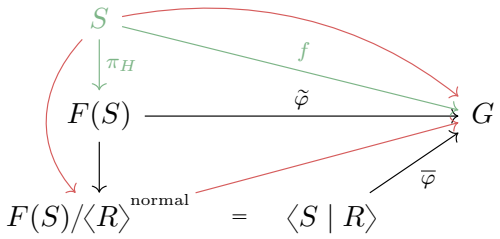
3.6 Universal Mapping Property of Presentation Groups

Theorem 3.6.1 (Universal Mapping Property of Presentation Groups)**.** Let S be a set, let R be a set of relations on S, and let G be a group. Then if $f\colon S \to G$ is a set map such that $f(a_1)f(a_2)\cdots f(a_k) = 1$ whenever the elements $a_1, \dots, a_r \in S$ have the word $a_1 \cdots a_k \in R$, then there exists a unique $\varphi\colon \langle S \mid R\rangle \to G$ such that the diagram



commutes. We call φ the **group homomorphism determined by f**.

Proof. By the universal property of free groups, there exists $\widetilde{\tau}\colon F(S) \to G$ such that $\widetilde{\varphi}(r) = e$, so $\langle R\rangle \subset \ker\widetilde{\varphi}$. Hence $\langle R\rangle^{\text{normal}} \subset \ker\widetilde{\varphi}$. And by the universal mapping property of quotient groups, there exists a unique group homomorphism $\overline{\varphi}$ that makes the diagram



commute. This completes the proof. □

Example 3.6.2. What is the size of $\mathrm{Aut}(D_8)$? We need bijective maps sending the element x of order n in D_8 to an element ρ of order n in the other copy of D_8, and the element y of order 2 in D_8 must be sent to an element τ of order 2 in the other copy of D_8. So, the possible maps are

$$\begin{aligned} D_8 &\longrightarrow D_8, \\ x &\longmapsto \rho \text{ or } \rho^3, \\ y &\longmapsto \rho^2 \text{ or } \tau\rho^i \text{ for some } i = 0, 1, 2, 3. \end{aligned}$$

Suppose $y \mapsto \rho^2$. Then although $f(x)^4 = f(y)^2 = f(x)f(y)f(x)f(y) = 1$, but $\rho^i\rho^2\rho^i\rho^2 = \rho^{4+2i} = \rho^{2i} = \rho^2 \neq 1$. //

3.7 Homework 2

Exercise 3.7.1. Fix $n \in \mathbb{Z}_{>0}$. We often express $\sigma \in S_n$ using the following cycle notation: for distinct elements $i_1, \cdots, i_r \in \{1, \cdots n\}$, we write $(i_1 i_2 \cdots i_r)$ for the r-cycle $\sigma \in S_n$ given by $\sigma(i_k) = i_{k+1}$ for all $k \in 1 \cdots, r$, with the convention $i_{r+1} = i_1$; and for all $m \in \{1, \cdots, n\} \smallsetminus \{i_1, \cdots, i_r\}$, $\sigma(m) = m$.

(a) Show that any $\sigma \in S_n$ can be written as a product (composition) of disjoint cycles.

(b) Prove that disjoint cycles commute.

Solution. Let n be a positive integer and let $\sigma \in S_n$. We first prove two auxiliary lemmas about σ:

Lemma 3.7.2. If $1 \leqslant r \leqslant n$, then there is some for some integer $0 \leqslant k_r \leqslant n!$ such that

$$\sigma|_{C_r} = (1, \sigma(r), \dots, \sigma^{k_r - 1}(r))|_{C_r},$$

where $C_r = \{1, \sigma(r), \dots, \sigma^{k_r-1}(r)\}$.

Lemma 3.7.3. For all $k \geqslant 1$, if $m_1, \dots, m_k \in \{1, \dots, n\}$ and $m_{k+1} \in \{1, \dots, n\} \smallsetminus (\bigcup_{j=1}^{k} C_{m_j})$, then C_{k+1} is disjoint from $\bigcup_{j=1}^{k} C_{m_j}$.

Proof of **??**. The existence of such an integer k_r follows by noting that if no such k_r exists, then the maps σ^j are distinct for all positive integers j, contrary to $|S_n| = n!$. It remains to show $\sigma|_{C_r} = (1, \sigma(r), \dots, \sigma^{k_r-1}(r))|_{C_r}$. Let $q \in C_r$. Then $q = \sigma^j(r)$ for some $0 \leqslant q \leqslant k_m - 1$, so

$$\begin{aligned}\sigma(q) = \sigma(\sigma^j(r)) = \sigma^{j+1}(r) &= (1, \sigma(r), \dots, \sigma^{k_r-1}(r))|_{C_r}(\sigma^{j+1}(r)) \\ &= (1, \sigma(r), \dots, \sigma^{k_r-1}(r))|_{C_r}(q).\end{aligned}$$

Since q was an arbitrary element of C_r, we conclude $\sigma|_{C_r} \equiv (1, \sigma(r), \dots, \sigma^{k_r-1}(r))_{C_r}$, which is what we wanted to show. □

Proof of **??**. We prove the claim by induction on the number k of distinct sets over which the union is taken. We first argue the base case $k = 1$: If $C_{m_1} = \{1, \dots, n\}$ then the claim is vacuously affirmed, so we may assume $C_{m_1} \neq \{1, \dots, n\}$. Now suppose C_{m_1} and C_{m_2} share a common element, say $\sigma^j(m_1) = \sigma^{j'}(m_2)$, for some integers j, j'. Applying $\sigma^{-j'}$ to both sides, we obtain $\sigma^{j-j'}(r) = m_2$. But this shows m_2 is an element of C_{m_1}, contrary to our assumption.

Now suppose the claim holds for all integers up to some k. Then suppose for a contradiction there exists some element in both $C_{m_{k+1}}$ and $\bigcup_{j=1}^{k} C_j$. Then this element is of the form $\sigma^\ell(m_{k+1}) = \sigma^{\ell'}(m_j)$ for some integers ℓ, ℓ', j. Applying $\sigma^{-\ell'}$ to both sides, we obtain $\sigma^{\ell-\ell'}(m_{k+1}) = m_j$. But this shows m_{k+1} is an element of C_ℓ, and hence of $\bigcup_{j=1}^{k} C_{m_j}$, contrary to our assumption. This completes the proof. □

We can now prove the statements of **??**:

(a) If $C_1 = \{1, \dots, n\}$, then σ is already a cycle in S_n, namely the n-cycle given by $(1, \sigma(1) \dots, \sigma^{n-1}(1))$.

Now suppose $C_1 \neq \{1, \dots, n\}$, and denote by m_1 some element of $\{1, \dots, n\} \smallsetminus C_1$. By **??**, the sets C_1 and C_{m_1} determine cycles $(1, \sigma(1), \dots, \sigma^{k_1-1}(1))$ and $(1, \sigma(1), \dots, \sigma^{k_{m_1}-1})$, respectively. By **??**, the corresponding sets C_1 and C_{m_1} are disjoint. Thus for any $q \in C_1 \cup C_{m_1}$, we can write

$$\begin{aligned}\sigma|_{C_1 \cup C_{m_1}}(q) &= \begin{cases}(1, \sigma(1), \dots, \sigma^{k_1-1}(1))|_{C_1}(q) & \text{if } q \in C_1, \\ (1, \sigma(m_1), \dots, \sigma^{k_{m_1}-1}(m_1))(q) & \text{if } q \in C_{m_1}; \end{cases} \\ &= (1, \sigma(m_1), \dots, \sigma^{k_{m_1}-1}(m_1))|_{C_1 \cup C_r} \circ (1, \sigma(1), \dots, \sigma^{k_1-1}(1))|_{C_r}(q) \\ &= ((1, \sigma(m_1), \dots, \sigma^{k_{m_1}-1}(m_1)) \circ (1, \sigma(1), \dots, \sigma^{k_1-1}(1)))|_{C_1 \cup C_{m_1}}(q).\end{aligned}$$

Hence $\sigma|_{C_1 \cup C_{m_1}}$ is a product (composition) of cycles. If $C_1 \cup C_{m_1} = \{1, \dots, n\}$, then $\sigma = \sigma|_{C_1 \cup C_{m_1}}$, which affirms the claim.

If $C_1 \cup C_{m_1} \neq \{1, \dots, n\}$, then let m_2 be some element of $\{1, \dots, n\} \smallsetminus (C_1 \cup C_{m_1})$. By **??**, C_{m_2} is disjoint from $\{C_1 \cup C_{m_1}\}$, so arguing similarly to the previous paragraph we obtain that

$$\sigma|_{C_1 \cup C_{m_1} \cup C_{m_2}} = (1, \dots, \sigma^{k_{m_2}-1}(m_2)) \circ (1, \dots, \sigma^{k_{m_1}-1}(m_1)) \circ (1, \dots, \sigma^{k_1-1}(1))|_{C_1 \cup C_{m_1} \cup C_{m_2}}.$$

Since $\{1, \dots, n\}$ is finite, this process terminates after finitely many steps, and leaves us with a partition $C_1, \dots, C_\ell$ of $\{1, \dots, n\}$ and the expression σ as a product of disjoint cycles corresponding to the C_j. This completes the proof.

(b) Consider an m-cycle $\sigma = (i_1, \dots, i_m)$ and an n-cycle $\tau = (j_1, \dots, j_n)$ in S_n, and suppose the sets $C_\sigma \coloneqq \{i_1, \dots, i_m\}$ and $C_\tau \coloneqq \{j_1, \dots, j_n\}$ are disjoint. Since σ and τ are cycles, we can

write

$$\sigma(r) = \begin{cases} i_{k+1} & \text{if } r = i_k \in C_\sigma, \\ r & \text{if } r \notin C_\sigma, \end{cases}$$

and

$$\tau(r) = \begin{cases} j_{\ell+1} & \text{if } r = j_\ell \in C_\tau, \\ r & \text{if } r \notin C_\tau. \end{cases}$$

Then

$$\begin{aligned} \tau(\sigma(r)) &= \begin{cases} j_{\ell+1} & \text{if } \sigma(r) = j_\ell \in C_\tau, \\ \sigma(r) & \text{if } \sigma(r) \notin C_\tau; \end{cases} \\ &= \begin{cases} j_{\ell+1} & \text{if } r = i_k \in C_\sigma \text{ and } i_k = j_\ell \in C_\tau, \qquad \longleftarrow \text{ impossible} \\ j_{\ell+1} & \text{if } r \notin C_\sigma \text{ and } r = j_\ell \in C_\tau, \\ i_{k+1} & \text{if } r = i_k \in C_\sigma \text{ and } r = j_\ell \in C_\tau, \\ r & \text{if } r \notin C_\sigma \text{ and } r \notin C_\tau; \end{cases} \\ &= \begin{cases} j_{\ell+1} & \text{if } r \notin C_\sigma \text{ and } r = j_\ell \in C_\tau, \\ i_{k+1} & \text{if } i_k \in C_\sigma \text{ and } r \in C_\tau, \\ r & \text{if } r \notin C_\sigma \text{ and } r \notin C_\tau. \end{cases} \end{aligned}$$

On the other hand,

$$\begin{aligned} \sigma(\tau(r)) &= \begin{cases} i_{k+1} & \text{if } \sigma(r) = i_k \in C_\sigma, \\ \tau(r) & \text{if } \sigma(r) \notin C_\sigma; \end{cases} \\ &= \begin{cases} i_{k+1} & \text{if } r = j_\ell \in C_\tau \text{ and } j_\ell = i_k \in C_\sigma, \qquad \longleftarrow \text{ impossible} \\ i_{k+1} & \text{if } r \notin C_\tau \text{ and } r = i_k \in C_\sigma, \\ j_{\ell_1} & \text{if } r = j_\ell \in C_\tau \text{ and } r \notin C_\sigma, \\ r & \text{if } r \notin C_\tau \text{ and } r \notin C_\sigma; \end{cases} \\ &= \begin{cases} i_{k+1} & \text{if } r \notin C_\tau \text{ and } r = i_k \in C_\sigma, \\ j_{\ell+1} & \text{if } r = j_\ell \in C_\tau \text{ and } r \notin C_\sigma, \\ r & \text{if } r \notin C_\tau \text{ and } r \notin C_\sigma, \end{cases} \end{aligned}$$

which is the same as $\tau(\sigma(r))$ above. Hence σ and τ commute. □

Exercise 3.7.4. For $n \geqslant 2$, and for any two integers $i \neq j, 1 \leqslant i, j \leqslant n$ define the transposition σ_{ij} in the symmetric group S_n to be the 2-cycle (ij), that is, $\sigma_{ij}(i) = j, \sigma_{ij}(j) = i$, and $\sigma_{ij}(k) = k$ for all $k \in \{1, \ldots, n\} \backslash \{i, j\}$. Show the following:

(a) The transpositions $s_i \coloneqq \sigma_{i,i+1}$ (for varying $i \in \{1, \ldots, n\}$) generate S_n. (In particular, the transpositions generate S_n.)

(b) Check the relations $s_i^2 = 1$ (the identity), $s_i s_j = s_j s_i$ whenever $|j - i| > 1$, and

$$s_i s_{i+1} = (i, i+1, i+2).$$

Solution.

(a) Fix $\sigma \in S_n$. It suffices to show σ is a product of σ_{ij}, because $\sigma_{ij} \in \langle s_i \mid i = 1, .., n \rangle$. Indeed, if $i < j$ then $\sigma_{ij} = s_{j-1} s_{j-2} \cdots s_{i+1} s_i s_{i+1} \cdots s_{j-2} S_{j-1}$. Then the cycle $(i_1 i_2 i_3) = \sigma_{i_2 i_3} \circ \sigma_{i_1 i_2}$,

$(i_1 i_2 i_3 i_4) = \sigma_{i_1 i_4}\sigma_{i_2 i_4}\sigma_{i_3 i_4}$, and in general

$$(i_1 i_2 \cdots i_n) = \sigma_{i_1 i_n}\sigma_{i_2 i_n}\cdots\sigma_{i_{n-1} i_n}.$$

Since each element of S_n is a product of disjoint cycles in S_n by **??**, it follows that the transpositions s_i generate S_n.

(b) We have

$$\begin{aligned}\sigma_{i,i+1}\circ\sigma_{i,i+1}(k) &= \begin{cases}\sigma_{i,i+1}(k) & \text{if } k\notin\{i,i+1\},\\ \sigma_{i,i+1}(i+1) & \text{if } k=i,\\ \sigma_{i,i+1}(i) & \text{if } k=i+1;\end{cases}\\ &= \begin{cases}k & \text{if } k\notin\{i,i+1\},\\ i & \text{if } k=i,\\ i+1 & \text{if } k=i+1;\end{cases}\\ &= k,\end{aligned}$$

so $\sigma_{i,i+1}^2 = 1$.

Now suppose $|i > j| > 1$. Then $\{i, i+1\}$ and $\{j, j+1\}$ are disjoint, so by **??**(b), the cycles $s_i = (i, i+1)$ and $s_j = (j, j+1)$ commute.

Now notice that

$$\begin{aligned}s_i s_{i+1}(k) = \sigma_{i,i+1}\circ\sigma_{i+1,i+2}(k) &= \begin{cases}\sigma_{i,i+1}(k) & \text{if } k\notin\{i+1,i+2\},\\ \sigma_{i,i+1}(i+2) & \text{if } k=i+1,\\ \sigma_{i,i+1}(i+1) & \text{if } k=i+2;\end{cases}\\ &= \begin{cases}i+1 & \text{if } k=1,\\ k & \text{if } k\notin\{i+1,i+2\}\\ i+2 & \text{if } k=i+1,\\ i & \text{if } k=i+2;\end{cases}\\ &= (i, i+1, i+2),\end{aligned}$$

as claimed. □

Exercise 3.7.5. This problem refers to the groups D_{2n} and Q_8 defined in Exercise 1.2.

(a) Prove that D_{2n} is isomorphic to

$$\langle x, y \mid x^n, y^2, xyxy\rangle.$$

(Recall this means $F(\{x,y\})/\langle x^n, y^2, xyxy\rangle^{\text{normal}}$.)

(b) Prove that Q_8 is isomorphic to

$$\langle x, y \mid x^4, y^2x^{-2}, y^{-1}xyx\rangle.$$

Solution.

(a) Define $\psi\colon \{x,y\} \to D_{2n}$ by $\psi(x) = \rho$, $\psi(y) = \tau$. Since $x \neq y$, this is a well-defined map. In addition, we have

$$\begin{aligned}\psi(x)^n &= \rho^n = 1,\\ \psi(y)^2 &= \tau^2 = 1,\\ \psi(x)\psi(y)\psi(x)\psi(y) &= \rho\tau\rho\tau = \rho\rho^{-1} = 1,\end{aligned}$$

so ψ respects the relations of $\langle x, y \mid x^n, y^2, xyxy\rangle$. Then by the universal property of presentation groups, there exists a unique group homomorphism $\varphi\colon \langle x, y \mid x^n, y^2, xyxy\rangle \to D_{2n}$ making the diagram

$$\begin{array}{ccc} \{x, y\} & \xrightarrow{\quad\psi\quad} & D_{2n} \\ {\scriptstyle i}\big\downarrow & & \big\uparrow{\scriptstyle \varphi} \\ F(\{x, y\}) & \xrightarrow[\pi]{} & \langle x, y \colon x^n, y^2, xyxy\rangle \end{array}$$

commute, where i is the inclusion and π is the canonical quotient map. We claim φ is an isomorphism.

We first show φ is surjective. Suppose we are given some element of D_{2n}, so that $\tau^i\rho^j$ for some integers i, j. Then φ maps y^ix^j of $\langle x, y \mid x^n, y^2, xyxy\rangle$ to $\tau^i\rho^i$, since

$$\begin{aligned} \varphi(y^ix^j) = \varphi(\pi(y)^i\pi(x)^j) &= \varphi(\pi(y))^i\varphi(\pi(x))^j \\ &= \varphi(\pi(i(y)))\varphi(\pi(i(x))) = \psi(y)^i\psi(x)^j = \tau^i\rho^j. \end{aligned}$$

Hence φ is surjective.

We now show $|\langle x, y \mid x^n, y^2, xyxy\rangle| \leqslant 2n$, and hence that φ is injective since $|D_{2n}| = 2n$. By the relation $y^2 = 1$ in G, any element of G has the form $x^{i_1}yx^{i_2}\cdots yx^{i_r}y$. Since $xy = yx^{-1}$ is also a relation, which implies $x^{i_j}y = yx^{-i_j}$, the arbitrary element simplifies further as

$$\begin{aligned} x^{i_1}yx^{i_2}\cdots x^{i_r}y &= yx^{-i_1}x^{i_2}yx^{i_3}y\cdots x^{i_r}y \\ &= y^2x^{i_1-i_2+i_3}yx^{i_4}\cdots x^{i_r} \\ &= y^3x^{-i_1+i_2-i_3+i_4}yx^{i_4}\cdots x^{i_r}y \\ &= \vdots \\ &= y^Mx^N, \end{aligned}$$

for some integers M, N. So, the elements of G are contained in the set $\{y^Mx^N \mid M, N \text{ are integers}\}$. But $y^2 = x^n = 1$ in G, so the underlying set of G is contained in the set

$$\{y^ix^j \mid i \in \{0, 1\}, j \in \{0, 1, \ldots, n-1\}\}.$$

But the relation $x^{n-1} = yxy$ gives that for all $j \in \{0, 1, \ldots, n-1\}$, $yx^{-j} = x^jy$ and $x^{-j} = x^{n-j}$ are elements of the set

$$\mathcal{E} \coloneqq \{y^ix^j \mid i \in \{0, 1\}, j \in \{0, 1, \ldots, n-1\}\},$$

which hard cardinality $2n$. We now have a surjective map from the set $\mathcal{E}$ of cardinality $\leqslant 2n$ onto a set of cardinality $2n$, and hence this is a bijection. Thus $\varphi\colon \langle x, y \mid x^4, y^2, xyxy\rangle \to D_{2n}$ is a group isomorphism. This completes the proof.

(b) Define $\psi\colon \{x, y\} \to Q_8$ by $\psi(x) = -i, \psi(y) = j$. Now, $-i \neq j$ in Q_8, so ψ is a well-defined set map. We have $\psi(x)^4 = \psi(y)^2\psi(x)^{-2} = (j^2)(-i^2) = (-1)\cdot(-1) = 1$, and

$$\psi(y)^{-1}\psi(x)\psi(y)\psi(x) = (j)^{-1}(-i)(j)(-i) = (-jiji) = -(-k)^2 = -(-1)^2 = 1.$$

By the universal property of presentation groups, there exists a unique $\varphi\colon \langle x, y \mid x^4y^2x^{-2}y^{-1}xyx\rangle \to Q_8$ making the diagram

$$\begin{array}{ccc} \{x, y\} & \xrightarrow{\quad\psi\quad} & Q_8 \\ \big\downarrow & & \big\uparrow{\scriptstyle \varphi} \\ F(\{x, y\}) & \xrightarrow[\pi]{} & \langle x, y \mid x^4, y^2x^{-2}, y^{-1}xyx\rangle \end{array}$$

commute. First note that φ is surjective. Indeed, $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, and by using that φ is a group homomorphism, we see that $\varphi(1) = 1, \varphi(x^2) = -1, \varphi(yx) = -k$, $\varphi(x^2yx) = k, \varphi(x^2)\varphi(x) = i, \varphi(x) = -i, \varphi(y) = j$, and $\varphi(x^2y) = -j$. We now have a surjective map φ onto the order 8 set Q_8, so to show φ is injective it is enough to show $|\langle x, y \mid x^4, y^2x^{-2}, y^{-1}xyx\rangle| \leqslant 8$.

It now only remains to show $|\langle x, y \mid x^4, y^2x^{-2}, y^{-1}xyx\rangle| \leqslant 8$. A general element of $|\langle x, y \mid x^4, y^2x^{-2}, y^{-1}xyx\rangle| \leqslant 8$ takes the form $x^{i_1}y^{j_1}\cdots x^{j_r}y^{j_r}$ for some integers $i_1, j_1, \ldots, i_r, j_r$. Using the relation $yx^{-1} = xy$ and arguing as in part (a), we can move the ys to the right and the xs to the left, which means we can write this element as x^My^N for some integers M, N. The relations $x^4 = 1$ and $y^2 = x^2$ imply $y^4 = x^4 = 1$. Then together with the last relation $y = xyx$, we obtain

$$y^2 = xyx^2yx = xyx^{-2}yx = xyy^{-2}yx = x^2,$$

and more generally,

$$x^My^N = x^Mx^2x^{-2}y^N = x^Mx^{-2}y^2y^N = x^{M-2}y^{N+2}.$$

Lastly, note that we can write everything in powers $M, N \in \{0, 1, 2, 3\}$, because $x^{-1} = x^3$ and $y^{-1} = y^3$ follow from our findings above. This leaves us with the following possible elements, which we cross out with something they equal that is not already crossed out:

1	y	~~y^2~~ $\to x^2$	~~y^3~~ $\to x^2y$
x	xy	~~xy^2~~ $\to x^3$	~~xy^3~~ $\to x^3y$
x^2	x^2y	~~x^2y^2~~ $\to 1$	~~x^2y^3~~ $\to y$
x^3	x^3y	~~x^3y^2~~ $\to x$	~~x^3y^3~~ $\to xy$

It follows that $|\langle x, y \mid x^4, y^2x^{-2}, y^{-1}xyx\rangle| \leqslant 2n$, and hence φ is bijective. Thus $\varphi\colon \langle x, y \mid x^4, y^2x^{-2}, y^{-1}xyx\rangle \to Q_8$ is a group isomorphism by our previous remarks. This completes the proof. □

The following exercise presents the Universal Mapping Property of the Abelianization of a group G.

Exercise 3.7.6. Let G be any group. Define the **abelianization** G^{ab} of G to be $G^{\text{ab}} = G/[G, G]$, with the canonical quotient map $\pi\colon G \to G^{\text{ab}}$.

(a) Prove that G^{ab} is abelian.

(b) Prove that for any abelian group A and any group homomorphism $\varphi : G \to A$, there is a unique $\overline{\varphi}\colon G^{\text{ab}} \to A$ such that

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & A \\ {\scriptstyle\pi}\downarrow & \nearrow_{\overline{\varphi}} & \\ G^{\text{ab}} & & \end{array}$$

commutes, and the assignment $\varphi \mapsto \overline{\varphi}$ induces a bijection

$$\text{Hom}_{\text{Grp}}(G, A) \xrightarrow{\cong} \text{Hom}_{\text{Grp}}(G^{\text{ab}}, A).$$

Solution. We first need to show that $[G, G]$ is a normal subgroup of G, so that $G^{\text{ab}}/[G, G]$ is indeed a group. We will do this in two lemmas:

Lemma 3.7.7. If G is a group, then

$$[G, G] = \left\{ \prod_{i=1}^{n} [a_i, b_i] \,\middle|\, n_i \geqslant 0 \text{ and } a_i, b_i \in G \text{ for all } 1 \leqslant i \leqslant n \right\}. \qquad \square$$

Proof. Define a set T by

$$T = \left\{ \prod_{i=1}^{n} [a_i, b_i] \,\middle|\, n_i \geqslant 0 \text{ and } a_i, b_i \in G \text{ for all } 1 \leqslant i \leqslant n \right\}.$$

We claim $T = [G, G]$.

- $T \subset [G, G]$: Let S be the collection of elements of G of the form $[a, b]$ for some $a, b \in G$, so that $[G, G] = \langle S \rangle$. If $H < G$ contains S, then for all $[a, b], [c, d] \in S$, we have $[a, b], [c, d] \in H$ because H is a subgroup of G. Similarly, finite products of commutators of G lie in H. Thus $T \subset H$. Since H was an arbitrary subgroup containing S, and $[G, G]$ is the intersection over all such subgroups, we have
$$T \subset \bigcap\nolimits_{S \subset H < G} [G, G].$$

- $[G, G] \subset T$: To show $[G, G]$ is contained in T, it is enough to show T is a subgroup of G containing S. We already know T contains S, so it suffices to show T is a subgroup of G. It is enough to show $(\prod_{i=1}^{n} [a_i, b_i])(\prod_{j=1}^{m} [c_j, d_j])^{-1} \in T$ for any $n, n' \geqslant 0$ and any elements $a_i, b_i, c_j, d_j \in G$ for all $1 \leqslant i \leqslant n$ and $1 \leqslant j \leqslant n'$. First note that if $[a, b]$ is the commutator of elements $a, b \in G$, then $[a, b]^{-1} = [b, a]$; we can see this by writing
$$[a, b][b, a] = aba^{-1}b^{-1}bab^{-1}a^{-1} = 1 = bab^{-1}a^{-1}aba^{-1}b^{-1} = [b, a][a, b].$$
It follows that
$$\begin{aligned} \left(\prod_{i=1}^{n} [a_i, b_i] \right) \left(\prod_{j=1}^{m} [c_j, c_i] \right)^{-1} &= \left(\prod_{i=1} [a_i, b_i] \right) \left(\prod_{j=1}^{m} [c_{m-j}, d_{m-j}] \right) \\ &= \left(\prod_{i=1} [a_i, b_i] \right) \left(\prod_{j=1}^{m} [d_{m-j}, c_{m-j}]^{-1} \right), \end{aligned}$$
which is an element of T. Thus $T < G$, so we are done by our initial remarks. □

Lemma 3.7.8. Let G be a group. Then $[G, G] \lhd G$.

Proof. Suppose we are given an element of T, which by **??** we can write as $(\prod_{i=1}^{n} [a_i, b_i])$ for some $n \geqslant 0$ and $a_i, b_i \in G$ for each $1 \leqslant i \leqslant n$. Then for any $g \in G$, we can write
$$\begin{aligned} g \left(\prod_{i=1}^{n} [a_i, b_i] \right) g^{-1} &= g[a_1, b_1][a_2, b_2] \cdots [a_n, b_n] g^{-1} \\ &= g[a_1, b_1] g^{-1} g[a_2, a_3] g^{-1} \cdots g[a_n, b_n] g^{-1} \\ &= \left(\prod_{i=1}^{n} g[a_i, b_i] g^{-1} \right) \\ &= \left(\prod_{i=1}^{n} [g a_i g^{-1}, g b_i g^{-1}] \right), \end{aligned}$$
where we used that for any $a, b \in G$,
$$\begin{aligned} [gag^{-1}, gbg^{-1}] &= gag^{-1}gbg^{-1}(gag^{-1})^{-1}(gbg^{-1})^{-1} \\ &= gabg^{-1}ga^{-1}g^{-1}gb^{-1}g^{-1} \\ &= gaba^{-1}b^{-1}g^{-1} \\ &= g[a, b]g^{-1}. \end{aligned}$$
Thus $[G, G] \lhd G$. □

(a) By **??**, the set $G^{\text{ab}} = G/[G, G]$ of left cosets of $[G, G]$ forms a group under left coset multiplication. To show G^{ab} is an abelian group, let $a[G, G]$ and $b[G, G]$ be arbitrary elements of G^{ab}. Then
$$\begin{aligned} [a[G, G], b[G, G]] &= a[G, G]b[G, G](a[G, G])^{-1}(b[G, G])^{-1} \\ &= a[G, G]b[G, G]a^{-1}[G, G]b^{-1}[G, G] \end{aligned}$$

$$\begin{aligned} &= aba^{-1}b^{-1}[G,G] \\ &= [a,b][G,G] \\ &= 1 \cdot [G,G], \end{aligned}$$

where the last equality holds because $[a,b] \in [G,G]$ (since if $[a,b] \in \{[x,y] \mid x,y \in G\} =: S$, then $[a,b]$ is in any subgroup containing S, and hence in the intersection taken over all such subgroups). It follows that the commutator of any two elements of G is the identity $1 \cdot [G,G]$, so G^{ab} is abelian.

(b) Let A be an abelian group and let $\varphi\colon G \to A$ be a group homomorphism.

– $\overline{\varphi}(g[G,G]) \coloneqq \varphi(g)$ *is well-defined*: If $g[G,G] = g'[G,G]$ in G^{ab}, then

$$\begin{aligned} \overline{\varphi}(g[G,G]) = \varphi(g') &= \varphi\Big(g \textstyle\prod_{i_1}^{n} [a_i,b_i]\Big) \\ &= \varphi(g) \textstyle\prod_{i=1}^{n} \varphi([a_i,b_i]) = \varphi(g) \prod_{i=1}^{n} [\varphi(a_i),\varphi(b_i)] \\ &= \varphi(g) \textstyle\prod_{i=1}^{n} 1 = \varphi(g') = \varphi(g'[G,G]), \end{aligned}$$

where we used that $[\varphi(a_i),\varphi(b_i)] = 1$ for each $1 \leqslant i \leqslant n$, since A is an abelian group. It follows that $\overline{\varphi}$ is well-defined.

– $\overline{\varphi}(g[G,G]) \coloneqq \varphi(g)$ *is a group homomorphism*: If $g[G,G], g'[G,G] \in G^{\mathrm{ab}}$, then

$$\overline{\varphi}(g[G,G]g'[G,G]) = \varphi(gg') = \varphi(g)\varphi(g') = \overline{\varphi}(g[G,G])\overline{\varphi}(g'[G,G]),$$

where we used that φ is a group homomorphism. Thus $\overline{\varphi}$ is a group homomorphism.

– *The given diagram commutes*: Indeed, for any $g \in G$, we have $\overline{\varphi} \circ \pi(g) = \overline{\varphi}(g[G,G]) = \varphi(g)$. Hence $\overline{\varphi} \circ \pi = \varphi$, so the given diagram commutes.

– $\overline{\varphi}$ *is the unique group homomorphism with the above properties*: Suppose $\psi\colon G^{\mathrm{ab}} \to A$ were another such map. Then for each $g[G,G] \in G$, we can write

$$\psi(g[G,G]) = \psi \circ \pi(g) = \pi(g) = \overline{\varphi}(g[G,G]),$$

so since $g[G,G]$ was an arbitrary element of G^{ab}, $\psi = \overline{\varphi}$. Thus $\overline{\varphi}$ is the unique map with the above properties.

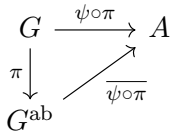
– *The assignment* $\varphi \mapsto \overline{\varphi}$ *is a bijection* $\mathrm{Hom}_{\mathrm{Grp}}(G,A) \xrightarrow{\cong} \mathrm{Hom}_{\mathrm{Grp}}(G^{\mathrm{ab}},A)$: We claim the inverse to the assignment $\varphi \mapsto \overline{\varphi}$ is the map sending group elements $\psi\colon G^{\mathrm{ab}} \to A$ of $\mathrm{Hom}_{\mathrm{Grp}}(G^{\mathrm{ab}},A)$ to the element $\psi \circ \pi\colon G \to A$ of $\mathrm{Hom}_{\mathrm{Grp}}(G,A)$, where π is the canonical quotient map $G \to G/[G,G] = G^{\mathrm{ab}}$. Indeed, for any $\varphi \in \mathrm{Hom}_{\mathrm{Grp}}(G,A)$, we have

$$\varphi \longmapsto \overline{\varphi} \mapsto \overline{\varphi} \circ \pi = \varphi,$$

where the equality is by the commutativity of the given diagram. On the other hand, if $\psi \in \mathrm{Hom}_{\mathrm{Grp}}(G^{\mathrm{ab}},A)$, then these assignments yield

$$\psi \longmapsto \psi \circ \pi \longmapsto \overline{\psi \circ \pi},$$

so it only remains to show $\overline{(\psi \circ \pi)} = \psi$. By our arguments from above, we know $\overline{\psi \circ \pi}$ is the unique group homomorphism making the diagram



commute. But the diagram

$$\begin{array}{ccc} G & \xrightarrow{\psi\circ\pi} & A \\ {\scriptstyle\pi}\downarrow & \nearrow_{\psi} & \\ G^{\mathrm{ab}} & & \end{array}$$

commutes, forcing $\psi = \overline{\psi \circ \pi}$. Hence these assignments are mutual inverses, so we conclude that the correspondence

$$\begin{aligned} \mathrm{Hom}_{\mathrm{Grp}}(G, A) &\longleftrightarrow \mathrm{Hom}_{\mathrm{Grp}}(G^{\mathrm{ab}}, A), \\ \varphi &\longmapsto \overline{\varphi}, \\ \psi \circ \pi &\longmapsfrom \psi, \end{aligned}$$

is a bijection.

Exercise 3.7.9. Compute D_{2n}^{ab}.

Solution. We showed in **??** that the underlying set of $[D_{2n}, D_{2n}]$ is the collection of all finite products of commutators of elements of D_{2n}. Suppose $\tau^i\rho^j$ and $\tau^k\rho^\ell$ are arbitrary elements of D_{2n}, so that $i, k \in \{0, 1\}$ and $j, \ell \in \{0, 1, \ldots, n-1\}$. Marking each location where we use the relation $\tau\rho^j = \rho^{-j}\tau$, we can write the commutator as

$$\begin{aligned} [\tau^i\rho^j, \tau^k\rho^\ell] &= \overline{\tau^i\rho^j}\,\overline{\tau^k\rho^\ell}\,\overline{\rho^{-j}\tau^i}\,\overline{\rho^{-\ell}\tau^k} \\ &= \rho^{-j}\,\overline{\tau^i\rho^{-\ell}}\,\tau^{i+k}\,\overline{\rho^j\tau^k}\,\rho^\ell \\ &= \rho^{\ell-j}\,\cancel{\tau^{2(i+k)}}\,\rho^{\ell-j} \\ &= \rho^{2(\ell-j)}. \end{aligned}$$

Thus $\langle\rho\rangle \subset [D_{2n}, D_{2n}]$. But $\ell, j \in \{0, 1, \ldots, n-1\}$ were arbitrary, so there are pairs of elements in D_{2n} whose commutator is any even power of ρ, so the reverse inclusion also holds. Thus $\langle\rho^2\rangle = [D_{2n}, D_{2n}]$. Since

$$|\langle\rho^2\rangle| = \begin{cases} n & \text{if } n \text{ is odd,} \\ n/2 & \text{if } n \text{ is even,} \end{cases}$$

we have

$$|D_{2n}^{\mathrm{ab}}| = |D_{2n}|/|[D_{2n}, D_{2n}]| = \frac{2n}{|\langle\rho^2\rangle|} = \begin{cases} 4 & \text{if } n \text{ is odd,} \\ 2 & \text{if } n \text{ is even.} \end{cases}$$

It follows that if n is even, then $D_{2n} \cong C_2$, where C_2 is the cyclic group of order 2. If n is odd, then

$$D_{2n}^{\mathrm{ab}} = \{[\rho], [\tau], [\tau\rho], [\rho\tau]\};$$

There are exactly two groups of order 4, namely the Klein 4-group, $C_2 \times C_2$, and C_4, the cyclic group of order 4. None of these elements have order 4, so D_{2n}^{ab} cannot be cyclic, and hence is the Klein-4 group. In summary,

$$D_{2n}^{\mathrm{ab}} \cong \begin{cases} C_2 & \text{if } n \text{ is even,} \\ C_2 \times C_2 & \text{if } n \text{ is odd.} \end{cases}$$

□

4 Group Actions

4.1 Background and Motivation

Definition 4.1.1. A (left) action of group on a set X is a group homomorphism $G \to S_G$, where S_G denotes the group $\mathrm{Aut}_{\mathrm{Set}}(X) = (\{\text{bijections } f\colon X \to X\}, \circ)$. Equivalently, a (left) group action is a map

$$\begin{aligned} \alpha\colon G \times X &\longrightarrow X \\ (g, x) &\longmapsto g \cdot x = \alpha(g, x), \end{aligned}$$

such that

- For all $g \in G$ and all $x \in X$, $(gh) \cdot x = g \cdot (h \cdot x)$, and
- For all $x \in X$, $1 \cdot x = x$.

Claim 4.1.2. To show the above definitions are equivalent, since given a group homomorphism φ, define $\alpha(g, x) = \varphi(g)(x)$, and given α, define φ by the same formula.

Proof. For a homomorphism φ, $\varphi(g, x) = \varphi(g)(x)$ is an action in the second sense, because

$$(gx) \cdot x = gx\varphi(gh) = (\varphi(g) \circ \varphi(h))(x) = g \cdot (h \cdot x),$$

and $\varphi(1) = 1$, so $1 \cdot x = \varphi(1)(x) = \mathrm{id}_X(x) = x$. Conversely, given α, the same check shows that setting $\varphi(g)(x) = g \cdot x$ gives a group homomorphism $G \to \mathrm{Aut}(X)$ (by condition (i)), and $\varphi(g)$ is a bijection for all $g \in G$ because $\varphi(g^{-1})$ is an inverse: for all $x \in X$,

$$\varphi(g) \circ \varphi(g^{-1})(x) = \varphi(g)(g^{-1} \cdot x) = g \cdot (g^{-1} \cdot x) \overset{\text{(i)}}{=} (gg^{-1}) \cdot x = 1 \cdot x \overset{\text{(ii)}}{=} x,$$

so

$$\varphi(g) \circ \varphi(g^{-1}) = \mathrm{id}_X,$$

and likewise $\varphi(g^{-1}) \circ \varphi(g) = \mathrm{id}_X$. □

Definition 4.1.3. For any group $(H, \cdot)$, the **opposite group** $(H^{\mathrm{op}}, *)$ is the group with underlying set H and operation $g * h = h \cdot g$.

Remark 4.1.4. We sometimes also consider right actions of G on X. A **right-action** of G on X is equivalently

(1) a group homomorphism $\varphi\colon G \to \mathrm{Aut}_{\mathrm{Set}}(X)^{\mathrm{op}}$, that is, $\varphi(g) * \varphi(h) = \varphi(h) \circ \varphi(g)$, where $*$ is the op relation, or

(2) a map $\alpha\colon X \times G \to X$ such that

  (i) For all $g \in G$ and all $x \in X$, $x \cdot (gh) = (x \cdot g) \cdot h$, and

  (ii) For all $x \in X$, $x \cdot 1 = x$.

Any right action $(x, g) \mapsto x \cdot g$ can be converted into a left action by defining

$$g \cdot x = x \cdot g^{-1}.$$

In the language of group homomorphisms, this amounts to composing the isomorphism $\mathrm{Aut}_{\mathrm{Set}}(X) \cong \mathrm{Aut}_{\mathrm{Set}}(X)^{\mathrm{op}}$ with the inverse of the map $\mathrm{Aut}_{\mathrm{Set}}(X)^{\mathrm{op}} \to \mathrm{Aut}_{\mathrm{Set}}(X)$ sending $f \mapsto f^{-1}$. (For any group H, H is isomorphic to H^{op} by the map $h \mapsto h^{-1}$. This is straightforward to show, and is left as an exercise.)

Notation 4.1.5. We will sometimes write $G \curvearrowright X$ to mean that G acts on X. Going forward, unless we specify otherwise, all actions are assumed to be left actions.

4.2 Examples of Group Actions

Example 4.2.1. Where k is any field (or in fact ring), the group $\mathrm{GL}_n(k) \curvearrowright k^n$ as invertible matrices left-multiplying column vectors. //

Example 4.2.2. $D_{2n} \curvearrowright \mathbb{R}^2$ as distance preserving maps $\mathbb{R}^2 \to \mathbb{R}^2$ preserving the vertices of a fixed regular n-gon (centered at 0, say). This can be interpreted with **??** as follows: There is a group homomorphism $r\colon D_{2n} \to \mathrm{GL}_2(\mathbb{R})$ given by

$$\begin{aligned}((2\pi j/n)\text{-rotation}) = \rho^j &\longmapsto \begin{pmatrix}\cos(2\pi j/n) & -\sin(2\pi j/n)\\ \sin(2\pi j/n) & \cos(2\pi j/n)\end{pmatrix},\\ \substack{\text{reflection of}\\ \text{the } x\text{-axis}} = \tau &\longmapsto \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix},\\ \tau\rho^j &\longmapsto \begin{pmatrix}\cos(2\pi j/n) & -\sin(2\pi j/n)\\ -\sin(2\pi j/n) & \cos(2\pi j/n)\end{pmatrix},\end{aligned}$$

where we assume that the n-gon has a vertex on the x-axis. This action is the action of $\mathrm{GL}_2(\mathbb{R}) \curvearrowright \mathbb{R}^2$ precomposed with $r\colon D_{2n} \to \mathrm{GL}_2(\mathbb{R})$.

It remains to check r is a homomorphism. We will use the usual presentation of D_{2n} given by $D_{2n} = \langle \rho, \tau \mid \rho^n, \tau^2, \tau\rho\tau\rho\rangle$. It suffices to define the set map

$$\begin{aligned}\{\rho,\tau\} &\xrightarrow{r^{\mathrm{set}}} \mathrm{GL}_2(\mathbb{R}),\\ r^{\mathrm{set}}(\varphi) &= \begin{pmatrix}\cos(2\pi/n) & -\sin(2\pi/n)\\ \sin(2\pi/n) & \cos(2\pi/n)\end{pmatrix},\\ r^{\mathrm{set}}(\tau) &= \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}.\end{aligned}$$

By the universal mapping property of presentation groups, we obtain a unique homomorphism $F(\{\rho,\tau\}) \xrightarrow{r} \mathrm{GL}_2(\mathbb{R})$ determined by $r(\varphi) = r^{\mathrm{set}}(\rho)$ and $r(\tau) = r^{\mathrm{set}}(\tau)$. It remains to check this is the r we wrote down, and to check that $r(\rho^n) = 1$, $r(\tau^2) = 1$, and $r(\tau\rho\tau\rho) = 1$. Having done that, r uniquely factors as

$$\begin{array}{ccc} F(\{\rho,\tau\}) & \xrightarrow{\ r\ } & \mathrm{GL}_2(\mathbb{R}) \\ \big\downarrow & \nearrow & \\ D_{2n} & & \end{array}$$

//

Example 4.2.3. $S_n \curvearrowright \{1,\dots,n\}$ by permutations. More generally, for any set X, $\mathrm{Aut}_{\mathrm{Set}} \curvearrowright X$ in the obvious way. //

Example 4.2.4. For any group G,

(a) $G \curvearrowright G$ by left multiplication, that is, $g \cdot h = gh$,

(b) G acts on G by conjugation, that is, for all $g \in G$ and all $x \in G$, $g \cdot x = gxg^{-1}$. (The corresponding homomorphism into $\mathrm{Aut}_{\mathrm{Set}}(G)$ appears on Homework 1). Note that this is indeed a left group action, since $g \cdot (h \cdot x) = g(hxh^{-1})g^{-1} = (g \cdot h) \cdot x$ and $1 \cdot x = 1x1^{-1} = x$.

(c) For any $H < G$, G acts on the set of left cosets G/H by left multiplication, that is, $g \cdot (xH) = (gx) \cdot H$. //

Example 4.2.5. Suppose G acts on sets X and Y. Then G acts on $\mathrm{Hom}_{\mathrm{Set}}(X,Y) = \{\text{set maps } f\colon X \to Y\}$ by

$$(g \cdot f)(x) = g \cdot_Y f(g^{-1} \cdot_X x), \qquad //$$

where $g \in G$, $x \in X$, $y \in Y$, and $f\colon X \to Y$ are given.

4.3 The Sign Homomorphism and the Alternating Group

We have seen $S_n \curvearrowright \{1,\dots,n\}$. Consider the related action of S_n on $\{\text{functions } f\colon \mathbb{Z}^n \to \mathbb{Z}\}$ given by $(\sigma \cdot f)(x_1,\dots,x_n) = f(x_{\sigma(1)},\dots,x_{\sigma(n)})$. (This is an action: $1 \cdot f = f$ is clear, and $((\sigma\tau)\cdot f)(x_1,\dots,x_n) = f(x_{\sigma\tau(1)},\dots,x_{\sigma\tau(n)})$, while $\sigma\cdot(\tau\cdot f)(x_1,\dots,x_n) = (\tau\cdot f)f(x_{\sigma(1)},\dots,x_{\sigma(n)})$.) Note that $\sigma\cdot(f+g) = \sigma\cdot f + \sigma\cdot g$ and $\sigma\cdot(fg) = (\sigma\cdot f)(\sigma\cdot g)$, where by fg we mean the usual product of f and g.

Now consider the element $\Delta\colon \mathbb{Z}^n \to \mathbb{Z}$ given by

$$\Delta = \prod\nolimits_{1\leqslant i<j\leqslant n}(x_i - x_j).$$

Claim 4.3.1. For all $\sigma \in S_n$, $\sigma(\Delta) = \varepsilon(\sigma)\Delta$ for a unique $\varepsilon(\sigma) \in \{\pm 1\}$.

Proof. *Existence of* $\varepsilon(\sigma)$: Since S_n is generated by transpositions and acts on $\{\mathbb{Z}^n \xrightarrow{f} \mathbb{Z}\}$, it suffices to show that for all transpositions $\tau = \begin{pmatrix} r & s \end{pmatrix}$ in S_n, we have $\tau\Delta = -\Delta$. We may assume $r < s$.

τ affects only the terms

$$\begin{cases} x_r - x_k & \text{if } r < k, \\ x_k - x_r & \text{if } k < r, \\ x_k - x_s & \text{if } k < s, \\ x_s - k_k & \text{if } s < k. \end{cases}$$

These can be grouped as

(1) $x_r - x_s$;

(2) $(x_r - x_k)(x_s - x_k)$ for $s < k$;

(3) $(x_k - x_r)(x_k - x_s)$ for $k < r$;

(4) $(x_r - x_k)(x_k - x_s)$ for $r < k < s$.

τ fixes (2), (3), (4), and $\tau(x_r - x_s) = -(x_r - x_s)$, so $\tau\Delta = -\Delta$.

Uniqueness of $\varepsilon(\sigma) \in \{\pm 1\}$: If $\sigma\Delta = \Delta$ and $\sigma\Delta = -\Delta$, then $0 = \sigma\Delta - \sigma\Delta = \Delta - (-\Delta) = 2\Delta$, so $\Delta = 0$. But Δ is a nonzero function, since for example $\Delta(1,2,\dots,n) = 1\cdot 2\cdot\cdots\cdot n$, which is nonzero. □

Lemma 4.3.2. The map $\varepsilon\colon S_n \to \pm 1$ is a group homomorphism. It is surjective for all $n \geqslant 2$.

Proof. For all $\sigma,\tau \in S_n$, $\varepsilon(\sigma\tau)\Delta = (\sigma\tau)(\Delta) = \sigma(\tau(\Delta)) = \sigma(\varepsilon(\tau)\Delta) = \varepsilon(\tau)\sigma(\Delta) = \varepsilon(\tau)\varepsilon(\sigma)\Delta$, so $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$. Thus ε is a group homomorphism. Showing surjectivity for all $n \geqslant 2$ is left as an exercise. □

Definition 4.3.3. The group homomorphism $\varepsilon\colon S_n \to \{\pm 1\}$ is called the **sign homomorphism**, and the **sign of a permutation** $\sigma \in S_n$ is the value of $\varepsilon(\sigma)$.

We define the **alternating group** on n elements, denoted A_n, by the kernel of ε, that is, the collection of elements of S_n with positive sign.

Lemma 4.3.4. A_n is generated by 3-cycles of S_n.

Proof. For all $i \neq j$, $\varepsilon(\begin{pmatrix} i & j \end{pmatrix}) = -1$. Any $\sigma \in A_n$ is a product of an even number of transpositions (since transpositions generate S_n, and $\varepsilon(\text{product of } k \text{ transpositions}) = (-1)^k$). So, it suffices to show any product $\begin{pmatrix} i & j \end{pmatrix}\begin{pmatrix} k & \ell \end{pmatrix}$ is in $\langle \text{all 3-cycles} \rangle$. There are three cases:

- If $\{i,j\} = \{k,\ell\}$, then $\begin{pmatrix} i & j \end{pmatrix}\begin{pmatrix} k & \ell \end{pmatrix} = 1 \in \langle \text{all 3-cycles} \rangle$, affirming the claim.
- If $|\{i,j\} \cap \{k,\ell\}| = 1$, say $j = k, i \neq \ell$, then $\begin{pmatrix} i & j \end{pmatrix}\begin{pmatrix} k & \ell \end{pmatrix} = \begin{pmatrix} i & j & k \end{pmatrix} \in \langle \text{all 3-cycles} \rangle$.
- If $\{i,j\} \cap \{k,\ell\} = \varnothing$, then $\begin{pmatrix} i & j \end{pmatrix}\begin{pmatrix} k & \ell \end{pmatrix} = \begin{pmatrix} i & j & k \end{pmatrix}\begin{pmatrix} j & k & \ell \end{pmatrix} \in \langle \text{all 3-cycles} \rangle$. □

4.4 Orbits, Stabilizers, and Special Group Actions

Definition 4.4.1. Let a group G act on a set X.

- For all $x \in X$ let $G \cdot x = \{g \cdot x \mid g \in G\} \subset X$. We call $G \cdot x$ the **orbit** of x (under G).
- For all $x \in X$, let $\text{Stab}(x) = \{g \in G \mid g \cdot x = x\}$. This is a subgroup of G (Check!), called the **stabilizer subgroup** (or **isotropy group**) of x in G.
- For all $x \in X$, let $X^g = \{x \in X \mid g \cdot x = x\}$. We call X^g the **fixed points** (of g).

Example 4.4.2. Let S_n act on $\{1, \dots, n\}$ by $\sigma \cdot x = \sigma(x)$.

- For all $x \in \{1, \dots, n\}$, $S_n \cdot x = \{1, \dots, n\}$.
- Let $x = n$. Then $\text{Stab}(n) = \{\text{permutations of } \sigma \text{ such that } \sigma(n) = n\} \cong S_{n-1}$ (isomorphic as groups).
- Let $g = (12, \cdots n)$. Then $X^g = \{i \in \{1, \dots, n\} \mid gi = i\} = \varnothing$ $(n \geqslant 2)$.
- Let $g = (12)$. Then $X^g = \{3, 4, \dots, n\}$ $(n \geqslant 3)$. //

Definition 4.4.3. Let G be any group and let X be any set.

(1) A group action of G on X is called **transitive** if there is only one orbit of G on X, that is, for all $x, y \in X$, there exists $g \in G$ such that $gx = y$.

(2) A group action of G on X is **faithful** if the associated homomorphism $G \to \text{Aut}_{\text{Set}}(X)$ is injective. That is, if you can identify G as a subgroup of $\text{Aut}_{\text{Set}}(X)$.

(3) A group action of G on X is **free** (think: "fixed-point free") if for all $x \in X$, $gx = x$ implies $g = 1$. That is, for all $x \in X$, $\text{Stab}(x) = \{1\}$.

Remark 4.4.4. Note that the kernel of the map $\alpha \colon G \to \text{Aut}_{\text{Set}}(X)$ associated to a group action of G on X is

$$\ker \alpha = \bigcap\nolimits_{x \in X} \text{Stab}_G(x),$$

so the corresponding group action is faithful if and only if the intersection of all stabilizers is trivial.

Example 4.4.5.

(1) $S_n \curvearrowright \{1, \dots, n\}$ is transitive and faithful. It is not free for $n \geqslant 3$, which can be seen by using the previous example.

(2) $\mathrm{GL}_n(\mathbb{C})$ by conjugation. This is not transitive since if $x = I_2$, $y \neq I_2$, then $gxg^{-1} = x \neq y$ for any $g \in \mathrm{GL}_n(\mathbb{C})$. It is not faithful because any scalar matrix of the form $\mathrm{diag}(z, z, \dots, z)$ for some $z \in \mathbb{C}^\times$ acts trivially by conjugation. And it is certainly not free, since free is a stronger condition than faithful. //

Lemma 4.4.6. Let $G \curvearrowright X$. Then

(1) For all $x \in X$, the action of G induces a bijection $G/\operatorname{Stab}(x) \xrightarrow{\cong} G \cdot x$, and

(2) For all $x \in X$ and all $a \in G$, we have a group isomorphism

$$\begin{aligned} \operatorname{Stab}(x) &\xrightarrow{\cong} \operatorname{Stab}(a \cdot x), \\ g &\longmapsto aga^{-1}. \end{aligned}$$

So, $\operatorname{Stab}(a \cdot x) = a \operatorname{Stab}(x) a^{-1} < G$.

Proof. The map $f \colon G \to X$ sending $g \mapsto g \cdot x$ has image contained in $G \cdot x$, so we can write f as a map $G \to G \cdot x$. We claim this factors through a bijection $\overline{f}$ as

$$\begin{array}{ccc} G & \xrightarrow{\quad f \quad} & G \cdot x \\ \downarrow & \nearrow_{\overline{f}} & \\ G/\operatorname{Stab}(x) & & \end{array}$$

Suppose $g, h \in G$. Then

$$g \cdot x = h \cdot x \iff h^{-1} g \cdot x = x \iff h^{-1} g \in \operatorname{Stab}(x) \iff g \operatorname{Stab}(x) = h \operatorname{Stab}(x),$$

which proves (1). For (2), note

$$\begin{aligned} g \in \operatorname{Stab}(x) &\iff g \cdot x = x \iff agx = ax \\ &\iff (aga^{-1}) \cdot ax = ax \iff aga^{-1} \in \operatorname{Stab}(a \cdot x), \end{aligned}$$

so the map of (2) is a bijection. We have already seen that conjugation is a group homomorphism, so this map is in fact an isomorphism. This completes the proof. □

4.5 Table of Common Group Actions

Several group actions are used so often that it is useful to remember what certain orbits, stabilizers, kernels, and properties they have. These are presented in **??**

Group	Set	Action	Orb(x)	Stab(x)	$\ker\alpha$
G	G	$g\cdot x = gx$	G	$\{1\}$	$\{1\}$
G	G	$g\cdot x = gxg^{-1}$	$\{gxg^{-1} \mid g\in G\}$	$C_G(x)$	$Z(G)$
G	$\mathcal{P}(G)$	$g\cdot S = gSg^{-1}$	gSg^{-1}	$N_G(S)$	$\bigcap_{S\in\mathcal{P}(S)} N_G(S)$
G	G/H	$g\cdot aH = gaH$	G/H	aHa^{-1}	$\bigcap_{a\in G} aHa^{-1}$
H	G	$h\cdot g = hg$	Hg	$\{1\}$	$\{1\}$

Table 2: Table of common group actions. Here G is any group, H is any subgroup of G, x is an arbitrary element of the set on which the group is acting, and $\alpha\colon G\to S_G$ is group homomorphism correspond to the given action. When we write $\mathcal{P}(G)$, we mean the collection of *nonempty* subsets of G.

4.6 Counting Lemmas

Write $G\backslash X$ for the set of orbits (equivalently, equivalence classes with respect to the equivalence relation $x\sim y$ if and only if there exists $g\in G$ such that $g\cdot x = y$).

Lemma 4.6.1. Let $G\curvearrowright X$.

(1) The orbits of G on X partition the set X:
$$X = \coprod_{G\cdot x\in G\backslash X} G\cdot x.$$
So in particular, $|X| = \sum_{G\cdot x\in G\backslash X}|G\cdot x|$.

(2) For all $x\in X$, $|G\cdot x| = [G:\mathrm{Stab}(x)] = |G|/|\mathrm{Stab}(x)|$.

(3) $|X| = \sum_{x\in G\backslash X}[G:\mathrm{Stab}(x)]$.

For all cardinality statements above, we assume all the relevant sets are finite.

Proof. Point (1) is immediate. Point (2) is by taking cardinalities from **??**. Point (3) follows from combining points (1) and (2). □

Example 4.6.2. Let G be a finite group and let G act on itself by conjugation. Then **??** tells us that
$$|G| = \sum_{\substack{\text{conjugacy}\\ \text{classes } C_x}}[G\,:\,\mathrm{Stab}(x)].$$
(We may sometimes write x to refer to the conjugacy class of x in G, when there is no ambiguity). To compute $\mathrm{Stab}(x)$, note
$$g\in\mathrm{Stab}(x) \iff gxg^{-1} = x \iff gx = xg \iff g\in C_G(x),$$
where $C_G(x)$ is the centralizer of x (that is, the centralizer of the cyclic subgroup generated by x). Observe that in the sum on the right-hand side, we have
$$[G:\mathrm{Stab}(x)] = 1 \iff C_G(x) = G \iff x\in Z(G),$$
where $Z(G)$ is the center of G. Thus we can write
$$|G| = |Z(G)| + \sum_{\substack{\text{non-trivial}\\ \text{conjugacy}\\ \text{classes } C_x}}[G:\mathrm{Stab}(x)].$$
This is called the **class equation** of G. //

The following is an application of the class equation (**??**):

Proposition 4.6.3. Let p be a prime and G a finite group such that $|G| = p^a$ for some $a \in \mathbb{Z}_{\geqslant 1}$. (We call such a group G a ***p*-group**). Then $Z(G) \neq \{1\}$.

Proof. Look at the class equation of G. All terms $[G : \mathrm{Stab}(x)]$ are either 1 or are divisible by p. If $Z(G) = \{1\}$, then we get

$$p^a = 1 + (\text{sum of terms each divisible by } p),$$

a contradiction, since the left-hand side is divisible by p, while the right-hand side is not. □

Lemma 4.6.4. Let G be a finite group acting on a finite set X. Then the number of orbits is the average number of fixed points. In other words,

$$|G\backslash X| = \frac{1}{|G|}\sum\nolimits_{g\in G} X^g = \frac{1}{|G|}\sum\nolimits_{x\in X}|\mathrm{Stab}(x)|.$$

Proof. Let $F = \{(g, x) \in G \times X \mid g \cdot x = x\}$. Then

$$|F| = \sum\nolimits_{g\in G}|X^g|.$$

On the other hand, we can instead range over the xs, to get

$$|F| = \sum\nolimits_{x\in X}|\mathrm{Stab}(x)|.$$

Recall by **??** that $|\mathrm{Stab}(x)| = |\mathrm{Stab}(a \cdot x)|$ for all $a \in G$, since these stabilizers are isomorphic. Thus

$$|F| = \sum\nolimits_{x\in X}|\mathrm{Stab}(x)| = \sum\nolimits_{x\in G\backslash X} \underbrace{|G \cdot x| \cdot |\mathrm{Stab}(x)|}_{= |G|, \text{ by } \textbf{??}} = |G\backslash X| \cdot |G|. \tag{4.6.4.1}$$

Combining **????**, we obtain

$$|G\backslash X| = \frac{1}{|G|}\sum\nolimits_{g\in G}|X^g|,$$

and the other equality in the lemma comes from dividing through by $|G|$ in (2). □

Example 4.6.5. Let G be the group of all symmetries of a tetrahedron T. What is G? Well, $G \curvearrowright X$, where $X = \{v_1, \ldots, v_4\}$ is the set of vertices v_j of T.

Fix $v_1 \in X$. Then by the Orbit-Stabilizer Theorem,

$$\begin{aligned} |G| &= |G \cdot v_1| \cdot |\mathrm{Stab}(v_1)| \\ &= 4 \cdot |\mathrm{Stab}(v_1)|. \end{aligned}$$

Denote by G_1 the subgroup of G given by $\mathrm{Stab}(v_1)$. Then $|G| = 4 \cdot |G_1|$. The group G_1 acts on the set $\{v_2, v_3, v_4\}$, and we can play the same game as before: fixing v_2 gives, by the Orbit-Stabilizer Theorem,

$$\begin{aligned} |G_1| &= |G_1 \cdot v_2| \cdot |\mathrm{Stab}(v_2)| \\ &= 3 \cdot |\mathrm{Stab}(v_2)| = 3 \cdot 2. \end{aligned}$$

Thus $|G| = 4 \cdot 3 \cdot 2 = 24$. So, it is reasonable to try to show $G \cong S_4$.

But we started with a group action, which equivalently is a group homomorphism $G \to S_4$. Since these are finite groups, to show this map is a bijection it is enough to show it is an injection, which is to say this group action is faithful. We then need to show for all $g \in G$, if $gx = x$ for all $x \in X$, then $g = 1$. But if g fixes all vertices, then g does nothing to the vertices, and hence g maps to the identity.

It is an exercise to the subgroup of rotations of G is A_4. Since A_4 is the only subgroup of S_4 of order 12 (Check!), it is enough to show the rotation subgroup has 12 elements and is not the whole group. Or perhaps you can show it contains all 3 cycles and is not the whole group. //

Example 4.6.6. Consider the group

$$G = \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, a, b, c, d \in \mathbb{Z}/2\mathbb{Z} \text{ and } ad - bc \neq 0 \right\}.$$

Then G acts on vectors in $(\mathbb{Z}/2\mathbb{Z})^2$. Write $\mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2$. Note

$$\mathbb{F}_2^2 = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}.$$

What are the orbits? For all $g \in G$, we need

$$g \cdot \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

On the other hand, if $g \cdot v = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, then $v = g^{-1} \cdot \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$. Hence the orbit of $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ is a singleton. Now notice that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ c \end{pmatrix}$$

Since we can choose $b, d \in \mathbb{C}$ freely so that the determinant is nonzero, we can obtain any of the remaining three vectors. Thus the other orbit is of size 3 and contains all elements of $\mathbb{F}_2^2$ other than the zero vector. Now the Orbit-Stabilizer Theorem says

$$|G| = \left| G \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right| \cdot \left| \mathrm{Stab} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right| = 3 \cdot \left| \mathrm{Stab} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right|.$$

To compute $\left| \mathrm{Stab} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right|$, suppose $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. The left-hand side equals $\begin{pmatrix} a \\ c \end{pmatrix}$, so $a = 1$ and $c = 0$. The only matrices $\begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix}$ with entries in $\mathbb{F}_2$ with nonzero determinant is either

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \text{or} \qquad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Thus $\left| \mathrm{Stab} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right| = 2$, so

$$|G| = \left| G \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right| \cdot \left| \mathrm{Stab} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right| = 3 \cdot 2 = 6.$$

Since G is non-abelian (Check!), it must be S_3, since S_3 is the only non-abelian group of order 6. But suppose we did not know this. If $g \in G$ and $g \cdot x = x$ for all $x \in X$, then does $g = 1$? Yes, because

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix},$$

which implies $\begin{pmatrix} a \\ c \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, so $a = 1$ and $c = 0$. //

Example 4.6.7. Let G be the group of rotations of the cube C. What is G? Let $= \{v_1, \ldots, v_8\}$ be the eight vertices of C. Then G acts on V, so by the Orbit-Stabilizer Theorem we have

$$|G| = |G \cdot v_1| \cdot |\mathrm{Stab}(v_1)|.$$

We can rotate the cube however we please, so there exist $g \in G$ sending v_1 to any vertex of our choice. Thus $|G \cdot v_1| = 8$. What is $|\mathrm{Stab}(v_1)|$? This may be hard to compute, so let us instead

consider the action of G on the six faces of C. Let $F = \{F_1, \dots, F_6\}$ be the set of vertices of G. Rolling a die can return any of the six faces of the cube, and rolling is just a rotation in G, so $|G \cdot F_1| = 6$. On the other hand, $|\text{Stab}(F_1)| = 4$ (Check!), so by the Orbit-Stabilizer Theorem we have

$$|G| = |G \cdot F_1| \cdot |\text{Stab}(F_1)| = 24.$$

Then clearly $G \neq S_6$, since $24 \neq 6!$. It turns out that $G \cong S_4$. This can be seen either by embedding the tetrahedron in the cube in a particular way and appealing to **??** above, or by considering a certain 4 diagonals between vertices of the cube. //

Example 4.6.8. Consider $G = S_n$ and

$$X = \left\{ \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} \dots, \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \right\} = \{e_1, \dots, e_n\}.$$

There is a group action $S_n \curvearrowright \text{GL}_n(\mathbb{R})$, for example, for $n = 4$, with $g = (1234)$ that sends $ge_1 = e_2$, $ge_2 = e_3$, $ge_3 = e_4$, and $ge_4 = e_1$. Thus g can be represented by the matrix

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

Similarly, $g = (12)(34)$ is represented by the matrix

$$\begin{pmatrix} & 1 & & \\ 1 & & & \\ & & & 1 \\ & & 1 & \end{pmatrix}$$

Call matrices where every row and every column has a single entry 1 and all other entries 1 the **permutation matrix**. A simple argument shows the n-by-n permutation matrices are in bijection with S_n. If $g \in S_n$, then $\varphi(g) \in \text{GL}_n(\mathbb{R})$, so a natural question to then ask is the value of $\det(\varphi(g))$? Since we can obtain to the identity by a sequence of swapping rows and columns, and each such swap flips the sign of the determinant, $\det(\varphi(g)) \in \{\pm 1\}$. This means that the diagram

$$\begin{array}{ccc} G = S_n & \xrightarrow{\varphi} & \text{GL}_n(\mathbb{R}) \\ {\scriptstyle \det}\downarrow & & \downarrow{\scriptstyle \det} \\ \{\pm 1\} & \hookrightarrow & \mathbb{R} \end{array}$$

commutes. It turns out that this is because the definition of the sign homomorphism in terms of the map Δ is precisely the definition of the determinant in terms of signs of permutations of the rows and columns of that matrix! //

4.7 Homework 3

Exercise 4.7.1. Consider an element σ of the symmetric group S_n with cycle decomposition

$$\sigma = (i_1 \cdots i_{r_1})(i_{r_1+1} \cdots i_{r_1+r_2}) \cdots (i_{r_1+\cdots r_{k-1}+1} \cdots i_{r_1+\cdots+r_k}).$$

Here we may assume that $r_1 \leqslant r_2 \leqslant \cdots r_k$ and $r_1 + \cdots + r_k = n$ (we include cycles of length 1), and that the integers $i_1, \dots, i_n$ are distinct; we then call the sequence of cycle lengths $(r_1, \dots, r_k)$ the **cycle type** of σ.

(a) Let τ be any element of S_n. Show that
$$\tau\sigma\tau^{-1} = (\tau(i_1)\cdots\tau(i_{r_1}))(\tau(i_{r_1+1})\cdots\tau(i_{r_1+r_2}))\cdots(\tau(i_{r_1+\cdots+r_{k-1}+1})\cdots\tau(i_{r_1+\cdots r_k})).$$

(b) Deduce that two elements of S_n are conjugate if and only if they have the same cycle type, and thus that conjugacy classes in S_n are in bijection with partitions of n, that is, with decompositions $n = r_1 + \cdots + r_k$ with $r_1 \leqslant r_2 \leqslant \cdots \leqslant r_k$ positive integers summing to n.

Solution.

(a) First note
$$\tau\sigma\tau^{-1} = \tau(i_1\cdots i_{r_1})\tau^{-1}\tau(i_{r_1+1}\cdots i_{r_1+r_2})\tau^{-1}\cdots\tau(i_{r_1+\cdots+r_{k-1}+1}\cdots i_{r_1+\cdots+r_k})\tau^{-1}.$$
Thus it suffices to show the claim in the case σ is a cycle $(i_1,\ldots,i_r)$. That is, we want to show $\tau(i_1\cdots i_r)\tau^{-1} = (\tau(i_1)\cdots\tau(i_r))$. We have
$$\begin{aligned}\tau(i_1\cdots i_r)\tau^{-1}(q) &= \begin{cases}\tau(i_{k+1}) & \text{if } \tau^{-1}(q) = i_k \text{ for some } 1\leqslant k\leqslant r,\\ \tau(\tau^{-1}(q)) & \text{if } \tau^{-1}(q)\notin\{i_1,\ldots,i_r\};\end{cases}\\ &= \begin{cases}\tau(i_{k+1}) & \text{if } q = \tau(i_k) \text{ for some } 1\leqslant k\leqslant r,\\ q & \text{if } q\notin\{\tau(i_1),\ldots,\tau(i_r)\};\end{cases}\\ &= (\tau(i_1)\cdots\tau(i_r))(q),\end{aligned}$$
where the second equality follows from simplifying expressions and rewording conditionals, and the third equality is by definition of the r-cycle $(\tau(i_1)\cdots\tau(i_r))$. Since this holds for all $q\in\{1,\ldots,n\}$, we conclude $\tau(i_1\cdots i_r)\tau^{-1} = (\tau(i_1)\cdots\tau(i_r))$. This completes the proof.

(b) We first show that two elements of S_n are conjugate if and only if they have the same cycle type.

($\Rightarrow$) Suppose σ,σ' are conjugate, so that there exists $\tau\in S_n$ satisfying $\sigma' = \tau\sigma\tau^{-1}$. Then, where σ has cycle type $(r_1,\ldots,r_k)$ and is given by $\sigma = (i_1\cdots i_{r_1})\cdots(i_{r_1+\cdots+r_{k-1}+1}\cdots i_{r_k})$, we have
$$\begin{aligned}\sigma' &= \tau\sigma\tau^{-1}\\ &= \tau(i_1\cdots i_{r_1})(i_{r_1+1}\cdots i_{r_1+r_2})\cdots(i_{r_1+\cdots+r_{k-1}+1}\cdots i_{r_1+\cdots+r_k})\tau^{-1}\\ &= \tau(i_1\cdots i_{r_1})\tau^{-1}\tau(i_{r_1+1}\cdots i_{r_1+r_2})\tau^{-1}\cdots\tau(i_{r_1+\cdots+r_{k-1}+1}\cdots i_{r_1+\cdots+r_k})\tau^{-1}\\ &= (j_1\cdots j_{r_1})(j_{r_1+1}\cdots j_{r_1+r_2})\cdots(j_{r_1+\cdots+r_{k-1}+1}\cdots j_{r_1+\cdots+r_k}), \qquad \text{(by part (a))}\end{aligned}$$
where $j_\ell = \tau(i_\ell)$ for each $1\leqslant\ell\leqslant r_1+\cdots+r_k$. Thus σ' also has cycle type $(r_1,\ldots,r_k)$, as claimed.

($\Leftarrow$) Suppose σ,σ are both elements of S_n with cycle type $(r_1,\ldots,r_k)$. Then we can write
$$\sigma = (i_1\cdots i_{r_1})(i_{r_1+1}\cdots i_{r_1+r_2})\cdots(i_{r_1+\cdots+r_{k-1}+1}\cdots i_{r_1+\cdots+r_k})$$
and
$$\sigma' = (j_1\cdots j_{r_1})(j_{r_1+1}\cdots j_{r_1+r_2})\cdots(j_{r_1+\cdots+r_{k-1}+1}\cdots j_{r_1+\cdots+r_k}).$$
We are done by part (a) if there exists some τ such that $j_\ell = \tau(i_\ell)$ for all $1\leqslant\ell\leqslant r_1+\cdots+r_k$. But this restraint determines a well-defined element τ of S_n: to see this, define the map $\tau\colon\{1,\ldots,n\}\to\{1,\ldots,n\}$ by
$$\tau(q) = j_\ell \quad\text{when}\quad q = i_\ell.$$
By disjointness of the cycles in the cycle decompositions of σ and σ', we know $i_\ell\neq i_{\ell'}$ and $j_\ell\neq j_{\ell'}$ whenever $\ell\neq\ell'$. Since $r_1+r_2+\cdots+r_k = n$, it follows from the previous sentence

that each $q \in \{1, \dots, n\}$ can be written as $q = i_\ell = j_{\ell'}$ for some $1 \leqslant \ell, \ell' \leqslant r_1 + \cdots + r_k = n$. It follows that the assignment $i_\ell \mapsto j_\ell$ is a well-defined map from $\{1, \dots, n\} \to \{1, \dots, n\}$, so τ is well-defined. τ is injective, since to say that $\tau(i_\ell) = \tau(i_{\ell'})$ for some $\ell \neq \ell'$ means $j_\ell = j_{\ell'}$ for $\ell \neq \ell'$, contradicting the fact $j_\ell \neq j_{\ell'}$ for any $\ell \neq \ell'$. To see τ is bijective, note that since each $q \in \{1, \dots, n\}$ can be written as j_ℓ for some ℓ, we have $\tau(i_\ell) = j_\ell$. Hence τ is bijective, so $\tau \in S_n$.

We now show this implies conjugacy classes in S_n are in bijection with partitions of n. Consider the map sending the conjugacy class of any given $\sigma \in S_n$ of cycle type $(r_1, \dots r_k)$ to the partition $r_1 + \cdots + r_n$ of n. All elements of the conjugacy class have the same cycle type by the above argument, so this is a well-defined map from the conjugacy classes of S_n into the partitions of n. This map is injective, since if two conjugacy classes map to the same partition $r_1 + \cdots + r_n$, then the collection of elements in both classes share a cycle type, and thus are conjugate, and hence the conjugacy classes coincide. This assignment is surjective, since given a partition $r_1 + \cdots + r_k$ of n with $r_1 \leqslant \cdots \leqslant r_k$, the element of S_n that is the product of disjoint cycles $(1 \cdots r_1)((r_1 + 1) \cdots r_2)((r_{k-1} + 1) \cdots r_k)$ is assigned the partition $r_1 + \cdots + r_k$. Thus our assignment is a bijection between the conjugacy classes of S_n to partitions of n. □

Exercise 4.7.2. Prove that for all $n \geqslant 2$, S_n^{ab} is cyclic of order 2, with any transposition representing the non-identity coset. Hint: Show that the normal subgroup generated by the commutators contains all 3-cycles.

Solution. Let $n \geqslant 2$. The sign homomorphism $\varepsilon \colon S_n \to \{\pm 1\}$ is surjective for all $n \geqslant 2$, as we can always multiply by a transposition. It is then enough to show $[S_n, S_n] = A_n$, since then $S_n^{\text{ab}} = S_n/[S_n, S_n] = S_n/A_n \cong C_2$. Since any transposition is not an element of A_n, it would then follow that the non-identity element of S_n^{ab} can be represented by any transposition.

- $A_n \subset [S_n, S_n]$: This follows from showing $[S_n, S_n]$ contains all 3-cycles. Let $i, j, k \in \{1, \dots, n\}$ be distinct. Then $(kji) = (ijk)^2 = [(ij), (jk)]$, so since i, j, k were arbitrary, we conclude $[S_n, S_n]$ contains all 3-cycles.

- $[S_n, S_n] \neq S_n$: Let $\sigma, \tau \in S_n$ be arbitrary. Then
$$\begin{aligned} \operatorname{sgn}([\sigma, \tau]) &= \operatorname{sgn}(\sigma\tau\sigma^{-1}\tau^{-1}) = (\operatorname{sgn}\sigma)(\operatorname{sgn}\tau)(\operatorname{sgn}\sigma)^{-1}(\operatorname{sgn}\tau)^{-1} \\ &= (\operatorname{sgn}\sigma)(\operatorname{sgn}\sigma)^{-1}(\operatorname{sgn}\tau)(\operatorname{sgn}\tau)^{-1} = 1 \cdot 1 = 1. \end{aligned}$$
Hence $[\sigma, t] \in \ker \operatorname{sgn}$ for all $\sigma, \tau \in S_n$, so the subgroup of S_n generated by all such elements is as well, that is, $[S_n, S_n] \subset \ker \operatorname{sgn} = A_n$. This completes the proof. □

Exercise 4.7.3. Let G be a group. Show that G is isomorphic to a subgroup of $S_G = \{\text{bijections } f \colon G \to G\}$. For instance, when G is finite with n elements, this shows G is isomorphic to a subgroup of S_n. Hint: consider the action of G on itself by (left) multiplication.

Solution. Let $G \curvearrowright G$ by left multiplication, and denote by $\alpha \colon G \to S_G$ the corresponding group homomorphism. Given $g, g' \in G$, we have $g' \cdot g = g$ if and only if $g' = 1$, so $\operatorname{Stab}(g) = \{1\}$. Thus the kernel of α is given by
$$\ker \alpha = \bigcap\nolimits_{g \in G} \operatorname{Stab}(g) = \bigcap\nolimits_{g \in G} \{1\} = \{1\},$$
so α is injective. Then by the First Isomorphism Theorem,
$$G \cong G/\{1\} \cong G/\ker \alpha \cong \operatorname{im} \alpha < S_G,$$
so G is isomorphic to a subgroup of S_G. (This is known as **Cayley's Theorem**.)

In particular, when G is a finite group with n elements, so that we can write the underlying set of G as $G = \{g_1, \dots, g_n\}$, then $S_G \cong S_n$. (Indeed, any bijection of $G = \{g_1, \dots, g_n\}$ onto itself can be thought of as a bijection of set $\{1, \dots, n\}$, by composing with the bijection $g_j \to j$.) Thus G is isomorphic to a subgroup of S_n. □

Exercise 4.7.4. Let G be a finite group, and let p be the smallest prime dividing $|G|$. Show that any subgroup $H < G$ with index p (i.e., $|G/H| = p$) is normal. Hint: Consider an appropriate action of G. The possibilities for this include analyzing the orbit of the subgroup H under G-conjugation or analyzing the left multiplication action of G on G/H.

Solution. We provide three alternate solutions.

Proofs 1 and 2.

- Proof 1: Let $G \curvearrowright X = \{aHa^{-1} \mid a \in G\}$ by $g \cdot (aHa^{-1}) = (ga)H(ga^{-1})$. Then $|X| = \mathrm{Orb}(H) = 1 \iff H \lhd G$. We have $\mathrm{Stab}_G(H) = \{g \in G \mid gHg^{-1} = H\} = N_G(H)$. Now $\mathrm{Stab}_G(gHg^{-1}) = gN_G(H)g^{-1}$.
- Proof 2: Let $G \curvearrowright X = \{gH \mid g \in G\}$ by $g \cdot (aH) = gaH$. Then $|\mathrm{Orb}(H)| = |X| = |G : H| = p$, and $\mathrm{Stab}_G(gH) = gHg^{-1}$.
- End of Proofs 1 and 2: We want to show $|X| = 1$. But by the Orbit-Stabilizer Theorem,
$$|X| = |\mathrm{Orb}\, H| = [G : \mathrm{Stab}_G(H)] = [G : N_G(H)] = [G : H] = p.$$
Assume $|X| = p$, in which case $H = N_G(H)$. Then $G \curvearrowright X$ where $|X| = p$, so we get a group homomorphism $\varphi \colon G \to S_p$ with
$$\ker \varphi = \bigcap\nolimits_{x \in X} \mathrm{Stab}_G(x) \subset \mathrm{Stab}_G(H) = H.$$
Now $|G/\ker\varphi| \mid p!$ as a subgroup of S_p by Lagrange's Theorem, so since $p! = p(\text{ primes} < p\ )$ and $|G = p^a(\text{ primes} > p\ )|$, we conclude $|G/\ker\varphi| \mid p$. But $G \neq \ker\varphi$ because $\ker\varphi \subset H \subsetneq G$, so $|G/\varphi| = p$. Then $\ker\varphi \leqslant H \subset G$, so
$$[G : \ker\varphi] = p = [G : H],$$
and thus $H = \ker\varphi$. This completes the proof. □

Proof 3. Let $H \curvearrowright X$ by left multiplication. Then $\mathrm{Orb}(H) = \{H\}$, $\mathrm{Stab}_H(H) = H$, $|\mathrm{Orb}(gH)|$ divides $|G|$ and hence divides $|G|$, and $|\mathrm{Orb}(gH)| \leqslant p - 1$. Because $\mathrm{Orb}(H) = \{H\}$, $\mathrm{Orb}(gH) \cap \{H\} \neq \varnothing$. So $|\mathrm{Orb}(gH)| = 1$. Then $\mathrm{Orb}(gH) = \{gH\}$ for all $g \in G$.

Now for all $g \in G$ and all $h \in H$,
$$hgH = gH \iff g^{-1}hgH = H \iff g^{-1}hg \in H,$$
so $H \lhd G$. □

□

Exercise 4.7.5. For a field K and a positive integer n, we set $\mathrm{SL}_n(K) = \{g \in \mathrm{GL}_n(K) \mid \det(g) = 1\}$. This is a subgroup of $\mathrm{GL}_n(K)$ known as the special linear group. We write 1_n for the $n \times n$ identity matrix and E_{ij} for the $n \times n$ matrix that is 0 everywhere except for a 1 in the (i, j) position.

(a) Show that the elementary matrices of the form $1_n + cE_{ij}$ for some $1 \leqslant i \neq j \leqslant n$ and $c \in K$ generate $\mathrm{SL}_n(K)$. (Interpret multiplication by these as row and column operations.)

(b) Groups G satisfying the property $[G, G] = G$ are called **perfect**. When $K = \mathbb{C}$, show that $[\mathrm{SL}_n(\mathbb{C}), \mathrm{SL}_n(\mathbb{C})] = \mathrm{SL}_n(\mathbb{C})$ by showing the elementary matrices from part (a) are commuta-

tors. Deduce that $\mathrm{GL}_n(\mathbb{C})^{\mathrm{ab}}$ is isomorphic (via the determinant) to $\mathbb{C}^\times$.

Solution.

(a) Let S be the set of matrices of the form $1_n + cE_{ij}$ such that $1 \leqslant i \neq j \leqslant n$ and $c \in K$. Any $1_n + cE_{ij}$ has determinant 1, since it is either an upper triangular matrix (if $i < j$) or a lower triangular matrix (if $i > j$) with diagonal entries 1. Thus $S \subset \mathrm{SL}_n(K)$, so

$$\langle S \rangle \subset \mathrm{SL}_n(K).$$

It remains to show the reverse inclusion. To show this, it is enough to show A can be written as a product of elements of S. As $\det A = 1 \neq 0$, we know A is invertible. Thus A has reduced row echelon from 1_n, so because all elements of S are invertible, it is enough to show 1_n can be obtained from A by left and right multiplications from elements of S.

If $B = (cE_{ij})A$, then the (k, ℓ)-entry of B is

$$b_{k,\ell} = \sum_{r=1}^n (cE_{ij})_{k,r} a_{r,\ell} = \sum_{r=1}^n c\delta_{ik}\delta_{jr}a_{r\ell} = \begin{cases} 0 & \text{if } k \neq i, \\ ca_{j\ell} & \text{if } k = i. \end{cases}$$

Therefore,

$$(1_n + cE_{ij})A = A + (cE_{ij})A = \begin{pmatrix} a_{11} & a_{1j} & a_{1n} \\ a_{i1} + ca_{j1} & a_{ij} + ca_{jj} & a_{in} + ca_{jn} \\ a_{n1} & a_{nj} & a_{nn} \end{pmatrix}.$$

On the other hand, if $B = B(cE_{ij})$, then the (k, ℓ)-entry of B is

$$B_{k,\ell} = \sum_{r=1}^n a_{k,r}(cE_{ij})_{r,\ell} = \sum_{r=1}^n c\delta_{ir}\delta_{j\ell}a_{kr} = \begin{cases} 0 & \text{if } \ell \neq j, \\ ca_{ki} & \text{if } \ell = j. \end{cases}$$

Therefore,

$$A(1_n + cE_{ij}) = A + A(cE_{ij}) = \begin{pmatrix} a_{11} & a_{1j} + ca_{1i} & a_{1n} \\ a_{j1} & a_{jj} + ca_{ji} & a_{jn} \\ a_{n1} & a_{nj} + ca_{ni} & a_{nn} \end{pmatrix}.$$

Hence, left (resp. right) multiplication of A by $1_n + cE_{ij}$ is the row (resp. column) operation of adding row j scaled by c to row i (resp. adding column i scaled by c to row j).

We now need to show that, starting with

$$A = \begin{pmatrix} a_{11} & a_{1n} \\ & \ddots \\ a_{n1} & a_{nn} \end{pmatrix},$$

we can obtain 1_n by a sequence of left and right multiplications by elements of S. In the following, we will abuse notation by identifying entries of left and right multiples of A by elements of S as simply altering the elements of A.

– Step 1. Identify the smallest $1 \leqslant j \leqslant n$ such that column j of A is not equal to the jth

standard ordered basis vector e_j of $\mathbb{R}^n$.

- Step 2. Perform column operations to make $a_{jj} = 1$. Note that row j has some nonzero element a_{jk}, since otherwise $\det A = 0 \neq 1$. There are now two cases:
  - If $a_{jj} = 0$, then perform the column operation that adds $1/a_{ki}$ times column k to column j. This makes $a_{jj} = 1$.
  - If $a_{ii} \neq 0$, then perform the column operation that adds $(a_{ii} - 1)/a_{ki}$ times column k to column j. This makes $a_{jj} = 1$.
- Step 3. Zero out all entries $a_{\ell,j}$ below entry a_{jj} in column j by performing the column operation adding $1/a_{\ell,k}$ times row j to row ℓ. Any column to the left of column j has 0s in rows $1, \dots, j-1$ by our choice of j, so this does not change any entries in columns to the left of j.
- Step 4. Zero out all entries $a_{\ell,j}$ above entry $a_{j,j}$ in row j: To do this, add $1/a_{\ell,j}$ times column ℓ to column j. Since column ℓ is the standard basis vector e_ℓ, this zeroes out $a_{\ell,j}$ and affects nothing else. We have now transformed column j of A to the standard basis vector e_j. Let A' be this new matrix.

By repeatedly applying the above algorithm to A, we make all n columns the respective standard basis vector, and hence A is transformed to the identity matrix. By our initial remarks, this completes the proof.

(b) Let $i \neq j$ and $c \in K$, and pick $q \in \mathbb{C}$ such that $q \neq 0, 1$. Consider the diagonal matrix $A = \operatorname{diag}(a_1, \dots, a_n)$, where

$$a_j = \begin{cases} 1 & \text{if } k \neq i, j, \\ q & \text{if } k = i, \\ 1/q & \text{if } k = j. \end{cases}$$

As a diagonal matrix, $\det A$ is the product of its diagonal entries, so $\det A = q(1/q) = 1$. Thus $A \in \mathrm{SL}_n(\mathbb{C})$. Then A^{-1} is the matrix obtained from A by swapping the ith and jth diagonal entries.

Now consider the matrix $1_n + \left(\frac{c}{q-1}\right)E_{ij}$, which we already know from part (a) is an element of $\mathrm{SL}_n(\mathbb{C})$. Its inverse is $1_n - \left(\frac{c}{q-1}\right)E_{ij}$. Now

$$AB = A\left(1_n + \left(\frac{c}{q-1}\right)E_{ij}\right) = A + \left(\frac{cq}{q-1}\right)E_{ij},$$

and

$$A^{-1}B^{-1} = A^{-1}\left(1_n - \left(\frac{c}{q-1}\right)E_{ij}\right) = A^{-1} - \left(\frac{c}{q(q-1)}\right)E_{ij},$$

so

$$\begin{aligned} [A, B] &= ABA^{-1}B^{-1} \\ &= \left(A + q\left(\frac{c}{q-1}\right)E_{ij}\right)\left(A^{-1} - \frac{1}{q}\left(\frac{c}{q-1}\right)E_{ij}\right) \\ &= 1_n + \left(\frac{c}{q-1}\right)\left(qAE_{ij} - \frac{1}{q}E_{ij}A^{-1}\right) \\ &= 1_n + \frac{c}{q(q-1)}(q^2AE_{ij} - E_{ij}A^{-1}) \end{aligned}$$

$$= 1_n + c(q+1)E_{ij}.$$

Since we can choose $q, c \in \mathbb{C}$ with $q \neq 0, 1$ such that $c(q+1)$ is any given complex number, we have shown that any element of S can be written as a commutator of elements of $\mathrm{SL}_n(\mathbb{C})$.

It remains to show that the determinant map descends to a group isomorphism $\mathrm{GL}_n(\mathbb{C})^{\mathrm{ab}} \xrightarrow{\cong} \mathbb{C}^\times$. Recall that if $A \in \mathrm{GL}_n(\mathbb{C})$, then $\det(A^{-1}) = 1/\det A$. Therefore, for all $A, B \in [\mathrm{GL}_n(\mathbb{C}), \mathrm{GL}_n(\mathbb{C})]$, we have

$$\det([A,B]) = \det(ABA^{-1}B^{-1}) = (\det A)(\det B)(\det A)^{-1}(\det B)^{-1} = 1,$$

so $[A,B] \in \mathrm{GL}_n(\mathbb{C})$. We showed on Homework 2 that $[\mathrm{GL}_n(\mathbb{C}), \mathrm{GL}_n(\mathbb{C})]$ is the subgroup of finite products of commutators of $\mathrm{GL}(\mathbb{C})$, so, again using that the determinant is multiplicative, we have $[\mathrm{GL}_n(\mathbb{C}), \mathrm{GL}_n(\mathbb{C})] \subset \mathrm{SL}_n(\mathbb{C})$. Conversely, if $X \in \mathrm{SL}_n(\mathbb{C})$, then by the above argument there exist elements $A, B \in \mathrm{SL}_n(\mathbb{C})$ (and hence elements of $\mathrm{GL}_n(\mathbb{C})$) such that $X = [A,B]$, which means $X \in [\mathrm{GL}_n(\mathbb{C}), \mathrm{GL}_n(\mathbb{C})]$. This proves $[\mathrm{GL}_n(\mathbb{C}), \mathrm{GL}_n(\mathbb{C})] = \mathrm{SL}_n(\mathbb{C})$. Thus $\mathrm{GL}_n(\mathbb{C})^{\mathrm{ab}}$. As the determinant map $\det : \mathrm{GL}_n(\mathbb{C}) \to \mathbb{C}^\times$ is surjective, by the First Isomorphism Theorem the determinant map $\mathrm{GL}_n(\mathbb{C}) \to \mathbb{C}^\times$ descends to an isomorphism

$$\mathrm{GL}_n(\mathbb{C})^{\mathrm{ab}} = \mathrm{GL}_n(\mathbb{C})/\mathrm{SL}_n(\mathbb{C}) = \mathrm{GL}_n(\mathbb{C})/\ker(\det) \xrightarrow{\cong} \mathbb{C}^\times,$$

as claimed. □

5 Sylow Theorems

The Sylow Theorems are quite surprising, yet quite useful theorems in finite group theory. We will use group actions to prove them. They pertain to taking any given finite group G, picking a prime p dividing the order of G, and zooming into the "p-part" of the group.

5.1 Sylow p-Subgroups

Definition 5.1.1. Let G be a finite group, let p be a prime, and set $|G| = p^a \cdot m$ for some $m \in \mathbb{Z}_{\geqslant 1}$ not divisible by p, and $a \in \mathbb{Z}_{\geqslant 0}$. A **Sylow p-subgroup** of G is a subgroup H of G such that $|H| = p^a$. Let $\mathrm{Syl}_p(G)$ denote the set of p-Sylow subgroups of G ,and let $n_p(G)$ be the number $|\mathrm{Syl}_p(G)|$ of p-Sylow subgroups.

Theorem 5.1.2 (Sylow Theorems)**.** Let G be a finite group and let p be a prime number such that $|G| = p^a \cdot m$ for some $m \in \mathbb{Z}_{\geqslant 1}$ not divisible by p and $a \in \mathbb{Z}_{\geqslant 0}$. Then the following hold.

(I) $\mathrm{Syl}_p(G) \neq \varnothing$.

(II) Let K be *any* subgroup of G and $P \in \mathrm{Syl}_p(G)$. Then there exists some $g \in G$ such that $K \cap gPg^{-1} \in \mathrm{Syl}_p(K)$. Then in particular, if $P, Q \in \mathrm{Syl}_p(G)$, there exists $g \in G$ such that $gPg^{-1} = Q$. As another special case, if K is *any* p-subgroup of G, then $K < Q$ for some $Q \in \mathrm{Syl}_p(G)$.

(III) The number of p-Sylow subgroups, $n_p(G)$ satisfies

$$\begin{cases} n_p(G) \equiv 1, \\ n_p(G) \mid m, \\ n_p(G) = [G : N_G(P)] \text{ for any } P \in \mathrm{Syl}_p(G). \end{cases}$$

Warning 5.1.3. For a general finite group G and integer d dividing $|G|$, there is no reason to expect that G has a subgroup of order d. For instance, the group A_4 of order $12 = 2^2 \cdot 3$ has no subgroup of order 6. Indeed, suppose $H < A_4$ has order 6. (Then H has to be normal as an order 2 subgroup, but we will not use this.) Then H has an element σ of order 3 and an element τ of order 2 and $\langle\sigma\rangle \lhd H$. To see this we can use the Sylow theorems, or, using Sylow III, $n_3(H)$ must be congruent to 1 (mod 3), and on the other hand, $n_3(H) \mid 2$, and the only integer with this property is $n_3(H) = 1$. Hence, $\langle\sigma\rangle \lhd H$, using Sylow II. (Here we used that whenever $n_p(G) = 1$, that is, $\mathrm{Syl}_p(G)$ is a singleton, then by Sylow II we have $P \lhd G$.) Thus $\tau\sigma\tau^{-1} \in \{\sigma, \sigma^2\}$.

But the number of 3-cycles in A_4 is $\binom{4}{3} \cdot 2 = 8$ (since choose 3 elements to permute by the 3-cycle, and there are two nontrivial 3-cycles permuting those 3 numbers), and the remaining three non-identity elements of A_4 are products of 2 disjoint transpositions (since no product of disjoint transpositions can be a 3-cycle, as we showed on Homework 3), and those are (12)(34), (13)(24), and (14)(23). Thus

$$\tau = (ab)(cd) \text{ and } \sigma = (efg)$$

Then by Exercise 3.1, $\tau\sigma\tau^{-1} = (\tau(e)\tau(f)\tau(g))$. Hence the shape of τ is $\{e, f, g\} \neq \{\tau(e), \tau(f), \tau(g)\}$. In particular, $\tau\sigma\tau^{-1} \notin \{\sigma, \sigma^2\}$, a contradiction. Hence no subgroup $H < A_4$ of order 6 exists. ⁂

5.2 Proof of Sylow I

We are given a finite group $|G| = p^a \cdot m =: n$, where $p \nmid m$. Let

$$\mathcal{S} = \{\text{subsets } X \subset G \mid |X| = p^a\},$$

and let $G \curvearrowright \mathcal{S}$ by left multiplication. Take the orbit decomposition to get

$$\binom{n}{p^a} = |\mathcal{S}| = \sum_{\text{orbits } O} |O|. \tag{$*$}$$

Let us assume that p does not divide $\binom{n}{p^a}$, so that we can see why this fact is useful, and then we will come back to prove it with an elementary proof later. Since $\binom{n}{p^a} \nmid p$, we know something on the right-hand side of $*$ is not divisible by p, that is, some orbit of our group action, say $G \cdot X$ (for some $X \subset G$), has size *not* divisible by p. But by the Orbit-Stabilizer Theorem,

$$|G| = \underbrace{|G \cdot X|}_{\substack{\text{not divisible} \\ \text{by } p}} \cdot |\mathrm{Stab}(X)|,$$

so p^a must divide $|\mathrm{Stab}(X)|$. But also

$$|\mathrm{Stab}(X)| \mid |X|$$

is true for *any* subset $X \subset G$, since X is a union of right $\mathrm{Stab}(X)$-cosets. (Indeed, for any $x \in X$, by definition of the stabilizer subgroup of x, we have $\mathrm{Stab}(X) \cdot x \subset X$). We conclude (since $|X| = p^a$ for $X \in \mathcal{S}$) that

$$p^a = |\mathrm{Stab}(X)|,$$

and $\mathrm{Stab}(X) \in \mathrm{Syl}_p(G)$. This proves Sylow I, modulo the claim made above that $\binom{n}{p^a}$ is not divisible by p.

It only remains to show $\binom{n}{p^a}$ is not divisible by p. We have $n = p^a m$, where $m \nmid m$. Then

$$\binom{n}{p^a} = \frac{n(n-1)\cdots(n-p^a+1)}{p^a(p^a-1)\cdots 1}.$$

Observe that for any numerator term $n - k$, p divides $n - k$ the same number of times as the

corresponding denominator term $p^a - k$: to see this, write $k = p^i\ell$, where $0 \leqslant i \leqslant a-1$ and ℓ is coprime to p ($p \nmid \ell$) , so

$$n - k = p^a m - p^i \ell = p^i \boxed{(p^{a-i}m - \ell)},$$
$$p^a - k = p^a - p^i \ell = p^i \boxed{(p^{a-i} - \ell)}.$$

Both of the boxed terms are coprime to p since $a - i \geqslant 1$ and $p \nmid \ell$, so this completes the proof. □

5.3 Proof of Sylow II

Let $K < G$ be any subgroup and let $P \in \mathrm{Syl}_p(G)$. Such a P exists by Sylow I. We want $g \in G$ such that $K \cap gPg^{-1} \in \mathrm{Syl}_p(K)$. We consider the action of G on the set of left cosets G/P of P in G by left multiplication. Then for any $g \in G$, $\mathrm{Stab}(gP) = gPg^{-1}$, since

$$x \cdot gP = gP \iff x \in \mathrm{Stab}(gP) \iff x \in g\,\mathrm{Stab}(P)g^{-1} \iff x \in gPg^{-1}.$$

Now restrict the action to the subgroup K, to get an action $K \curvearrowright G/P$. We find

$$\mathrm{Stab}_K(gP) = K \cap \mathrm{Stab}_G(gP) = K \cap gPg^{-1}.$$

Taking the orbit decomposition for the action $K \curvearrowright G/P$, we get

$$|G/P| = \sum_{K\text{-orbits}} (|K|\text{-orbit}).$$

Since $P \in \mathrm{Syl}_p(G)$, $|G/P|$ is coprime to p, and thus there exists K-orbit with order coprime to p. Say $K \cdot gP$ is such an orbit. Then by the Orbit-Stabilizer Theorem,

$$|K| = \underbrace{|K \cdot gP|}_{\text{coprime to } p} \cdot |\mathrm{Stab}_K(gP)|,$$

so $K \cap gPg^{-1} = \mathrm{Stab}_K(gP)$ has all the p-divisibility in K, and therefore is an element of $\mathrm{Syl}_p(K)$, since it is a p-group and has $|K|/|\mathrm{Stab}_K(gP)|$ coprime to p. This completes the proof. □

5.4 Proof of Sylow III

We claim that

(1) $n_p(G) = [G : N_G(P)]$ for any $P \in \mathrm{Syl}_p(G)$,

(2) $n_p(G) \mid m$, and

(3) $n_p(G) \equiv 1 \pmod p$.

We will use both Sylow I and Sylow II here. Let $G \curvearrowright \mathrm{Syl}_p(G)$ by conjugation. By Sylow II, there is only one orbit, so $n_p(G) = [G : \underbrace{\mathrm{Stab}(P)}_{=N_G(P)}]$ for any $P \in \mathrm{Syl}_p(G)$.

For (2), $m = [G : P] = [G : N_G(P)] = [N_G(P) : P]$, so $n_p(G) \mid m$.

For (3), let $P \curvearrowright \mathrm{Syl}_p(G)$, again by conjugation, and consider its orbit decomposition. We claim that the only orbit with one element for this action is $\{P\}$. This claim implies the result, because then

$$n_p(G) = \sum_{\substack{\text{orbits } O \\ \text{of } P \text{ on} \\ \mathrm{Syl}_p(G)}} |O| = \sum_{\substack{O \text{ with} \\ |O|=1}} |O| + \sum_{\substack{O \text{ with} \\ |O|>1}} \underbrace{|O|}_{\substack{\text{all these are} \\ \text{divisible by } p}}.$$

Thus

$$n_p(G) \equiv |\{\text{orbits of } P \text{ on } \mathrm{Syl}_p(G) \text{ of size } 1\}| \pmod p,$$

so the claim would imply $n_p(G) \equiv 1 \pmod{p}$, which is what we want to show. We now show why the claim is true. To show the claim, let $Q \in \mathrm{Syl}_p(G)$ such that $\{Q\}$ is an orbit of P on $\mathrm{Syl}_p(G)$. Then for all $x \in P$, $xQx^{-1} = Q$, and hence $P < N_G(Q)$. Applying Sylow II to the group $N_G(Q)$, we find P and Q are both in $\mathrm{Syl}_p(N_G(Q))$. Then by Sylow II, P and Q are conjugate in $N_G(Q)$. That is, there exists $g \in N_G(Q)$ such that $P = gQg^{-1} = Q$, and this equality is because $g \in N_G(Q)$. □

5.5 Applications of the Sylow Theorems

Example 5.5.1. One can check that

$$A_4 = \{1\} \cup \left\{ \binom{4}{3} \cdot 2 = \text{eight 3-cycles} \right\} \cup \{(12), (34), (13)(24), (14)(23)\}.$$

By Sylow III,

$$\begin{cases} n_2 \equiv 1 \pmod{2} & \text{and } n_2 \mid 3 \implies n_2 \in \{1, 3\}, \\ n_3 \equiv 1 \pmod{3} & \text{and } n_3 \mid 4 \implies n_3 \in \{1, 4\}. \end{cases}$$

If $n_3 = 1$, then all eight 3-cycles would lie in the same Sylow 3-subgroup (which has order 3), a contradiction. Thus $n_3 = 4$.

And $n_2 = 1$, because $\{1, (12)(34), (13)(24), (14)(23)\}$ is a Sylow 2-subgroup, and any other Sylow 2-subgroup would have some other element in A_4 with some 2-power order, but none such exist. //

Corollary 5.5.2. Let G be a group and $P \in \mathrm{Syl}_p(G)$. Then $P \lhd G \iff n_p(G) = 1$.

Proof. ($\Rightarrow$) If $g \in G$ and $P \lhd G$, then $gPg^{-1} = P$. So if $P' \in \mathrm{Syl}_p(G)$, then by Sylow II there exists $g \in G$ such that $P = gPg^{-1} = P'$, so $n_p(G) = 1$.

($\Leftarrow$) Conversely, if $n_p(G) = 1$, then by Sylow II we have $gPg^{-1} = P$ for any $g \in G$. Thus $P \lhd G$. □

5.6 Showing A_5 is a Simple Group

Definition 5.6.1. A group is **simple** if it has no nontrivial proper normal subgroups.

Example 5.6.2. The groups $\mathbb{Z}/p\mathbb{Z}$ for any prime p and A_5 are simple groups. Simplicity of the former is clear, and we will show why A_5 is simple soon. (In fact, A_5 is the smallest non-abelian simple group.) //

Example 5.6.3. If $|G| = 20 = 2^2 \times 5$, then $n_5(G) = 1 \pmod{5}$ and $n_5(G) \mid 4$, so $n_5(G) = 1$. Thus G cannot be simple, since it has a normal subgroup of order 5. //

Example 5.6.4. Suppose $|G| = 6 = 2 \times 3$. Then $n_2(G) \in \{1, 3\}$ and $n_2(G) \mid_6$, so $n_3(G) = 1$. And

$$G \cong C_6, \text{ which has } n_3 = n_2 = 1,$$

and

$$G \cong D_6, \text{ which has } n_1 = n_2 = 3.$$ //

Example 5.6.5. Suppose $|G| = 15 = 3 \times 5$. Then $n_3(G) \equiv 1 \pmod{3}$ and $n_3(G) \mid 5$, so $n_3(G) = 1$. Showing $n_5(G) = 1$ is similar.

This gives us normal subgroups $P_3, P_5 \lhd G$. As these are cyclic of coprime order, we have

$$P_3 \cap P_5 = \{1\}.$$

Now $x \in P_5$, $y \in P_5$, and $1 = x(yx^{-1}y^{-1}) = (xyx^{-1})y^{-1} \in P_5$. (Why?) Now the product xy of the generators of P_3, P_5 generate $G \cong \mathbb{Z}/15\mathbb{Z}$, since

$$(xy)^i = x^i y^i = 1 \iff 3 \mid i \text{ and } 5 \mid i$$

We can use similar reasoning to show that if $p \neq q$ are primes and $p \not\equiv 1 \pmod{p}$, then any group of order pq is cyclic. //

Example 5.6.6. $|G| = 12 = 2^2 \times 3$. Then $n_2 \equiv 1 \pmod{2}$ and $n_2 \mid 3$. On the other hand, $n_3 \equiv 1 \pmod{3}$ and $n_3 \mid 4$. Intuitively, it would be surprising if G has 3 distinct Sylow 2 subgroups, *and* 4 distinct Sylow 3-subgroups, which motivates us to argue otherwise. Suppose $H_1, H_2, H_3, H_4 \in \mathrm{Syl}_3(G)$. Since 3 is prime and the H_i are distinct for $i = 1, 2, 3, 4$, any pair of these intersect trivially. (More generally, if $p = p^1$ is the maximal power of p dividing $|G|$, then all Sylow p-subgroups intersect trivially). This means there are $1 + 4 \cdot (3 - 1) = 9$ distinct elements in the H_js.

Since $n_2 \geqslant 1$, there exists $P \in \mathrm{Syl}_2(G)$. But P has order 4 since the largest power of 2 dividing 12 is 4, and hence $|P \cup \bigcup_{j=1}^4 H_j| = 12$, so there is no more room. Thus either $n_2 = 1$ or $n_3 = 1$. For example, $V_4 \lhd A_4$, where $V_4 = \{(12)(34), (14)(23), (13)(24), 1\}$, which is isomorphic to the **Klein-4 group** $C_2 \times C_2$. On the other hand, $\langle \rho^2 \rangle \lhd D_{12}$. //

Recall that if $N \lhd H$ and $H \lhd G$, it is false in general that $N \lhd G$. However, the situation for Sylow p-groups is much nicer:

Lemma 5.6.7. Let G be a group and $H \lhd G$. If $P \in \mathrm{Syl}_p(H)$, then $P \lhd G$. In other words,

$$\mathrm{Syl}_p(G) \ni P \lhd H \lhd G \implies P \lhd G.$$

Proof. Since $P \lhd H$, $n_p(H) = 1$. But if $g \in G$, then $gPg^{-1} \subset gHg^{-1} = H$, so gPg^{-1} is a subgroup of H with the same order as P. But only one such subgroup of H exists, so $gPg^{-1} = P$, and hence $P \lhd G$. □

Example 5.6.8. Suppose G is any group of order 30. We claim $|G|$ is not simple. $|G| = 30 = 2{\times}3{\times}5$, then

$$n_2 \in \{1, 3, 5, 15\},$$

$$n_3 \in \{1, 10\},$$

and

$$n_5 \in \{1, 6\}$$

We claim $n_3 = n_5 = 1$. Let $G \curvearrowright G$ by left multiplication. This induces a map

$$G \xrightarrow{\varphi} \mathrm{Aut}_{\mathrm{Set}}(G) \cong S_{30}.$$

[The idea here is to consider the commuting diagram

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & S_{30} \\ & \searrow^{\mathrm{sgn} \circ \varphi} & \downarrow \mathrm{sgn} \\ & & \{\pm 1\} \end{array}$$

Suppose $\mathrm{sgn} \circ \varphi$ is surjective. Then its kernel $N \lhd G$ has $|N| = 15$, so

$$N \cong \mathbb{Z}/15\mathbb{Z}$$

by **??** above. Then $P_3 \lhd N$ and $P_5 \lhd N$. But then by **??**, $P_3 \lhd G$ and $P_5 \lhd G$. And $n_3(G) = n_5(G) = 1$.]

Let $g \in G$ have order 2, and let $K = \langle g \rangle$. What are the orbits of G under the left multiplication action? Well, since

g has order 2, the orbits are $\{x, gx, g^2x, g^3x, \dots\} = \{x, gx, x, gx, \dots\} = \{x, gx\}$. As the orbits partition the group and each orbit has size 2, we know there are 15 orbits under this action $K \curvearrowright G$. As an element of S_{30}, g is a product of 15 transpositions. So, $\operatorname{sgn}(\varphi(g)) = -1$. The upshot is that if we have a group of order 30, it has a unique Sylow 3 subgroup and a unique Sylow 5-subgroup. //

The above examples show the following:

- $|G| = 6 \implies n_3 = 1$,
- $|G| = 12 \implies n_2$ or $n_3 = 1$,
- $|G| = 15 \implies n_3 = n_5 = 1$,
- $|G| = 12 \implies n_5 = 1$,
- $|G| = 30 \implies n_3 = n_5 = 1$.

Using these, we can show A_5 is simple:

Theorem 5.6.9. A_5 is a simple group.

Proof. Suppose $N \lhd G$ is nontrivial proper subgroup of A_5. Without loss of generality, $|N|$ is the minimal of these. Then

$$|N| \in \{2, 3, 4, 5, 6, 10, 12, 15, 30\}.$$

We now use the Sylow theorems, together with the above facts:

- Case 1: $5 \mid |N|$: If $P' \in \operatorname{Syl}_5(G)$ and $P \in \operatorname{Syl}_5(N)$, then there exists $g \in G$ such that $gPg^{-1} = P'$. But then $P' = gPg^{-1} \subset gNg^{-1}$. Hence every Sylow 5-subgroup of G is a Sylow 5-subgroup of N, which in particular means that $n_5(G) = n_5(N)$.

  Now $n_5(G) \in \{1, 6\}$. But $n_5(G) \neq 1$, since $A_5 \supset \langle (12345) \rangle = \langle (13245) \rangle$, so $n_5(A_5) = n_5(G) = 6$. So, N has 6 Sylow 5-subgroups, say $H_1, \dots H_6 \leqslant N$. But how many elements are there in these together? Well,

  $$|N| \geqslant \left| \bigcup_{j=1}^{6} H_i \right|.$$

  But $|N| = 30$, so $n_5(N) = 1$, a contradiction since we just showed $n_5(N) = 6$. We now have the remaining possibilities:

  $$|N| \in \{2, 3, 4, \cancel{5}, 6, \cancel{10}, 12, \cancel{15}, \cancel{30}\}.$$

- Case 2: $|N| = 6$ or $|N| = 12$. Then $|N|$ is not minimal. Assume $|N| = 2, 3, 4$. Then $|G/N| = 30, 20, 15$, $n_5(G/N) = 1$. So, the unique Sylow 5-subgroup of G/N, call it $\overline{P}_5$, is normal. Then by the Correspondence Theorem, the preimage $P \coloneqq \pi^{-1}(P_5) \lhd G$ and $5 \mid |P|$ (Why?). But we just showed in Case 1 that G cannot have a normal subgroup whose order is divisible by 5. (Check!) □

Remark 5.6.10. It turns out that A_5 is the *only* simple group of order 60, which we will soon show.

5.7 Cauchy's Theorem

Corollary 5.7.1 (Cauchy's Theorem)**.** Let G be a finite group with order divisible by a prime p. Then G contains an element (and hence a subgroup) of order p.

Proof. By Sylow I, there exists a Sylow p-subgroup $1 \neq P < G$. Let $y \in P \smallsetminus \{1\}$. Then $|y| \mid |P| = p^a$ by Lagrange's theorem, so $|y| = p^r$ for some $1 \leqslant r \leqslant a$. But then the element $y^{p^{r-1}} \in P$ has order p, so we are done. □

Corollary 5.7.2. Let G be a finite group with $|G| = p^a \mid m$, where $p \nmid m$. Then for each $1 \leqslant i \leqslant a$, there exists a subgroup $H_i < G$ of order p^i.

Proof. We induct on a, over all groups. The case $a = 0$ is clear. So assume the corollary is known for all groups G' such that $p^a \nmid G'$, that is, such that G' has order whose maximal power of p is strictly smaller than p^a.

Let G be as in the corollary, with $|G| = p^a m$ such that $p \nmid m$. By the Sylow I, there exists some $P \in \mathrm{Syl}_p(G)$. P is a non-trivial p-group (non-trivial since $a > 0$), so by a corollary to the Class Equation we know $Z(P) \neq \{1\}$. Then there exists an element $x \in Z(P)$ of order p by Cauchy's theorem. Since $\langle x \rangle$ is a subgroup of $Z(P)$, we have $\langle x \rangle \lhd P$ since its centrality in P implies $gxg^{-1} = x \in \langle x \rangle$ for all $g \in P$. We can then consider the quotient

$$P \twoheadrightarrow P/\langle x \rangle.$$

Moreover, $|P/\langle x \rangle| = p^{a-1}$, so the induction hypothesis applies to $G' = P/\langle x \rangle$, and hence to all $i = 1, \ldots, a$: There exists $\overline{H_i}$ such that $\left|\overline{H_i}\right| = p^{i-1}$. Now consider

$$H_i = \pi^{-1}(\overline{H_i}) < P < G.$$

Then $|H_i| = p^i$, since the map $H_i \overset{\pi}{\twoheadrightarrow} \overline{H_i}$ with kernel $\langle x \rangle$, so $H_i/\langle x \rangle \overset{\cong}{\to} \overline{H_i}$, and hence

$$|H_i|/|\langle x \rangle| = \left|\overline{H_i}\right| = p^{i-1}.$$

□

5.8 A_5 is the Only Simple Group of Order 60

Theorem 5.8.1. Let G be a simple group of order 60. Then $G \cong A_5$.

Proof. We will show that if G has an index 5 subgroup then we win, and then that such a subgroup exists in G. Suppose $H \leqslant G$ and $[G : H] = 5$. G acts on the set G/H of left cosets by left multiplication. Let $\varphi \colon G \to S_5$ be the corresponding group homomorphism.

Since G is simple, $\ker \varphi$ is either 1 or G. If $\ker \varphi = G$, then φ is the trivial group action, which it is not. Thus $\ker \varphi = G$, so φ is an injection. Thus G embeds as $G \overset{\varphi}{\hookrightarrow} S_5$.

Now we can show G lives inside A_5 by showing that

$$\begin{array}{ccc} G & \xrightarrow{\ \varphi\ } & S_5 \\ & \searrow^{\operatorname{sgn}\circ\varphi} & \downarrow{\scriptstyle \operatorname{sgn}} \\ & & \{\pm 1\} \end{array}$$

commutes but that $\operatorname{sgn} \circ \varphi = \mathrm{id}$. Because G is simple, $\ker(\operatorname{sgn} \circ \varphi) = G$ or $\{1\}$. If $\ker = \{1\}$, then $G \hookrightarrow \{\pm 1\}$. But G is too big. So $\ker \varepsilon \circ \varphi = G$, so $\ker \varepsilon \circ \varphi = G$. So $\operatorname{im}(\operatorname{sgn} \circ \varphi) = \{1\}$, so

$$G \cong \operatorname{im} \varphi \hookrightarrow A_5.$$

As $|G| = 60 = |A_5|$, we have $G \cong A_5$. By Sylow III, where $|G| = p^a m$,

$$\begin{cases} n_p \equiv 1 \pmod p, \\ n_p \mid m, \\ n_p = [G : N_G(P)] \text{ for any } P \in \mathrm{Syl}_p(G). \end{cases}$$

for $P \in \mathrm{Syl}_p(G)$. What is n_2?

Assume $n_2 = 3$. Consider $N_G(P)$. Then $[G : N_G(P)] = 3$. G acts on $G/N_G(P)$, so $G \xrightarrow{\varphi} S_3$ group homomorphism. But $\ker\varphi \neq G$ and $\ker\varphi \neq 1$ since $|G > |S_3| = 6|$, contradiction.

Now assume $n_2 = 15$. Then we have $P_1, P_2, \dots P_{15} < G$, each of size 2. Assume $P_i \cap P_j = \{1\}$ for all i, j. Then G has $15 \times 3 + 1 = 46$ elements, but since $n_5 = 6$, there are another 6×4 elements, which gives 70 total elements in G, a contradiction.

Hence there exist $P, Q \in \mathrm{Syl}_2(G)$ such that $|P \cap Q| = 2$. Then $N_G(P \cap Q) \neq G$, $P \cap Q \lhd P, Q$. Yes, because $|P| = 4$, so P is abelian.

Then $P \cup QN_G(P \cap Q)$. The size of the normalizer $N_G(P \cap Q)$ must divide 60, so it can have size one of ~~2~~, ~~3~~, ~~4~~, ~~5~~, ~~6~~, ~~10~~, 12, ~~15~~, ~~20~~, ~~30~~. So, either $[G : N] = 3$ (which is false) or $[G : N] = 5$. This completes the proof. □

5.9 Showing A_n is Simple For All $n \geqslant 5$

It turns out that A_n is simple for all $n \geqslant 5$:

Theorem 5.9.1. A_n is simple for all $n \geqslant 5$.

Proof. We argue by induction over $n \geqslant 5$. We have already shown the base case that A_5 is simple. Now suppose the claim holds for some $n \geqslant 6$ and that A_{n-1} is simple. Let $H \lhd A_n$. We want to show either $H = \{1\}$ or $H = A_n$. Let A_n act on the integers $\{1, \dots, n\}$ in the usual way, and let $G_i = \mathrm{Stab}(i)$. Then G_i is all the even permutations of $\{1, \dots, n\}$ that fix i. Perhaps after relabeling, we can make the identification $G_i \cong A_{n-1}$.

Consider $H_i = G_i \cap H$. Then $H_i \lhd G_i$, because if $g \in G_i < A_n$ and $h \in H_i < G_i$, then $ghg^{-1} \in H$ and $ghg^{-1} \in G_i$, so $ghg^{-1} \in G_i \cap H = H_i$. Now by our induction hypothesis, one of the two cases hold.

- *Case 1.* $H_i = G_i$. We claim $H_j = G_j$ for all j. *Proof of Claim.* Let $\sigma \in A_n$. Then
$$\begin{aligned} G_{\sigma(i)} &= \mathrm{Stab}_{A_n}(\sigma(i)) = \sigma\,\mathrm{Stab}_{A_n}(i)\sigma^{-1} = \sigma G_i\sigma^{-1} = \sigma(G_i \cap H)\sigma^{-1} \\ &= (\sigma G_i\sigma^{-1}) \cap (\sigma H\sigma^{-1}) = G_{\sigma(i)} \cap H = H_i. \end{aligned}$$
We know $G_i = H_i = G_i \cap H$, so $G_i \leqslant H$ for all i. So $\langle G_1, G_2, \dots, G_n\rangle \leqslant H$. We now show that if $n \geqslant 5$, then $\langle G_1, \dots, G_n\rangle = G$. (That is, every element of G is a product of elements having fixed points). To see this, let $g \in G$. Then
$$g = \lambda_1\lambda_2 \cdots \lambda_t,$$
where each $\lambda_k = (ab)(cd)$ is a product of two transpositions. Since $n \geqslant 5$ for all n ,$\lambda_n \in G_i$ for some i. So $g = \lambda_1, \dots, \lambda_n \in \langle G_1, \dots, G_n\rangle$. Hence $G = \langle G_1, \dots, G_n\rangle < H < G$, so $H = G$.
- *Case 2.* $H_i = \{1\}$ for all i. By definition, if $h \in H$ and $h \in \mathrm{Stab}_{A_n}(i)$, then $h = 1$. Equivalently, if $h(i) = i$ for all $i = 1, \dots, n$, then $h = 1$. Equivalently, if $h_1, h_2 \in H$ and $h_1(i) = h_2(i)$, then $h_2^{-1}h_1(i) = i$. Then $h_2^{-1}h_1(i) = i$, so $h_2^{-1}h_1 = 1$, so $h_1 = h_2$.

  Now $n \geqslant 6$ and g is a non-identity element of H. Write g as a product of disjoint cycles. Then we have the following cases.

  (a) $g = (a_1a_2)(a_3a_4)(a_5a_6)\cdots$.

  (b) g has a cycle of length $k \geqslant 3$, $g = (a_1a_2a_3\cdots a_n)$.

  In case (a), let $\sigma = (a_1a_2)(a_3a_5)$. Then $\sigma \in A_n$ since it is a pair of transpositions, and
$$\sigma g\sigma^{-1} = (\sigma(a_1)\sigma(a_2))\ (\sigma(a_3)\sigma(a_4))\ (\sigma(a_5)\sigma(a_6)) = (a_2a_1)(a_5a_4)(a_3a_6).$$

Then $g \neq \sigma g \sigma^{-1}$, because $\sigma g \sigma^{-1}$ sends a_3 to a_6 while g sends a_3 to a_4. But $g(a_1) = a_2 = \sigma g \sigma^{-1}(a_1)$, a contradiction.

In case (b), choose $\sigma \in A_n$ such that $\sigma(a_1) = a_1$ and $\sigma(a_2) = a_2$, but $\sigma(a_3) \neq a_3$. Then

$$H \ni \sigma g \sigma^{-1} = (\sigma(a_1)\sigma(a_3)) \cdots) = (a_1 a_2 \sigma(a_3))$$

so in conclusion if we have any non-identity element of H, we obtain a contradiction. It follows that $H = \{1\}$. (This argument only works for $n \geqslant 6$ because we needed three disjoint two cycles).

We have now shown that if $N \lhd A_5$ then either $H = \{1\}$ or $H = A_n$, so A_n is a simple group. □

5.10 Homework 4

Exercise 5.10.1. Let p be a prime. Show that any group of order p^2 is isomorphic to C_{p^2} or to $C_p \times C_p$, where C_n is the cyclic group of order n.

Solution. Let G be a group of order p^2, where p is prime. $G \cong C_{p^2}$ if and only if G has an element of order p^2, so assume no such element exists. We may assume G contains no element of order p^2, since otherwise $G \cong C_p$, which affirms the claim.

By Cauchy's Theorem, G has an element k of order p. Let $K = \langle k \rangle$, and let $h \in G \setminus K$. Then $h \neq 1$ and has order not equal to p^2, so h has order p by Lagrange's Theorem.

- *Step 1: Show $K \cap H = \{1\}$.* Note $K \cap H$ is a subgroup of both K and H, so $|K \cap H|$ divides p by Lagrange's Theorem, and hence $|K \cap H| \in \{1, p\}$. If $|K \cap H| = p$, then since $K \cap H$ is a subgroup of both K and H, both of which also have order p, we would have $K = P$. But this contradicts $h \notin K$, so $K \cap H = \{1\}$.

- *Step 2: Show $K \lhd G$.* Since p is the smallest prime dividing $|G| = p^2$ and $[G : H] = p$, we conclude by Exercise 3.4 that $K \lhd G$.

- *Step 3: Show $KH = G$.* It suffices to show $|KH| = p^2$. To see this, note that $HK/K \cong H/(K \cap H)$ by the Third Isomorphism Theorem, so

$$|HK|/p = |HK|/|K| = \frac{|H|}{|H \cap K|} = p/1 = p,$$

so $|HK| = p^2$. By Steps 1,2, and 3, we conclude G equals the internal semidirect product $K \rtimes H$.

- *Step 4: Show $H \lhd G$.* Arguing *verbatim* as in Step 2 after replacing any appearance of 'H ' with 'K', we have $H \lhd G$. Thus $H \lhd G = N \rtimes H$, so equivalently we have $G = N \rtimes H \cong N \times H \cong C_p \times C_p$, as claimed. □

Exercise 5.10.2. Describe (by giving generators or by listing elements) a Sylow 2-subgroup of S_5 and show that it is isomorphic to the dihedral group D_8. What is $n_2(S_5)$?

Solution.

Since $|S_5| = 5! = 120 = 2^3 \times 3 \times 5$, it suffices to find any subgroup of order $2^3 = 8$. It is enough to show the group homomorphism $\varphi : \langle x, y \mid x^4, y^2, xyxy \rangle \to S_5$ determined by $x \mapsto (1234), y \mapsto (13)$ is injective. This group homomorphism φ exists and is unique by **??**, since $\varphi(x)^4 = 1$, $\varphi(y)^2 = 1$, and $\varphi(x)\varphi(y)\varphi(x)\varphi(y) = (13)(13) = 1$.

Injectivity of φ follows from showing $|\operatorname{im}\varphi| \geqslant 8$, since $8 = |D_8|$ and $D_8 \cong \langle x, y \mid x^4, y^2, xyxy\rangle$ by Exercise 2.3. We have

$$\begin{array}{ccccc} 1 & \longmapsto & \mathrm{id} & = & \mathrm{id}, \\ x & \longmapsto & (1234) & = & (1234), \\ x^2 & \longmapsto & (1234)^2 & = & (13)(24), \\ x^3 & \longmapsto & (1234)^3 & = & (1432), \\ y & \longmapsto & (13) & = & (13), \\ yx & \longmapsto & (13)(1234) & = & (14)(23), \\ yx^2 & \longmapsto & (13)(1234)^2 & = & (24), \\ yx^3 & \longmapsto & (13)(1234) & = & (12)(34). \end{array}$$

The 4-cycles (1234) and (1432) are distinct, since as elements of S_5 they permute the ordered set $(1, 2, 3, 4, 5)$ as $(4, 1, 2, 3, 5)$ and $(2, 3, 4, 1, 5)$, respectively. These are also distinct from (12)(34), (14)(23), and (13)(24), which permute $(1, 2, 3, 4, 5)$ as $(2, 1, 4, 3, 5)$, $(4, 3, 2, 1, 5)$, and $(3, 4, 1, 2, 5)$, respectively. The two cycles (13) and (24) are distinct since they fix different elements. We now have seven distinct non-identity elements of $\operatorname{im}\varphi$, so $\operatorname{im}\varphi$ has at least 8 elements. Thus φ is injective, so by the First Isomorphism Theorem the subgroup $\operatorname{im}\varphi$ satisfies $\operatorname{im}\varphi \cong \langle x, y \mid x^4, y^2, xyxy\rangle \cong D_8$. As $\operatorname{im}\varphi$ is an order 8 subgroup of S_5, we conclude $\operatorname{im}\varphi$ is a 2-Sylow subgroup of S_5 and is isomorphic to D_8.

We now compute $n_2(S_5)$. Since $5! = 120 = 2^3 \cdot 15$, $n_2(S_5)$ divides 15 by Sylow III. Hence $n_2(S_5) \in \{1, 3, 5, 15\}$. Let j be a given element of $\{1, 2, 3, 4, 5\}$, and let K_j be the subgroup of permutations in S_5 that fix j. Then K_j is isomorphic to S_4 after identifying the points $\{1, 2, 3, 4, 5\} \smallsetminus \{j\}$ with $\{1, 2, 3, 4\}$. Since $4! = 24 = 2^3 \cdot 3$, Sylow 2-subgroups of S_4 are also subgroups of order 8, and therefore are also Sylow 2-subgroups of S_5. Moreover $n_2(S_4)$ divides 3 by Sylow III, so $n_2(S_4) \in \{1, 3\}$. We claim $n_2(S_4) = 3$.

Since elements of $\operatorname{im}\varphi$ are permutations of $\{1, 2, 3, 4, 5\}$ that fix 5, we can identify $\operatorname{im}\varphi$ as a subgroup of S_4. By Sylow II, all Sylow 2-subgroups of S_4 are the conjugate subgroups of $\operatorname{im}\varphi$, so it suffices to find $\sigma \in \operatorname{im}\varphi$ and $\lambda \in S_4$ such that $\lambda\sigma\lambda^{-1} \notin \operatorname{im}\varphi$. If $\lambda = (12)$, then

$$\lambda(13)\lambda^{-1} = (\lambda(1)\lambda(3)) = (23),$$

But $(23) \notin \operatorname{im}\varphi$, since it fixes the subset $\{1, 4\}$ when acting on the ordered set $(1, 2, 3, 4)$, but no element of $\operatorname{im}\varphi$ fixes precisely these elements. Thus $\lambda(\operatorname{im}\varphi)\lambda^{-1}$ is another Sylow 2-subgroup of S_4, so $n_2(S_4) \neq 1$, thus forcing $n_2(S_4) = 3$. The key point here is that there are more than one Sylow 2-subgroup whose elements fix 5.

When defining and computing φ, we saw that $\operatorname{im}\varphi$ fixes 5, and this is because we chose the images of the generators to fix 5. On the other hand, the image of the generator x under φ does not fix 1, 2, 3, or 4. We could have chosen φ to map into K_j instead of K_1 for $j = 2, 3, 4, 5$, which gives four more Sylow 2-subgroup of S_5, which are all distinct because they fix j but not $\{1, 2, 3, 4, 5\} \smallsetminus \{j\}$, wherexas the Sylow subgroups in the other K_j do not have this property. This itself gives 5 distinct Sylow 2-subgroups of S_5. But we showed above that there are more than one Sylow 2-subgroup of S_5 that fixes 5, which gives us at least six Sylow 2-subgroups, thus forcing $n_2(S_5) = 15$. This completes the proof. □

Exercise 5.10.3. Let p be a prime.

(a) For any $n \in \mathbb{Z}_{\geqslant 1}$, show that

$$|\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}).$$

(b) Determine $n_p(\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}))$.

Solution. By $\mathbb{F}_p$ we will mean $\mathbb{Z}/p\mathbb{Z}$.

(a) Let p be prime and $n \geqslant 1$. An element of $\mathrm{GL}_n(\mathbb{F}_p)$ is equivalently an n-by-n matrix with linear independent vectors in the n-dimensional vector space $\mathbb{F}_p$, say with respect to the standard ordered basis, so it suffices to count the number of linear independent sets of size n in $\mathbb{F}_p^n$. We do this by induction on n.

The base case $n = 1$ holds because there are $p^n - 1$ linear independent singleton sets $\{v_1\}$, since the only requirement for v_1 so that $\{v_1\}$ is linearly independent is that $v_1 \neq 0$. (Indeed, if $v_1 = 0$ and $a_1 \in \mathbb{F}_p$, then $a_1 v_1 = 0$ does *not* imply $a_1 = 0$).

Now suppose for some $2 \leqslant k \leqslant n$ we know the number of linear independent sets of size $k-1$ in $\mathbb{F}_p^n$ is $(p^n - 1)(p^{n-1} - p) \cdots (p^n - p^{k-2})$. We claim the number of linear independent sets of size k in $\mathbb{F}_p^n$ is $(p^n - 1)(p^n - p) \cdots (p^n - p^{k-1})$. Given a linear independent set $\{v_1, \ldots, v_{k-1}\} \subset \mathbb{F}_p^n$, the set $\{v_1, \ldots, v_{k-1}, w\}$ is linearly *dependent* if and only if $w = a_1 v_1 + \cdots + a_{k-1} v_{k-1}$. The set of such w therefore corresponds with the set of $k-1$ tuples $(a_1, \ldots, a_{k-1}) \subset \mathbb{F}_p^{k-1}$, which has size p^{k-1}. It follows that the number of $v_k \in \mathbb{F}_p^n$ such that the set $\{v_1, \ldots, v_n\}$ is linearly *independent* has size $p^n - p^{k-1}$. Therefore, by our induction hypothesis, it follows that the number of linearly independent sets of size n in $\mathbb{F}_p^n$ is

$$(p^n - 1)(p^n - p) \cdots (p^n - p^{k-2})(p^n - p^{k-1}),$$

as claimed.

(b) By part (a), the order of the group $\mathrm{GL}_2(\mathbb{F}_p)$ is $(p^2-1)(p^2-p) = p(p-1)^2(p+1)$. Since p cannot divide $p \pm 1$, the maximal power of p in the order of $\mathrm{GL}_2(\mathbb{F}_p)$ is p^1. Consider the subgroup H of $\mathrm{GL}_2(\mathbb{F}_p)$ consisting of matrices of the form $\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$, where $a \in \mathbb{F}_p$. Since elements of this set satisfy $\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & a+b \\ 0 & 1 \end{smallmatrix}\right)$ holds, we have $H \cong \mathbb{F}_p$, and in particular $|H| = p$. Thus $H \in \mathrm{Syl}_p(\mathrm{GL}_2(\mathbb{F}_p))$. By Sylow III, $n_p = n_p(\mathrm{GL}_2(\mathbb{F}_p))$ satisfies

$$n_p = [\mathrm{GL}_2(\mathbb{F}_p) : T],$$

where T denotes the normalizer of H in $\mathrm{GL}_2(\mathbb{F}_p)$. Recall that T is the subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ consisting of matrices of the form $\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right)$, where $a, b, c \in \mathbb{F}_p$ satisfy $ac \neq 0$, that is, with $a \neq 0$ and $c \neq 0$. This means there are precisely $p-1$ choices for a, $p-1$ choices for c, and p choices for b (corresponding to any element of $\mathbb{F}_p \smallsetminus \{0\}$, any element of $\mathbb{F}_p \smallsetminus \{0\}$, and any element of $\mathbb{F}_p$, respectively) such that $\left(\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right) \in T$. Thus $|T| = p(p-1)^2$, so

$$n_p = [\mathrm{GL}_2(\mathbb{F}_p) : T] = \frac{|\mathrm{GL}_2(\mathbb{F}_p)|}{|T|} = \frac{p(p-1)^2(p+1)}{p(p-1)^2} = p + 1. \qquad \square$$

Exercise 5.10.4. Let G be a finite group, and let $H < G$ be a proper subgroup. Show that G is not the union of all conjugates of H, i.e.,

$$\bigcup_{g \in G} gHg^{-1} \subsetneq G$$

is a strict containment.

Solution. Let G be a finite group and let H be a proper subgroup of G.

(1) Subgroups conjugate to H in G are isomorphic to H, so all conjugate subgroups have the same size. Since the union of all conjugate subgroups is maximized when they have trivial pairwise

intersection, the union of all conjugate subgroups of G contains *at most*

$$\underbrace{1}_{\text{identity}} + \underbrace{k}_{\substack{\#\text{distinct conjugate} \\ \text{subgroups}}} \cdot \underbrace{(|H| - 1)}_{\substack{\#\text{non-identity} \\ \text{elements in each} \\ \text{conjugate subgroup}}} \tag{$*$}$$

elements.

(2) If $g_1, g_2 \in G$ and $g_2 \in g_1 H$ then $g_2 H g_2^{-1} = g_1 H g_1^{-1}$. Indeed, if $g_2 = g_1 h$ for some $h \in H$, then $g_2 H g_2^{-1} = g_1 h H h^{-1} g_1^{-1} = g_1 H g_1^{-1}$. Thus, the number of distinct conjugate subgroups of H cannot exceed the number of left cosets of G in H.

(3) $[G : H] \geqslant 2$, since H is a *proper* subgroup of G. Hence $k \leqslant [G : H]$, where k is as in $(*)$.

Combining these observations, we have

$$\begin{aligned} \left| \bigcup_{g \in G} g H g^{-1} \right| &\leqslant 1 + k(|H| - 1) && \text{(by (1))} \\ &\leqslant 1 + [G : H](|H| - 1) && \text{(by (2))} \\ &= 1 + [G : H]|H| - [G : H] = |G| + (1 - [G : H]). \end{aligned}$$

The term $(1 - [G : H])$ is *strictly* positive by (3). Hence the right-hand side is strictly less than $|G|$, which completes the proof. □

Exercise 5.10.5. Let H be a normal subgroup of a finite group G, and let p be a prime. Show:

(a) For any $P \in \mathrm{Syl}_p(G)$, PH/H is a Sylow p-subgroup of G/H, and that all elements of $\mathrm{Syl}_p(G/H)$ arise this way. (Here PH denotes the subgroup $\langle ph \mid p \in P, h \in H \rangle$ of G, and PH/H denotes the image of PH under the quotient map $G \twoheadrightarrow G/H$.)

(b) $n_p(G/H)$ divides $n_p(G)$.

Solution. We first state and four auxiliary lemmas:

Lemma 5.10.6. If G is a finite group and p is prime, then

$$P \in \mathrm{Syl}_p(G) \iff p \nmid [G : P].$$ □

Lemma 5.10.7. Let G be a finite group and let N be a normal subgroup of G. If K is another subgroup containing N, then

$$[G : K] = [G/N : K/N].$$

Lemma 5.10.8. Let G be a finite group with a subgroup K and normal subgroup N. Then there exists some integer b such that

$$[G/H : N_G(KN)/N] = b[G/H : N_{G/H}(KN/N)].$$

Lemma 5.10.9. Let G be a finite group and suppose $H < K < G$. Then

$$[G : H] = [G : K][K : H].$$

Proof of **??**. Since G is a finite group, we can write $|G| = p^a m$, where $p \nmid m$.

($\Rightarrow$) Suppose $P \in \mathrm{Syl}_p(G)$. Then

$$p^a m = |P|[G : P] = p^a [G : P].$$

Dividing through by p^a, we obtain $m = [G : P]$. Then $p \nmid m = [G : P]$, which is given.

($\Leftarrow$) Conversely, suppose $p \nmid [G : P]$. Since $p^a m = |P|[G : P]$ implies all factors of p are factors of $|P|$. Thus $p^a \mid |P|$. But $p^k \leqslant p^a$ since $|P| \mid |G| = p^a m$, forcing $p^k = p^a$. Hence $P \in \mathrm{Syl}_p(G)$. □

Proof of **??**. By the Correspondence Theorem, K/N is a subgroup of G/N, and hence $[G/N : K/N]$ is well-defined. Now write

$$\frac{|G|}{|N|} = |G/N| = |K/N|[G/N : K/N] = \frac{|K|}{|N|}[G/N : K/N].$$

Multiplying through by $|N|$, we obtain $|G| = |K|[G/N : K/N]$. But we can also write $|G| = |K|[G : K]$, so

$$|K|[G : K] = |G| = |K|[G/N : K/N].$$

Dividing through by $|K|$, we conclude

$$[G : K] = [G/N : K/N].$$ □

Proof of **??**. Let $\pi(g) \in N_G(KN)/N$, so that $g \in N_G(KN)$. Then $gKNg^{-1} = KN$, which implies $\pi(g)\pi(KN)\pi(g)^{-1} = \pi(KN)$. Then $\pi(g) \in N_{G/H}(\pi(KN)) = N_{G/N}(KN/N)$, so we conclude $\pi(g) \in N_{G/H}(KN)$. Thus $N_G(KN)/N < N_{G/N}(KN/N)$, so $|N_G(KN)/N|$ divides $|N_{G/H}(KN/N)|$. Then in particular the index $[G/H : N_{G/H}(KN/N)]$ divides the index $[G/H : N_G(KN)/N]$. □

Proof of **??**. We have

$$|G| = |K|[G : K]$$

and

$$|K| = |H|[K : H],$$

so

$$|G| = |K|[G : K] = |H|[K : H][G : K].$$

But we also know $|G| = |H|[G : K]$, so $|H| = [G : K][K : H]$. □

We can now prove the statements of **??**.

(a) Let G be a finite group, let H be a normal subgroup of G, let p be a prime, let $\pi : G \twoheadrightarrow G/H$ be the canonical quotient map, and let $P \in \mathrm{Syl}_p(G)$. Since G is a finite group, we can write $|G| = p^a m$, where $p \nmid m$. We will prove the statement by establishing two claims.

- Claim 1: $PH/H \in \mathrm{Syl}_p(G)$.
- Claim 2: If $Q \in \mathrm{Syl}_p(G/H)$, then $Q = PH/H$ for some $P \in \mathrm{Syl}_p(G)$.

Proof of Claim 1.

- *Step 1. Show PH is a subgroup of G.* As $P < G$ and $H \lhd G$, we have by the Third Isomorphism Theorem that $\{ph : p \in P, h \in H\}$ is a subgroup of G. Since PH is defined as the subgroup generated by this set, it follows that PH is equal to $\{ph : p \in P, h \in H\}$.
- *Step 2: Show PH/H is a subgroup of G/H.* As the image of the subgroup PH of G under the group homomorphism π, PH/H is indeed a subgroup of G/H.
- *Step 3: Show $p \nmid [G/H : PH/H]$.* To see $PH/H \in \mathrm{Syl}_p(G/H)$, by **??** it suffices to show $p \nmid [G/H : PH/H]$. Since G is a finite group, $H \lhd G$, and PH is a subgroup of G

containing H, by **??** we have

$$[G/H : PH/H] = [G : PH].$$

It therefore is enough to show $p \nmid [G : PH]$. Suppose toward a contradiction $[G : PH] = pM$ for some integer M. Note $P < PH$, so $p^a \mid |PH|$ by Lagrange's Theorem. Thus $|PH| = rp^a$ for some integer r. But then

$$|G| = |PH|[G : PH] = r|P| \cdot [G : PH] = rp^a \cdot pM = rp^{k+1}M,$$

so $p^{a+1} \mid |G|$, contradicting that p^a is the maximal power of p dividing G. Hence $p \nmid [G/H : PH/H]$, so PH/H is a Sylow p-subgroup of G/H. □

This completes the proof of Claim 1.

Proof of Claim 2. By Sylow I, there exists some $P \in \mathrm{Syl}_p(G)$. Let $Q = PH/H$, and suppose Q' is an arbitrary element of $\mathrm{Syl}_p(G/H)$. Note $Q \in \mathrm{Syl}_p(G/H)$ by Claim 1, so by Sylow II, there exists $q \in G/H$ such that

$$Q' = qQq^{-1} = q \cdot \pi(PH) \cdot q^{-1}$$

Since π is surjective, there exists $g \in G$ such that $q = \pi(g)$; hence

$$Q' = \pi(g) \cdot \pi(PH) \cdot \pi(g)^{-1} = \pi(gPHg^{-1}).$$

Since H is normal in G, we have $Hg^{-1} = g^{-1}H$, so we can write this as

$$Q' = \pi(gPg^{-1}H) = \pi(gPg^{-1})\pi(H) = \pi(gPg^{-1}) \cdot 1 = \pi(gPg^{-1}),$$

and $gPg^{-1} \in \mathrm{Syl}_p(G)$ because $gPg^{-1} \cong P$ implies $|gPg^{-1}| = |P| = p^a$. We conclude $Q = (gPg^{-1})H/H$ for the Sylow p-subgroup gPg^{-1} of G. Hence each element of $\mathrm{Syl}_p(G/H)$ arises in this way, proving Claim 2. This completes the proof of part (a). □

(b) Let $P \in \mathrm{Syl}_p(G)$. By part (a), $PH/H \in \mathrm{Syl}_p(G/H)$. Then by Sylow III, we have

$$n_p(G/H) = [G/H : N_{G/H}(PH/H)] \qquad \text{and} \qquad n_p(G) = [G : N_G(P)].$$

Note $N_G(P) < N_G(PH)$, since $gPg^{-1} \in P$ implies $gPHg^{-1} = gPg^{-1}H \in nPH$ by normality of H in G. Thus

$$\begin{aligned}
n_p(G) &= [G : N_G(P)] \\
&= [G : N_G(PH)][N_G(PH) : N_G(P)] && \text{(by **??**)} \\
&= [G/H : N_G(PH)/H][N_G(PH) : N_G(P)] && \text{(by **??**)} \\
&= b[G/H : N_{G/H}(PH/H)][N_G(PH) : N_G(P)] && \text{(by **??**)} \\
&= b \cdot n_p(G/H) \cdot [N_G(PH) : N_G(P)], && \text{(by Sylow III)}
\end{aligned}$$

where b is an integer. This shows $n_p(G/H)$ divides $n_p(G)$, which proves part (b).

6 Assembling Larger Groups from Smaller Groups

Recall the definition of a simple group: Any group G is simple if it has no nontrivial proper normal subgroups. A big problem in finite group theory is to classify all finite simple groups, that is, to determine a complete list, up to isomorphism, of all finite simple groups. This is "done" in the sense that although the proofs in the literature are a bit incomplete, but it is widely accepted as a theorem by most mathematicians.

Some examples of infinite families of finite simple groups are A_n for $n \geqslant 5$. There are also so-called "sporadic" groups which are not fit in any of these families. There are finitely many of them.

6.1 Direct Products of Groups

Our first example of building larger groups from smaller groups is the construction of the direct product.

Definition 6.1.1. Let $\{G_i\}_{i\in I}$ be a collection of groups G_i indexed by elements of I. Define the **direct product** of this collection by

$$G = \prod_{i\in I} G_i$$

whose underlying set is the set-theoretic Cartesian product, that is, $\{(g_i)_{i\in I} \mid g_i \in G_i \text{ for all } i \in I\}$, and whose group operation is given by the coordinate-wise on the components, by which we mean

$$(g_i)_{i\in I} \cdot (g_i')_{i\in I} = (g_i g_i')_{i\in I}.$$

When $|I| < \infty$, say $I = \{1, 2, \dots, n\}$, then we often write $G_1 \times G_2 \times \cdots \times G_n$.

Note that $G = \prod_{i\in I}$ is in fact a group, since the identity is the $(1_i)_{i\in I}$, associativity follows from associativity in each component, and inverses follow from inverses in each component.

Observe that for all j, we have surjective homomorphisms

$$\begin{aligned} G = \prod_{i\in I} &\xrightarrow{\pi} G_j, \\ \pi_j &\longmapsto g_i, \end{aligned}$$

and for all $j \in I$, we have injective group homomorphisms

$$\begin{aligned} G_j &\xhookrightarrow{\rho} G = \prod_{i\in I} G_i \\ g_i &\longmapsto \rho_j(g_j) = (g_i)_{i\in I} \text{ such that } \begin{cases} g_i & \text{if } i \neq j, \\ g_i = 0 & \text{otherwise.} \end{cases} \end{aligned}$$

We will often regard G_j as a subgroup of $\prod_{i\in I} G_i$ (with ρ_j implicit). Then for all $i \neq j$, the subgroups G_i and G_j commute and have trivial intersection.

Finally, we have for all groups H bijections

$$\begin{aligned} \mathrm{Hom}_{\mathrm{Grp}}\Big(H, \prod_{i\in I} G_i\Big) &\xrightarrow{\cong} \prod_{i\in I} \mathrm{Hom}_{\mathrm{Grp}}(H, G_j), \\ \varphi &\longmapsto (\pi_i \circ \varphi)_{i\in I}. \end{aligned}$$

Checking this is an exercise.

Given groups G_1 and G_2, G_1 and G_2 can be thought of as subgroups of the direct product group $G_1 \times G_2$ via the inclusions $g_1 \mapsto (g_1, 1)$ and $g_2 \mapsto (1, g_2)$. With this identification we have $G_1 \lhd G_1 \times G_2$ and $G_2 \lhd G_1 \times G_2$, $G_1 \cap G_2 = \{1\}$, and $G_1 \cdot G_2 = G_1 \cdot G_2$.

6.2 Semidirect Products of Groups

Definition 6.2.1. Let G be a group and suppose we have subgroups $N, H < G$. We say G is the **(internal) semidirect product of H acting on N** if

(1) $N \lhd G$,

(2) $H \cap N = \{1\}$, and

(3) $H \cdot N = G$.

Note that we *do not* require H be normal in G.

Example 6.2.2. Consider $D_6 = \langle \rho, \tau \mid \rho^3 = 1, \tau^2 = 1, \tau\rho\tau^{-1} = \rho^2 \rangle$. Then $N = \langle \rho \rangle$, $H = \langle \tau \rangle$. Then conditions (1), (2), and (3) in **??** hold, so D_6 is the internal semidirect product of $\langle \tau \rangle$ by $\langle \rho \rangle$. //

Remark 6.2.3. In general, suppose G is an internal semidirect product of H acting on N. Then for all $n_1, n_2 \in N$, $h_1, h_2 \in H$, we have

$$(n_1h_1) \cdot (n_2h_2) = n_1h_1n_2(h_1h_1^{-1})h_2 = \underbrace{n_1(h_1n_2h_1^{-1})}_{\in N} \cdot \underbrace{h_1h_2}_{\in H}.$$

This last equation suggests the more abstract notion of a semidirect product.

Definition 6.2.4. Let N and H be any groups, and suppose we are given a group homomorphism

$$\varphi \colon H \longrightarrow \mathrm{Aut}_{\mathrm{Grp}}(N).$$

(So, in the internal semidirect product, φ is the conjugation-by-h automorphism of N.) Then we define the **(external) semidirect produt of H acting on N (with respect to φ)**, written $N \rtimes_\varphi H$ as the group with underlying set $N \times H$, but with the group operation

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1 \cdot \varphi(h_1)(n_2), h_1 \cdot h_2).$$

If the automorphism φ of N is understood, we will sometimes write $N \rtimes_\varphi H$ as simply $N \rtimes H$.

Lemma 6.2.5. Let N and H be groups and let φ be a group automorphism of N.

(1) $G = N \rtimes_\varphi H$ is a group, with identity $(1, 1)$ and $(n, h)^{-1} = (h^{-1} \cdot n^{-1}, h^{-1})$.

(2) $N \xrightarrow{\cong} \{(n, 1) \mid n \in N\} \lhd G$ is a normal subgroup of $H \rtimes_\varphi H$. $H \xrightarrow{\cong} \{(1, h \mid h \in H)\} < G$ is a subgroup. With these identifications as subgroups, we have $H \cap N = \{1\}$, $H \cdot N = G$, and

$$\varphi(h)(n) = (1, h)(n, 1)(1, h)^{-1} \xleftarrow{\cong} hnh^{-1}.$$

Proof. (1) For all $n \in N$, $h \in H$,

$$(1_N, 1_H)(n, h) = (1_N(1_H \cdot n), 1_H \cdot h) = (n, h) = (1_N, 1_H = (n(h \cdot 1_N), h_{1H})) = (n, h),$$

so G has identity. For inverses, we have

$$(n, h)(h^{-1} \cdot n^{-1}, h^{-1}) = (n(h \cdot (h^{-1} \cdot n^{-1})), h \cdot h^{-1}) = (n(\underbrace{hh^{-1}}_{=1_H}) \cdot 1_H) = (1, 1).$$

Likewise for the multiplication from the left, which is left as an exercise. For associativity,

$$\begin{aligned}((a, x)(b, y))(c, z) &= (a(x \cdot b), xy)(c, z) = (a, (x \cdot b)((xy) \cdot c), x \cdot yz) \\ &= (a(x \cdot (b(y \cdot c))), xyz) = (a, x)(b(y \cdot c), yz) = (a, x)((b, y)(c, z)).\end{aligned}$$

Thus G is a group.

(2) Showing that, under the given identifications, we have $N \lhd G$, $H < G$, and $N \cdot H = N \rtimes H$, and $N \cap H = \{1\}$ is left as an exercise.

For the last claim, note that

$$\underbrace{hnh^{-1}}_{\in N \rtimes_\varphi H} = (1, h)(n, 1)(1, h)^{-1} = (h \cdot n, h)(1, h^{-1}) = (\underbrace{h \cdot n}_{\varphi(h)(n)}, 1).$$ □

Proposition 6.2.6. Given groups N, H and a group automorphism φ of N, the following are equivalent:

(1) $\mathrm{id} \colon N \rtimes_\varphi H \to N \times H$ is a group isomorphism,

(2) $\varphi \colon H \to \mathrm{Aut}_{\mathrm{Grp}}(N)$ is trivial, and

(3) $H \lhd N \rtimes_\varphi H$, when making the identification $H \xrightarrow{\cong} \{(1,h) \mid h \in H\}$.

Proof of **??**. We only prove (3) $\implies$ (2), and leave the other implications as exercises. Given (3), for all $h \in H$ and $n \in N$,

$$\underbrace{n\overbrace{hn^{-1}}^{\in N}h}_{\in H} \in H \cap N = \{1\},$$

so inside $N \rtimes_\varphi H$, $hn = nh$ for all $n \in N$ and all $h \in H$, so $hnh^{-1} = n$. Thus φ is trivial. □

6.3 Examples with Semidirect Products

Example 6.3.1. Let $N = H = (\mathbb{Z}, +)$. We want to build a semidirect product of N and H. To do this, we need to choose a map $H \to \mathrm{Aut}(N) = \mathrm{Aut}((\mathbb{Z},+)) = \{1 \mapsto \pm 1\} \cong \{(\pm 1, \cdot)\}$. Consider

$$\begin{aligned} \varphi\colon \mathbb{Z} &\longrightarrow \{\pm 1\}, \\ 1 &\longmapsto -1. \end{aligned}$$

Then $H \ni n \mapsto (-1)^n$. As a set, $\mathbb{Z} \rtimes_\varphi \mathbb{Z}$ has elements $(n,h) \in \mathbb{Z}^2$, and has group operation

$$(n_1,h_1) * (n_2,h_2) = (n_1 + \varphi(h_1)(n_2), h_1 + h_2) = (n_1 + (-1)^{h_1}n_2, h_1 + h_2).$$

The identity is $(0,0)$, so the inverse of a general element $(n,h) \in \mathbb{Z} \rtimes_\varphi \mathbb{Z}$ is

$$((-1)^{h+1}n, -h). \qquad //$$

Example 6.3.2. Let $N = (\mathbb{R}, +)$, $H = (\mathbb{R}^\times, \times)$.

$$\begin{array}{ccccc} \mathbb{R}^\times & \xrightarrow[y \longmapsto x(y)]{\varphi} & \mathrm{Aut}(\mathbb{R}) & \cong & \mathbb{R}^\times \\ x & \longmapsto & & & x \end{array}$$

Now $\mathbb{R} \rtimes \mathbb{R}^\times$, $(n_1,h_1) * (n_2,h_2) = (n_1\varphi(h_1)h_2, h_1h_2) = (n_1 + h_1n_2, h_1h_2)$. The identity is $(0,1)$, so the inverse of a general element $(n,h) \in \mathbb{R} \rtimes_\varphi \mathbb{R}^\times$ is

$$(n,h)^{-1} = (-n/h, h^{-1})$$

This group may look familiar—indeed, it is

$$\begin{pmatrix} h_1 & n_1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} h_2 & n_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} h_1h_2 & n_1 + h_1n_2 \\ 0 & 1 \end{pmatrix}$$

with the group

$$G = \left\{ \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} \;\middle|\; y \in \mathbb{R}^\times, x \in \mathbb{R} \right\},$$

under the isomorphism $\left(\begin{smallmatrix} y & x \\ 0 & 1 \end{smallmatrix}\right) \longmapsto (x,y)$. //

Example 6.3.3. Let p be prime. Whereas all groups of order p or p^2 are abelian, there are for $p \neq 2$ non-isomorphic, non-abelian groups of order p^3. In fact, there are exactly two of them, up to isomorphism. (For -2, there are also two non-isomorphic groups of order $2^3 = 8$, namely D_8 and Q_8, and we showed in Exercise 1.2 that these are not isomorphic.)

(a) The **Heisenberg group** $H_p = (\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \rtimes_\varphi \mathbb{Z}/p\mathbb{Z}$, where $\varphi\colon \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}_{\mathrm{Grp}}(\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}) \xrightarrow{\cong} \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ given by $\varphi(a) = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$, where this isomorphism is an exercise. (Hint: Try the obvious choice of basis for $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$). Here we think of elements of $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ as column vectors acted on by left $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$-multiplication. (Explicitly,

$$a \cdot (x,y) = (x, ax + y),$$

where the '$\cdot$' is induced by φ. We may sometimes write $a \underset{\varphi}{\cdot} (x, y)$ to indicate this.). Note that choosing $\varphi(a) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ would also work, but it would yield a slightly different action '$\cdot$' induced by φ. Recall that for *any* semidirect product, the action $a \underset{\varphi}{\cdot} (x, y)$ *is* conjugation in the group, $a(x, y)a^{-1}$, and hence this group is non-abelian. Writing this action using multiplicative notation, we can write

$$H_p = (C_p \times C_p) \times_\varphi C_p = (\langle x \rangle \times \langle y \rangle) \rtimes_\varphi \langle t \rangle,$$

Where $t \cdot_\varphi x = x$, $t \cdot_\varphi y = xy$

(b) Consider $C_{p^2} \rtimes_\varphi C_p$ via $\langle x \rangle \rtimes \langle t \rangle$, where $\varphi \colon C_p \to \mathrm{Aut}_{\mathrm{Grp}}(C_p^2) \cong (\mathbb{Z}/p^2\mathbb{Z})^\times (\cong C_{p(p-1)})$ is determined by

$$t \underset{\varphi}{\cdot} x = x^{p+1},$$

where again by $t \underset{\varphi}{\cdot} x = \varphi(t)(x)$. To check that t acts with order p, compute

$$\underbrace{t \cdot t \cdot t \cdots t}_{p \text{ times}} \cdot (x) = x^{(p+1)^p} = x^{1+u} = x,$$

where $u \in p^2\mathbb{Z}$, since by binomial expansion we have $(1 + p)^p = 1^p + p \cdot$ (something) $+ \cdots$.

(c) Finally, for p an *odd* prime, the groups in (a) and (b) are not isomorphic: we can check this by showing every element of H_p has order p, whereas the group in (b) has elements of order p^2. //

Example 6.3.4 (Classification of Groups of Order pq for Prime p, q)**.** Let p and q be distinct primes, say with $p < q$. Let G be a group of size pq. Then there exist $P \in \mathrm{Syl}_p(G)$ and $Q \in \mathrm{Syl}_q(G)$. Then $Q \lhd G$; this can be seen by noting the index of Q is the prime factor of Q, or alternatively by using Sylow III (since $n_q(G) \mid p$ and $n_q(G) \equiv 1 \pmod q$, so $p < q$ forces $n_q(G) = 1$, and hence that $Q \lhd G$). Since

- $Q \lhd G$,
- $P \cap Q = \{1\}$ (as $p \neq q$) by Lagrange's theorem, and
- $PQ = G$ (since $|PQ| = pq$ by the third isomorphism theorem),

we conclude $G \cong Q \rtimes_\varphi P$, where $\varphi \in \mathrm{Aut}\, Q$ is the map $\varphi(x)(y) = xyx^{-1}$. Since $Q \cong C_q$, we have $\mathrm{Aut}(Q) \cong C_{q-1}$, and φ is trivial unless $p \mid (q - 1)$ since $|\mathrm{im}\, \varphi| \mid \gcd(p, q - 1)$.

- Case I: $q \not\equiv 1 \pmod p$. Then $\varphi = \mathrm{id}$ and $G \cong Q \times P \cong C_q \times C_p \cong C_{pq}$.
- Case II: $q \equiv 1 \pmod p$. Since $\mathrm{Aut}(Q) \cong (\mathbb{Z}/q\mathbb{Z})^\times$, there exists a unique order p-subgroup of $\mathrm{Aut}(Q)$, say $\langle \gamma \rangle < \mathrm{Aut}(Q)$. Let $P = \langle x \rangle$. Any group homomorphism $\varphi \colon P \to \mathrm{Aut}(Q)$ then has the form $\varphi_i(x) = \gamma^i$ for some $i = 0, 1, \ldots, p - 1$. Then
  - $i = 0$ gives $G \cong Q \times P$, whereas
  - all $0 < i < p$ give isomorphic non-abelian groups: to see this, that is, that $Q \rtimes_{\varphi_1} P \cong Q \rtimes_{\varphi_i} P$ for all $2 \leqslant i \leqslant p - 1$, note that $\varphi_i(x^j) = \gamma^{ij} = \gamma$ if we choose j such that $ij \equiv 1 \pmod p$. Let $Q = \langle y \rangle$ and set $\psi \colon Q \rtimes_{\varphi_1} P \to Q \rtimes_{\varphi_i} P$ by

$$\begin{aligned} \psi \colon Q \rtimes_{\varphi_1} P &\longrightarrow Q \rtimes_{\varphi_i} P, \\ x &\longmapsto x^j, \end{aligned}$$

$$y \longmapsto y,$$

that is, $\psi(y^r x^s) = y^r x^{js}$. We claim ψ is a bijection and a group homomorphism, and hence an isomorphism. It is clear that ψ is a bijection since $G = \langle y \rangle$ and $p = \langle x \rangle = \langle xj \rangle$. To see

psipsi is a group homomorphism, note that

$$\psi(y^r x^s \cdot y^t x^u) = \psi(y^r \underbrace{(x^s y^t x^{-s}) x^{s+u}}_{=\varphi_1(x^s)(y^t)}) = \psi(y^r \gamma^s(y^t) x^{s+u}) = y^r \gamma^s(y^t) x^{j(s+u)},$$

while

$$\psi(y^r x^s) \cdot \psi(y^t x^u) = y^r x^{js} \cdot y^t x^{ju} = y^r \underbrace{(x^{js} y^t x^{-js})}_{\varphi_i(x^{js})(y^t)} x^{j(s+u)} = y^r \cdot \gamma^{ijs}(y^t) x^{j(s+u)}.$$

But $\gamma^{ij} = \gamma$, so this is also $y^r \gamma^s(y^t) x^{j(s+u)}$, so we are done.

So, for example, every group of order 15 is cyclic, that is, there is exactly one group of order 15 up to isomorphism. On the other hand, there are exactly two groups of order $21 = 7 \cdot 3$ up to isomorphism, namely the cyclic group C_{21} and the non-abelian group $C_7 \rtimes C_3$, where C_3 acts on C_7 by conjugation. //

Example 6.3.5. (1) D_{2n} with $N = \langle \rho \rangle$ and $H = \langle \tau \rangle$ satisfies these, so

$$D_{2n} = \langle \rho \rangle \rtimes \langle \tau \rangle.$$

(2) S_n with $N = A_n$, $H = \langle (12) \rangle$ satisfies these, so

$$S_n = A_n \rtimes \langle (12) \rangle.$$

(3) A_4 with N the Klein 4-group $V = \{1, (12)(34), (13)(24), (14)(13)\}$, and $H = \langle (123) \rangle$. Then

$$A_4 = V \rtimes \langle (123) \rangle.$$ //

Proposition 6.3.6. Let $G = N \rtimes H$. Then $G/N \cong H$.

Proof. We have

$$\frac{G}{N} = \frac{HN}{N} \cong \frac{H}{N \cap H} = \frac{H}{\{1\}} \cong H,$$

where the second step is by the third isomorphism theorem. □

Example 6.3.7. Let $N = C_n = \langle g \rangle$, and $H = \{\pm 1\}$, and

$$\varphi \colon H \longrightarrow \mathrm{Aut}_{\mathrm{Grp}} N,$$
$$-1 \longmapsto (g \mapsto g^{-1}).$$

Then $N \rtimes_\varphi H \cong D_{2n}$. //

Example 6.3.8. Let $N = \mathbb{Z}/4\mathbb{Z}$, $H = \mathbb{Z}/3\mathbb{Z}$. What can we choose as $\varphi \colon H \to \mathrm{Aut}_{\mathrm{Grp}}(N)$? Well, this means choosing the image of the order 3 generator α of H, but then $\varphi \colon \mathbb{Z}/3\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/4\mathbb{Z}) \cong (\mathbb{Z}/4\mathbb{Z})^\times = \{1, 3\} \cong \mathbb{Z}/2\mathbb{Z}$, so the only option for $N \rtimes_\varphi H$ is the direct product $N \times H = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}/12\mathbb{Z}$. //

Example 6.3.9. Let $N = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $H = \mathbb{Z}/3\mathbb{Z}$. Then we need

$$\varphi \colon \langle g \rangle = H \to \mathrm{Aut}_{\mathrm{Grp}}(N) \cong \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3 = \left\langle \underbrace{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}}_{:=A}, \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_{:=B} \right\rangle.$$

We can choose φ to be the map determined by any of $g \mapsto 1$ (which yields the direct product group), $g \mapsto A$, or $g \mapsto A^2$. //

There are many sufficient conditions to show semidirect products are isomorphic to each other, but not many necessary conditions. The following is an example of a useful sufficient condition:

Theorem 6.3.10. Let N, H be groups, and suppose $f \in \mathrm{Aut}(H)$. Then if $\varphi\colon H \to \mathrm{Aut}(N)$, then
$$N \rtimes_{\varphi} H \cong N \rtimes_{\varphi \circ f} H.$$

Proof. We will construct an explicit isomorphism. Consider the map
$$\begin{aligned} \theta\colon N \rtimes_{\varphi\circ f} H &\longrightarrow N \rtimes_{\varphi} H, \\ (n,h) &\longmapsto (n, f(h)). \end{aligned}$$
Then θ is clearly a bijection of sets since it is a bijection of sets in each component. It only remains to check θ is a group homomorphism. We have
$$\theta(n_1,h_1) * \theta(n_2,h_2) = (n_1, f(h_1)) * (n_2, f(h_2)) = (n_1\varphi \circ f(h_1)(n_2), f(h_1)f(h_2)).$$
On the other hand,
$$\theta((n_1,h_1) * (n_2,h_2)) = \theta((n_1\varphi \circ f(h_1)n_2, h_1h_2)) = (n_1, \varphi \circ f(h_1)n_2, f(h_1h_2)).$$ □

Example 6.3.11. We can return to a previous example now. The group $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \rtimes_{\varphi} \mathbb{Z}/3\mathbb{Z}$. Identifying $(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z})$ with V and $\langle(123)\rangle$ with $\mathbb{Z}/3\mathbb{Z}$, we see that $(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}) \rtimes_{\varphi} \mathbb{Z}/3\mathbb{Z} \cong A_4$, where $(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z})$ corresponds to the subgroup of A_4 isomorphic to the Klein 4-group and $\mathbb{Z}/3\mathbb{Z}$ correspjonds to the three 4-cycles of A_4.

In the above example, let us now swap N and H. Let $N = \mathbb{Z}/3\mathbb{Z}$ and $H = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \{(0,0),(1,0),(0,1),(1,1)\}$, and
$$H \xrightarrow{\varphi} \mathrm{Aut}(N) \cong \{\pm 1\},$$
and $(1,0) \longmapsto -1$, $(0,1) \longmapsto -1$, $(1,1) \longmapsto 1$. If $H = \{1, a, b, c = a + b\}$, then $\mathrm{Aut}(H) \cong \mathrm{GL}_2((\mathbb{Z}/2\mathbb{Z})^2) \cong S_3$. Any $\varphi\colon H \to \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z} = \{\pm 1\}$ can be written as $\varphi \circ f$ for some $f \in \mathrm{Aut}(H)$ for φ, so $(1,0) \longmapsto 1$, $(0,1) \longmapsto -1$, $(1,1) \longmapsto -1$. Let
$$\mathbb{Z}/2\mathbb{Z} \rtimes_{\varphi} (\underbrace{\mathbb{Z}/2\mathbb{Z}}_{=\langle y\rangle} \times \underbrace{\mathbb{Z}/2\mathbb{Z}}_{=\langle z\rangle}).$$
Then $G = \langle x, y, z \mid x^3 = y^2 = z^2 = 1, yz = zy, yxy^{-1} = x, zxz^{-1} = x^{-1}\rangle$. We claim $G \cong D_{12}$, where the isomorphism is given by $G \to D_{12}$, $x \mapsto \rho^2$, $y \mapsto \rho^3$, and $z \mapsto \tau$. //

Example 6.3.12. Now consider $H = \mathbb{Z}/4\mathbb{Z}, N = \mathbb{Z}/3\mathbb{Z}$, $H \longrightarrow \mathrm{Aut}(N) \cong \{\pm 1\}$, $g \longmapsto -1$. Now
$$G = \underbrace{\mathbb{Z}/3\mathbb{Z}}_{=\langle x\rangle} \rtimes \underbrace{\mathbb{Z}/4\mathbb{Z}}_{=\langle y\rangle}$$
satisfies $G = \langle x, y \mid x^3 = y^4 = 1, yxy^{-1} = x^{-1}\rangle$. This group is called the **dicyclic group of order 12**. //

So far we have constructed $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times/2\times\mathbb{Z}/3\mathbb{Z}$, A_4, and Dic_{12}. It turns out that these are *all* groups of order 12!

Warning 6.3.13. Note that even if a group G is not simple, then it is not necessarily true that G can be written as a semidirect product. Indeed, neither Q_8 nor C_{p^n} for any integer $n \geqslant 1$ can be written as a semidirect product.

6.4 Exact Sequences

Suppose we have group homomorphisms

$$G_1 \xrightarrow{\varphi} G_2 \xrightarrow{\psi} G_3.$$

We say the sequence is **exact** at G_2 if $\ker\psi = \operatorname{im}\varphi$. More generally, we say a sequence

$$G_1 \xrightarrow{\varphi_1} G_2 \xrightarrow{\varphi_2} G_3 \xrightarrow{\varphi_3} \cdots \xrightarrow{\varphi_{n-1}} G_{n-1}$$

is **exact** if for each $i = 1, \ldots, n-2$, it is exact at G_i, that is, if $\ker(\varphi_{i+1}) = \operatorname{im}(\varphi_i)$. A common situation is that of a **short exact sequence (short exact sequence)**, which is an exact sequence of the form

$$\{1\} \longrightarrow G_1 \xrightarrow{\varphi} G_2 \xrightarrow{\psi} G_3 \longrightarrow \{1\}.$$

Here we do not name the leftmost and rightmost group homomorphisms, since they are uniquely determined (both must be the identity group homomorphism). By exactness, one can deduce that

(a) φ is injective ($\ker\varphi = \{1\}$),

(b) $\ker\psi = \operatorname{im}\varphi$, and

(c) ψ is surjective ($\operatorname{im}\psi = G_3$),

and these imply G_1 is isomorphic to $\varphi(G_1) \lhd G_2$, and $G_2/\varphi(G_1) \xrightarrow{\cong} G_3$.

Example 6.4.1. Given a semidirect product $N \rtimes_\varphi H$, we have a short exact sequence

$$\begin{array}{ccccccc} 1 & \longrightarrow & N & \longrightarrow & N \rtimes_\varphi H & \longrightarrow & H \longrightarrow 1 \\ & & n & \longmapsto & (n,1) & & \\ & & & & (n,h) & \longmapsto & h \end{array}$$

//

6.5 Characterization of Semidirect Products as Split Group Extensions

Definition 6.5.1. Given a short exact sequence of groups $1 \to G' \to G \to G'' \to 1$, we say G is a **group extension of G'' by G'**.

Example 6.5.2. For any semidirect product $G = N \rtimes_\varphi H$, G is an extension of H by N by considering the short exact sequence

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

where $N \to G$ by $n \mapsto (n,1)$ and $G \to H$ by $(n,h) \mapsto h$. These extensions for $G = N \rtimes_\varphi H$ has the following property: π admits a **section**, which means there exists a homomorphism $s\colon H \to G$ such that $\pi \circ s = \mathrm{id}_H$, namely the map $s\colon h \mapsto (1,h)$. This *is* a group homomorphism. (Note that for a map to have a section, that map must be surjective.) //

Theorem 6.5.3 (Characterization of Semidirect Products as Split Group Extensions)**.** A group extension $1 \longrightarrow K \xrightarrow{i} G \xrightarrow{\pi} H \longrightarrow 1$ admits a section $s\colon H \to G$ if and only if there exists a group isomorphism $f\colon G \xrightarrow{\cong} K \rtimes_\varphi H$ for some group homomorphism $\varphi\colon H \to \mathrm{Aut}_{\mathrm{Grp}}(K)$ such that the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K & \xrightarrow{\quad i \quad} & G & \xrightarrow{\quad \pi \quad} & H & \longrightarrow & 1 \\ & & \| & & \cong\uparrow f & & \| & & \\ 1 & \longrightarrow & K & \xrightarrow[\alpha\colon k\mapsto(k,1)]{} & K \rtimes_\varphi H & \xrightarrow[\beta\colon (k,h)\mapsto h]{} & H & \longrightarrow & 1 \end{array}$$

commutes. And in this case, $\varphi(h)(k) = i^{-1}(s(h)i(k)s(h^{-1}))$

Proof. The "if" direction follows from **??**. Conversely, assume $\pi\colon G \to H$ admits a section $s\colon H \to G$. We need to build $\varphi\colon H \to \mathrm{Aut}_{\mathrm{Grp}}(K)$. Define $\varphi(h) \in \mathrm{Aut}_{\mathrm{Grp}}(K)$ to be conjugation by $s(h)$; more precisely, for all $h \in H$, $k \in K$, $\varphi(h)(k) = s(h)i(k)s(h)^{-1}$, which is an element of $\operatorname{im} i$, and since i is injective it makes perfectly good sense to take its preimage in K. Then define a function $f\colon K \rtimes_\varphi H \to G$ by $f(k,h) = i(k)s(h)$. Then the claim is that f makes the given diagram commute, and that f is a group isomorphism.

For the square

$$\begin{array}{ccc} K & \xrightarrow{\quad i \quad} & G \\ \| & & \uparrow f \\ K & \xrightarrow[\alpha\colon k \mapsto (k,1)]{} & K \rtimes_\varphi H \end{array}$$

we need to check that for all $k \in K$,

$$i(k) = f(\alpha(k)) = f(k,1) = i(k)s(1) = i(k). \quad \checkmark$$

For the square

$$\begin{array}{ccc} G & \xrightarrow{\quad \pi \quad} & H \\ f\uparrow & & \| \\ K \rtimes_\varphi H & \xrightarrow[\beta\colon (k,h) \mapsto h]{} & H \end{array}$$

we must check for all $(k,h) \in K \rtimes_\varphi H$,

$$h = \pi(s(h)) = \pi(i(k)s(h)) = \pi(f(k,h)) = \beta(k,h) = h,$$

where we used $\pi \circ i(k) = 1$ that s is a section of π.

Note f is a homomorphism, since for all pairs $k_1, k_2 \in K$, $h_1, h_2 \in H$, we have

$$\begin{aligned} f((k_1,h_1)\cdot(k_2,h_2)) &= f((k_1\varphi(h_1)(k_2), h_1h_2)) = i(k_1\varphi(h_1)(k_2))s(h_1h_2) \\ &= i(k_1)i(i^{-1}(s(h_1)i(k_2)s(h_1)^{-1}))s(h_1)s(h_2) = i(k_1)s(h_1)i(k_2)s(h_2) \\ &= f(k_1,h_1)\cdot f(k_2,h_2). \end{aligned}$$

It only remains to show f is a bijection. For injectivity it suffices to prove

$$f(k,h) = 1 \implies (k,h) = (1,1)$$

(because f is a group homomorphism). If $f(k,h) = 1$, then $i(k)s(h) = 1$. Apply π to deduce $h = 1$. Then $i(k) = 1$, and hence $k = 1$. To see f is surjective, let $g \in G$. Then since $\pi \circ s = \mathrm{id}_H$,

$$g \cdot s(\pi(g))^{-1} \ker(\pi).$$

And $\ker \pi = \mathrm{im}(i)$, so there exists $k \in K$ such that $i(k) = g \cdot s(\pi(g))^{-1}$. Hence

$$g = i(k)\cdot s(\pi(g)) = f(k, \pi(g)), \qquad \checkmark$$

Thus f is surjective. Hence group extensions are precisely semidirect products. □

When a short exact sequence admits a section, we say the short exact sequence **splits**. Not all short exact sequences split, however, as the following example shows.

Example 6.5.4. Recall the group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ from Homework 1. There is an extension

$$1 \longrightarrow \{\pm 1\} \longrightarrow Q_8 \xrightarrow{\pi} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to 1,$$

where π is determined by $\pi(i) = (1,0)$ and $\pi(j) = (0,1)$. There is no section of π, since $\pi(s(1,0)) = (1,0)$, and hence $s(1,0) \in \{\pm 1\}$. But $(1,0)$ has order 2, whereas $\pm i$ has order 4, so s cannot be a group homomorphism. This shows by the previous theorem that Q_8 cannot be a semidirect product of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $\{\pm 1\}$. To show Q_8 cannot be *any* semidirect product, consider the other normal

subgroups and subgroups that multiply to the same group and use similar arguments. //

6.6 Homework 5

Exercise 6.6.1. (1) We define a group G to be **solvable** when it has a normal tower

$$\{1\} = G_r \lhd G_{r-1} \lhd \cdots \lhd G_1 \lhd G_0 = G$$

such that G_i/G_{i+1} is abelian for all $i = 0, \ldots, r-1$. Now let G be a group, and let H be a normal subgroup of G. Prove that if G is solvable, then H and G/H are solvable.

Remark 6.6.2. This is in fact, an if and only if statement. We explain the converse on September 25, 2023.

Solution. Let H be a normal subgroup of a solvable group G. Since G is solvable, there exists a normal tower

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = \{1\}$$

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

- *Step 1: Show G/H is solvable.* Let $\overline{G}_i = G_iH/H$. Then $\overline{G} = \overline{G}_0 > \overline{G}_1 > \cdots > \overline{G}_r$ is a tower of subgroups.

  To see $\overline{G}_{i+1} \lhd \overline{G}_i$, note that if $g_{i+1}hH \in \overline{G}_{i+1}$ and $g_ihH \in \overline{G}_i$, then

  $$\begin{aligned}(g_{i+1}h_iH)(g_ih_{i+1}H)(g_{i+1}h_iH)^{-1} &= (g_iH)(g_{i+1}H)(h^{-1}g_i^{-1}H)\\ &= (g_iH)(g_{i+1}H)(g_i^{-1}H)\\ &= (g_ig_{i+1}g_i^{-1})H,\end{aligned}$$

  which is an element of $G_{i+1}/H \subset \overline{G}_{i+1}$ because $G_{i+1} \lhd G$. Hence

  $$G/H = \overline{G}_0 \rhd \overline{G}_1 \rhd \cdots \rhd \overline{G}_r = \{1\}$$

  is a normal tower of G/H.

  To see $\overline{G}_i/\overline{G}_{i+1}$ is abelian for each $0 \leqslant i \leqslant r-1$, write

  $$\begin{aligned}\frac{\overline{G}_i}{\overline{G}_{i+1}} &= \frac{G_iH/H}{G_{i+1}H/H}\\ &\cong \frac{G_iH}{G_{i+1}H} && \text{(by the Second Isomorphism Theorem)}\\ &= \frac{G_i(G_{i+1}H)}{G_{i+1}H} && \text{(since } G_{i+1} \subset G_i \text{ implies } G_iH = G_i \cap G_{i+1}H)\\ &\cong \frac{G_i}{(G_i \cap G_{i+1}H)} && \text{(by the Third Isomorphism Theorem)}\\ &\cong \frac{G_i/G_{i+1}}{(G_i \cap G_{i+1}H)/G_{i+1}}, && \text{(by the Second Isomorphism Theorem)}\end{aligned}$$

  where we were able to apply the Second Isomorphism Theorem in the last step because $G_{i+1} \lhd G_i \cap G_{i+1}H$, which follows from the fact $G_{i+1} \subset G_i \cap G_{i+1}H \subset G_i$. Now we know $\overline{G}_i/\overline{G}_{i+1}$ is isomorphic to a quotient group of the abelian group G_i/G_{i+1}. But any quotient group of an abelian group is abelian, so $\overline{G}_i/\overline{G}_{i+1}$ is abelian. Hence G/H is solvable.

- H is solvable: Let $H_i = G_i \cap H$. Then $H = H_0 > H_1 > \cdots > H_r$ is a tower of subgroups.

  We claim $H_{i+1} \lhd H_i$ for each i. If $g_{i+1} \in H_{i+1} = G_{i+1} \cap H$ and $g_i \in H_i = G_i \cap H$, then $g_i, g_{i+1} \in H$, so $g_ig_{i+1}g_i^{-1} \in H$. On the other hand, since $g_i \in G_i$ and $g_{i+1} \in G_{i+1}$ and

$G_{i+1} \lhd G_i$, we know $g_i g_{i+1} g_i^{-1} \in G_{i+1}$. Hence $g_i g_{i+1} g_i^{-1} \in G_{i+1} \cap H = H_{i+1}$, so $H_{i+1} \lhd H_i$. Thus

$$H = H_0 \rhd H_1 \rhd \cdots \rhd H_r = \{1\}$$

is a normal tower. To see H_i/H_{i+1} is abelian, write

$$\begin{aligned} \frac{H_i}{H_{i+1}} &= \frac{G_i \cap H}{G_{i+1} \cap H} \\ &= \frac{G_i \cap H}{G_{i+1} \cap (G_i \cap H)} && \text{(since } G_{i+1} \subset G_i \text{ implies } G_{i+1} = G_{i+1} \cap G_i\text{)} \\ &\cong \frac{(G_i \cap H)G_{i+1}}{G_{i+1}}, && \text{(by the Third Isomorphism Theorem)} \end{aligned}$$

which is a subgroup of G_i/G_{i+1} by the Correspondence Theorem, since $(G_i \cap H)G_{i+1}$ is a subgroup of G_i. But G_i/G_{i+1} is abelian, and any subgroup of an abelian group is abelian, so we conclude H_i/H_{i+1} is abelian. Thus H is solvable. □

Exercise 6.6.3. Let G be a finite p-group. Prove that G is solvable.

Solution. We argue by induction over n. To see the base case note that any group of order $p^0 = 1$ is isomorphic to the trivial group, and $G = \{1\}$ is a normal tower and vacuously has abelian factor groups, and hence is solvable.

Now suppose for all $1 \leqslant k \leqslant n-1$ that if $|G| = p^k$ then G is solvable. Let G be a group of order p^n. By a corollary to Cauchy's Theorem , there exists a subgroup $H < G$ of order p^{n-1}. Then H is solvable by the induction hypothesis. Since $[G : H] = p$ and p is the smallest prime dividing $|G| = p^n$, by Exercise 3.4. Thus G/H is a group of order $p^n/p = p^{n-1}$, and hence is also solvable by the induction hypothesis. Then G is solvable by Exercise 5.1. We conclude that any finite p-group is solvable. □

Exercise 6.6.4. Let p be an odd prime. Show that every group G of order $2p$ is isomorphic to one of C_{2p} or D_{2p}.

Solution. Let p be an odd prime and let G be a group of order $2p$. If G has an element of order $2p$ then $G \cong C_{2p}$, affirming the claim. Now suppose no such element of G exists. By Cauchy's Theorem, there exist elements $r, t \in G$ of order 2 and p, respectively. Then $\langle t \rangle \cap \langle r \rangle = 1$, since cyclic group of different prime orders intersect trivially.

We showed in lecture that for any group G of order qp, where q, p are primes such that $p \equiv 1 \pmod q$, then G is isomorphic to either C_{qp} or $P \rtimes_\varphi Q$, where Q and p are *any* elements of $\mathrm{Syl}_q(G)$ and $\mathrm{Syl}_p(G)$, respectively, $\varphi \colon Q \to \mathrm{Aut}_{\mathrm{Grp}}(P)$ is any nontrivial group homomorphism, and that all groups of the latter type are isomorphic.

In the current setting we have primes p, q with $q = 2 < p$, $p \equiv 1 \pmod 2$, and $\langle t \rangle \in \mathrm{Syl}_2(G)$, $\langle r \rangle \in \mathrm{Syl}_p(G)$. The conditions mentioned above are satisfied, so $G \cong \langle r \rangle \rtimes_\varphi \langle t \rangle$, where $\varphi : \langle t \rangle \to \mathrm{Aut}(\langle r \rangle)$ is the nontrivial group homomorphism given by $\varphi(t)(r) = r^{p-1}$. □

Solution. (Alternate Solution). By Cauchy's Theorem, there exists $x, y \in G$ with $\operatorname{ord} y = 2, \operatorname{ord} x = p$. Now

$$[G : \langle x \rangle] = 2,$$

so $N = \langle x \rangle \lhd G$, $H = \langle y \rangle \leqslant G$. And $N \cap H = \{1\}$, $|NH| = |N||H|/|N \cap H| = |N||H| = 2p$, so $NH = G$. Thus $G \cong N \rtimes H$. Any homomorphism $\varphi \colon \langle g \rangle \cong C_2 \cong H \to \mathrm{Aut}(N) \cong (\mathbb{Z}/p\mathbb{Z})^\times \cong C_{p-1}$ is either $g \mapsto 0$, $g \mapsto (p-1)/2$ is the only such homomorphism because we need $\mathbb{Z}/2\mathbb{Z} \ni 0 = g^2 \mapsto \varphi(p)^2 = 0 \in \mathbb{Z}/(p-1)\mathbb{Z}$. □

Exercise 6.6.5. Let H_p for p an odd prime be the group constructed in class: it is a semidirect product $H_p = N \rtimes_\varphi H$ where $N = (\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}), H = \mathbb{Z}/p\mathbb{Z}$, and $\varphi\colon H \to \mathrm{Aut}_{\mathrm{Grp}}(N)$ is the homomorphism

$$\varphi(a) = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$$

for all $a \in H = \mathbb{Z}/p\mathbb{Z}$, and where the matrix $\varphi(a)$ is regarded as an automorphism of $N = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ by matrix multiplication on column vectors. Prove that H_p is isomorphic to the subgroup of matrices

$$\left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; x, y, z \in \mathbb{Z}/p\mathbb{Z} \right\} < \mathrm{GL}_3(\mathbb{Z}/p\mathbb{Z}).$$

Solution. We will use additive notation throughout. Since 1 is a generator for $\mathbb{Z}/p\mathbb{Z}$, we will make the identification $H_p = (C_p \times C_p) \rtimes_\varphi C_p \cong (\langle 1\rangle \rtimes_\varphi \langle 1\rangle) \rtimes_\varphi \langle 1\rangle$. Now let G be the given matrix group and define a map $\Phi\colon H_p \to G$ by

$$\Phi((a,b),c) = \begin{pmatrix} 1 & c & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{pmatrix}.$$

There is no issue with Φ being well-defined, so it remains to show Φ is a bijective group homomorphism. To see Φ is bijective, it is enough to show Φ is surjective because $|G| = |H_p| = p^3$. (Indeed, $|H_p| = p^3$ because $|H_p| = |(C_p \times C_p) \times C_p| = p^3$, and $|G| = p^3$ because any of the p^3 matrices of the form $\left(\begin{smallmatrix} 1 & c & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{smallmatrix}\right) \in G$ has determinant $1 \neq 0$ and hence are in the subgroup G of $\mathrm{GL}_3(\mathbb{Z}/p\mathbb{Z})$.) And Φ is surjective, since any $\left(\begin{smallmatrix} 1 & c & b \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{smallmatrix}\right) \in G$ can be written as $\Phi((a,b),c) = \left(\begin{smallmatrix} 1 & c & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{smallmatrix}\right) \in G$. Thus Φ is bijective. And Φ is a group homomorphism, since if $((i_1,j_1),k_1), ((i_2,j_2),k_2) \in G$, then

$$\begin{aligned} \Phi(((i_1,i_1),k_1) * ((i_2,i_2),k_2)) &= \Phi(((i_1,j_1)\cdot(i_2,k_1i_2+j_2),k_1+k_2)) \\ &= \begin{pmatrix} 1 & k_1+k_2 & j_1+j_2+k_1i_2 \\ 0 & 1 & i_1+i_2 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & k_1 & j_1 \\ 0 & 1 & i_1 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & k_2 & j_2 \\ 0 & 1 & i_2 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \Phi(((i_1,j_1),k_1))\Phi(((i_2,j_2),k_2)) \end{aligned}$$

so Φ is a bijective group homomorphism, and hence a group isomorphism. □

Exercise 6.6.6. Show that $\mathrm{Aut}(Q_8)$ is isomorphic to S_4. Hint: analyze the short exact sequence

$$1 \to \mathrm{Inn}(Q_8) \to \mathrm{Aut}(Q_8) \to \mathrm{Aut}(Q_8)/\mathrm{Inn}(Q_8) \to 1,$$

where $\mathrm{Inn}(Q_8)$ is the group of inner automorphisms of Q_8: See Exercises 3.1 and 4.1(a).

Remark 6.6.7. Some terminology: for any group G, the quotient $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ is called the group of **outer automorphisms** of G and is typically denoted $\mathrm{Out}(G)$.

Solution. We first prove a lemma about S_4:

Lemma 6.6.8. Identify the Klein four-group V_4 with the subgroup

$$\{1, (12)(34), (13)(24), (14)(23)\} < S_4,$$

and identify S_3 with the subgroup of all elements of S_4 that fix 4. Then S_4 can be written as an internal semidirect product

$$S_4 = V_4 \rtimes S_3. \qquad \square$$

Proof. We have $V_4 \lhd S_4$ because $V_4 \in \mathrm{Syl}_2(A_4)$ and $V_4 \lhd A_4 \lhd S_4$. Also $V_4 \cap S_3 = \{1\}$, since no non-identity element of V_4 fixes 4, whereas non-identity elements of S_3 do. Then by the Third Isomorphism Theorem, $|V_4S_3| = |V_4||S_3|/|V_4 \cap S_3| = 4 \cdot 6/1 = 24 = |S_4|$, so $V_4S_3 = S_4$. Thus $S_4 = V_4 \rtimes S_3$. $\square$

Lemma 6.6.9. We have $\mathrm{Inn}(Q_8) \cong V_4$, where V_4 is the Klein four-group.

Proof. Recall $\mathrm{Inn}(Q_8) = \mathrm{im}\, c$, where $c\colon Q_8 \to \mathrm{Aut}(Q_8)$ is the conjugation map sending elements $g \in Q_8$ to the group automorphism $c_g\colon Q_8 \xrightarrow{\cong} Q_8$ given by $c_g(h) = ghg^{-1}$. Applying the First Isomorphism Theorem, c descends to a group isomorphism

$$\overline{c}\colon Q_8/\ker c = Q_8/Z(Q_8) = \{1, \{\pm i\}, \{\pm j\}, \{\pm k\}\} \xrightarrow[\{\pm g\} \mapsto c_g]{\cong} \mathrm{Inn}(Q_8).$$

In particular, this means

$$\mathrm{Inn}(Q_8) = \overline{c}(\{\{\pm 1\}, \{\pm i\}, \{\pm j\}, \{\pm k\}\}) = \{\mathrm{id}_{Q_8}, c_i, c_j, c_k\} = \langle c_i, c_j \rangle,$$

where for the last equality we used that $c_k = c_{ij}$ (because c is a group homomorphism and $ij = k$). We showed at the end of Exercise 1.4 that $Q_8/Z(Q_8) = \{\mathrm{id}_{Q_8}, \{\pm i\}, \{\pm j\}, \{\pm k\}\} \cong V_4$, where V_4 is the Klein four-group. $\square$

Lemma 6.6.10. $\mathrm{Out}(Q_8) \cong S_3$.

Proof. Let $\mathrm{Aut}(Q_8)$ act on the set $X = \{\{\pm i\}, \{\pm j\}, \{\pm k\}\}$ of non-identity left cosets of $Q_8/Z(Q_8)$ by $\sigma \cdot \{\pm \ell\} = \{\pm\sigma(\ell)\}$ for each $\ell \in \{i, j, k\}$. (This is indeed a group action: the only element of order 2 in Q_8 is -1, so any automorphism $\sigma \in \mathrm{Aut}(Q_8)$ must have $\sigma(-1) = -1$, and hence $\sigma(-\ell) = \sigma(-1)\sigma(\ell) = -\sigma(\ell)$ for each $\ell \in \{i, j, k\}$. It follows that this group action is well-defined. Since $\{\pm 1\}$ is sent to the identity by the identity automorphism and function composition is associative, this is a valid group action). Let $\alpha\colon \mathrm{Aut}(Q_8) \to S_X \cong S_3$ be the group homomorphism corresponding to this action.

- *Step 1: Show* $\mathrm{im}\,\alpha = S_3$. Suppose we are given an element $\sigma \in S_3$, which we identify as permuting (i, j, k) as it permutes the ordered set $(1, 2, 3)$. Then the transpositions τ_{ij} and τ_{jk} swapping i with j and j with k, respectively, are the images under α of the group automorphisms determined by $i \mapsto j$, $j \mapsto i$, and $i \mapsto i$, $j \mapsto k$, respectively. But τ_{ij} and τ_{jk} generate S_3, so $\mathrm{im}\,\alpha = S_3$.
- *Step 2: Show* $\ker\alpha = \mathrm{Inn}(Q_8)$. Note that for any $\sigma \in \mathrm{Aut}(Q_8)$,

$$\begin{aligned} \sigma \in \mathrm{Stab}(\{\pm i\}) \cap \mathrm{Stab}(\{\pm j\}) &\implies \sigma(k) = \sigma(i)\sigma(j) = \{\pm k\} \qquad \implies \sigma \in \mathrm{Stab}(\{k\}) \\ &\implies \alpha \in \mathrm{Stab}(\{\pm k\}) \\ &\implies \sigma \in \bigcap\nolimits_{x \in X} \mathrm{Stab}(x) = \ker\alpha \end{aligned}$$

  Then since But $\mathrm{Inn}(Q_8) < \ker\alpha$ since c_j since $\mathrm{Inn}(Q_8) < \mathrm{Stab}(\{\pm i\}) \cap \mathrm{Stab}(\{\pm j\})$.

  On the other hand, $|\ker\alpha| = 4$, because only 4 set bijections $Q_8 \to Q_8$ exist that descend to elements of both $\mathrm{Stab}(\{i\})$ and $\mathrm{Stab}(\{\pm j\})$, namely the maps those determined by $i \mapsto \pm i$ and $j \mapsto \pm j$. Since $\mathrm{Inn}(Q_8) < \ker\alpha$ and $\ker\alpha \leqslant |\mathrm{Inn}(Q_8)| = 4$, we conclude $\ker\alpha = \mathrm{Inn}(Q_8)$.
- *Step 3: Conclude* $\mathrm{Out}(Q_8) \cong S_3$. By the First Isomorphism Theorem, Steps 1 and 2 imply $\mathrm{Out}(Q_8) = \mathrm{Aut}\, Q_8/\mathrm{Inn}\, Q_8 \cong S_3$. $\square$

We can now prove the statement of **??**. Under the identifications $V_4 = \mathrm{Inn}(Q_8)$ and $\mathrm{Out}(Q_8) = S_3$, there are two short exact sequences of the form

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Inn}(Q_8) & \xrightarrow{i} & \mathrm{Aut}(Q_8) & \xrightarrow{\pi} & \mathrm{Out}(Q_8) & \longrightarrow & 1 \\ & & \| & & & & \| & & \\ 1 & \longrightarrow & V_4 & \longrightarrow & S_4 = V_4 \rtimes S_3 & \longrightarrow & S_3 & \longrightarrow & 1, \end{array}$$

where the bottom row is the usual short exact sequence corresponding to the semidirect product $V_4 \rtimes S_3$. To show $\mathrm{Aut}(Q_8) \cong S_4$, by a theorem proven in lecture it is enough to find a section s of π. By the universal mapping property of the quotient group, there exists a unique group homomorphism $s\colon \mathrm{Out}(Q_8) \to \mathrm{Aut}(Q_8)$ such that the diagram

$$\begin{array}{ccc} \mathrm{Aut}(Q_8) & \xrightarrow{\mathrm{id}_{Q_8}} & \mathrm{Aut}(Q_8) \\ & {\scriptstyle\pi}\searrow \quad \nearrow{\scriptstyle s} & \\ & \mathrm{Out}(Q_8) & \end{array}$$

commutes. We recall that s is defined by $s([\sigma]) = \mathrm{id}_{\mathrm{Aut}(Q_8)}(\sigma) = \sigma$ for all $[\sigma] \in \mathrm{Out}(Q_8)$. Then in particular, $\pi \circ s([\sigma]) = \pi(\sigma) = [\sigma]$ for all $[\sigma] \in \mathrm{Out}(Q_8)$, so $\pi \circ s = \mathrm{id}_{\mathrm{Out}(Q_8)}$. Thus s is a section of π, so we conclude $\mathrm{Aut}(Q_8) \cong S_4$.

7 The Jordan-Hölder theorem and More General Classes of Groups

7.1 Normal Towers and Composition Series

Definition 7.1.1. Let G be a group. A sequence of subgroups

$$\{1\} = G_r < G_{r-1} < \cdots < G_1 < G_0 = G$$

is called a **tower of subgroups**. If $G_{i+1} \lhd G_i$, then it is a **normal tower**; if it is a normal tower *and* for all i, G_i/G_{i+1} is a simple group, it is called a **composition series**.

Example 7.1.2. $\mathbb{Z}$ has no composition series. However, we will soon see that every finite group has a composition series. (This is not entirely surprising, since one might imagine how a possible argument by induction over the order of the group.) //

A group G can have many different composition series, as the following example shows.

Exercise 7.1.3. We can write

$$G = C_2 \times C_2 \times C_2 \rhd \{1\} \times C_2 \times C_2 \rhd \{1\} \times \{1\} \times C_2 \rhd \{1\},$$

and

$$G = C_2 \times C_2 \times C_2 \rhd C_2 \times \{1\} \times C_2 \rhd C_2 \times \{1\} \times \{1\} \rhd \{1\}.$$

But, up to isomorphism and ordering, the sets of simple quotients G_i/G_{i+1} are in both cases the same 3 copies of C_2. It turns out that this is true in general for finite groups. We will soon prove a general uniqueness statement along these lines.

7.2 Solvable Groups

Definition 7.2.1. A group G is called **solvable** if it has a normal tower $G_0 \rhd G_1 \rhd \cdots \rhd G_r = \{1\}$ such that each G_i/G_{i+1} is abelian.

Exercise 7.2.2. Given a composition series with abelian quotients, that means those quotients are abelian simple groups. But the only abelian simple groups up to isomorphism are C_p for a prime p. Indeed, for any simple abelian group G, anny cyclic subgroup $1 \subsetneq \langle g \rangle \lhd G$ for all non-identity $g \in G$, so since G is simple we must have $\langle g \rangle = G$, that is, G is cyclic. But the only simple cyclic groups are C_p where p is a prime, so we are done.

Lemma 7.2.3. Let G be a group and let $H \lhd G$. Then G is solvable if and only if G and G/H are solvable.

Proof. The implication G is solvable implies H and G/H is solvable is on Homework 5. Conversely, suppose H and G/H is solvable. We want to show G is solvable. There is a normal tower

$$H = H_0 \rhd H_1 \rhd \cdots \rhd H_r = \{1\}$$

and

$$G/H = \overline{G}_0 \rhd \overline{G}_1 \rhd \cdots \rhd \overline{G}_s = \{1\}$$

such that H_i/H_{i+1} is abelian for all $i = 0, \ldots, i-1$ and $\overline{G}_j/\overline{G}_{j+1}$ is abelian for all $j = 0, \ldots, s-1$. The preimage G_j of $\overline{G}_j$ in G (under the canonical map $G \twoheadrightarrow G/H$) is a normal subgroup of G containing H, so we look at

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_s = H_0 \rhd H_1 \rhd H_2 \rhd \cdots \rhd r = \{1\}.$$

Since $G_j/G_{j+1} \cong \overline{G}_j/\overline{G}_{j+1}$ by the second isomorphism theorem, we see that G is solvable. □

The following is a very difficult theorem that will state but not prove.

Theorem 7.2.4 (Feit-Thompson)**.** Finite groups of odd order are solvable; equivalently, all finite simple groups of odd order are isomorphic to C_p for some odd prime p.

The contrapositive of this theorem is that all non-cyclic groups of odd order are not simple, which is quite a surprising result.

7.3 Equivalence of Normal Towers

Definition 7.3.1. (1) Let $G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = \{1\}$ be a normal tower. A **refinement** of this normal tower is any normal tower containing this normal tower as a subtower, that is, is any normal tower obtained from this one by inserting finitely many additional subgroups into the tower.

(2) Normal towers $G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = \{1\}$ and $G = H_0 \rhd H_1 \rhd \cdots \rhd H_s = \{1\}$ of G are **equivalent normal towers** if

(a) $r = s$, and

(b) there exists a permutation σ of $\{0, 1, \ldots, r-1\}$ such that for all $i = 0, \ldots, r-1$,

$$G_i/G_{i+1} \cong H_{\sigma(i)}/H_{\sigma(i)+1}.$$

Remark 7.3.2 (Intuition for Composition Series). The tagline of composition series is that every finite group G is "built" from simple groups: If G is not simple then there is some nontrivial proper normal subgroup $G_1 \lhd G$. If G_1 is not simple then there exists some nontrivial proper normal subgroup $G_2 \lhd G_1$. Repeating this process until we are forced to pick the normal subgroup to be the identity element $\{1\}$, we obtain a normal tower of G. Zooming in on the inclusion $G_{i+1} \lhd G_i$,

if G_i/G_{i+1} is not simple, then there exists $H/G_{i+1} \lhd G_i/G_{i+1}$, we obtain $G_{i+1} \lhd H \lhd G_i$. We can refine our normal tower of G by adding all possible Hs so to make the quotient G/G_i simple.

Warning 7.3.3. This does *not* mean that all groups G have composition series! (Why?)

Example 7.3.4. Consider the group $G = C_6$, say generated by g. Then

$$\{1\} \lhd \langle g^2 \rangle \lhd C_6$$

is a composition series, as the quotient $C_6/\langle g^2 \rangle = \langle g \rangle / \langle g^2 \rangle \cong C_3$ is simple and $\langle g^2 \rangle / \{1\} \cong \langle g \rangle \cong C_3$ is simple. But also

$$\{1\} \lhd \langle g^3 \rangle \lhd C_6.$$

This is also a composition series for similar reasons. These two composition series are equivalent, since

$$\{1\} \underset{C_3}{\lhd} \langle g^2 \rangle \underset{C_2}{\lhd} C_6,$$
$$\{1\} \underset{C_2}{\lhd} \langle g^3 \rangle \underset{C_3}{\lhd} C_6.$$ //

Example 7.3.5. If we know the quotients, however, we *cannot* recover the groups in general. Consider the following example. D_{12} and A_4 are then built out of the same groups, since

$$\{1\} \overset{C_3}{\triangleleft} \langle \rho^2 \rangle \overset{C_2}{\triangleleft} \langle \rho \rangle \overset{C_2}{\triangleleft} D_{12}$$
$$\{1\} \overset{C_2}{\triangleleft} \langle \rho^3 \rangle \overset{C_3}{\triangleleft} \langle \rho \rangle \overset{C_2}{\triangleleft} D_{12}$$

and notice that we have a different (but equivalent) composition series for D_{12} given by

$$\{1\} \overset{C_2}{\triangleleft} \langle \tau \rangle \overset{C_3}{\triangleleft} \langle \rho^2, \tau \rangle \underset{C_2}{\triangleleft} D_{12}.$$
$$\{1\} \overset{C_3}{\triangleleft} \langle \rho^2 \rangle \overset{C_2}{\triangleleft} \langle \rho \rangle \underset{C_2}{\triangleleft} D_{12}.$$

But

$$\{1\} \underset{C_2}{\lhd} \langle (12)(34) \rangle \underset{C_2}{\lhd} V_4 \underset{C_3}{\lhd} A_4 \qquad V_4 = \{1, (12)(34), (13)(24), (14)(23)\}$$ //

7.4 Uniqueness of Composition Series

Theorem 7.4.1. Let G be any group. Then the following hold.

(1) *(Schreier's Theorem).* Any two normal towers of G admit equivalent refinements.

(2) *(Jordan-Hölder Theorem).* Let G be a group. Then any two composition series of G are equivalent. Any finite group admits a composition series.

The proof of these statements do not require any high-powered ideas, but are drawn out by the admittedly cumbersome notation. To prove these, we will first show that Schreier's theorem implies the Jordan-Hölder theorem, and then return to prove Schreier's theorem.

Proof that Schreier's theorem Implies the Jordan-Hölder theorem. Let G be a group and suppose

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_{r-1} \rhd G_r = \{1\}$$

is a composition series of G. For any refinement

$$G = G_0 = G_{0,0} \rhd G_{0,1} \rhd \cdots \rhd G_{0,n_1} = G_{0,n_1}$$
$$\rhd G_1 = G_{1,0} \rhd G_{1,1} \rhd \cdots \rhd G_{r-1,n_r-1} \rhd G_{r-1,n_r} = G_r = \{1\},$$

for each $i = 0, \dots, r-1$, all but one $G_{i,j}$ equals G_{ij+1} and the remaining j has $G_{ij}/G_{i,j+1} \cong G_i/G_{i+1}$ (because G_i/G_{i+1} is already simple). In particular, the multiset of isomorphism classes of nontrivial quotients in $\{G_{i,j}/G_{i,j+1}\}_{i,j}$ is the same as that of $\{G_i/G_{i+1}\}_i$. Thus, for any other composition series of G, $G = H_0 \rhd H_1 \rhd \cdots \rhd H_s$, by Schreier's theorem, they have equivalent refinements and so must already be equivalent.

We now show existence of composition series for finite groups. We induct on the order of G, so we may assume all groups of order smaller than G admit a composition series. If G is simple then $1 \lhd G$ is a composition series for G, so assume G is not normal. Then G has some nontrivial proper normal subgroup H. Then H admits a composition series by the induction hypothesis, so we obtain a composition series for G in the exact same way as when showing that if H and G/H are solvable then G is solvable. This proves Schreier's theorem implies the Jordan-Hölder theorem. □

It only remains to prove point (1). The proof of point (1) is a bit difficult and a bit technical. To prove point (1), we use the following lemma, sometimes called the **Butterfly Lemma**. (Look in Lang's *Algebra* to find a picture of a butterfly, which you may or may not find convincing.) It is attributed to Zassenhaus, who was here at The Ohio State University.

Lemma 7.4.2 (Zassenhaus's Butterfly Lemma)**.** Let $H, K < G$, and even though $H' \lhd H$ and $K' \lhd K$. Then

(1) $H' \cdot (H \cap K) \lhd H'(H \cap K)$ and $(H' \cap K)K' \lhd (H \cap K)K'$.

(2) We have
$$\frac{H \cdot (H \cap K)}{H' \cdot (H \cap K')} \cong \frac{(H \cap K) \cdot K'}{(H' \cap K) \cdot K'}.$$

Proof of **??**. We first make two observations.

(a) For all groups G with $N \lhd G$, $H_1 \lhd H_2 < G$, we have $NH_1 \lhd NH_2$. The reason is that
$$n_2h_2(n_1h_1)h_2^{-1}n_2^{-1} = \underbrace{n_2}_{\in N} \cdot \underbrace{(h_2n_1h_2^{-1})}_{\in N} \underbrace{(hh_1h_2^{-1})}_{\in H_1} \underbrace{n_2^{-1}}_{\in N} \in NH_1,$$
since $N \lhd G$.

(b) Take $G = H$, $N = H'$, $H_1 = H \cap K'$, $H_2 = H \cap K$. Then (a) gives that $H'(H \cap K') \lhd H'(H \cap K)$.

Swapping H with K and H' with K' in (b), we have proved the other part of part (1) of the Butterfly Lemma. To see part (2) of the Butterfly Lemma, we use that if $M < G$, $N \lhd G$, then by the third isomorphism theorem $(MN)/N \cong M/(M \cap N)$. Then, where $M = H \cap K$, $N = H'(H \cap K')$ regarded as subgroups of $H' \cdot (H \cap K)$ (N is normal in $H'(H \cap K)$ by (1)), we have

$$\frac{MN}{N} = \frac{H'(H \cap K)}{H'(H \cap K')} \cong \frac{H \cap K}{(H'(H \cap K)) \cap (H \cap K)} \overset{(*)}{\cong} \frac{H \cap K}{(H' \cap K)(H \cap K')} \cong \frac{K'(H \cap K)}{K'(H' \cap K)},$$

where we will return to $(*)$ in a moment and where for the last isomorphism is for the following reason: we used that this is symmetric in $H \leftrightarrow K, H' \leftrightarrow K'$, so swapping the roles of those groups and reversing the steps we get this last isomorphism.

Now to complete the proof of the Butterfly Lemma it remains to show $(*)$. We have

$$(H' \cap K)(H \cap K') \subset [H'(H \cap K')] \cap (H \cap K)$$

is clear. For the reverse inclusion, let $g \in [H'(H \cap K') \cap (H \cap K)]$, write $g = x \cdot y$, where $x \in H'$, $y \in H \cap K'$. Then $x = gy^{-1} \in H \cap K$, and hence $x \in H' \cap K$. This completes the proof. □

Proof of Schreier's theorem. We need to show that when G is a group with two normal towers

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = \{1\}$$

and

$$G = H_0 \rhd H_1 \rhd \cdots \rhd H_s = \{1\},$$

then these towers admit equivalent refinements. For each $i = 0, \ldots, r-1$ and each $j = 0, \ldots, s$, define

$$G_{ij} = G_{i+1}(G_i \cap H_j).$$

Note $G_{is} = G_{i+1} = G_{i+1,0}$. So the groups G_{ij} are all inserted between G_i and G_{i+1}. By the Butterfly Lemma, $G_{i,j+1} \lhd G_{ij}$. [The Butterfly Lemma here is applied by taking $H' = G_{i+1} \lhd H$ and $K' = H_{j+1} \lhd K = H_j$.] Thus

$$G = G_0 = G_{0,0} \rhd G_{0,1} \rhd \cdots \rhd G_{r-1,0} \rhd G_{r-1,1} \rhd \cdots \rhd G_{r-1,s} = G_r = \{1\}$$

is a normal tower refining $G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = \{1\}$. Likewise, set $H_{ji} = H_{j+1}(H_j \cap G_i)$ to get a refinement of the second tower.

Note that we can omit the $G_{i,s}$ terms and the $H_{j,r}$ terms, since $H_{j,r} = H_{j+1,0}$ and $G_{i,s} = G_{i+1,0}$. When we account for this omission, each tower will have $rs + 1$ elements (since $i \in \{0, \ldots, r-1\}$ and $j \in \{0, \ldots, s-1\}$), and the extra term $+1$ in the sum accounts for the trivial subgroup $\{1\}$ at the bottom of the tower. Now by the Butterfly part (2),

$$\frac{G_{ij}}{G_{i,j+1}} = \frac{G_{i+1}(G_i \cap H_j)}{G_{i+1}(G_i \cap H_{j+1})} \cong \frac{H_{j+1}(G_i \cap H_j}{H_{j+1}(G_{i+1} \cap H_j)} = \frac{H_{j,i}}{H_{j,i+1}},$$

so up to a permutation the refined towers have isomorphic successive quotients. □

Remark 7.4.3. We should reiterate that of these results are especially deep; the ideas here are straightforward and almost staring us in the face, but are cumbersome, and their notation is unwieldy to write down, which draws out their arguments significantly.

7.5 Nilpotent Groups and More On Solvable Groups

Definition 7.5.1. For any group G, define that **derived series** $\{\mathcal{D}^n(G)\}_{n \geqslant 0}$ recursively by

$$\begin{cases} \mathcal{D}^0(G) = G, \\ \mathcal{D}^{n+1}(G) = [\mathcal{D}^n(G), \mathcal{D}^n(G)] \text{ for all } n \geqslant 0. \end{cases}$$

Define the **lower central series** recursively by

$$\begin{cases} \mathcal{C}^0(G) = G, \\ \mathcal{C}^{n+1}(G) = [G, \mathcal{C}^n(G)] \text{ for all } n \geqslant 0. \end{cases}$$

Warning 7.5.2. The notation here is not yet entirely standard. One may also see $G^{(n)}$ for the derived series $\mathcal{D}^n(G)$, and G^n for the lower central series.

Notation 7.5.3. Here we recall the notation that for any $H, K < G$, we write

$$[H, K] = \langle \{hkh^{-1}k^{-1} \mid h \in H, k \in K\} \rangle < G.$$

Proposition 7.5.4. For all $n \geqslant 0$, we have

- $\mathcal{D}^n(G)/\mathcal{D}^{n+1}(G)$ is abelian,
- $\mathcal{C}^{n+1}(G) \lhd \mathcal{C}^n(G) \lhd G$,
- $\mathcal{C}^n(G)/\mathcal{C}^{n+1}(G) < Z(G/\mathcal{C}^{n+1}(G))$. (This is **??**.)
- $\mathcal{D}^n(G) < \mathcal{C}^n(G)$, and these coincide when $n = 0$ or $n = 1$ (but not in general).

Proof. We used the third point to prove **??**. This is left as an exercise. □

Example 7.5.5. Let $G = S_3$. Then

$$S_3 = \mathcal{D}^0(S_3) \rhd \mathcal{D}^1(S_3) = [S_3, S_3] = A_3.$$

For example, $(12)(23)(12)^{-1}(23)^{-1} = (132)$. We also have

$$\mathcal{D}^1(S_3) = A_3 \cong C_3 \rhd \mathcal{D}^2(S_3) \cong [C_3, C_3] = \{1\}.$$

On the other hand,

$$S_3 = \mathcal{C}^0(S_3) \rhd \mathcal{C}^1(S_3) = [S_3, S_3] = A_3 \rhd \mathcal{C}^2(S_3) = [S_3, A_3] = A_3 = \mathcal{C}^n(S_3) \text{ for all } n \geqslant 1\!\!1.$$

Lemma 7.5.6. G is solvable if and only if $\mathcal{D}^n(G) = \{1\}$ for some $n \geqslant 0$.

Proof. If $\mathcal{D}^n(G) = 1$ for some n, then

$$G = \mathcal{D}^0(G) \rhd \mathcal{D}^1(G) \rhd \cdots \rhd \mathcal{D}^n(G) = \{1\}$$

is a normal tower with abelian quotients, and hence G is solvable. Conversely, assume $G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = \{1\}$ with (G_i/G_{i+1}) abelian for all $i = 0, \ldots, r-1$. Then $\mathcal{D}^i(G) < G_i$ for all i, which we can check by induction:

- The base case is $i = 0$ and indeed $G = G_0 = \mathcal{D}^0(G)$, so $\mathcal{D}^0(G) < G_0$. On the other hand, assume this is true for all indices less than i. Then $\mathcal{D}^{i-1}(G) < G_{i-1}$. Then G_{i-1}/G_i is abelian, so
$$\mathcal{D}^i(G) = [\mathcal{D}^{i-1}(G), \mathcal{D}^{i-1}(G)] < [G_i, G_i] < G_i.$$
We can now conclude $1 = G_r > \mathcal{D}^r(G), \mathcal{D}^r(G) = 1$. □

Thus, a group G is solvable if and only if its derived series terminates.

Definition 7.5.7. A group G is **nilpotent** if $\mathcal{C}^n = \{1\}$ for some n.

For example, S_3 is solvable but *not* nilpotent. Indeed, $\mathcal{C}^n(S_3) = A_3$ for all $n \geqslant 1$.

Definition 7.5.8. Define the **upper central series** of G by

$$\mathcal{Z}_0(G) = \{1\} < \mathcal{Z}_1(G) < \mathcal{Z}_2(G) < \cdots < \mathcal{Z}_n(G) < \cdots,$$

where

$$\begin{cases} \mathcal{Z}_0(G) = \{1\}, \\ \mathcal{Z}_n(G) = H \text{ if } n \geqslant 1, \text{ where } \mathcal{Z}_{n-1}(G) \subset H < G \text{ and } \dfrac{H}{\mathcal{Z}_{n-1}(G)} = \mathcal{Z}\left(\dfrac{G}{\mathcal{Z}_{n-1}(G)}\right), \end{cases}$$

Remark 7.5.9. Note that $\mathcal{Z}_n(G)$ is well-defined for all $n \geqslant 1$ because there exists exactly one such subgroup in G by the correspondence theorem. Using that the Correspondence Theorem is also a correspondence between normal subgroups, we can argue inductively that $Z_n(G) \lhd G$ for all n.

The proof of the following lemma is left as an exercise.

Lemma 7.5.10. A group G is nilpotent if and only if $\mathcal{Z}_n(G) = G$ for some n.

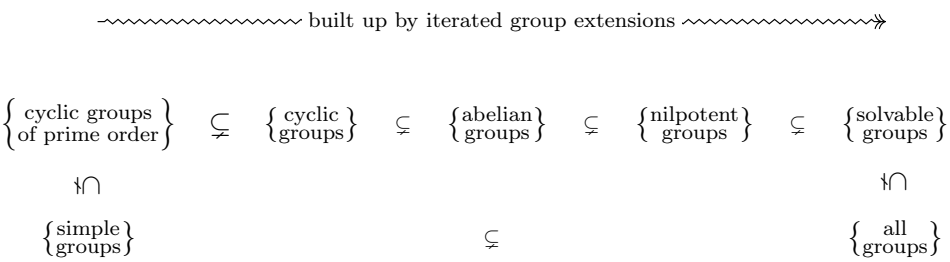


Figure 1: Hierarchy of Groups

7.6 Characterization of Finite Nilpotent Groups

The following theorem is somewhat surprising on the surface; it says that the finite simple groups are precisely those finite groups that are products of their Sylow p-subgroups.

In particular, it says that to understand nilpotent groups it is enough to understand p-groups.

Theorem 7.6.1 (Characterizations of Finite Nilpotent Groups)**.** Let G be a finite group. Let $p_1, \dots, p_s$ be the distinct primes dividing $|G|$. For all $i = 1, \dots, s$, let $P_i \in \mathrm{Syl}_{p_i}(G)$. Then the following are equivalent:

(1) G is nilpotent.

(2) For all proper subgroups H of G, $H \subsetneq N_G(H)$.

(3) For all $i = 1, \dots, s$, $P_i \lhd G$.

(4) $G \cong P_1 \times \cdots \times P_s$.

Proof. We will prove (1) $\implies$ (2) $\implies$ (3) $\implies$ (4).

- (1) $\implies$ (2): Assume (1). We will prove (2) by induction on $|G|$. Let G be nilpotent and let H be a proper subgroup of G. Note $N_G(H) > H \cdot Z(G)$, which properly contains H *unless* $Z(G) < H$. In the case $Z(G) < H$, we get $H/Z(G) < G/Z(G)$, and $|G/Z(G)| < |G|$ ($Z(G) \neq \{1\}$ because G is nilpotent). Since $H/Z(G)$ is a proper subgroup of $G/Z(G)$ (as H is a proper subgroup of G), by induction we have
$$\overline{N} \coloneqq N_{G/Z(G)}(H/Z(G))$$
properly contains $H/Z(G)$. Let N be the corresponding subgroup of G, that is, the subgroup of G equal to the preimage of N under the natural map $G \twoheadrightarrow G/Z(G)$. Then $H \subsetneq N < N_G(H)$, where the inclusion is proper because for $n \in N$, $h \in H$, $nhn^{-1} \pmod{Z(G)} \in H/Z(G)$, so $nhn^{-1} \in H \cdot Z(G) = H$, and hence $n \in N_G(H)$. This proves (2).

- (2) $\implies$ (3): Let $N_i = N_G(P_i)$ for $i = 1, \dots, s$. We want $N_i = G$. Since $\mathrm{Syl}_{p_i} \ni P_i \lhd N_i \lhd N_i \lhd N_G(N_i)$ (where the last normal relation is because $n_{p_i} = 1$), it follows from **??** that $P_i \lhd N_G(N_i)$. (In short, it is because for all $x \in N_G(N_i)$, the map $c_x \colon N_i \to N_i$ given by

$c_x \colon g \mapsto xgx^{-1}$ is an automorphism of N_i, so

$$\{P_i\} = \mathrm{Syl}_{p_i}(N_i) = c_x(\mathrm{Syl}_{p_i}(N_i)) = c_x(\{P_i\}),$$

so $xP_ix^{-1} \in P_i$, which means $P_i \lhd N_G(N_i)$.)

But then we see that

$$N_i < N_G(N_i) < N_G(P_i) = N_i,$$

so equality holds, and in particular $N_i = N_G(N_i)$. This forces $N_i = G$, that is, $P_i \lhd G$.

[Note that not only is P_i preserved by inner automorphisms, but it turns out that any unique Sylow p-subgroup of a finite group G is a **characteristic subgroup** of G, which means any automorphism of G maps P_i isomorphically onto itself.]

- (3) $\implies$ (4): This follows inductively from our characterization of direct products. Namely, for all $1 \leqslant r \leqslant s$, we check $P_1 \cdot P_2 \cdots P_r \cong P_1 \times P_2 \times \cdots \times P_r$. This is true for $r = 1$, so it only remains to show the induction step. If $P_1 \cdots P_{r-1} \cong P_1 \times \cdots \times P_{r-1}$, note $|P_1 \cdots P_{r-1}| = |P_1| \cdot |P_2| \cdots |P_{r-1}|$ is coprime to p_r, so by Lagrange's theorem $(P_1 \cdots P_{r-1}) \cap P_r = \{1\}$. By (3), $P_1 \cdots P_{r-1} \lhd G$ and $P_r \lhd G$, so our characterization of direct products shows

  $$(P_1 \cdots P_{r-1}) \cdot P_r \cong (P_1 \cdots P_{r-1}) \times P_1 \cong P_1 \times \cdots \times P_r.$$

  Thus $G > P_1 \cdots P_s \cong P_1 \cong P_1 \times \cdots \times P_s$, and since $G = |P_1| \cdots |P_s|$, equality holds, so $G \cong P_1 \times \cdots \times P_s$.

- (4) $\implies$ (1): Given $G \cong P_1 \times \cdots \times P_s$, we have $Z(G) \cong Z(P_1) \times \cdots \times Z(P_s)$, so

  $$G/Z(G) = \frac{P_1 \times \cdots \times P_s}{Z(P_1) \times \cdots \times Z(P_s)} \cong P_1/Z(P_1) \times \cdots \times P_s/Z(P_s).$$

  Recall $Z(P_i) \neq \{1\}$ for all i, so $|G/Z(G)| < |G|$, and $G/Z(G)$ also satisfies (4), so by induction we may assume that $G/Z(G)$ is nilpotent. But this forces G to be nilpotent, as from the upper central series characterization of nilpotence, we have

  $$Z_2(G)/Z(G) = Z(G/Z(G)) = Z_1(G/Z(G)).$$ □

Definition 7.6.2. A normal tower

$$\{1\} \lhd H_0 \lhd H_1 \lhd \cdots \lhd H_n = G$$

is called a **central series** if for all i, $H_i \lhd G$ and

$$H_{i+1}/H_i \leqslant Z(G/H_i).$$

Thus the upper central series is the *largest* possible central series, in the sense that given any other central series, the components are contained in the corresponding components of $\mathcal{Z}(G)$. (Check!)

Let G be a group and let $H \lhd G$. We claim $[G, H] \lhd G$ if $g \in G$. Given $g \in G$, $h \in H$, and $a \in G$, we want to show

$$a[g, h]a^{-1} \in [G, H].$$

But we can write this as

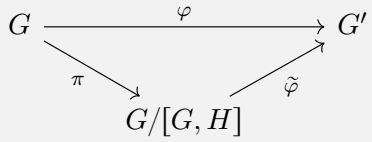
$$a[g,h]a^{-1} = aghg^{-1}h^{-1}a^{-1} = (aga^{-1})(aha^{-1})(ag^{-1}a^{-1})(ah^{-1}a^{-1}) = [\underbrace{aga^{-1}}_{\in G}, \underbrace{aha^{-1}}_{\in H}] \in [G, H],$$

so we are done.

Proposition 7.6.3. Given H and a normal subgroup $H \triangleleft G$, we have
$$\frac{H}{[G,H]} \leqslant Z\left(\frac{G}{[G,H]}\right).$$

Proof. Let $g \in G$, $h \in H$. We want to show $gh[G,H] = hg[G,H]$. This is equivalent to $ghg^{-1}h^{-1}[G,H] = [G,H]$. □

Theorem 7.6.4 (Universal Mapping Property of $[G,H]$ for $H \triangleleft G$)**.** Suppose there exists a group homomorphism $\varphi\colon G \to G'$ such that $\varphi(H) \leqslant Z(G')$. Then there exists a unique map $\widetilde{\varphi}\colon G/[G,H] \to G'$ such that the diagram



commutes.

Proof. This is a routine application of the universal mapping property of quotient groups. If $g \in G$, $h \in H$, then $\varphi([g,h]) = \varphi(g)\varphi(h)\varphi(g)^{-1}\varphi(h)^{-1} = 1$, so $[G,H] \subset \ker\varphi$. Then by the universal mapping property of quotient groups, there exists a unique group hsomorphismsm $\widetilde{\varphi}$ making the given diagram commute. □

Corollary 7.6.5. If $\mathcal{C}^{n-k}(G) \leqslant \mathcal{Z}_k(G)$, then $\mathcal{C}^{n-(k+1)}(G) \leqslant \mathcal{Z}_{k+1}(G)$.

Proof of **??**. Suppose $\mathcal{C}^{n-k}(G) \leqslant \mathcal{Z}_k(G)$. Consider the map
$$\begin{aligned} \pi\colon G/\mathcal{C}^{n-k}(G) &\longrightarrow G/\mathcal{Z}_k(G), \\ a\mathcal{C}^{n-k}(G) &\longmapsto a\mathcal{Z}_k(G). \end{aligned}$$
Then $\pi(\mathcal{C}^{n-k-1}(G)/\mathcal{C}^{n-k}(G)) \leqslant \pi(Z(G/\mathcal{C}^{n-k}(G))) = \mathcal{Z}_{k+i}(G)/\mathcal{Z}_k(G)$, so π is a map of the form
$$\begin{aligned} \pi\colon \frac{\mathcal{C}^{n-k-1}(G)}{\mathcal{C}^{n-k}(G)} &\longrightarrow \frac{\mathcal{Z}_{k+1}(G)}{\mathcal{Z}_k(G)} \\ \alpha^{n-k}(G) &\longmapsto a\mathcal{Z}_k(G) \end{aligned}$$
Now
$$\frac{\mathcal{C}^{n-k-1}(G)}{\mathcal{C}_k(G)} \leqslant \frac{\mathcal{Z}_{k+1}(G)}{\mathcal{Z}_k(G)},$$
so $\mathcal{C}^{n-k-1}(G) \leqslant \mathcal{Z}_{k+1}(G)$. □

Corollary 7.6.6. If $\mathcal{C}^{n-k}(G) \leqslant \mathcal{Z}_k(G)$, then $\mathcal{C}^{n-(k-1)}(G) \leqslant \mathcal{Z}_{k-1}(G)$.

Proof. Suppose $\mathcal{C}^{n-k}(G) \leqslant \mathcal{Z}_k(G)$. Then $\mathcal{C}^{n-k+1}(G) = [G, \mathcal{C}^{n-k}(G)] \leqslant [G, \mathcal{Z}_k(G)] \leqslant \mathcal{Z}_{k-1}(G)$. Now $\mathcal{Z}_k(G)/\mathcal{Z}_{k-1}(G) = Z(G/\mathcal{Z}_{k-1}(G))$, so we are done. □

These facts together give are used in the solution to 6.1. To see this, note that if G is nilpotent, so that $\mathcal{C}^n(G) = \{1\}(= \mathcal{Z}_0(G))$ by definition for some n, then by applying the corollary n times we have $\mathcal{C}^0(G) = G \leqslant \mathcal{Z}_n(G) = G$, so the upper central series $\mathcal{Z}_n(G)$ terminates.

Conversely, if the upper central series terminates, so that there exists some n such that $\mathcal{Z}_n(G) = G$ $(= \mathcal{C}^0(G)$ by definition), then by applying the other corollary n times we obtain $\mathcal{C}^n(G) \subset \mathcal{Z}_0(G)\{1\}$, so the lower central series $\mathcal{C}(G)$ terminates, and hence G is nilpotent.

Example 7.6.7 (A non-split short exact sequence)**.** Consider the short exact sequence

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & \mathbb{Z}/4\mathbb{Z} & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0 \\ & & 1 & \longmapsto & 2 & & & & \\ & & & & 1 & \longmapsto & 1 & & \end{array}$$

does not split. //

Recall that the Characterization of Semidirect Products as Split Group Extensions says that the short exact sequence $1 \longrightarrow N \xrightarrow{\varphi} G \xrightarrow{\psi} H \longrightarrow 1$ splits if and only if $G \cong N \rtimes H$. We gave a nice proof, but we can provide an alternative proof, which is much more brief, but provides less information about the structure of G, and in particular says nothing about the automorphism of G.

Alternate Proof of the Characterization of Semidirect Products as Split Group Extensions. First note that if $s\colon H \longrightarrow G$ is a splitting of the map $G \longrightarrow H$ in the short exact sequence, then s must be injective (Check!). Thus $K \coloneqq s(H) \cong H$. Now if $g \in N \cap K$, then $\psi(g) = 1$, $g = \varphi(h)$, $\psi(g) = t(s(h)) = 1$. So $N \cap K = \{1\}$. We want to show $G = NK$. Let $g \in G$ and let $a = s(\psi(g))g^{-1}$. Then $\psi(a) = \psi(s(\psi(g)))\psi(g^{-1}) = \psi(g) \cdot \psi(g^{-1}) = 1$. So $a \in N$. Now

$$g = \underbrace{a^{-1}}_{\in N}\underbrace{s(\psi(g))}_{\in K},$$

so $G = NK$, $N \cap K = \{1\}$, and $N \lhd G$. Thus $H \cong K \leqslant G$. □

7.7 Homework 6

Exercise 7.7.1. We defined a group G to be **nilpotent** if its lower central series $\mathcal{C}^n(G)$ eventually reaches the trivial subgroup of G. Prove that G is nilpotent if and only if there exists n such that the nth term $\mathcal{Z}_n(G)$ of the upper central series equals G.

Solution. We first prove two useful lemmas.

Lemma 7.7.2. If G is a group with $N, K \lhd G$ and $N \subset K$, then the map $\Pi : G/N \to G/K$ given by $\Pi(aN) = \Pi(aK)$ is a well-defined surjective group homomorphism, and

$$\Pi(Z(G/N)) \subset Z(G/K).$$ □

Conversely, if $K, N \lhd G$ and the map $\Pi : G/K \to G/N$ by $gK \mapsto gN$ is a well-defined group homomorphism, then $K \subset N$.

Proof of **??**. Note that much of this argument is similar to the Third Isomorphism Theorem. For the first statement, note that since $N \subset K$, any element ak of the coset aN is an element of the coset aK because $k \in K$. Hence if $aN = a'N$, then $\Pi(aN) = aK = a'K = \Pi(a'N)$. Thus Π is well-defined. And Π is a surjection, since if $aK \in G/K$ then $\Pi(aN) = aK$.

Now let $aN \in Z(G/N)$ be given. We claim Π maps aN into the center of G/K. To see this, let $gK \in G/K$. Then $\Pi(gH) = gK$, so since aN is central in G/N we have

$$1 = \Pi(1) = \Pi([aN, gN]) = \Pi(aN)\Pi(gN)\Pi(aN)^{-1}\Pi(gN)^{-1} = [\Pi(aN), \Pi(gN)] = [\Pi(aN), gK].$$

Thus $\Pi(aN)$ and gK commute. Since gK was an arbitrary element of G/K, $\Pi(aN)$ is central in G/K. This completes the proof.

To see the second statement, suppose $\Pi\colon gK \mapsto gN$ is a well-defined group homomorphism. Then by well-definedness, if $gK = g'K$ for some $k, k' \in K$ (that is, if $gg'^{-1} \in K$), then $gN = g'N$. So, letting $k \in K$ be arbitrary and putting $g = k$, $g' = 1$, we conclude $gg' \in N$, that is, that $k \in N$. Hence $K \subset N$. □

Lemma 7.7.3. If G is a group, then $\mathcal{C}^r(G)/\mathcal{C}^{r+1}(G) \subset Z(G/\mathcal{C}^{r+1}(G))$ for all $r \geqslant 0$.

Proof of **??**. Fix $r \geqslant 0$. Note $\mathcal{C}^r(G)/\mathcal{C}^{r+1}(G) = \mathcal{C}^r(G)/[G, \mathcal{C}^r(G)]$. Thus given any element $a[G, \mathcal{C}^r(G)]$ and any $b[G, \mathcal{C}^r(G)] \in \mathcal{C}^r(G)/\mathcal{C}^{r+1}(G)$ (so $a \in \mathcal{C}^r(G)$ and $b \in G$), we have

$$[a[G, \mathcal{C}^r(G)], b[G, \mathcal{C}^r(G)]] = [a, b][G, \mathcal{C}^r(G)] = [G, \mathcal{C}^r(G)],$$

which is the identity element of $\mathcal{C}^r(G)/\mathcal{C}^{r+1}(G) = \mathcal{C}^r(G)/[G, \mathcal{C}^r(G)]$. Hence $a[G, \mathcal{C}^n(G)] \in Z(G/\mathcal{C}^{r+1}(G))$. Since $a[G, \mathcal{C}^n(G)] \in \mathcal{C}^n(G)/\mathcal{C}^{n+1(G)}$ was arbitrary, $\mathcal{C}^r(G)/\mathcal{C}^{r+1}(G) \subset Z(G/\mathcal{C}^{r+1}(G))$. □

We can now prove the statement of Exercise 6.1. ($\Rightarrow$) Suppose G is nilpotent. Then there is some $n \geqslant 0$ such that $\mathcal{C}^n(G) = \{1\}$. We will argue by induction over k that for all $0 \leqslant k \leqslant n$,

$$\mathcal{C}^{n-k}(G) \subset \mathcal{Z}_k(G). \tag{7.7.3.1}$$

If $k = 0$ then $\mathcal{C}^{n-k}(G) = \mathcal{C}^n(G) = \{1\} = \mathcal{Z}_0(G)$, affirming the claim. Now suppose for some $1 \leqslant k \leqslant n$ we have $\mathcal{C}^{n-k+1}(G) \subset \mathcal{Z}_{k-1}(G)$. Then by **??**, there is a group homomorphism $\Pi : G/\mathcal{C}^{n-k+1}(G) \to G/\mathcal{Z}_{k-1}(G)$ such that

$$\begin{aligned}
\mathcal{C}^{n-k}(G)/\mathcal{Z}_{k-1}(G) &= \Pi(\mathcal{C}^{n-k}(G)/\mathcal{C}^{n-k+1}(G)) && \text{(by definition of } \Pi \text{ in } \textbf{??}) \\
&\subset \Pi(Z(G/\mathcal{C}^{n-k+1}(G))) && \text{(by } \textbf{??}) \\
&\subset Z(G/\mathcal{Z}_{k-1}(G)) && \text{(by } \textbf{??}) \\
&= \mathcal{Z}_k(G)/\mathcal{Z}_{k-1}(G) && \text{(by definition of } \mathcal{Z}_k(G) \text{ for } k \geqslant 1)
\end{aligned}$$

Then by definition of Π,

$$\mathcal{C}^{n-k}(G)/\mathcal{Z}_{k-1}(G) = \Pi(\mathcal{C}^{n-k}(G)/\mathcal{C}^{n-k+1}(G)) \subset \mathcal{Z}_k(G)/\mathcal{Z}_{k-1}(G),$$

We conclude by the Correspondence Theorem that $\mathcal{C}^{n-k}(G) \subset \mathcal{Z}_k(G)/\mathcal{Z}_{k-1}(G)$. This proves **??**. In particular, $G = \mathcal{C}^0(G) \subset \mathcal{Z}_n(G)$, so $\mathcal{Z}_n(G) = G$.

($\Leftarrow$) Conversely, suppose G is a group such that $\mathcal{Z}_n(G) = G$ for some n. We claim G is nilpotent. To see this, we will argue by induction on k that for all $0 \leqslant k \leqslant n$, that $\mathcal{C}^k(G) \subset \mathcal{Z}_{n-k}(G)$. This implies the claim because $\mathcal{Z}_n(G) \subset \mathcal{C}_0(G) = \{1\}$ implies $\mathcal{C}^n(G) = \{1\}$, and hence that G is nilpotent. The base case $k = 0$ holds because $\mathcal{C}^0(G) = G = \mathcal{Z}_n(G)$. For the induction step, suppose $\mathcal{C}^{k-1}(G) \subset \mathcal{Z}_{n-k+1}(G)$ for some $1 \leqslant k \leqslant n$. To see why $\mathcal{C}^k(G) \subset \mathcal{Z}_{n-k}(G)$, first note that by the induction hypothesis, we have $\mathcal{C}^{k-1}(G) \subset \mathcal{Z}_{n-k+1}(G)$, and hence that

$$\frac{\mathcal{C}^{k-1}(G)}{\mathcal{Z}_{n-k}(G)} \subset \frac{\mathcal{Z}_{n-k+1}(G)}{\mathcal{Z}_{n-k}(G)} = Z\left(\frac{G}{\mathcal{Z}_{n-k}(G)}\right). \tag{$*$}$$

Then the natural map $\pi : G \twoheadrightarrow G/\mathcal{Z}_{n-k}(G)$ sends $\mathcal{C}^k(G) = [G, \mathcal{C}^{k-1}(G)]$ to $\{1\}$, since $(*)$ shows that any element of the form $a\mathcal{Z}_{n-1}(G) \in G/\mathcal{Z}_{n-k}(G)$ for some $a \in \mathcal{C}^{k-1}(G)$ is central in $G/\mathcal{Z}_{n-k}(G)$, and in particular that element has $1 = [g, a]\mathcal{Z}_{n-k} = [g\mathcal{Z}_{n-k}(G), a\mathcal{Z}_{n-k}(G)]$ for all $g\mathcal{Z}_{n-k}(G) \in G/\mathcal{Z}_{n-k}$. But $[G, \mathcal{C}^{k-1}(G)]/\mathcal{Z}_{n-k}(G)$ is the quotient of the group generated by elements of the form $[g, a]$ where $g \in G$ and $a \in \mathcal{C}^{k-1}(G)$, which we showed on a previous homework to be the collection of all finite products of commutators of the form $[g, a]$. Thus the quotient of this group by $\mathcal{Z}_{n-k}(G)$, $[G, \mathcal{C}^{k-1}(G)]/\mathcal{Z}_{n-k}(G)$, is the image under the quotient map of all finite products of commutators, each of which is 1 by the above reasoning. In other words, $\mathcal{C}^k(G)$ is in the kernel of the quotient map $G \twoheadrightarrow G/\mathcal{Z}_{n-k}(G)$, and hence $\mathcal{C}^k(G) \subset \mathcal{Z}_{n-k}(G)$.

Exercise 7.7.4. Which dihedral groups D_{2n} are nilpotent?

Solution.

We first prove two lemmas about D_{2n} when $n \geqslant 3$, along with a lemma useful for showing nilpotence

of any group G (for example, in induction arguments in the case G is finite).

Lemma 7.7.5. Let $n \geqslant 3$. Then

$$Z(D_{2n}) = \begin{cases} \{1\} & \text{if } n \text{ is odd,} \\ \{1, \rho^{n/2}\} & \text{if } n \text{ is even.} \end{cases}$$

□

Lemma 7.7.6. Let $n \geqslant 3$ and suppose n is even. Then under an appropriate identification,

$$D_{2n}/Z(D_{2n}) = D_n.$$

Lemma 7.7.7. If G is any group and $G/Z(G)$ is nilpotent, then G is nilpotent.

Proof of **??**. Let $\tau^i\rho^j, \tau^k\rho^\ell \in D_{2n}$, where $i, k \in \{0, 1\}$ and $j, \ell \in \{0, 1, \ldots, n-1\}$.

Then $\rho^j \in Z(G)$ if and only if for all $\ell \in \{0, 1, \ldots, n-1\}$, the elements $[\rho^j, \rho^\ell]$ and $[\rho^j, \tau\rho^\ell]$ equal 1. The former is 1 since ρ commutes with itself, and the latter can be written as

$$[\rho^j, \tau\rho^\ell] = \rho^j\tau\rho^\ell\rho^{-\ell}\tau\rho^{-j} = \rho^j\tau^2\rho^{-j} = \rho^{2j},$$

which equals 1 if and only if $j = 0$ or $j = n/2$.

On the other hand, the element $\tau\rho^j \in Z(G)$ if and only if for all $\ell \in \{0, 1, \ldots, n-1\}$, the elements $[\tau\rho^j, \rho^\ell]$ and $[\tau\rho^j, \tau\rho^\ell]$ equal 1. We can write the former as

$$[\tau\rho^j, \rho^\ell] = \tau\rho^j\rho^\ell\rho^{-j}\tau\rho^{-\ell} = \tau\rho^\ell\tau\rho^{-\ell} = \rho^{-2\ell},$$

which equals 1 if and only if $\ell = n/2$, and in particular cannot equal 1 for all $\ell \in \{0, 1, \ldots, n-1\}$. Hence no element of the form $\tau\rho^j$ is central, so the result follows. □

Proof of **??**. Define a map $\varphi : D_{2n} \to D_{2n}$ by $\tau^i\rho^j \mapsto \tau^i\rho^j$. This map is a surjective group homomorphism, and $\tau^i\rho^j \in D_{2n}$ is an element of $\ker\varphi$ if and only if the element $\tau^i\rho^j$ in D_n equals 1, that is, if and only if $\tau^i = 1$ and $\rho^j = 1$, which occurs precisely when $i = 0$ and $j \in \{0, n/2\}$. Hence $\ker\varphi = \{1, n/2\}$, and since n is even we have by **??** that $\ker\varphi = Z(D_{n/2})$. Then the First Isomorphism Theorem implies $D_{2n}/Z(D_{2n}) \cong D_n$, as desired. □

Proof of **??**. Suppose $G/Z(G)$ is nilpotent. We claim that for $k \geqslant 1$, $Z_{k+1}(G)/Z(G) \cong \mathcal{Z}_k(G/Z(G))$. We argue this by induction on k. The base case is $Z(G)/Z(G) \cong \{1\}$, so suppose the claim holds for some k and write

$$\begin{aligned}
\frac{\mathcal{Z}_{k+1}(G)/Z(G)}{\mathcal{Z}_{k-1}(G/Z(G))} &\cong \frac{\mathcal{Z}_{k+1}(G)/Z(G)}{\mathcal{Z}_k(G)/Z(G)} && \text{(by the induction hypothesis)} \\
&= \frac{\mathcal{Z}_{k+1}(G)}{\mathcal{Z}_k(G)} && \text{(by the Second Isomorphism Theorem)} \\
&= Z\left(\frac{G}{\mathcal{Z}_{k-1}(G)}\right) && \text{(by the definition of } \mathcal{Z}_{k-1}(G)) \\
&= Z\left(\frac{G/Z(G)}{\mathcal{Z}_{k-1}(G/Z(G))}\right) && \text{(by the Second Isomorphism Theorem)} \\
&= \frac{\mathcal{Z}_k(G/Z(G))}{\mathcal{Z}_{k-1}(G/Z(G))} && \text{(by the definition of } \mathcal{Z}_k(G/Z(G)))
\end{aligned}$$

Then by the Correspondence Theorem, we conclude $\mathcal{Z}_{k+1}(G)/Z(G) \cong \mathcal{Z}_k(G/Z(G))$.

We now show nilpotence of $G/Z(G)$ implies nilpotence of G. If $G/Z(G)$ is nilpotent, then there exists an integer n such that $\mathcal{Z}_n(G/Z(G)) = G/Z(G)$. Applying the result from the above argument,

we obtain

$$G/Z(G) = \mathcal{Z}_n(G/Z(G)) \cong \mathcal{Z}_{n+1}(G)/Z(G),$$

so by the Correspondence Theorem we conclude $G = \mathcal{Z}_{n+1}(G)$. Hence G is nilpotent. □

We can now prove the statement of Exercise 6.2. We claim D_{2n} is nilpotent if and only if $n = 2^k$ for some integer $k \geqslant 0$. Since $D_{2\cdot 2^k}$ is a p-group for any integer $k \geqslant 0$ (with $p = 2$), by the Classification Theorem of Finite Nilpotent Groups it follows that D_{2n} is nilpotent whenever n is a power of 2.

Conversely, suppose D_{2n} is nilpotent. By Exercise 6.1, it suffices to show $\mathcal{Z}_k(D_{2n}) = 2^k$ for all nonnegative integers $k \geqslant 0$. We argue by induction on $k \geqslant 0$. For the base case, we compute

$$\mathcal{Z}_1(D_{2n}) = \frac{\mathcal{Z}_1(D_{2n})}{\{1\}} = \frac{\mathcal{Z}_1(D_{2n})}{\mathcal{Z}_0(D_{2n})} = Z\left(\frac{D_{2n}}{\mathcal{Z}_0(D_{2n})}\right) = Z\left(\frac{D_{2n}}{\{1\}}\right) = Z(D_{2n}).$$

By repeating this calculation by replacing the subscripts 0 (resp. 1) with $j+1$ (resp. j), we obtain that if $\mathcal{Z}_j(D_{2n}) = \{1\}$ for any $j \geqslant 1$, then $\mathcal{Z}_k(D_{2n}) = \{1\}$ for all $k \geqslant 0$. In particular, since $D_{2n} \neq \{1\}$ and D_{2n} is nilpotent, this shows n must be even. Thus $\mathcal{Z}_2(D_{2n})/\mathcal{Z}_1(D_{2n}) = \{1, \rho^{n/4}\}$, so $|\mathcal{Z}_1(D_{2n})| = 2$, affirming the base case.

For the induction step, suppose nilpotence of D_{2k} is equivalent to k being a power of 2 for all $0 \leqslant k \leqslant n-1$, and suppose D_{2n} is nilpotent. We claim n is a power of 2. Since n is even, $D_{2n}/Z(D_{2n}) \cong D_n$ by **??**, and by the induction hypothesis this is nilpotent if and only if $n/2 = 2^N$ for some integer N. Thus $n = 2 \cdot 2^N = 2^{N+1}$, so n is a power of 2. This completes the proof.

Exercise 7.7.8. Compute the derived series, lower central series, and upper central series for the group H_p.

Solution. We first prove a lemma.

Lemma 7.7.9. Let G be any group. If $G = \langle S \rangle$ for some subset S of G, then

$$[G, G] = \langle \{[s_i, s_j] \mid s_i, s_j \in S\} \rangle^{\text{normal}}. \qquad \square$$

Proof of **??**. Let $Q = \{[s_1, s_1] \mid s_1, s_2 \in S\}$, let $W = \{[g_1, g_2] \mid g_1, g_2 \in G\}$, and let $N = \langle Q \rangle^{\text{normal}}$. Then $Q \subset W$, so $\langle W \rangle \subset \langle Q \rangle \subset N$. To see $N \subset \langle W \rangle$, first note G/N is abelian, which we justify as follows. the subset of G/N given by $\{sN \mid s \in S\}$ generates G/N, and given any two elements $sN, s'N$ in this subset, we have $[sN, s'N] = [s, s']N = N$ (since $[s, s'] \in N$), which is the identity element of G/N. It follows that the generators of G/N commute, so G/N is abelian.

Then by the universal mapping property of the abelianization $G^{\text{ab}} = G/[G, G]$, there exists a (unique) group homomorphism $\Pi : G/[G, G] \to G/N$ making the diagram

commute, where the unlabeled maps are the canonical quotient maps. Thus $\Pi(g[G, G]) = gN$, and Π is surjective because for any $gN \in G/N$, we have $\Pi(g[G, G]) = gN$. Then by **??**, $N \subset [G, G]$. Thus $N = [G, G]$, as claimed. □

We can now prove the statement of Exercise 6.3. By Exercise 5.4, H_p is isomorphic to the matrix group G given by

$$G = \left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; x, y, z \in \mathbb{Z}/p\mathbb{Z} \right\}.$$

We will make this identification throughout. Recall G is generated by $X = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

First note $\mathcal{C}^0(G) = \mathcal{D}^0(G) = G$. We also have

$$\mathcal{C}^1(G) = \mathcal{D}^1(G) = [G, G] = \langle [X, T] \rangle = \langle Y \rangle,$$

where $Y = [T, X] = \left(\begin{smallmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$ and the penultimate equality is by **??**. To compute $\mathcal{D}^2(G)$, write

$$\mathcal{D}^2(G) = [\mathcal{D}^1(G), \mathcal{D}^1(G)] = \langle [Y, Y] \rangle = \{1\}$$

where the penultimate equality is again by **??**. To compute $\mathcal{C}^2(G)$, write

$$\mathcal{C}^2(G) = [G, \mathcal{C}^1(G)] = [G, \langle Y \rangle] \overset{(*)}{=} [G, Z(G)] = 1,$$

where the last equality is because $Z(G)$ commutes with any element of G (and hence $[G, Z(G)]$ is generated by elements of G of the form $[g, z]$ where $g \in G$ and $z \in Z(G)$, so $[g, z] = 1$), and the equality at $(*)$ is justified as follows. $Z(G) \neq 1$ because G is a p-group. $Z(G) \neq G$ since G is non-abelian. $|Z(G)| \neq p^2$ because otherwise $G/Z(G)$ is cyclic (as a group of order p) and hence by Exercise 1.4 G is abelian, which contradicts the fact X and T do not commute. It only remains to show $Y \in Z(G)$, since then the fact Y is a non-identity element of the cyclic group $Z(G)$ of prime order implies $\langle Y \rangle = Z(G)$. And indeed $Y \in Z(G)$, since $[X, Y] = [T, Y] = 1$ and hence any finite product of X, T and their inverses, which means Y commutes with any element of G.

We now compute the upper central series of G. We have $\mathcal{Z}_0(G) = \{1\}$ and $\mathcal{Z}_1(G) = Z(G)$ (since $Z(G)$ is the unique subgroup of G containing $\mathcal{Z}_0(G) = \{1\}$ such that $Z(G)/\{1\} = Z(G/\{1\})$), which we already showed equals $\langle Y \rangle$. We have $\mathcal{Z}_2(G)$ is the unique subgroup of G containing $Z(G)$ such that

$$\frac{\mathcal{Z}_2(G)}{Z(G)} = Z\left(\frac{G}{Z(G)}\right).$$

But $G/Z(G) = G/\langle Y \rangle$ is a group of order p^2, and hence is abelian. Thus $Z(G/Z(G)) = G/Z(G)$, so $\mathcal{Z}_2(G) = G$. We conclude that the derived series, the lower central series, and the upper central series of G all coincide, and the common series is $\{1\} \lhd \langle Y \rangle \lhd G$.

Exercise 7.7.10. A subgroup K of a group G is called a **characteristic subgroup** if for every $\sigma \in \mathrm{Aut}(G)$, $\sigma(K) = K$ (i.e., every group automorphism of G preserves K). We'll write $K \operatorname{char} G$ to indicate that K is a characteristic subgroup of G.

(a) If K char H and $H \lhd G$, then $K \lhd G$. (Contrast this with the failure of normality to be transitive.) In particular, characteristic subgroups are always normal.

(b) For $d \in \mathbb{Z}_{\geqslant 1}$, if K is the unique subgroup of G with order d, then $K \operatorname{char} G$. (In particular, if a p-Sylow subgroup of a finite group is normal, then it is a characteristic subgroup.)

(c) Give an example of a group G and a subgroup K that is normal but is not characteristic.

Solution.

(a) Fix $g \in G$. Since $H \lhd G$, $gHg^{-1} = H$, so the group homomorphism $c_g^H : H \to H$ given by conjugation by g is a well-defined of $\mathrm{Aut}(H)$. Since $K \operatorname{char} H$, it follows that $K = c_g^H(K) = gKg^{-1}$. Since $g \in G$ was arbitrary, $K \lhd G$. In particular, since $G \lhd G$, if $K \operatorname{char} G$ then $K \lhd G$.

(b) Suppose K is the unique subgroup of G such that $|K| = d$. Let $\sigma \in \mathrm{Aut}(G)$. Then the restriction $\sigma|_K : K \to G$ is a group homomorphism (as $a, b \in K$ have $\sigma|_K(ab) = \sigma(ab) = \sigma(a)\sigma(b)$), and injectivity of σ implies injectivity of the restriction $\sigma|_K : K \to G$. Thus $\sigma|_K$ is an isomorphism onto its image $\operatorname{im} K$, which is a subgroup of G. Thus any $\sigma \in \mathrm{Aut}(G)$ maps subgroups to isomorphic subgroups, so since $K \cong \sigma|_K(K) = \sigma(K)$ implies $|K| = |\sigma(K)|$, we conclude $K = \sigma(K)$. Since $\sigma \in \mathrm{Aut}(G)$ was arbitrary, we conclude $K \operatorname{char} G$.

If p is a prime and $P \in \mathrm{Syl}_p(G)$, then recall that $P \lhd G$ implies $n_p(G) = 1$. It follows that any normal Sylow p-subgroup is the unique subgroup of G whose order is p, and hence $P \operatorname{char} G$ by the previous paragraph.

(c) Consider the subgroup $\langle i \rangle = \{\pm 1, \pm i\}$ of Q_8. We showed on Exercise 5.5 that any conjugation (that is, any inner automorphism) sends $\langle i \rangle$ to $\langle i \rangle$, so $\langle i \rangle \lhd Q_8$. But the group homomorphism $\sigma \in \mathrm{Aut}(G)$ determined by $i \mapsto k$, $j \mapsto -j$ is an automorphism, and $\langle i \rangle \mapsto \sigma(\langle i \rangle) = \langle j \rangle \neq \langle i \rangle$. ($\sigma$ is indeed an automorphism of Q_8, since the fact $\{k, -j\}$ generates Q_8 implies σ is surjective, and σ is an injection as a surjective map homomorphism of finite sets of the same cardinality.)

Remark 7.7.11. Recall from Homework 5 that $\mathrm{Out}(Q_8) \cong S_3$. And indeed, more generally, if a group G has normal subgroups that are not characteristic, then $\mathrm{Out}(G)$ must be nontrivial. Is the converse true? The answer is no. For example, if $G = C_n$, then all automorphisms are outer (as $\mathrm{Inn}(G) = G/Z(G) = \{1\}$). But G has a unique subgroup of order d for all integers d dividing n, so every subgroup is characteristic. Alternatively, $\mathrm{Out}(A_5) = C_2 \neq \{1\}$, but all normal subgroups of A_5 are trivial, hence characteristic. □

Exercise 7.7.12. Compute a composition series of the group $\mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$.

Hint: One of the simple quotients coming from the composition series will have order 60; you can prove it is simple using the argument from recitation showing that A_5 is simple—in fact, the group in question is isomorphic to A_5, which you can after-the-fact deduce from another result from recitation, that any simple group of order 60 is isomorphic to A_5.

Solution. Let $G = \mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$. Then by a previous homework exercise, $|G| = (5^2-1)(5^2-5) = 480$. Let $S = \mathrm{SL}_2(\mathbb{Z}/5\mathbb{Z})$. Since $S = \ker \det$, by the First Isomorphism Theorem $|G|/|S| \cong |(\mathbb{Z}/5\mathbb{Z}) \smallsetminus \{0\}| = 4$. Hence $|S| = 120$.

Let Q be the subgroup of G whose elements have determinant ± 1. (This is a subgroup, as it is the preimage of the subgroup $\{\pm 1\} < (\mathbb{Z}/5\mathbb{Z})^\times$ under the determinant map). Since Q properly contains the order 120 subgroup S and $Q \neq G$, by Lagrange's Theorem we must have $|Q| = 240$. Then in particular $[G : Q] = [Q : S] = 2$, which implies $S \lhd Q \lhd G$.

Next consider $Z(S)$, which equals $\left\{\pm \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\right\}$ for the following reason. If $Z = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in Z(S)$, then the elements $T, T' \in S$ given by $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $T' = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ commute with Z if and only if $\left(\begin{smallmatrix} -c & a-d \\ 0 & c \end{smallmatrix}\right) = 0$ and $\left(\begin{smallmatrix} b & 0 \\ d-a & -b \end{smallmatrix}\right) = 0$. Solving for such $a, b, c, d \in \mathbb{Z}/5\mathbb{Z}$, we conclude $a = d$ and $c = b = 0$, so $Z = \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda \end{smallmatrix}\right)$ for some $\lambda \in \mathbb{Z}/5\mathbb{Z}$. Since $\det A = 1$, it follows that $Z \in \left\{\pm \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\right\}$. Since $\left\{\pm \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\right\} \subset Z(S)$, we conclude $Z(S) = \left\{\pm \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\right\}$. As $1 \lhd Z(S) \lhd S$, we now have a normal tower

composition series	$\{1\}$	$\lhd$	$Z(S)$	$\lhd$	S	$\lhd$	Q	$\lhd$	G
order	1		2		120		240		480

We claim this normal tower is a composition series for G. By noting each has order 2, the factor groups $Z(S)/\{1\}$, Q/S, and G/Q are all isomorphic to C_2, and hence are simple. It only remains to show $S/Z(S)$ is simple. Note that $S/Z(S)$ is a group of order 60. The only part in our proof that A_5 is simple that uses any feature of A_5 other than the fact $|A_5| = 60$ of A_5 being 60 is when we used that $\langle (12345) \rangle \neq \langle (13245) \rangle$ and both are normal subgroups. Since both A_5 and $S/Z(S)$ have order 60, it therefore suffices to find two elements of $S/Z(S)$ that generate distinct cyclic subgroups of order 5. It follows from the fact $Z(S) = \left(\begin{smallmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{smallmatrix}\right)$, that we can write matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) Z(S) \in S/Z(S)$ where $a, b, c, d \in \mathbb{Z}/5\mathbb{Z} = \{-2, -1, 0, 1, 2\}$ as $\{\pm 2\}, \{\pm 1\}, 0, \{\pm 1\}, \{\pm 2\}$, respectively, since left or right multiplication by $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ identifies these. Consider the elements

$$A = \left(\begin{smallmatrix} 1 & -1 \\ -1 & 2 \end{smallmatrix}\right) Z(S) = \left(\begin{smallmatrix} \pm 1 & \pm 1 \\ \pm 1 & \pm 2 \end{smallmatrix}\right) \text{ and } B = \left(\begin{smallmatrix} 1 & 2 \\ -2 & 2 \end{smallmatrix}\right) Z(S) = \left(\begin{smallmatrix} \pm 1 & \pm 2 \\ \pm 2 & \pm 2 \end{smallmatrix}\right).$$

Their orbits $\langle A\rangle$ and $\langle B\rangle$ in $S/Z(S)$ are then

$$\langle A\rangle = \left\{\left(\begin{smallmatrix}\pm1 & \pm1\\ \pm1 & \pm2\end{smallmatrix}\right), \left(\begin{smallmatrix}\pm2 & \pm2\\ \pm2 & 0\end{smallmatrix}\right), \left(\begin{smallmatrix}0 & \pm2\\ \pm2 & \pm2\end{smallmatrix}\right), \left(\begin{smallmatrix}\pm2 & \pm1\\ \pm1 & \pm1\end{smallmatrix}\right), \left(\begin{smallmatrix}\pm1 & 0\\ 0 & \pm1\end{smallmatrix}\right)\right\}$$

and

$$\langle B\rangle = \left\{\left(\begin{smallmatrix}\pm1 & \pm2\\ \pm2 & \pm2\end{smallmatrix}\right), \left(\begin{smallmatrix}\pm2 & \pm1\\ \pm1 & 0\end{smallmatrix}\right), \left(\begin{smallmatrix}0 & \pm1\\ \pm1 & \pm2\end{smallmatrix}\right), \left(\begin{smallmatrix}\pm2 & \pm2\\ \pm2 & \pm1\end{smallmatrix}\right), \left(\begin{smallmatrix}\pm1 & 0\\ 0 & \pm1\end{smallmatrix}\right)\right\}.$$

In particular $\langle A\rangle \neq \langle B\rangle$, so we have found two distinct Sylow 5-subgroups of $S/Z(S)$, which by our previous remarks proves $S/Z(S)$ is a simple group. (In fact, $S/Z(S)$ is isomorphic to A_5, as A_5 is the unique simple group of order 60). □

8 Math 6111 Midterm Qualifying Exam: Fall 2023

8.1 Review Exercises and Solutions

Here are a few additional problems of appropriate difficulty. These are not exhaustive, and every topic discussed in the course is important and admissible for the exam.

Exercise 8.1.1 (RE1)**.** Construct a group homomorphism $\rho\colon S_n \to \mathrm{GL}_n(\mathbb{C})$ such that $\det(\rho)$ is the sign homomorphism $S_n \to \{\pm1\}$.

Solution. Let $e_1, \dots, e_n$ be a basis of $\mathbb{C}^n$. For $\sigma \in S_n$, define $\rho(\sigma)$ by $\rho(\sigma)(e_i) = e_{\sigma(i)}$ for $i = 1, \dots, n$, and then extending $\mathbb{C}$-linearly, we obtain a function $\rho\colon S_n \to M_n(\mathbb{C})$.

Then for $\sigma, \tau \in S_n$, $\rho(\sigma\tau)(e_i) = e_{\sigma\tau(i)}$, while $\rho(\sigma)(\rho(\tau)e_i) = \rho(\sigma)e_{\tau(i)} = e_{\sigma\tau(i)}$; thus $\rho(\sigma)$ is invertible for all σ since $\rho(\sigma)\rho(\sigma^{-1}) = \rho(1) = I$, and ρ is a group homomorphism $\rho\colon S_n \to \mathrm{GL}_n(\mathbb{C})$.

S_n is generated by transpositions (ij), so to show $\det(\rho) = \varepsilon$ it suffices to verify this equality on transpositions, i.e., $\det(\rho(ij)) = -1$ for all $i \neq j$. But $\rho(ij)$ is the identity matrix with rows i and j swapped, which has determinant -1. □

Exercise 8.1.2 (RE2)**.** Which of the following short-exact sequences splits? (Justify!)

- $1 \to \mathrm{SL}_n(\mathbb{C}) \to \mathrm{GL}_n(\mathbb{C}) \xrightarrow{\det} \mathbb{C}^\times \to 1$, where the first map is the inclusion.
- $0 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$, where the first map is $x \mapsto 2x$ and the second map is reduction mod 2.
- $1 \to A_n \to S_n \xrightarrow{\varepsilon} \{\pm1\} \to 1$, where ε is the sign homomorphism and the first map is inclusion.

Solution.

(a) The map $\mathbb{C}^\times \to \mathrm{GL}_n(\mathbb{C})$ given by $z \mapsto \mathrm{diag}(z, \dots, z)$ is a splitting since it is clearly a group homomorphism and $\det(\mathrm{diag}(z, \dots, z)) = z^n$.

(b) This sequence does not split: suppose $s\colon \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ were a splitting. Then $s(1)$ has order 2, hence $s(1) = 2$, but then $s(1) \bmod 2 = 0 \neq 1$, a contradiction.

(c) For $n \geqslant 2$, the map $\{\pm1\} \to S_n$ given by $-1 \mapsto (12)$ is a splitting since it is clearly a group homomorphism and $\varepsilon((12)) = -1$. □

Exercise 8.1.3 (RE3)**.** Compute Jordan-Hölder series for the groups S_4 and $\mathbb{Z}/p^n\mathbb{Z}$ (where p is any prime and $n \in \mathbb{Z}_{\geqslant 1}$).

Solution. Where we write the quotient groups under the corresponding inclusions, we have

$$S_4 \underset{C_2}{\rhd} A_4 \underset{C_3}{\rhd} V_4 = \{(12)(34), (13)(24), (14)(23), \mathrm{id}\} \underset{C_2}{\rhd} \{(12)(34), 1\} \underset{C_2}{\rhd} 1$$

is a composition series for S_4, and

$$\mathbb{Z}/(p^n\mathbb{Z}) \underset{C_p}{\rhd} p\mathbb{Z}/p^n\mathbb{Z} \underset{C_p}{\rhd} p^2\mathbb{Z}/p^n\mathbb{Z} \underset{C_p}{\rhd} \cdots \underset{C_p}{\rhd} p^{n-1}\mathbb{Z}/p^n\mathbb{Z} \underset{C_p}{\rhd} \{0\}$$

is a composition series for $\mathbb{Z}/p^n\mathbb{Z}$ for any $n \in \mathbb{Z}_{\geqslant 1}$. □

Exercise 8.1.4 (RE4)**.** Show that no group G of order p^2q is simple, where p and q are primes (not necessarily distinct).

Hint: If $p \geqslant q$, show $n_p(G) = 1$ using the Sylow theorems. If $p < q$, show $n_q(G) = p^2$ and then that G contains enough elements of order q to have only one p-Sylow subgroup.

Solution.

- Case 1: $p \geqslant q$. $n_p(G) \mid q$ and $n_p(G) \equiv 1 \bmod p$ force $n_p(G) = 1$, making the p-Sylow subgroup of G normal. Thus G is not simple.
- Case 2: $p < q$. $n_q(G) \mid p^2$ and $n_q(G) \equiv 1 \bmod q$. Assuming $n_q(G) \neq 1$ (else G is not simple as in case 1), we have $n_q(G) = p^2$. Each $Q \in \mathrm{Syl}_q(G)$ is isomorphic to C_q, and if $Q \cap Q' \neq \{1\}$ for $Q, Q' \in \mathrm{Syl}_q(G)$, then $Q = Q'$ (since any non-trivial element of either group generates it). Thus

$$\left|\bigcup_{Q \in \mathrm{Syl}_q(G)} Q\right| \geqslant \underset{1 \in Q}{1} + \underbrace{n_q(G)(q-1)}_{\substack{\text{non-identity elemenets} \\ \text{of } Q \text{ are disjoint} \\ \text{as } Q \text{ varies}}} = 1 + p^2q - p^2.$$

  Since $|G| = p^2q$, we deduce $|\bigcup_{P \in \mathrm{Syl}_p(G)} P| \leqslant p^2$, since $\bigcup_{P \in Syl_p(G)} P \cap \bigcup_{Q \in Syl_q(G)} = \{1\}$ (by Lagrange's theorem and the fact $p \neq q$). Hence, recalling that $|P| = p^2$ for each $P \in \mathrm{Syl}_p(G)$, we have $n_p(G) = 1$. Therefore, G has a normal p-Sylow subgroup, which is a nontrivial proper normal subgroup since $|G| = p^2q > p > 0$. Thus G is not simple. □

Exercise 8.1.5 (RE5)**.** Show that any subgroup of a cyclic group is cyclic.

Solution. Let $G = \langle x \rangle$ be a cyclic group, and let $H < G$ be a subgroup.

- Case (i): $|G| = \infty$.

  Let $S = \{n \in \mathbb{Z}_{>0} \mid x^n \in H\}$. If $S = \varnothing$, then $H = \{1\}$. Otherwise, S contains some smallest element d, and $H = \langle x^d \rangle$.
- Case (ii): $|G| < \infty$. A surjective homomorphism $\varphi\colon \mathbb{Z} \to G$ with $\varphi(1) = x$ implies $\varphi^{-1}(H) < \mathbb{Z}$ is cyclic, so $H = \varphi(\varphi^{-1}(H))$ is cyclic. □

Exercise 8.1.6 (RE6)**.** Let $G = \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})/Z$, where

$$Z = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \;\middle|\; a \in (\mathbb{Z}/3\mathbb{Z})^\times \right\}$$

is the subgroup of scalar matrices. Show that G is isomorphic to S_4.

Hint: Consider the natural action of G on {lines through the origin in $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$}.

Solution. Let $V = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. The group $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ acts on the set of lines through $(0,0)$ in V, which we denote as L_1, L_2, L_3, L_4. This action gives a group homomorphism $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) \to S_4$.

The kernel of this homomorphism consists of matrices in $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ that preserve each line. To calculate the kernel, consider that the lines are spanned by the vectors $\binom{1}{0}, \binom{0}{1}, \binom{1}{1}, \binom{2}{1}$. For a matrix $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$, the conditions for preserving each line are:

- $gL_1 = L_1 \Leftrightarrow \binom{a}{c} \in \langle \binom{1}{0} \rangle \Leftrightarrow c = 0$.
- $gL_2 = L_2 \Leftrightarrow \binom{b}{d} \in \langle \binom{0}{1} \rangle \Leftrightarrow b = 0$.
- $gL_3 = L_3$ implies $a + b = \lambda$, and knowing $b = c = 0$, this forces $a = \lambda$ and similarly $d = \lambda$.

Therefore, the kernel consists of scalar matrices. Hence, we obtain an injection $\varphi\colon G = \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})/Z \to S_4$. Since $|G| = \frac{(3^2-1)(3^2-3)}{2} = 24 = |S_4|$, φ is an isomorphism. □

8.2 The Exam and Solutions

Clearly state any results from the course that you use. You are not expected to finish the exam: there are many small questions to give you many opportunities to demonstrate your understanding.

Exercise 8.2.1 (E1)**.** Let H and K be subgroups of a group G.

(a) (1 point) If H is a normal subgroup of G, show that $HK \coloneqq \{hk \mid h \in H, k \in K\}$ is a subgroup of G.

(b) (1 point) Show by an example that when neither H nor K is assumed normal, HK need not be a subgroup of G.

(c) (3 points) Let $\varphi\colon A \to B$ be a group homomorphism. Define a subgroup (called the graph of φ) $\Gamma_\varphi < A \times B$ by

$$\Gamma_\varphi = \{(a, \varphi(a)) \mid a \in A\}.$$

Show that $\Gamma_\varphi A/A \cong \mathrm{im}(\varphi)$ and $\Gamma_\varphi B/B \cong A$. (Here as usual we identify A and B with the subgroups $A \times \{1\}$ and $\{1\} \times B$ of $A \times B$.)

Solution.

(a) Let $H \leqslant G, K \leqslant G$. For all $h_1, h_2 \in H, k_1, k_2 \in K$,

$$1 = 1 \cdot 1 \in HK,$$
$$\forall h \in H, k \in K, \quad (hk)^{-1} = k^{-1}h^{-1} = \underbrace{k^{-1}h^{-1}k}_{\in H} \cdot k^{-1} \in HK.$$

(b) Let $G = S_3, H = \langle (12) \rangle, K = \langle (23) \rangle$. Then $HK = \{1, (12), (23), (12)(23)\}$ is not a subgroup since $(123)^{-1} = (321) \notin HK$.

(c) Define $\Gamma_\varphi \coloneqq \{(a, \varphi(a)) \mid a \in A\} < A \times B$, which is a subgroup by the definition of homomorphism. Note $A \hookrightarrow A \times B$ and $B \hookrightarrow A \times B$ are normal subgroups of $A \times B$, so by the third isomorphism theorem,

$$\Gamma_\varphi A/A \simeq \Gamma_\varphi/(\Gamma_\varphi \cap A), \quad \Gamma_\varphi B/B \simeq \Gamma_\varphi/(\Gamma_\varphi \cap B).$$

Note $A \to \Gamma_\varphi \cap (\varphi, \varphi(\varphi))$ is an isomorphism by the first isomorphism theorem. $(a, \varphi(a)) \mapsto a \mapsto \varphi(a)$

$$\Gamma_\varphi \cap B = \{(1,b) \mid \varphi(1) = b\} = \{(1,1)\}, \quad \text{so} \quad \Gamma_\varphi/(\Gamma_\varphi \cap B) = \Gamma_\varphi \simeq A. \qquad \square$$

Exercise 8.2.2 (E2)**.** Let G be a group of order 30.

(a) (4 points) Let H be a 3-Sylow subgroup of G, and let K be a 5-Sylow subgroup of G. Show that at least one of H and K is a normal subgroup of G.

(b) (1 point) Show by an example that G is not necessarily abelian.

Solution.

(a) Let $|G| = 30, H \in \mathrm{Syl}_3(G), K \in \mathrm{Syl}_5(G)$. By Sylow theorems,

$$\begin{cases} n_3(G) \equiv 1 \pmod 3, \text{ and } n_3(G) \mid 10, \\ n_5(G) \equiv 1 \pmod 5, \text{ and } n_5(G) \mid 6. \end{cases}$$

Thus $n_3(G) = 1$ or 10 and $n_5(G) = 1$ or 6. We must show that $n_3(G) = 10$ and $n_5(G) = 6$ is impossible. Suppose $n_3(G) = 10$ and $n_5(G) = 6$. Each $P \in \mathrm{Syl}_3(G)$ has 2 elements of order 3, and as P varies these order 3 elements are distinct. Likewise, each $Q \in \mathrm{Syl}_5(G)$ has 4 elements of order 5, and as Q varies these order 5 elements are distinct. Thus $|G| \geqslant 1 + 10 \cdot 2 + 6 \cdot 4 = 45$, a contradiction.

(b) Let $G = C_{15} \rtimes_\varphi \{\pm 1\}$, where $\varphi\{\pm 1\} \to \mathrm{Aut}(C_{15})$ is a non-trivial homomorphism. For instance, let $C_{15} = \langle x \rangle$, define $\varphi(-1)(x) = x^4$. Then $\varphi(-1)^2(x) = \varphi(-1)(x^4) = (x^4)^4 = x^{16} = x$, so $\varphi(-1)^2 = \mathrm{id}$ and the homomorphism is well-defined. $\square$

Exercise 8.2.3 (E3)**.** Let $\{1, j\}$ be a cyclic group of order 2 with non-identity element j, and for $n \geqslant 2$ let

$$L = \mathrm{SL}_n(\mathbb{C}) \rtimes_\varphi \{1, j\}$$

be the semidirect product defined by the homomorphism

$$\varphi \colon \{1, j\} \to \mathrm{Aut}(\mathrm{SL}_n(\mathbb{C})), \quad \varphi(j)(g) = {}^t g^{-1}.$$

Here ${}^t g$ denotes the transpose of an element $g \in \mathrm{SL}_n(\mathbb{C})$.

(a) (1 point) Verify that the given formula for $\varphi(j)$ does in fact uniquely determine a well-defined group homomorphism.

(b) (1 point) Determine explicit conditions on a matrix $g \in \mathrm{SL}_n(\mathbb{C})$ that are necessary and sufficient to have $(g, j)^2 = 1 \in L$.

(c) (3 points) We have from the definition of L a short exact sequence

$$1 \longrightarrow \mathrm{SL}_n(\mathbb{C}) \xrightarrow{\iota} L \xrightarrow{\pi} \{1, j\} \longrightarrow 1,$$

where $\iota(g) = (g, 1)$ and $\pi(g, y) = y$. Show that there is a group homomorphism

$$r \colon L \to \mathrm{SL}_n(\mathbb{C})$$

such that $r \circ \iota = \mathrm{id}_{\mathrm{SL}_n(\mathbb{C})}$ if and only if there exists an order 2 element $x \in \mathrm{SL}_n(\mathbb{C})$ such that for all $g \in \mathrm{SL}_n(\mathbb{C})$,

$$xgx^{-1} = {}^t g^{-1}.$$

Such a homomorphism r is called a **retraction** of ι; having r is equivalent to giving an isomorphism $L \xrightarrow{\cong} \mathrm{SL}_n(\mathbb{C}) \times \{1, j\}$ (direct product!) compatible with ι and π. You don't need

to prove this.

(d) (Bonus: 1 point) For what n does x as above exist?

Solution.

(a) For $\varphi(j)(gh) = {}^t(gh)^{-1} = {}^t(h^{-1}g^{-1}) = {}^tg^{-1} \cdot {}^th^{-1} = \varphi(j)(g)\varphi(j)(h)$, $\varphi(j)$ is a homomorphism. Since $\varphi(j) \circ \varphi(j)(g) = {}^t({}^tg^{-1})^{-1} = g$, $\varphi(j)$ is an automorphism of order 2, and $\varphi\{1, j\} \to \mathrm{Aut}(\mathrm{SL}_n(\mathbb{C}))$ is well-defined.

(b) For $g \in \mathrm{SL}_n(\mathbb{C})$, $(g, j)(g, j) = (g\varphi(j)(g), j^2) = (g{}^tg^{-1}, 1)$, so $(g, j)^2 = 1$ iff $g = {}^tg$ is a symmetric matrix.

(c) Suppose there is a group homomorphism $rL \to \mathrm{SL}_n(\mathbb{C})$ such that $r \circ \iota = \mathrm{id}_{\mathrm{SL}_n(\mathbb{C})}$. Let $x = r((1, j))$. Then $x^2 = r((1, j)^2) = r(1) = 1$. For all $g \in \mathrm{SL}_n(\mathbb{C})$,

$$xgx^{-1} = r((1, j))r((g, 1))r((1, j))^{-1} = r((1, j)(g, 1)(1, j)) = r(({}^tg^{-1}, 1)) = {}^tg^{-1}.$$

Conversely, given such an x, define r by $r((g, 1)) = g, r((g, j)) = gx$. Check $r(ab) = r(a)r(b)$ for all $a, b \in L$ in each case. □

Alphabetical Index