Group Theory

Michael Nelson

January 1, 2021

Contents

Part I
Introduction to Groups

In this document, we will go over the basics of group theory.

1 Basic Definitions

Throughout this section, let X be a nonempty set.

1.1 Definition of a Group

Definition 1.1. A **binary operation** $\star$ on X is a function $\star\colon X \times X \to X$, which we denote by

$$(x, y) \mapsto x \star y.$$

A set X equipped with a binary operation $\star$ is called a **magma**, and is denoted $(X, \star)$. The pair $(X, \star)$ is called a **semigroup** if the binary operation is **associative**; that is

$$(x \star y) \star z = x \star (y \star z)$$

for all $x, y, z \in X$. The pair $(X, \star)$ is called a **monoid** if $(X, \star)$ is a semigroup and there exists a **left** and **right inverse element**; that is, there exists $e, e' \in X$ such that

$$e \star x = x = x \star e'$$

for all $x \in X$. In fact, we automatically have $e = e'$. Indeed, we have

$$\begin{aligned} e' &= e \star e' \\ &= e. \end{aligned}$$

For this reason, we say e is the **identity element**. The pair $(X, \star)$ is called a **group** if $(X, \star)$ and every element has a **left** and **right inverse**; that is, for all $x \in X$ there exists $y, z \in X$ such that

$$x \star z = e = y \star x.$$

In fact, associativity automatically implies $y = z$. Indeed, we have

$$\begin{aligned} y &= y \star e \\ &= y \star (x \star z) \\ &= (y \star x) \star z \\ &= e \star z \\ &= z. \end{aligned}$$

For this reason, we say x has an **inverse element**, rather than a left and right inverse since they are the same element anyways, and we denote the inverse of x by x^{-1}. The pair $(X, \star)$ is called an **abelian group** if $(X, \star)$ is a group and the binary operation is **commutative**; that is

$$x \star y = y \star x$$

for all $x, y \in X$.

Remark 1. We often denote a group by G where we view G as a set equipped with a binary operation. Arbitrary groups are usually denoted by G, H, and K, and abelian groups are usually denoted by A,B, and C. The binary operation for a group G is usually denoted by $\cdot$ rather than $\star$. To ease notation, if $g, h \in G$, then we often write gh rather than $g \cdot h$.

1.1.1 Abelian Groups $\mathbb{Z}$ and $\mathbb{Q}^\times$

Example 1.1. Addition is a binary operation on $\mathbb{N}$, however negation is not a binary operation on $\mathbb{N}$. For example, $1 - 5 \notin \mathbb{N}$. The pair $(\mathbb{N}, +)$ forms a semigroup with identity 0. It is not quite a group yet, but we can make it into a group by *adjoining* inverse elements. When we do this, we obtain the group of integers

under addition, denoted by $\mathbb{Z}$. Similarly, multiplication is a binary operation on $\mathbb{Z}$, but division is not a binary operation on $\mathbb{Z}$. The pair $(\mathbb{Z}, \cdot)$ forms a semigroup with identity 1. This semigroup is also not a group because we are again missing inverses as in the case of $(\mathbb{N}, +)$. This time however, if we try to adjoin inverses to *all* elements in $(\mathbb{Z}, \cdot)$, then we will run into a problem; namely adjoining an inverse to 0 will collapse the whole structure to the trivial group $(\{1\}, \cdot)$:

$$\begin{aligned} a &= 1 \cdot a \\ &= (0^{-1}0) \cdot a \\ &= 0^{-1}(0 \cdot a) \\ &= 0^{-1}0 \\ &= 1. \end{aligned}$$

In order to avoid this, we adjoint inverses to all elements in $\mathbb{Z}$ *except* 0. The pair $(\mathbb{Q}, \cdot)$ is still not a group yet, but if we restrict multiplication to $\mathbb{Q}\backslash\{0\} \times \mathbb{Q}\backslash\{0\}$, then we do get a group, denoted by $\mathbb{Q}^\times$. To see this, we just need to verify that restricting multiplication to $\mathbb{Q}\backslash\{0\} \times \mathbb{Q}\backslash\{0\}$ lands in $\mathbb{Q}\backslash\{0\}$. Indeed, assume for a contradiction that there exists $a, b \in \mathbb{Q}\backslash\{0\}$ such that $ab = 0$. As $a \neq 0$, we can multiply both sides by a^{-1} to obtain $b = 0$, which is a contradiction.

Example 1.2. Define a binary operation $\star$ on $\mathbb{Q}$ by

$$a \star b = ab + 3a + 3b + 6$$

for all $a, b \in \mathbb{Q}$. The binary operation is clearly abelian. It is also associative. Indeed, we have

$$\begin{aligned} (a \star b) \star c &= (ab + 3a + 3b + 6)c + 3(ab + 3a + 3b + 6) + 3c + 6 \\ &= abc + 3ab + 3ac + 3bc + 9a + 9b + 9c + 24 \\ &= a(bc + 3b + 3c + 6) + 3a + 3(bc + 3b + 3c + 6) + 6 \\ &= a \star (b \star c). \end{aligned}$$

There also exists an identity element; namely -2 $\in \mathbb{Q}$. To see this, we only need to check that -2 is a right inverse since the binary operation is abelian. For all $a \in \mathbb{Q}$, we have

$$\begin{aligned} a \star -2 &= a(-2) + 3a + 3(-2) + 6 \\ &= -2a + 3a - 6 + 6 \\ &= a. \end{aligned}$$

On the other hand, not every element in $\mathbb{Q}$ has an inverse. Indeed, let $a \in \mathbb{Q}$. To find the inverse of a, we solve for b in

$$ab + 3a + 3b + 6 = -2.$$

We obtain

$$a^{-1} = \frac{-3a - 8}{a + 3}.$$

Thus every element in $\mathbb{Q}\backslash\{-3\}$ has an inverse element, but -3 does not have an inverse element. Thus $(\mathbb{Q}, \star)$ is a monoid, but not quite a group. However, if we restrict the binary operation $\star$ to the set $\mathbb{Q}\backslash\{-3\} \times \mathbb{Q}\backslash\{-3\}$, then we do get a group $(\mathbb{Q}\backslash\{-3\}, \star)$. To see this, we just need to verify that $\star$ restricted to $\mathbb{Q}\backslash\{-3\} \times \mathbb{Q}\backslash\{-3\}$ lands in $\mathbb{Q}\backslash\{-3\}$. Indeed, assume for a contradiction that $a \star b = -3$ for some $a, b \in \mathbb{Q}\backslash\{-3\}$. Then

$$\begin{aligned} 0 &= a \star b + 3 \\ &= ab + 3a + 3b + 9 \\ &= (a + 3)(b + 3) \end{aligned}$$

implies either $a + 3 = 0$ or $b + 3 = 0$. In either case, we obtain a contradiction.

Later on we will show that the group $(\mathbb{Q}\backslash\{-3\}, \star)$ is in fact isomorphic (a term which we shall define later) to the group $\mathbb{Q}^\times$, with the isomorphism $\varphi\colon \mathbb{Q}^\times \to (\mathbb{Q}\backslash\{-3\}, \star)$ defined by

$$\varphi(a) = a - 3$$

for all $a \in \mathbb{Q}^\times$.

1.1.2 Abelian Group $(\mathcal{P}(X), \Delta)$

Definition 1.2. The **power set** of X, denoted by $\mathcal{P}(X)$, is the set of all subsets of X. The **symmetric difference** of two subsets A and B of X is defined by

$$A\Delta B = (A \cup B) \backslash (A \cap B).$$

This gives rise to a binary operation $\Delta \colon X \times X \to X$.

Proposition 1.1. *The pair $(\mathcal{P}(X), \Delta)$ forms an abelian group.*

Proof. The identity element for $(\mathcal{P}(X), \Delta)$ is clearly the empty set. Clearly Δ is abelian. Let us show that it is also associative. Let $A, B, C \in \mathcal{P}(X)$. Then we have

$$\begin{aligned}
(A\Delta B)\Delta C &= ((A\Delta B) \cup C) \cap ((A\Delta B) \cap C)^c \\
&= ((A\Delta B) \cup C) \cap ((A\Delta B)^c \cup C^c) \\
&= (((A \cup B) \cap (A \cap B)^c) \cup C)) \cap ((A \cap B^c) \cup (A^c \cap B))^c \cup C^c) \\
&= (A \cup B \cup C) \cap (A^c \cup B^c \cup C) \cap (((A \cap B^c)^c \cap (A^c \cap B)^c) \cup C^c) \\
&= (A \cup B \cup C) \cap (A^c \cup B^c \cup C) \cap ((A^c \cup B) \cap (A \cup B^c)) \cup C^c) \\
&= (A \cup B \cup C) \cap (A^c \cup B^c \cup C) \cap (A^c \cup B \cup C^c) \cap (A \cup B^c \cup C^c) \\
&= (B \cup C \cup A) \cap (B^c \cup C^c \cup A) \cap (B^c \cup C \cup A^c) \cap (B \cup C^c \cup A^c) \\
&= ((B \cup C \cup A) \cap (B^c \cup C^c \cup A)) \cap ((B^c \cup C) \cap (B \cup C^c)) \cup A^c) \\
&= ((B \cup C \cup A) \cap (B^c \cup C^c \cup A)) \cap (((B \cap C^c)^c \cap (B^c \cap C)^c) \cup A^c) \\
&= (((B \cup C) \cap (B \cap C)^c) \cup A)) \cap ((B \cap C^c) \cup (B^c \cap C))^c \cup A^c) \\
&= ((B\Delta C) \cup A) \cap ((B\Delta C)^c \cup A^c) \\
&= ((B\Delta C) \cup A) \cap ((B\Delta C) \cap A)^c \\
&= (B\Delta C)\Delta A \\
&= A\Delta(B\Delta C).
\end{aligned}$$

Inverse elements also exist; every subset of X is its own inverse. □

1.1.3 Matrix Groups

In linear algebra, matrices get into row echelon form by elementary row operations:

- Add a multilple of one row to another.
- Multiply a row by a nonzero scalar.
- Exchange two rows.

Elementary row operations on an $m \times n$ matrix can be expressed using left multiplication by an $m \times m$ matrix called an **elementary matrix**. These elementary matrices come in three flavors.

First we have $e_{ij}(a) = \exp(aE_{ij}) = I_n + aE_{ij}$. The effect of multiplying an $m \times n$ matrix A by $e_{ij}(\lambda)$ on the left is an elementary row operation:

$$e_{ij}(a)A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{i1} + aa_{j1} & \cdots & a_{in} + aa_{jn} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix},$$

and the effect of multiplying A by $e_{ij}(\lambda)$ on the right is an elementary column operation:

$$Ae_{ij}(a) = \begin{pmatrix} a_{11} & \cdots & a_{1j} + aa_{1i} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mj} + aa_{mi} & \cdots & a_{mn} \end{pmatrix}.$$

These elementary matrices satisfy the following relations, called the **Steinberg relations**:

$$\begin{aligned}
&e_{ij}(a)e_{ij}(b) = e_{ij}(a + b); \\
&e_{ij}(a)e_{jk}(b) = e_{ik}(ab)e_{jk}(b)e_{ij}(a), \quad \text{for } i \neq k; \\
&e_{ij}(a)e_{kl}(b) = e_{kl}(b)e_{ij}(a), \quad \text{for } i \neq l \text{ and } j \neq k.
\end{aligned}$$

It is useful to think of the second relation as, "you can move $e_{ij}(a)$ from the left to the right of $e_{jk}(b)$ at the cost of multiplying by an element $e_{ik}(ab)$". A similar interpretation can be given for the other relations.

Next we have $d_i(a)$, which has entries 1 on the main diagonal except for a nonzero $a \neq 1$ in the ith spot along the diagonal. The effect of multiplying an $m \times n$ matrix A by $d_i(a)$ on the left is an elementary row operation: multiply the ith row by a. The effect of multiplying an $m \times n$ matrix A by $d_i(a)$ on the right is an elementary column operation: multiply the ith column by a. These matrices together with the $e_{ij}(a)$'s satisfy the following relations:

$$\begin{aligned} d_i(a)d_i(b) &= d_i(ab); \\ d_i(a)d_j(b) &= d_j(b)d_i(a); \\ d_i(a)e_{ij}(b) &= e_{ij}(ab)d_i(a); \\ e_{ij}(b)d_j(a) &= d_j(a)e_{ij}(ab). \end{aligned}$$

It is useful to think of the third relation as "you can move $d_i(a)$ from the left to the right of $e_{ij}(b)$ at the cost of replacing $e_{ij}(b)$ with $e_{ij}(ab)$". A similar interpretation can be given for the other relations.

The last type of elementary matrix to discuss is s_{ij} with $i \neq j$, which is the matrix that has entry 1 in positions (i,j) and (j,i) and also in every diagonal position except the ith and jth, and 0's everywhere else. The effect of multiplying an $m \times n$ matrix A by s_{ij} on the left is an elementary row operation: swap the ith row and jth row. The effect of multiplying an $m \times n$ matrix A by s_{ij} on the right is an elementary column operation: swap the ith column and jth column. These matrices together with the $d_i(a)'s$ and $e_{ij}(b)'s$ satisfy the following relations

$$\begin{aligned} s_{ij}^2 &= I; \\ s_{ij} &= s_{ji}; \\ s_{ij}s_{jk}s_{ij} &= s_{jk}s_{ij}s_{jk}; \\ s_{ij}s_{kl} &= s_{kl}s_{ij}, \quad \text{for } i \neq k \neq j \text{ and } i \neq l \neq j; \\ s_{ij}e_{kl}(a) &= e_{\sigma(k)\sigma(l)}(a)s_{ij}, \quad \sigma = (1,2); \\ s_{ij}d_j(a) &= d_{\sigma(j)}(a)s_{ij}, \quad \sigma = (1,2); \end{aligned}$$

Example 1.3. Addition and multilpication are commutative on $\mathbb{R}$, but negation and division are not commutative on $\mathbb{R}$.

Example 1.4. Matrix multiplication is an associative binary operation which is not commutative: $e_{12}(a)e_{23}(b) = e_{23}(a)e_{12}(b)e_{13}(ab)$.

Example 1.5. Let $G = \{f : \mathbb{R} \to \mathbb{R}\}$. Composition $\circ$ of functions is an associative binary operation on G which is not commutative.

Example 1.6. Define $\star$ on $\mathbb{R}$ by $a \star b = \frac{a+b}{2}$. This is clearly commutative, however it is not associative since:

$$(a \star b) \star c = \frac{\frac{a+b}{2} + c}{2} = \frac{a+b+2c}{4}$$

$$a \star (b \star c) = \frac{a + \frac{b+c}{2}}{2} = \frac{2a+b+c}{4}$$

Definition 1.3. Let G be a nonempty set and let $\star$ be a binary operation on G. An **identity element** is an element $e \in G$ such that $a \star e = e \star a = a$ for all $a \in G$.

Example 1.7. Multiplication on $\mathbb{R} \setminus \{0\}$ has identity element $e = 1$. Every $a \in \mathbb{R}$ has an inverse, $\frac{1}{a}$.

Example 1.8. Let $\star$ be the binary operation $\mathbb{R} \setminus \{3\}$ be given by $a \star b = ab + 3a + 3b + 6 = (a+3)(b+3) - 3$. Let's verify that $\star$ really is a binary operation on $\mathbb{R} \setminus \{3\}$. For all $a, b \in \mathbb{R} \setminus \{-3\}$, we certainly have $a \star b \in \mathbb{R}$. If $a \star b = -3$, then

$$(a+3)(b+3) - 3 = -3 \quad \Longrightarrow \quad (a+3)(b+3) = 0 \quad \Longrightarrow \quad a = b = -3.$$

Thus, it is a binary operation on $\mathbb{R} \setminus \{-3\}$. Does $\star$ have an identity element? Does there exist $e \in \mathbb{R}$ such that $a \star e = e = e \star a$ for all $a \in \mathbb{R}$? In fact $e = -2$ works since $a \star e = (a-3)(-2+3) - 3 = a$. And since $\star$ is commutative, $a \star e = e \star a$. What about inverses? Given $a \in \mathbb{R}$, can we find a $b \in \mathbb{R}$ such that $a \star b = -2$? Suppose $a \star b = -2$.

$$(a+3)(b+3) - 3 = -2 \quad \Longrightarrow \quad (a+3)(b+3) = 1 \quad \Longrightarrow \quad (a+3)b = -3a - 8 \quad \Longrightarrow \quad b = \frac{-3a-8}{a+3}$$

So each element except -3, has an inverse. We have just proved that $(\mathbb{R} \setminus \{3\}, \star)$ is a group. Now we want to show that this group is actually isomorphic to $(\mathbb{R} \setminus \{0\}, \cdot\}$. The isomorphism $\varphi : \mathbb{R} \setminus \{0\} \to \mathbb{R} \setminus \{3\}$ will be given by $a \mapsto a - 3$, where $a \in \mathbb{R} \setminus \{0\}$. We need to show $\varphi(ab) = \varphi(a) \star \varphi(b)$. The left side equals

$$\varphi(ab) = ab - 3.$$

The right side equals

$$\varphi(a) \star \varphi(b) = (a - 3) \star (b - 3) = ab - 3.$$

So this is a homomorphism. In fact, it is an isomorphism since φ is a bijection, with inverse $\phi : \mathbb{R} \setminus \{3\} \to \mathbb{R} \setminus \{0\}$ given by $a \mapsto a + 3$, where $a \in \mathbb{R} \setminus \{3\}$.

1.2 Homomorphisms

Definition 1.4. Let G and G' be groups and let $\varphi \colon G \to G'$ be a function.

1. We say φ is a **homomorphism** is
$$\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$$
for all $g_1, g_2 \in G$.

2. We say φ is an **isomorphism** if it is a bijection homomorphism. In this case, we say G is **isomorphic** to G', and we denote this by $G \cong G'$.

Remark 2. In this document, if we write "let $\varphi \colon G \to G'$ be a homomorphism/isomorphism", then it is understood that φ is a group homomorpism/isomorphism between groups G and G'.

1.2.1 Inverse Map is also Homomorphism

Proposition 1.2. *Let $\varphi \colon G \to G'$ be an isomorphism and let $\psi \colon G' \to G$ denote its inverse. Then ψ is a homomorphism.*

Proof. Let $g_1', g_2' \in G'$. Then we have

$$\begin{aligned}\psi(g_1' g_2') &= \psi(\varphi(\psi(g_1'))\varphi(\psi(g_2'))) \\ &= \psi(\varphi(\psi(g_1')\psi(g_2'))) \\ &= \psi(g_1')\psi(g_2').\end{aligned}$$

□

1.2.2 Group Homomorphisms Sends Identities to Identities and Inverses to Inverses

Proposition 1.3. *Let G and G' be groups with identities e and e' respectively, and let $\varphi \colon G \to G$ be a group homomorphism. Then*

1. *φ sends the identity to the identity: we have $\varphi(e) = e'$*
2. *φ sends inverses to inverses: we have $\varphi(g^{-1}) = \varphi(g)^{-1}$ for all $g \in G$.*

Proof. 1. Observe that

$$\varphi(e) = \varphi(ee) = \varphi(e)\varphi(e). \tag{1}$$

Now we multiply both sides of (1) by $\varphi(e)^{-1}$ to get the desired result.

2. Let $g \in G$. Then we have

$$\begin{aligned}e' &= \varphi(e) \\ &= \varphi(gg^{-1}) \\ &= \varphi(g)\varphi(g^{-1}).\end{aligned}$$

It follows that $\varphi(g)^{-1} = \varphi(g^{-1})$. □

1.2.3 Determinant Homomorphism

Example 1.9. Let K be a field and let $n \in \mathbb{N}$. The determinant map $\det \colon \mathrm{GL}_n(K) \to K^\times$ is a homomorphism. Indeed, if $A, B \in \mathrm{GL}_n(K)$, then one learns from linear algebra that

$$\det(AB) = \det(A)\det(B).$$

1.2.4 Isomorphism from $\mathbb{R}$ to $\mathbb{R}^\times$

Example 1.10. The exponential map $\mathbb{R} \to \mathbb{R}^\times$, given by $x \mapsto e^x$, is an isomorphism. Indeed, for all $x, y \in \mathbb{R}$, we have

$$e^{x+y} = e^x e^y.$$

Furthemore, the exponential map is a bijection, with the logarithm map $\log\colon \mathbb{R}^\times \to \mathbb{R}$ being its inverse.

1.2.5 Automorphisms

Definition 1.5. Let $(G, \cdot)$ be a group. An **automorphism** of G is an isomorphism from G to G. Notation:

$$\mathrm{Aut}(G) = \{\varphi : G \to G \mid \varphi \text{ is an isomorphism}\}$$

Proposition 1.4. *$(Aut(G), \cdot)$ is a group.*

Proof. It suffices to show $\mathrm{Aut}(G) \leq S_G$. We have an identity $1_G \in \mathrm{Aut}(G)$. Let $\sigma, \tau \in \mathrm{Aut}(G)$. Then $\sigma\tau$ is bijective and

$$\sigma\tau(ab) = \sigma(\tau(ab)) = \sigma(\tau(a)\tau(b)) = \sigma(\tau(a))\sigma(\tau(b)) = \sigma\tau(a)\sigma\tau(b).$$

So $\sigma\tau$ is an automorphism. If $\varphi \in \mathrm{Aut}(G)$, then since φ is bijective, there exists an inverse funciton φ^{-1}. Now we show $\varphi^{-1} \in \mathrm{Aut}(G)$: For all $a, b \in G$, there exists $x, y \in G$ such that $\varphi(x) = a$ and $\varphi(y) = b$. Therefore

$$\varphi^{-1}(ab) = \varphi^{-1}(\varphi(x)\varphi(y)) = \varphi^{-1}(\varphi(xy)) = xy = \varphi^{-1}(a)\varphi^{-1}(b).$$

□

Definition 1.6. The set of **inner automorphisms** is

$$\mathrm{Inn}(G) = \{\sigma_g : G \to G,\ \sigma_g(x) = gxg^{-1} \mid g \in G\}$$

Proposition 1.5. *$Inn(G) \leq Aut(G)$.*

Proof. $1_G = \sigma_1$ where 1 is the identity of G. So $1_G \in \mathrm{Inn}(G)$. Suppose $\sigma_g, \sigma_h \in \mathrm{Inn}(G)$. Then for all $x \in G$ we have

$$\begin{aligned}\sigma_g\sigma_h(x) &= g\sigma_h(x)g^{-1} \\ &= ghxh^{-1}g^{-1} \\ &= \sigma_{gh}(x).\end{aligned}$$

So we have closure under the group operation. Lastly, if $\sigma_g \in \mathrm{Inn}(G)$, then $\sigma_g^{-1} = \sigma_{g^{-1}}$ since for all $x \in G$ we have

$$\begin{aligned}\sigma_g\sigma_{g^{-1}}(x) &= g\sigma_{g^{-1}}(x)g^{-1} \\ &= gg^{-1}xgg^{-1} \\ &= x.\end{aligned}$$

□

Proposition 1.6. *Let G be a group and let $H \trianglelefteq G$. Then G acts on H by conjugation by $\sigma_g(h) = g \cdot h = ghg^{-1}$ for all $g \in G$ and $h \in H$. The permutation representatoin is $\varphi : G \to Aut(H)$, given by $\varphi(g) = \sigma_g$ with $Ker\varphi = C_G(H)$. In particular, $G/C_G(H) \cong \varphi(G) \leq Aut(H)$.*

Proposition 1.7. *Let $G = \langle g \rangle$ be a cyclic group of order m, then $Aut(G) \cong \mathbb{Z}_m^\times$.*

Proof. Every automorphism $\psi : G \to G$ is completely determined by where it maps the generator. If$\psi(g) = g^a$, then a must be relatively prime to m since ψ is surjective. Thus for each $a \in \{1, 2, \ldots, m\}$ such that a is relatively prime to m, we have an automorphism $\psi_a(g) = g^a$. This assignment $a \mapsto \psi_a$ is in fact an isomorphism from $\mathbb{Z}_m^\times$ to $\mathrm{Aut}(G)$. We have just shown that the map is bijective. Given two automorphisms ψ_a and ψ_b, we have $(\psi_a \circ \psi_b)(g) = \psi_a(g^b) = g^{ab}$. So this map is a homomorphism too. □

Example 1.11. Let G be a finite group of order 45 and let $H \trianglelefteq G$ such that H is cyclic and $|H| = 9$. We will show G must be abelian. By the previous proposition, $|\mathrm{Aut}(H)| = 6$. The permutation representation is a homomoprhism $\varphi : G \to \mathrm{Aut}(H)$ given by $\varphi(g) = \sigma_g$ where σ_g is the conjugation map. We know that $\mathrm{Ker}\varphi = C_G(H)$. Then $G/C_G(H) \cong \varphi(G) \leq \mathrm{Aut}(H)$, which implies $|G/C_G(H)|$ divides $|\mathrm{Aut}(H)| = 6$. Since $|H| = 3^2$, H is abelian, which implies $H \leq C_G(H) \leq G$ which implies 9 divides $|C_G(H)|$ which divides 45. This implies $|C_G(H)| \in \{9, 45\}$. So $|G/C_G(H)| \in \{1, 5\}$, but since $|G/C_G(H)|$ divides 6, we must have $|G/C_G(H)| = 1$. Now $G/C_G(H)$ is cyclic and $C_G(H)$ is abelian, this implies G is abelian.

1.2.6 Characteristic Subgroups

Definition 1.7. A subgroup H of G is **characteristic** if $\sigma(H) = H$ for all $\sigma \in \text{Aut}(G)$. Notation: H char G

Example 1.12. $\{1\}$ char G and G char G.

Example 1.13. In $(\mathbb{Z}, +)$ any subgroup $m\mathbb{Z}$ is characteristic.

Example 1.14. Find the characteristic subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_2$. The only characteristic subgroups are $\{(0,0)\}$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$. To show this, we just need to find an autormorphism which does not fix any other subgroup. For example, the subgroup $\{(0,0),(1,0)\}$ is not fixed by the automorphism which maps $(1,0)$ to $(0,1)$ and $(1,1)$ to $(1,1)$.

Proposition 1.8. *(Properties of Characteristic Subgroups)*

1. *If H is a characteristic subgroup of G then it is normal in G.*
2. *If H is the unique subgroup of G of a given order m, then H is characteristic in G.*
3. *If K is a characteristic subgroup of H and H is normal in G, then K is normal in G.*

Proof. (1) : For every $g \in G$, we have σ_g is an inner automorphism. Since H is a characteristic subgroup of G, it must be fixed by σ_g. This means $gHg^{-1} = H$. (2) : Let $\sigma \in \text{Aut}(G)$, then $\sigma(H) \leq G$. Since σ is a bijective map, $\sigma(H)$ will have the same size as H. This implies $\sigma(H) = H$. (3) : For all $g \in G$, we have $\sigma_g \in \text{Aut}(H)$ since $H \trianglelefteq G$. Since K is characteristic in H, $\sigma_g(K) = K$. □

1.3 Subgroups

Definition 1.8. Let G be a group and let H be a nonempty subset of G. We say H is a **subgroup** of G, denoted $H \leq G$, if H forms a group under the group operation.

Thus if H is a subgroup of G, then $a, b \in H$ implies $ab \in H$. Similarly, $a \in H$ implies $a^{-1} \in H$. Note that these two conditions (toegether with the fact that H is nonempty) implies $e \in H$. So H and G necessarily share the same identity. In fact, to see that H is a subgroup of G, we just need to check that $a, b \in H$ implies $ab^{-1} \in H$. Indeed, in this case, $a \in H$ implies $e = aa^{-1} \in H$. Also $e, a \in H$ implies $a^{-1} = ea^{-1} \in H$. Finally, $a, b \in H$ implies $a, b^{-1} \in H$ which implies $ab = a(b^{-1})^{-1} \in H$. Let's use this test in the following example

Example 1.15. Let $G = \text{GL}_2(\mathbb{R})$ and let $H = \left\{ \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right) \mid a \in \mathbb{R}^\times \right\}$. Clearly H is nonempty, so to see that H is a subgroup of G, we just need to check that $A, B \in H$ implies $AB^{-1} \in H$. So given $A = \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} b & 0 \\ 0 & b \end{smallmatrix}\right)$ in H, we compute

$$\begin{aligned} AB^{-1} &= \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}^{-1} \\ &= \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} b^{-1} & 0 \\ 0 & b^{-1} \end{pmatrix} \\ &= \begin{pmatrix} ab^{-1} & 0 \\ 0 & ab^{-1} \end{pmatrix} \\ &\in H. \end{aligned}$$

Thus H is a subgroup of G.

Proposition 1.9. *Let H and K be subgroups of G. Then $H \cap K$ is a subgroup of G.*

Proof. First note that $e \in H \cap K$, so $H \cap K$ is nonempty. Now let $a, b \in H \cap K$. Then $a, b \in H$ and $a, b \in K$. Thus $ab^{-1} \in H$ and $ab^{-1} \in K$. This implies $ab^{-1} \in H \cap K$. Thus $H \cap K$ is a subgroup of G. □

1.4 Kernels, Centralizers, and Normalizers

Definition 1.9. Let $(G, \cdot)$ and $(G', \star)$ be two groups and let $\varphi : G \to G'$ be a homomorphism. Then

$$\textbf{ker}\varphi = \{a \in G \mid \varphi(a) = e\}$$

.

Definition 1.10. Let $(G,\cdot)$ and $(G',\star)$ be two groups and let $\varphi : G \to G'$ be a homomorphism. Then

$$\mathbf{im}\varphi = \{\varphi(a) \mid a \in G\}$$

.

Proposition 1.10. *Let $(G,\cdot)$ and $(G,\star)$ be two groups and let $\varphi : G \to G'$ be a homomorphism. Then $ker\varphi \leq G$ and $im\varphi \leq G'$.*

Proof. $e \in \ker\varphi$ since $\varphi(e) = e$, so $\ker\varphi$ is nonempty. Given $a, b \in \ker\varphi$, $\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} = e$, so $ab^{-1} \in \ker\varphi$. This proves $\ker\varphi \leq G$. $e \in \mathrm{im}\varphi$ since $\varphi(e) = e$, so $\mathrm{im}\varphi$ is nonempty. Given $a', b' \in \mathrm{im}\varphi$, there exists an $a, b \in G$ such that $\varphi(a) = a'$ and $\varphi(b) = b'$. Then $\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} = a'b'^{-1}$, so $a'b'^{-1} \in \mathrm{im}\varphi$. □

Example 1.16. Let $m \in \mathbb{Z}^+$ be fixed. Then $\pi : \mathbb{Z} \to \mathbb{Z}/(m)$, where $\pi(a) = \bar{\pi}$, is a group homomorphism: $\pi(a+b) = \overline{a+b} = \bar{a} + \bar{b} = \pi(a) + \pi(b)$. Notice that $\ker\pi = m\mathbb{Z}$ and $\mathrm{im}\pi = \mathbb{Z}/(m)$.

Definition 1.11. Let $(G,\cdot)$ be a group and let A be a nonempty subset of G. Then the **centralizer** of A in G is

$$C_G(A) = \{g \in G \mid ga = ag \quad \forall a \in A\}$$

Proposition 1.11. $C_G(A) \leq G$

Proof. $e \in C_G(A)$ since $ea = ae$ for all $a \in A$. So $C_G(A)$ is nonempty. Given $g, h \in C_G(A)$, $gh^{-1}a = gah^{-1} = agh^{-1}$ for all $a \in A$, so $gh^{-1} \in C_G(A)$. □

Example 1.17. Consider $(S_3,\cdot)$ and $A = \{(1,2)\}$. Then $C_{S_3}(A) = \{1, (1,2)\}$.

Example 1.18. Let G be an abelian group and A be a subset of G. Then $C_G(A) = G$.

Definition 1.12. The **center** of a group G is $Z(G) = \{g \in \mid ga = ag \ , \forall a \in G\}$

Remark 3. $Z(G) = C_G(G)$

Proposition 1.12. $Z(G) \leq G$

Proof. Obviously $e \in Z(G)$ so $Z(G)$ is nonempty. Given $g, h \in Z(G)$, $gh^{-1} \in Z(G)$ since

$$\ell gh^{-1} = g\ell h^{-1} = gh^{-1}\ell \qquad \forall \ell \in G$$

□

Remark 4.

$$Z(G) = \bigcap_{\emptyset \neq A \subseteq G} C_G(A)$$

Example 1.19. $Z(S_3) = \{1\}$. We have $Z(S_3) \subseteq C_{S_3}((1,2)) \cap C_{S_3}((1,3)) = \{1\}$.

Definition 1.13. Let G be a group and let A be a nonempty subset of G. Then for each $g \in G$

$$gAg^{-1} = \{gag^{-1} \mid a \in A\}$$

Definition 1.14. The **normalizer** of A in G is

$$N_G(A) = \{g \in G \mid gAg^{-1} = A\}$$

Proposition 1.13. *Let G be a group and let A be a nonempty subset of G. Then $N_G(A) \leq G$*

Proof. Obviously $e \in N_G(A)$ so $N_G(A)$ is nonempty. Given $g, h \in N_G(A)$, we have

$$gh^{-1}A = gAh^{-1} = Agh^{-1}$$

□

Remark 5. If $H \leq G$, then $H \leq N_G(H)$

Example 1.20. Let $A, B \subseteq S_3$ where $A = \{1, (1,2)\}$ and $B = \{1, (1,2,3), (1,3,2)\}$, then $N_{S_3}(A) = \{1, (1,2)\}$ and $N_{S_3}(B) = S_3$.

1.5 Quotient Groups and Homomorphisms

1.5.1 Normal Subgroups

Let G be a group and let $H \leq G$. Consider the relation $\sim$ on G:

$$a \sim b \quad \text{if} \quad a^{-1}b \in H$$

$\sim$ is an equivalence relation:

1. $\sim$ is reflexive: $a^{-1}a = e \in H \implies a \sim a, \forall a \in G$.
2. $\sim$ is symmetric: If $a^{-1}b \in H$, then $b^{-1}a = \left(a^{-1}b\right)^{-1} \in H$ since H is closed under inverses. Therefore $a \sim b$ if and only if $b \sim a$.
3. $\sim$ is transitive: Suppose $a \sim b$ and $b \sim c$. Then $a^{-1}b \in H$ and $b^{-1}c \in H$ implies $a^{-1}c = \left(a^{-1}b\right)\left(b^{-1}c\right) \in H$ since H is closed under products. Therefore $a \sim c$.

The equivalence class of $a \in G$ is

$$\{b \in G \mid a^{-1}b \in H\} = \{ah \mid h \in H\} = aH$$

aH is called the **left coset of H in G containing a**. We have

$$aH = bH \quad \text{if and only if} \quad a \sim b$$

The **right coset of H in G containing a** is given by

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

A subgroup H of G is **normal in G** if $aH = Ha$ for all $a \in G$. If H is normal in G, we write $H \trianglelefteq G$.

Example 1.21. $\{e\} \trianglelefteq G$ and $G \trianglelefteq G$.

Example 1.22. If G is abelian then any subgroup H is normal in G.

Theorem 1.1. *Let $H \leq G$. Any left H-coset in G has a bijection with H. In particular, when H is finite, the cosets of H all have the same size as H.*

Proof. Pick a left coset, say gH. We can pass from gH to H by left multiplication by g^{-1} : $g^{-1}(gh) = h \in H$. Conversely, we can pass from H to gH by left multiplication by g. These functions from gH to H and vice versa are inverses to each other, showing gH and H are in bijection with each other. □

Definition 1.15. Let $H \leq G$. The **index** of H in G is the number of left cosets of H in G. This number, which is a positive integer or ∞, is denoted $[G : H]$.

Remark 6. The number of left cosets of H in G is equal to the number of right cosets of H in G. A bijection from is given by the inverse map:

$$aH \mapsto Ha^{-1}$$

Theorem 1.2. *Let $H \leq G$. The following statements are equivalent*

1. $H \trianglelefteq G$
2. $gHg^{-1} = H$ *for all* $g \in G$, *where* $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$
3. $N_G(H) = G$
4. $gHg^{-1} \subseteq H$ *for all* $g \in G$

Proof. $(1 \implies 2)$: $H \trianglelefteq G$ means $gH = Hg$ for all $g \in G$. Multiply both sides by g^{-1} (a bijection) to get $gHg^{-1} = Hgg^{-1} = H$. $(2 \implies 3)$: Recall $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$. By assumption, $gHg^{-1} = H$ for all $g \in G$, therefore $N_G(H) = G$. $(3 \implies 4)$: By assumption $gHg^{-1} = H$ for all $g \in G$, therefore $gHg^{-1} \subseteq H$. $(4 \implies 1)$: We need to show $gHg^{-1} \supseteq H$ for all $g \in G$. Suppose $h \in H$. Then $g^{-1}hg \in H$ by assumption. Then $h = gg^{-1}hgg^{-1} \in gHg^{-1}$.

□

Example 1.23. We show $SL_2(\mathbb{R}) \trianglelefteq GL_2(\mathbb{R})$. It suffices to check $MAM^{-1} \subseteq SL_2(\mathbb{R})$ for all $M \in GL_2(\mathbb{R})$ and $A \in SL_2(\mathbb{R})$. Given any such M and A,

$$\det(MAM^{-1}) = \det(M)\det(A)\det(M^{-1}) = \det(M)\det(M^{-1}) = \det(I) = 1$$

Therefore $MAM^{-1} \in SL_2(\mathbb{R})$.

1.5.2 Quotient Group

Let $H \leq G$. Define multiplication on the left cosets by

$$(aH)(bH) = abH$$

Check that this is well-defined iff $H \trianglelefteq G$.

Definition 1.16. Let G be a group and let $H \leq G$. Let

$$G/H = \{gH \mid g \in G\}$$

Define multiplication on G/H by

$$(aH)(bH) = abH$$

Proposition 1.14. *Multiplication of left cosets is well defined if and only if $H \trianglelefteq G$.*

Proof. Choose different coset representatives a' and b'. So $b' = bh_1$ and $a' = ah_2$. Then

$$(a'H)(b'H) = (ah_2H)(bh_1H) = aHbH = abH'H$$

If $H' = H$ for all $b \in G$, then H is normal.

□

$$HK = \{hk \mid h \in H, k \in K\}$$

Proposition 1.15. *If $H \trianglelefteq G$, then $G/H = \{gH \mid g \in G\}$ is a group with multiplication $\cdot$ being $(aH)(bH) = abH$ for all $a, b \in G$. We say G/H is the quotient group $G \mod H$.*

Proof.

1. Binary Operation: For all $a, b \in G$, abH is a left coset of H. So $\cdot$ is a binary operation defined on the set of left cosets of H.
2. Associativity: For all, $a, b, c \in G$, we have$((aH)(bH))(cH) = (abH)(cH) = ((ab)cH) = (a(bc)H) = (aH)(bcH) = (aH)((bH)(cH))$
3. Identity: For all $a \in G$, we have $(aH)(eH) = aeH = aH = eaH = (eH)(aH)$
4. Inverse: For all $a \in G$, we have $(aH)(a^{-1}H) = aa^{-1}H = eH = H = eH = a^{-1}aH = (a^{-1}H)(aH)$.

□

Example 1.24. Let $K = \langle (1,2,3) \rangle \trianglelefteq S_3$. Then $(1,2)K = \{(1,2),(2,3),(1,3)\}$, $(2,3)K = \{(2,3),(1,3),(1,2)\}$, and $(1,3)K = \{(1,3),(1,2),(2,3)\}$. So $(1,2)K = (2,3)K = (1,3)K$ and $()K = (1,2,3)K = (3,2,1)K$. So there are two elements in S_3/K, and they are represented by $\{()K, (1,2)K\}$. Let $\varphi : S_3/K \to \mathbb{Z}_2$ be given by $\varphi(()K) = \bar{0}$ and $\varphi((1,2)K) = \bar{1}$. Then φ is an isomorphism.

Remark 7. If G is abelian then G/H is abelian: $(aH)(bH) = abH = baH = (bH)(aH)$. If G is cyclic then G/H is cyclic: Suppose $G = \langle a \rangle$. Then $bH = a^nH = (aH)^n$. Therefore $G/H = \langle aH \rangle$.

What does it mean to say G/H is abelian. It means for all $a, b \in G$, $ab = \varphi(a,b)ba$ where $\varphi(a,b) \in H$. So we have a function $\varphi : G \times G \to H$. What can we say about this function φ? First of all, $ab = ba$ if and only if $\varphi(a,b) = e$ for all $a, b \in G$. Next

$$ab = \varphi(a,b)ba = \varphi(a,b)\varphi(b,a)ab$$

tells us $\varphi(a,b) = \varphi(b,a)^{-1}$. Next, associativity tells us

$$\varphi(a,b)\varphi(b,ac)acb = \varphi(a,b)bac = abc = a\varphi(b,c)cb = \varphi(a,\varphi(b,c))\varphi(b,c)acb \qquad \forall a,b,c \in G$$

So

$$a\varphi(b,c)a^{-1} = \varphi(a,\varphi(b,c))\varphi(b,c) = \varphi(a,b)\varphi(b,ac) \qquad \forall a,b,c \in G \tag{2}$$

.
And finally, the identity element e tells us

$$a\varphi(e,a) = ae\varphi(e,a) = ea = a = ae = ea\varphi(a,e) = a\varphi(a,e)$$

So

$$\varphi(a,e) = \varphi(e,a) = e \qquad \forall a \in G \tag{3}$$

Given $b, c \in G$, suppose $bc = cb$ or in other words $\varphi(b, c) = e$. Then using (2) and (3) we get

$$e = \varphi(a, b)\varphi(b, ac)$$

What we've been calling φ actually goes by a better name.

Definition 1.17. Given $a, b \in G$, the **commutator** $[a, b]$ of a and b is

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

Check that $ab = [a, b]ba$ so what we've been calling $\varphi(a, b)$ can also be thought of as $[a, b]$. Next, what does it mean to say G/H is cyclic? It means for every $b \in G$, $b = a^{\psi(b)}\varphi(b)$ where $\varphi(b) \in H$ and $\psi(b) \in \mathbb{Z}$. Now suppose H is abelian. Then

$$a^{\psi(b)+\psi(c)}\varphi(b)\varphi(c) = a^{\psi(b)}\varphi(b)a^{\psi(c)}\varphi(c) = bc = a^{\psi(bc)}\varphi(bc)$$

Example 1.25. If $G/Z(G)$ is cyclic, then G is abelian.

Theorem 1.3. *A subgroup H of G is normal in G if and only if H is the kernel of a group homomorphism.*

Proof. If $H \trianglelefteq G$ then $G/H = \{aH \mid a \in G\}$ is a group. Let $\pi : G \to G/H$ be given by $\pi(a) = aH$. π is a homomorphism: $\pi(ab) = abH = (aH)(bH) = \pi(a)\pi(b)$ for all $a, b \in G$. And $\text{Ker}\pi = \{a \in G \mid \pi(a) = H\} = \{a \in G \mid aH = H\} = H$. Conversely, let $\varphi : G \to G'$ be a homomorphism. Then $a\text{Ker}\varphi a^{-1} \subset \text{Ker}\varphi$ since

$$\varphi(axa^{-1}) = \varphi(a)\varphi(x)\varphi(a^{-1}) = \varphi(a)\varphi(a^{-1}) = 1 \qquad \forall x \in \text{Ker}\varphi$$

We also have $\text{Ker}\varphi \subset a\text{Ker}\varphi a^{-1}$ since $x = a(a^{-1}xa)a^{-1}$ for all $x \in \text{Ker}\varphi$.

□

Example 1.26. $\det : (GL_n(\mathbb{R}), \cdot) \to (\mathbb{R} \setminus \{0\}, \cdot)$ is a homomorphism with $\text{Ker}\det = SL_n(\mathbb{R})$, so $SL_n(\mathbb{R})$ is a normal subgroup in $GL_n(\mathbb{R})$

1.6 Cyclic Groups and Subgroups

Proposition 1.16. *Let G be a group with identity e and let $a \in G$. Then*

$$H = \{a^m \mid m \in \mathbb{Z}\}$$

*is a subgroup of G. H is the **cyclic subgroup** generated by a. Notation: $H = \langle a \rangle$.*

Proof. H is nonempty since $a \in H$. Suppose $b, c \in H$, then $b = a^i$ and $c = a^j$ for some $i, j \in \mathbb{Z}$. So $bc^{-1} = \left(a^i\right)\left(a^j\right)^{-1} = a^{i-j} \in H$. □

Example 1.27. In $\mathbb{Z}$, $\langle 3 \rangle = \{3 \cdot m \mid m \in \mathbb{Z}\} = 3\mathbb{Z}$.

Example 1.28. In $\mathbb{Z}/10\mathbb{Z}$, $\langle \bar{2} \rangle = \{\bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{0}\}$

Example 1.29. In S_3, $\langle (1,2,3) \rangle = \{(1,2,3), (1,3,2), 1\}$

Definition 1.18. A group G is **cyclic** if $G = \langle a \rangle$ for some $a \in G$.

Example 1.30. $\mathbb{Z}$ is cyclic since $\mathbb{Z} = \langle 1 \rangle$.

Example 1.31. $\mathbb{Z}/m\mathbb{Z}$ is cyclic since $\mathbb{Z}/m\mathbb{Z} = \langle \bar{1} \rangle$.

Example 1.32. S_3 is not cyclic.

Example 1.33. $\mathbb{Q}$ is not cyclic: To obtain a contradiction, suppose $\langle \frac{a}{b} \rangle = \mathbb{Q}$. Then for any prime p, $\frac{1}{p} \in \langle \frac{a}{b} \rangle \implies \frac{1}{p} = n\frac{a}{b}$ for some $n \in \mathbb{Z}$. Thus $b = pma \implies p \mid b$ for any prime p which is a contradiction.

Proposition 1.17. *Let $H = \langle a \rangle$. Then $|H| = ord a$. More precisely:*

1. *If $ord a = m < \infty$ then $H = \{e, a, a^2, \ldots, a^{n-1}\}$*
2. *If $ord a = \infty$ then $a^k \neq a^\ell$ for $k, \ell \in \mathbb{Z}$ where $k \neq \ell$.*

Proposition 1.18. *Let $H = \langle a \rangle$ with $ord a = m < \infty$. Then $ord(a^k) = \frac{m}{gcd(m,k)}$.*

Proof. Let $m = \text{ord}(a)$ and $d = \gcd(m,k)$. Then $m = dm'$, $k = dk'$, and $\gcd(m',k') = 1$. We need to prove that $\text{ord}(a^k) = \frac{m}{d} = m'$. We have $(a^k)^{m'} = a^{km'} = a^{\frac{km}{d}} = a^{k'm} = (a^m)^{k'} = e^{k'} = e$. So $\text{ord}(a^k) \mid m'$. Let $\text{ord}(a^k) = t$. Then $(a^k)^t = e \implies a^{kt} = e \implies m \mid kt \implies dm' \mid dk't \implies m' \mid k't \implies m' \mid t$. So $m' \mid \text{ord}(a^k)$. □

Example 1.34. In $\mathbb{Z}/m\mathbb{Z}$, $\text{ord}(\bar{k}) = \frac{m}{\gcd(m,k)}$.

Corollary 1. *Let $H = \langle a \rangle$ with orda $= m < \infty$. Then $\langle a^k \rangle = H$ if and only if $gcd(m,k) = 1$.*

Exercise 1. Find the number of generators of $\mathbb{Z}/625\mathbb{Z}$.

Answer: $\varphi(625) = \varphi(5^4) = 5^4 - 5^3 = 500$.

Proposition 1.19. *Any two cyclic groups having the same order are isomorphic. More specifically:*

1. *If $\langle x \rangle$ and $\langle y \rangle$ both have order $m < \infty$, then $\varphi : \langle x \rangle \to \langle y \rangle$ given by $\varphi(x^k) = y^k$ is an isomorphism.*
2. *If $\langle x \rangle$ is an infinite cycle group, then $\psi : \mathbb{Z} \to \langle x \rangle$ given by $\psi(k) = x^k$ is an isomorphism.*

Theorem 1.4. *Every subgroup of a cyclic group $H = \langle x \rangle$ is still cyclic.*

Proof. Let $K \leq H$. If $K = \{e\}$, then $K = \langle e \rangle$. If $K \neq \{e\}$, then there exists $x^a \in K \setminus \{e\}$. Since K is a group, we can assume $a \in \mathbb{N}$. So $P = \{b \in \mathbb{N} \mid x^b \in K\} \neq \emptyset$. Let $d = \min P$. We will show $K = \langle x^d \rangle$. We have $\langle x^d \rangle \subseteq K$ since $x^{nd} \in K$. For the reverse inclusion, let $y \in K$. Since $K \leq \langle x \rangle$, we have $y = x^\ell$, for some integer ℓ. Now

$$\ell = gd + r \qquad \text{with } 0 \leq r \leq d-1$$

So $y = x^{dg+r} = x^{dg}x^r$. If $r \neq 0$, then $x^r = x^{-dg}y \in K$, which is a contradiction since $d = \min P$.

□

Corollary 2. *Let H be a cyclic group of order $m < \infty$. If $d \mid m$, then there exists a unique subgroup of H of order d.*

Proof. Let $H = \langle x \rangle$. We first prove existence. Recall

$$\text{ord}(x^a) = \frac{\text{ord}(x)}{\gcd(\text{ord}(x), a)} = \frac{m}{\gcd(m,a)}$$

$d \mid m \implies m = dk$ and so

$$|\langle x^k \rangle| = \text{ord}(x^k) = \frac{m}{\gcd(m,k)} = \frac{m}{k} = d$$

Now we prove uniqueness. Let $L \leq H$ such that $|L| = d$. Since $L \leq H$, $L = \langle x^t \rangle$ for some $t \in \mathbb{Z}$.

$$|L| = |\langle x^t \rangle| = \text{ord}(x^t) = \frac{m}{\gcd(m,t)} = d = \frac{m}{k}$$

So $\gcd(m,t) = k$ implies $k \mid t$ which implies $t = ku$. Then $x^t = x^{ku} \in \langle x^k \rangle$. Thus $\langle x^t \rangle = L \subseteq \langle x^k \rangle$. Since $|L| = \langle x^k \rangle$ and $L \subseteq \langle x^k \rangle$, we must have $L = \langle x^k \rangle$. □

Remark 8. The number of subgroups of a cyclic group of order m is equal to the number of divisors of m.

Exercise 2. Find all the subgroups of $\mathbb{Z}/12\mathbb{Z}$, giving a generator for each.

The number of subgroups of $\mathbb{Z}/12\mathbb{Z}$ is equal to the number of divisors of $12 = 2^2 \cdot 3$. If $m = p_1^{e_1} \cdots p_k^{e_k}$, then the number of divisors of m is $(e_1 + 1) \cdots (e_k + 1)$.

1.7 Subgroups generated by Subsets

Definition 1.19. Let G be a group. Let A be a nonempty subset of G. The subgroup of G **generated by** A is

$$\langle A \rangle = \bigcap_{A \subseteq K \leq G} K$$

Theorem 1.5. *Let G be a group. Let A be a nonempty subset of G. Let*

$$\bar{A} = \{a_1^{e_1} \cdots a_m^{e_m} \mid m \in \mathbb{N},\ a_i \in A,\ e_i = \pm 1,\ 1 \leq i \leq m\}$$

Then $\bar{A} = \langle A \rangle$.

Proof. First we note that $A \subseteq \bar{A}$ since for any $a \in A$, $a = a^1 \in \bar{A}$. Next we check that $\bar{A}$ is a subgroup of G. $\bar{A}$ is nonempty since $A \subseteq \bar{A}$. Let $a = a_1^{e_1} \cdots a_m^{e_m}$ and $b = b_1^{f_1} \cdots b_m^{f_m}$ be two elements in $\bar{A}$. Then $b^{-1} = b_m^{-f_m} \cdots b_1^{-f_1} \in \bar{A}$ and $ab = a_1^{e_1} \cdots a_m^{e_m} \cdot b_m^{-f_m} \cdots b_1^{-f_1} \in \bar{A}$. Since $\langle A \rangle$ is the smallest subgroup of G which contains A, we have $\langle A \rangle \subseteq \bar{A}$. For the reverse inclusion, suppose $a = a_1^{e_1} \cdots a_m^{e_m}$ and $A \subseteq K \leq G$. Then $a \in K$ since K is a subgroup of G which contains A. Therefore $\bar{A} \subseteq \langle A \rangle$. □

Remark 9. If G is abelian, then $\langle A \rangle = \{a_1^{e_1} \cdots a_m^{e_m} \mid m \in \mathbb{N}, a_i \in A, e_i \in \mathbb{Z}, 1 \leq i \leq m\}$. Notice in this case the exponents can be any integer.

Example 1.35. In $\mathbb{Z}$,$\langle a, b \rangle = \{ma + kb \mid m, k \in \mathbb{Z}\}$. Since $\mathbb{Z}$ is cyclic, $\langle a, b \rangle = \langle d \rangle$ for some $d \in \mathbb{Z}$. In fact $d = \gcd(a, b)$. Proof: Since $d \mid a$ and $d \mid b$, we must have $da' = a$ and $db' = b$ for some $a', b' \in \mathbb{Z}$. Then for all $m, k \in \mathbb{Z}$, we have$ma + kb = ma'd + kb'd = (ma' + kb')d \in \langle d \rangle$. So $\langle a, b \rangle \subseteq \langle d \rangle$. For the reverse inclusion, note that $d = ax + by$ for some $x, y \in \mathbb{Z}$, therefore $\langle d \rangle = \langle ax + by \rangle \subseteq \langle a, b \rangle$.

Example 1.36. In S_m

1. $\langle A \rangle = S_m$ where $A = \{(1,2), (1,3), \ldots, (1,m)\}$.
2. $\langle B \rangle = S_m$ where $B = \{(1,2), (2,3), \ldots, (m-1,m)\}$.
3. $\langle C \rangle = S_m$ where $C = \{(1,2), (1,2,\ldots,m)\}$.

To prove (1), we first note that any $\sigma \in S_m$ is a product of transpositions. So it suffices to show that any transposition $(i,j) \in \langle A \rangle$. Since $(i,j) = (1,i)(1,j)(1,i)$, we have $(i,j) \in \langle A \rangle$. To prove (2), it suffices to show any transposition $(i,j) \in \langle B \rangle$. Without loss of generality, assume $i < j$. Since $(i,j) = (j-1,j) \cdots (i+1,i+2)(i,i+1)(i+1,i+2) \cdots (j-1,j)$, we have $(i,j) \in \langle B \rangle$. To prove (3), note that $(1,2,\ldots,m)^k(1,2)(m,m-1,\ldots,1)^k = (k,k+1)$. Thus $B \in \langle C \rangle$ which implies $\langle C \rangle = S_m$.

1.8 Order

Definition 1.20. Let G be a group and let $g \in G$. The **order** of g is the least natural number $n \in \mathbb{Z}_{\geq 1}$ such that $g^n = e$. If no such integer exists, we say g has infinite order. We sometimes denote the order of g by $\mathrm{ord}(g)$.

Remark 10. The order of an element can also be thought of as the size of the cyclic group generated by g.

Example 1.37. In the group $\mathbb{Z}$, every nonzero element has infinite order.

Example 1.38. In the group $\mathbb{C}^\times$, there are infinitely many elements which have finite order. The elements in $\mathbb{C}$ which have finite order are called the **roots of unity**. The set of all roots of unity is given by

$$T = \{e^{2\pi i r} \mid r \in \mathbb{Q}\}.$$

Lemma 1.6. *Suppose G is a finite group. Then every $g \in G$ has finite order.*

Proof. Consider the set $\{g^n \mid n \in \mathbb{Z}_{\geq 1}\}$. Since G is finite, we must have $g^m = g$ for some $m \in \mathbb{Z}_{\geq 1}$. This implies $g^{m-1} = 1$. □

Lemma 1.7. *Let $g \in G$ and let m be the order of g. If $g^n = e$, then $m \mid n$.*

Proof. First note that $m \leq n$ since m is the least natural number which kills g. Since $\mathbb{Z}$ is a Euclidean domain and $m \leq n$, there exists $k \in \mathbb{Z}_{\geq 1}$ and $0 \leq r < m$ such that $n = mk + r$. Assume for a contradiction that $r \neq 0$. Then we have

$$\begin{aligned} e &= g^n \\ &= g^{mk+r} \\ &= (g^m)^k g^r \\ &= g^r. \end{aligned}$$

This contradicts the fact that m is least natural number which kills g. So we must have $r = 0$ which implies $m \mid n$. □

1.8.1 Order of a Product of Two Elements

Proposition 1.20. *Let G be a group and let $g_1, g_2 \in G$ with orders m and n respectively. If g_1 and g_2 commute with one another and m is relatively prime to n, then the order of $g_1 g_2$ is mn.*

Proof. Let k be the order of $g_1 g_2$. First note that since g_1 and g_2 commute with each other, we have

$$\begin{aligned}(g_1 g_2)^{mn} &= g_1^{mn} g_2^{mn} \\ &= (g_1^m)^n (g_2^n)^m \\ &= e^n e^m \\ &= e.\end{aligned}$$

Therefore $k \mid mn$. On the other hand, since k is the order of $g_1 g_2$ and g_1 commutes with g_2, we have

$$e = g_1^k g_2^k. \tag{4}$$

Raising both sides of (4) to the nth power gives us $e = g_1^{kn}$. Therefore $m \mid kn$, and since m is relatively prime to n, this implies $m \mid k$. A similar calculation shows $n \mid k$. Since both m and n divide k, we must have $mn \mid k$. So since $k \mid mn$ and $mn \mid k$, we must have $mn = k$. □

Note that we need *both* g_1 to commute with g_2 *and* m to be relatively prime to n in order to conclude (1.20). In one of these conditions do not hold, then the conclusion of (1.20) may not hold.

Example 1.39. If g_1 and g_2 do not commute, then the result can fail. For example, in S_3, let $g_1 = (13)$ and $g_2 = (12)$. Then $g_1 g_2 = (13)(12) = (123)$ has order 3, but g_1 and g_2 both have order 2. Even if g_1 and g_2 commute, if their order is not relatively prime, the result can still fail. For example, in $\mathbb{Z}/12\mathbb{Z}$, the order of $\overline{2}$ is 6 and the order of $\overline{6}$ is 2. But the order of $\overline{2} + \overline{6} = \overline{8}$ is 3.

Proposition 1.21. *Let g_1 and g_2 be elements in a group G with orders n_1 and n_2 respectively. Suppose g_1 commutes with g_2 and $\text{ord}(g_1 g_2) = n_1 n_2$. Then $(n_1, n_2) = 1$.*

Proof. Assume for a contradiction that $(n_1, n_2) \neq 1$. Denote $k = (n_1, n_2)$, so n_1/k Then n_1 and n_2 have a nontrivial factor

□

Suppose $\text{ord}(g_1 g_2) = mn$ and that is mn

Lemma 1.8. *Let m and n be positive integers. Denote $a = \gcd(m, n)$ and $b = \text{lcm}(m, n)$. Then*

$$ab = mn.$$

Proof. We will show $a = mn/b$. Observe that $m \mid m(n/b)$ and $n \mid (m/b)n$. Therefore $a \mid mn/b$. Conversely, observe that $mn/a \mid m$ since $(mn/a)(a/n) = m$. Similarly, $mn/a \mid n$ since $(mn/a)(a/n) = n$. It follows that $b \mid mn/a$. In other words, $mn/b \mid a$. Since we have $a \mid mn/b$ and $mn/b \mid a$, it follows that $a = mn/b$. □

2 Basic Theorems

2.1 Lagrange's Theorem

Lemma 2.1. *Let G be a group and let $H \leq G$. Then $|H| = |gH|$ for all $g \in G$.*

Proof. The idea is that multiplying H by g on the left is an isomorphism since g^{-1} exists. □

Theorem 2.2. *(Lagrange's Theorem) Let G be a finite group. If $H \leq G$ then $|H|$ divides $|G|$.*

Proof. The set of left cosets of H form a partition of G into equal sized parts. □

Remark 11.
1. $|G| = |H|[G : H]$.
2. If $H \trianglelefteq G$ then $|G/H| = \frac{|G|}{|H|} = [G : H]$

Corollary 3. *If G is a finite group then ord$a$ divides $|G|$ for any $a \in G$.*

Proof. Let $H = \langle a \rangle$. Then $|H| = \text{ord}a$ and by Lagrange's Theorem $|H|$ divides $|G|$. □

Corollary 4. *If G is a finite group with $|G| = p$, then G is cyclic.*

Proof. Choose $a \in G \setminus \{e\}$. Then since ord$a$ divides $|G| = p$ implies ord$a = p$, we have $G = \langle a \rangle$. □

Example 2.1. Recall if $G/Z(G)$ is cyclic then G is abelian (Proof: $G/Z(G)$ is cyclic means $\exists g \in G$ such that for all $h, h' \in G$, $h = zg^n$ and $h' = z'g^{n'}$ for some $z, z' \in Z(G)$ and $n, n' \in \mathbb{Z}$. So $hh' = zg^n z'g^{n'} = zz'g^{n+n'} = zz'g^{n'+n} = z'g^{n'}zg^n = h'h$). If G is a finite group of order pq where both p and q are prime, then either $Z(G) = \{e\}$ or G is abelian. The possibilities for $|G/Z(G)|$ are $1, p, q$, or pq. If $|G/Z(G)| = 1, p$, or q, then $G/Z(G)$ is cyclic which implies G is abelian. If $|G/Z(G)| = pq$, then $Z(G) = \{e\}$.

Theorem 2.3. *(Cauchy's Theorem) Let G be a finite abelian group and let p be a prime. If $p \mid |G|$ then G has an element of order p.*

Proof. We prove by induction on $|G|$. The base case is $|G| = p$. In this case, $G = \langle a \rangle$ for some $a \in G$ and thus a has order p. Now let $x \in G \setminus \{e\}$. If $p|\text{ord}x$, then $\text{ord}x = pm$ and $\text{ord}(x^m) = p$. So assume p does not divide $\text{ord}x$. Let $N = \langle x \rangle$. Then $N \trianglelefteq G$ because G is abelian and $|G| = |N||G/N|$. Since p divides G but does not divide $|N|$, p divides $|G/N|$. Since $p||G/N|$ and $|G/N| < |G|$, then by the induction hypothesis there exists $yN \in G/N$ such that $\text{ord}(yN) = p$. Then $(yN)^p = y^pN = N$ and this implies $y^p = n$ for some $n \in N$. Since $\langle y^p \rangle \subset \langle y \rangle$ and the inclusion is strict, it follows that $\text{ord}(y^p) = \dfrac{\text{ord}y}{\gcd(\text{ord}_{y,p})} < \text{ord}(y)$, which implies $1 < \gcd(\text{ord}y, p)$. It follows that $\gcd(\text{ord}y, p) = p$. So $p|\text{ord}y$. □

Alternate Proof: This part doesn't require the induction part. Let $G = \{g_1, \ldots, g_n\}$ and $m = \text{lcm}(\text{ord}g_1, \ldots, \text{ord}g_n)$. Assume no element in g has order p. Then p does not divide m. Construct homomorphism

$$\varphi : \mathbb{Z}_{(m)}^n \mapsto G, \qquad (\overline{a_1}, \ldots, \overline{a_n}) \mapsto g_1^{a_1} \cdots g_n^{a_n}$$

This implies $|\text{Ker}\varphi||G| = m^n$. Since $p \mid |G|$, it must divide m^n, which implies it divides m, which is a contradiction.

2.2 The Isomorphism Theorems

2.2.1 First Isomorphism Theorem

Theorem 2.4. *Let G and H be groups and let $\varphi\colon G \to H$ be a group homomorphism. Then*

1. *The kernel of φ is a normal subgroup of G.*
2. *The image of φ is a subgroup of H and moreover we have the isomorphism $G/\ker\varphi \cong \text{im}\,\varphi$.*

Proof. 1. First let us check $\ker\varphi$ is a subgroup of G. It is nonempty since $\varphi(e) = e$ implies $e \in \ker\varphi$. Let $g_1, g_2 \in \ker\varphi$. Then observe that

$$\begin{aligned}\varphi(g_1g_2^{-1}) &= \varphi(g_1)\varphi(g_2)^{-1}\\ &= ee\\ &= e\end{aligned}$$

implies $g_1g_2^{-1} \in \ker\varphi$. It follows that $\ker\varphi$ is a subgroup of G.

Next, we check that $\ker\varphi$ is a normal subgroup of G. Let $g \in G$ and let $x \in \ker\varphi$. Then observe that

$$\begin{aligned}\varphi(gxg^{-1}) &= \varphi(g)\varphi(x)\varphi(g)^{-1}\\ &= \varphi(g)e\varphi(g)^{-1}\\ &= \varphi(g)\varphi(g)^{-1}\\ &= e\end{aligned}$$

implies $gxg^{-1} \in \ker\varphi$. It follows that $\ker\varphi$ is a normal subgroup of G.

2. First let us check $\text{im}\,\varphi$ is a subgroup of H. It is nonempty since $\varphi(e) = e$ implies $e \in \text{im}\,\varphi$. Let $\varphi(g_1), \varphi(g_2) \in \text{im}\,\varphi$. Then observe that

$$\varphi(g_1)\varphi(g_2)^{-1} = \varphi(g_1g_2^{-1})$$

implies $\varphi(g_1)\varphi(g_2)^{-1} \in \text{im}\,\varphi$. It follows that $\text{im}\,\varphi$ is a subgroup of H.

Next, we define $\overline{\varphi}\colon G/\ker\varphi \to \text{im}\,\varphi$ by

$$\overline{\varphi}(\overline{g}) = \varphi(g) \tag{5}$$

for all $\overline{g} \in G/\ker\varphi$. We need to check that (5) is well-defined. Let gx be another coset representative of $\overline{g}$ (so $\varphi(x) = e$). Then

$$\begin{aligned}\overline{\varphi}(\overline{gx}) &= \varphi(gx)\\ &= \varphi(g)\varphi(x)\\ &= \varphi(g)e\\ &= \varphi(g)\\ &= \overline{\varphi}(\overline{g}).\end{aligned}$$

Thus (5) is well-defined. Now we show $\overline{\varphi}$ gives us an isomorphism from $G/\ker\varphi$ to $\operatorname{im}\varphi$. It is a group homomorphism since if $g_1, g_2 \in G$, then

$$\begin{aligned}\overline{\varphi}(\overline{g}_1\overline{g}_2) &= \varphi(g_1g_2)\\ &= \varphi(g_1)\varphi(g_2)\\ &= \overline{\varphi}(\overline{g}_1)\overline{\varphi}(\overline{g}_2).\end{aligned}$$

It is also surjective since if $\varphi(g) \in \operatorname{im}\varphi$, then $\overline{\varphi}(\overline{g}) = \varphi(g)$. Finally, it is injective since

$$\begin{aligned}\overline{\varphi}(\overline{g}) = e &\implies \varphi(g) = e\\ &\implies g \in \ker\varphi\\ &\implies \overline{g} = e.\end{aligned}$$

Thus $\overline{\varphi}$ is in fact a group isomorphism. □

.

2.2.2 Second Isomorphism Theorem

Theorem 2.5. *Let G be a group, let H be a subgroup of G, and let N be a normal subgroup of G. Then the following hold:*

1. *The product HN is a subgroup of G.*
2. *The intersection $H \cap N$ is a normal subgroup of H.*
3. *The quotient groups $(HN)/N$ and $H/(H \cap N)$ are isomorphic.*

Proof. 1. First note that HN is nonempty since $e = ee \in HN$. Let $h_1n_1, h_2n_2 \in HN$. Then

$$\begin{aligned}(h_1n_1)(h_2n_2)^{-1} &= h_1n_1n_2^{-1}h_2^{-1}\\ &= h_1(h_2^{-1}h_2)n_1n_2^{-1}h_2^{-1}\\ &= h_1h_2^{-1}(h_2n_1n_2^{-1}h_2^{-1})\\ &\in HN.\end{aligned}$$

It follows that HN is a subgroup of G.

2. Let us check that it is a subgroup of H first. It is nonempty since $e \in H \cap N$. Let $x, y \in H \cap N$. Then $xy^{-1} \in H \cap N$ also since both H and N are groups. Thus $H \cap N$ is a subgroup of H.

Now let us check that $H \cap N$ is a normal subgroup of H. Let $x \in H \cap N$ and let $h \in H$. Then $hxh^{-1} \in N$ since N is normal. Also $hxh^{-1} \in H$ since H is a group. Thus $hxh^{-1} \in H \cap N$. It follows that $H \cap N$ is a normal subgroup of H.

3. We shall define an isomorphism from $H/(H \cap N)$ to $(HN)/N$. To simplify notation in what follows, we denote by $\overline{h}$ to be the coset in $(HN)/N$ represented by $h \in H$ and we denote by $\underline{h}$ to be the coset in $H/(H \cap N)$ represented by $h \in H$. Define a map $\varphi\colon H/(H \cap N) \to (HN)/N$ by

$$\varphi(\underline{h}) = \overline{h} \tag{6}$$

for all cosets $\underline{h} \in H/(H \cap N)$. We need to check that (6) is well-defined (that is, does not depend on the coset representative). Suppose hx is another coset representative of $\underline{h}$ where $x \in H \cap N$. Then clearly hx is another coset representative of $\overline{h}$ since $x \in N$. Thus (6) is well-defined.

It is easy to see that φ is a group homomorphism. It is also surjective since every coset in $(HN)/N$ can be represented by an element in H (since $\overline{hn} = \overline{h}$ for all $h \in H$ and $n \in N$). Finally, let us check that φ is injective. Suppose $\underline{h} \in \ker\varphi$ (so $\overline{h} = \overline{e}$). This implies $h \in N$. Since $h \in H$ already, we see that $h \in H \cap N$. Thus $\underline{h} = \underline{e}$, which implies φ is injective. Thus φ is a group isomorphism, and we are done. □

Remark 12. Here's something to watch out for: It is tempting to define $\psi\colon (HN)/N \to H/(H\cap N)$ by

$$\psi(\overline{h}) = \underline{h} \tag{7}$$

for all cosets $\overline{h} \in HN/N$. While it is true that every coset in $(HN)/N$ can be represented by an $h \in H$, the definition of ψ in (7) does not make it clear what ψ is doing to a general coset representative of $(HN)/N$. One should instead define ψ by

$$\psi(\overline{hn}) = \underline{h} \tag{8}$$

for all cosets $\overline{hn} \in HN/N$. The definition of ψ in (6) makes it clear that we are chopping off the term which lies in N, unlike the definition of ψ in (7). When defining a map out of a quotient group, one should always describe how the map acts on a general coset representative, and then show that this map is well-defined by showing the map acts the same on another general coset representative which represents the same coset. Do not define a map out of a quotient group by describing how the map acts on a special coset representative!

2.2.3 Third Isomorphism Theorem

Theorem 2.6. *(The Third Isomorphism Theorem) Let $(G,\cdot)$ be a group. Let $H, K \trianglelefteq G$ such that $H \leq K$. Then*

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

Proof. Let $\varphi : G/H \to G/K$ be given by mapping $\varphi(aH) = aK$. To be sure this is well defined, suppose $aH = bH$. We want to show $\varphi(aH) = \varphi(bH)$ or $aK = bK$. Since $aH = bH$, then $b = ah$ where $h \in H \subset K$. This implies $b \in aK$, and therefore $bK = aK$. Next we check this is a homomorphism.

$$\begin{aligned}\varphi(aHbH) &= \varphi(abH)\\ &= abK\\ &= aKbK\\ &= \varphi(aH)\varphi(bH)\end{aligned}$$

By the first isomorhpism theorem, $(G/H)/\mathrm{Ker}\varphi \cong \varphi(G/H)$. So

$$\mathrm{Ker}\varphi = \{aH \in G/H \mid aK = K\} = \{aH \in G/H \mid a \in K\} = K/H$$

Also $\varphi(G/H) = G/K$ because for any $aK \in G/K$ we have $aK = \varphi(aH)$. □

Example 2.2. Let $H = 8\mathbb{Z}$, $K = 4\mathbb{Z}$. Then $H \trianglelefteq \mathbb{Z}$, $K \trianglelefteq \mathbb{Z}$ and $8\mathbb{Z} \leq 4\mathbb{Z}$. By the third isomorphism theorem, $(\mathbb{Z}/8\mathbb{Z})/(4\mathbb{Z}/8\mathbb{Z}) \cong \mathbb{Z}/4\mathbb{Z}$.

Proposition 2.1. *Let $(G,\cdot)$ be a group and let $H \trianglelefteq G$.*

1. *If $T \leq G/H$, then $T = A/H$ with $A \leq G$ such that $H \leq A$.*
2. *$A/H \trianglelefteq G/H$ if and only if $A \trianglelefteq G$.*

Proof. (1) : Let $A = \{a \in G \mid aH \in T\}$. We need to check that $A \leq G$ and $H \leq A$ and $A/H = T$. We have $e \in A$ because $eH \in T$. We have closure under multiplication because $a, b \in A$ implies $aH, bH \in T$, and since T is a group, we have $abH = (aH)(bH) \in T$ which implies $ab \in A$. Finally we check for inverses. $a \in A$ implies $aH \in T$. Since T is a group, aH has an inverse, namely $a^{-1}H$. This implies $a^{-1} \in A$. So $A \leq G$. Now if $x \in H$ then $xH = H \in T$, so $x \in A$. Thus $H \subset A$. Finally, we have $A/H = \{aH \mid a \in A\} = T$.

(2) : First assume $A/H \trianglelefteq G/H$. We need to show for all $g \in G$, we have $gAg^{-1} \subset A$. Let $g \in G$ and let $a \in A$. We know $gHaHg^{-1}H = gaHg^{-1}H = gag^{-1}H = a'H$. some $a' \in A$. Therefore $gAg^{-1} \subset A$. Thus $A \trianglelefteq G$. To prove the converse, assume $A \trianglelefteq G$. Then we want to show $gH(A/H)(gH)^{-1} \subset A/H$ for all $g \in G$. So let $g \in G$ and $a \in A$. We know that $gag^{-1} = a'$ for some $a' \in A$. Then $gHaH(gH)^{-1} = gag^{-1}H = a'H$. □

Example 2.3. All the subgroups of $\mathbb{Z}/10\mathbb{Z}$ are of the form $A/10\mathbb{Z}$ with $10\mathbb{Z} \leq A \leq \mathbb{Z}$. So any subgroup of $\mathbb{Z}/10\mathbb{Z}$ is of the form $d\mathbb{Z}/10\mathbb{Z}$ with $d|10$.

2.3 Cauchy's Theorem

Theorem 2.7. *Let G be a finite group and p be a prime factor of $|G|$. Then G contains an element of order p. Equivalently, G contains a subgroup of size p.*

We will use induction on $|G|$. Let $n = |G|$. The base case is $n = p$. In this case, any nonidentity element has order p. Now suppose $n > p$, $p|n$, and the theorem is true for all groups of order less than n and divisible by p.

Case 1: G is abelian. Assume no element of G has order p. If g has order kp for some $k \in \mathbb{N}$, then g^k has order p. Thus, no element has order divisible by p. Let $G = \{g_1, g_2, \ldots, g_n\}$ and let g_i have order m_i, so m_i is not divisible by p. Set m to be the least common multiple of the $m_i's$. Since $g_i^m = e$ for all $1 \leq i \leq n$, there exists a homomorphism of abelian groups $f : (\mathbb{Z}/(m))^n \to G$ given by $f(\overline{a_1}, \ldots, \overline{a_n}) = g_1^{a_1} \cdots g_r^{a_r}$. It is obviously surjective (for example, $f(\overline{1}, \overline{0}, \overline{0} \ldots, \overline{0}) = g_1$, $f(\overline{0}, \overline{1}, \overline{0} \ldots, \overline{0}) = g_2$, etc...), and so there is a short exact sequence given by:

$$1 \longrightarrow \ker f \longrightarrow (\mathbb{Z}/(m))^n \xrightarrow{f} G \longrightarrow 1$$

We deduce from this short exact sequence the equation

$$|\ker f| \cdot |G| = m^n$$

Since p divides $|G|$, it divides m^n too. But m^n is not divisible by p since m is not divisible by p, so we have reached a contradiction.

Case 2: G is nonabelian. If a proper subgroup H of G has order divisible by p, then by induction there is an element of order p in H, which gives us an element of order p in G. Thus we may assume no proper subgroup of G has order divisible by p. We will show $|Z(G)|$ is divisible by p, and hence $Z(G)$ can't be a proper subgroup of G, and the proof reduces to the abelian case. For any proper subgroup H, $|G| = |H| \cdot [G : H]$ and $|H|$ is not divisible by p, so $p|[G : H]$ for every proper subgroup H. Let the conjugacy classes in G with size greater than 1 be represented by $g_1, g_2, \ldots, g_k$. The conjugacy classes of size 1 are the elements in $Z(G)$. Since the conjugacy classes are a partition of G, counting $|G|$ by counting conjugacy classes implies

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

where $Z(g_i)$ is the centralizer of g_i. Since the conjugacy class of each g_i has size greater than 1, $[G : Z(g_i)] > 1$, so $Z(g_i) \neq G$. Therefore $p|[G : Z(g_i)]$. The left side is divisible by p and each index in the sum on the right side is divisible by p, so $|Z(G)|$ is divisible by p. Since proper subgroups of G don't have order divisible by p, $Z(G)$ has to be all of G. That means G is abelian, which is a contradiction.

2.4 Sylow Theorems

Let G be a group such that $|G| = p^k m$ where p is a prime and $k, m \geq 1$. Cauchy's Theorem tells us that there exists a subgroup of G whose order is p. In fact, we can do much better than this. It turns out that there exists a subgroup of G whose order is p^i for all $1 \leq i \leq k$. This is part of the content of what the Sylow Theorems tells us.

2.4.1 p-Sylow Subgroups

Definition 2.1. Let G be a group such that $|G| = p^k m$ where p is a prime and $k, m \geq 1$. Any subgroup of G whose order is p^k is called a p-**Sylow subgroup** of G. A p-Sylow subgroup for some p is called a **Sylow subgroup**.

Example 2.4. In $\mathbb{Z}/(12)$, where $|\mathbb{Z}/(12)| = 12 = 2^2 \cdot 3$, the only 2-Sylow subgroup is $\{0, 3, 6, 9\} = \langle 3 \rangle$. The only 3-Sylow subgroup is $\{0, 4, 8\} = \langle 4 \rangle$.

Example 2.5. In A_4, where $|A_4| = 12 = 2^2 \cdot 3$. The only 2-Sylow subgroup is $V = \langle (12)(34), (14)(23) \rangle$. There are four 3-Sylow subgroups:

$$\langle (123) \rangle \quad \langle (124) \rangle \quad \langle (134) \rangle \quad \langle (234) \rangle$$

A_4 arises as the Galois group of $f(T) = T^4 + 8T + 12 = (T - r_1)(T - r_2)(T - r_3)(T - r_4)$ over $\mathbb{Q}$. Here's how we know this: The discriminant of $f(T)$ is $-3^3 \cdot 8^4 + 4^4 12^3 = 331776$, which is a square, so the Galois group is contained in A_4. Here's how $f(T)$ factors modulo different primes:

$$f(T) \equiv (T + 1)(T^3 + 4T^2 + T + 2) \bmod 5$$
$$f(T) \equiv (T^2 + 4T + 7)(T^2 + 13T + 9) \bmod 17$$

From these factorizations, we know there is an element in the Galois group with cycle type $(1, 3)$ (i.e. a 3-cycle) and an element in the Galois group with cycle type $(2, 2)$. We can also see from these factorizations that $f(T)$ is irreducible over $\mathbb{Q}$ (There's no degree 2 factor mod 5, and there's no degree 1 factor mod 17). Since there exists a 3-cycle, we know the Galois group is divisible by 3. Since we know $f(T)$ has degree 4 and is irreducible over $\mathbb{Q}$, there is a sequence of field extensions

$$\begin{array}{c} L \\ {\scriptstyle n}\big| \\ \mathbb{Q}(r_1) \\ {\scriptstyle 4}\big| \\ \mathbb{Q} \end{array}$$

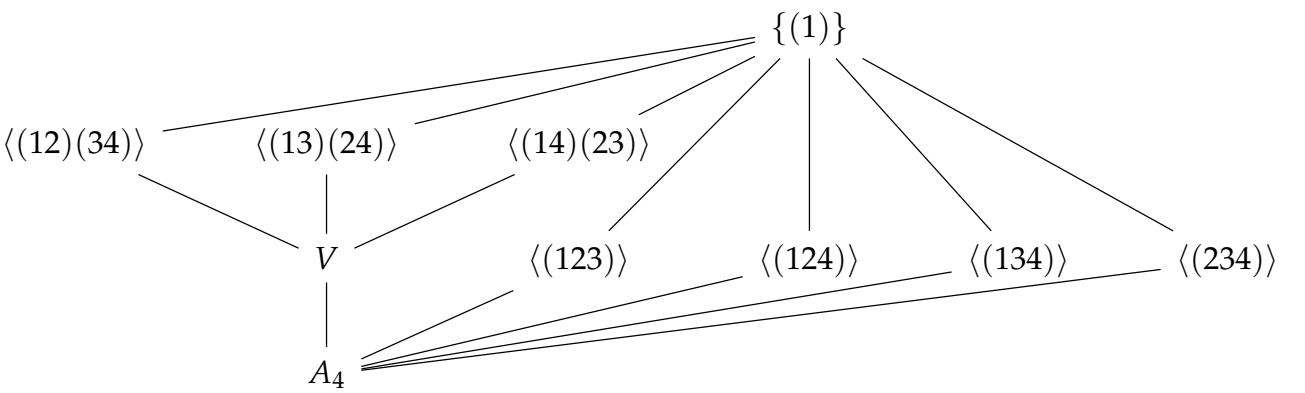
Where L is the splitting field of $f(T)$ and $\mathbb{Q}(r_1)$ has degree 4 Then as a field extension over $\mathbb{Q}$. This information tells us that $|Gal(L/\mathbb{Q})| = [L : \mathbb{Q}] = 4n$. Since the Galois group is divisible by 3 and 4, and is contained in A_4, it must be isomorphic to A_4. Since $|A_4| = 12$, $[L : \mathbb{Q}(r_1)] = 12/4 = 3$. So the set of all automorphisms of L that fix $\mathbb{Q}(r_1)$ must be a subgroup of A_4 which has order 3. This subgroup corresponds to one of the four 3-sylow subgroups, in particular, it is $\langle(234)\rangle$. Of course, I arbitrarly decided to focus on the field $\mathbb{Q}(r_1)$, but I could have easily focused on $\mathbb{Q}(r_2)$ instead. But this is just a relabeling of indices, and relabeling indices is the same as conjugating in S_4, so the corresponding Galois group for $\mathbb{Q}(r_2)$ is given by conjugating $\langle(234)\rangle$ with an element in A_4 that sends 1 to 2, like$(12)(34)$. The cubic resolvent of $f(T)$ is $T^3 - 48T - 64 = (T - (r_1r_2 + r_3r_4))(T - (r_1r_3 + r_2r_4))(T - (r_1r_4 + r_2r_3))$. The cubic resolvent of $f(T)$ is irreducible since it is irreducible mod 5. This means there is a sequence of field extensions

$$\begin{array}{c} L \\ {\scriptstyle n}\big| \\ \mathbb{Q}(r_1r_2 + r_3r_4) \\ {\scriptstyle 4}\big| \\ \mathbb{Q} \end{array}$$

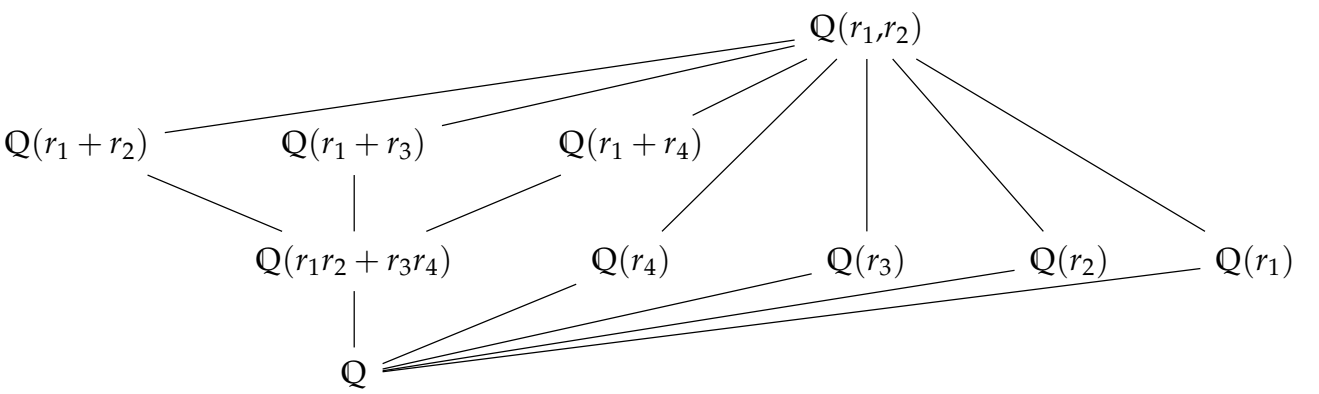
Again, we arbitrarily focused on the field $\mathbb{Q}(r_1r_2 + r_3r_4)$, but notice this time that the subgroup which corresponds to this field extension is normal in A_4, thus we get the nonobvious fact that:

$$\mathbb{Q}(r_1r_2 + r_3r_4) = \mathbb{Q}(r_1r_3 + r_2r_4) = \mathbb{Q}(r_1r_4 + r_2r_3)$$

Below is the lattice of subgroups of A_4:



And here is the corresponding lattice of fields:



Example 2.6. In D_6, where $|D_6| = 12 = 2^2 \cdot 3$, there are three 2-Sylow subgroups:

$$\{1, r^3, s, r^3s\} = \langle r^3, s\rangle, \quad \{1, r^3, rs, r^4s\} = \langle r^3, rs\rangle, \quad \{1, r^3, r^2s, r^5s\} = \langle r^3, r^2s\rangle$$

The only 3-Sylow subgroup in D_6 is $\{1, r^2, r^4\} = \langle r^2\rangle$.

Example 2.7. In $\mathrm{SL}_2(\mathbb{Z}/3)$, where $|\mathrm{SL}_2(\mathbb{Z}/3)| = (3^2-1)(3^2-3)/2 = 2^3 \cdot 3$, there is only one 2-Sylow subgroup, whose elements are listed below:

$$\begin{pmatrix}1&0\\0&1\end{pmatrix} \quad \begin{pmatrix}0&-1\\1&0\end{pmatrix} \quad \begin{pmatrix}1&1\\1&-1\end{pmatrix} \quad \begin{pmatrix}-1&1\\1&1\end{pmatrix}$$

$$\begin{pmatrix}-1&0\\0&-1\end{pmatrix} \quad \begin{pmatrix}0&1\\-1&0\end{pmatrix} \quad \begin{pmatrix}-1&-1\\-1&1\end{pmatrix} \quad \begin{pmatrix}1&-1\\-1&-1\end{pmatrix}$$

Note that this subgroup is isomorphic to Q_8 by labeling the matrices in the first row as $1, i, j, k$. There are four 3-Sylow subgroups:

$$\left\langle \begin{pmatrix}1&1\\0&1\end{pmatrix} \right\rangle \quad \left\langle \begin{pmatrix}1&0\\1&1\end{pmatrix} \right\rangle \quad \left\langle \begin{pmatrix}0&1\\2&2\end{pmatrix} \right\rangle \quad \left\langle \begin{pmatrix}0&2\\1&2\end{pmatrix} \right\rangle$$

2.4.2 Statement and Proof of Sylow Theorems

Before we state and prove the Sylow Theorems, we begin with a very important theorem called the fixed-point congruence.

Theorem 2.8. *Let G be a finite p-group acting on a finite set X. Then*

$$|X| = \sum_{i=1}^{t} |Orb_{x_i}|.$$

Since $|Orb_{x_i}| = [G : Stab_{x_i}]$ and $|G|$ is a power of p, $|Orb_{x_i}| \equiv 0$ mod p unless $Stab_{x_i} = G$, in which case Orb_{x_i} has length 1, i.e. x_i is a fixed point. Thus, when we reduce both sides of the equation above modulo p, all terms on the right side vanish except for a contribution of 1 for each fixed point. That implies

$$|X| \equiv \#\{\text{fixed points}\} \bmod p$$

Now we state the first Sylow theorem.

Theorem 2.9. *(Sylow I). A finite group G has a p-Sylow subgroup for every prime p and any p-subgroup of G lies in a p-Sylow subgroup of G.*

Proof. Let p^k be the highest power of p in $|G|$. We can assume $k \geq 1$, since the result is obvious if $k = 0$, hence $p||G|$. We will prove that there is a subgroup of order p^i for $0 \leq i \leq k$. If $|H| = p^i$ and $i < k$, we will show there is a p-subgroup $H' \supset H$ with $[H' : H] = p$, so $|H'| = p^{i+1}$. Then, starting with H as the trivial subgroup, we can repeat this process with H' in place of H to create a rising tower of subgroups

$$\{e\} = H_0 \subset H_1 \subset H_2 \subset \cdots$$

where $|H_i| = p^i$, and after k steps we reach H_k, which is a p-Sylow subgroup of G. Consider the left multiplication action of H on the left cosets G/H:

$$h \cdot \overline{g} = \overline{hg}$$

This is an action of a finite p-group H on the set G/H, and so by the fixed-point congruence for actions of nontrivial p-groups

$$|G/H| \equiv |\mathrm{Fix}_H(G/H)| \bmod p \tag{9}$$

What does it mean for a coset $\overline{g}$ in G/H to be a fixed point by the group H under left multiplication? For all $h \in H$, we need $hg = gh'$, for some $h' \in H$. This happens if and only if $g \in N(H)$. Thus

$$\mathrm{Fix}_H(G/H) = \{\overline{g} \mid g \in N(H)\} = N(H)/H.$$

So (9) becomes

$$[G : H] \equiv [N(H) : H] \bmod p \tag{10}$$

Because $H \lhd N(H)$, $N(H)/H$ is a group. When $|H| = p^i$ and $i < k$, the index $[G : H]$ is divisible by p, so the congruence 10 implies $[N(H) : H]$ is divisible by p, so $N(H)/H$ is a group with order divisible by p. Thus $N(H)/H$ has a subgroup of order p by Cauchy's theorem. All subgroups of the quotient group $N(H)/H$ have the form H'/H where H' is a subgroup between H and $N(H)$. Therefore a subgroup of order p in $N(H)/H$ is H'/H such that $[H' : H] = p$, so $|H'| = p|H| = p^{i+1}$. □

Theorem 2.10. *(Sylow II). For each prime p, the p-Sylow subgroups of G are conjugate.*

Proof. Pick two p-Sylow subgroups P and Q. We want to show they are conjugate. Consider the action of Q on G/P by left multiplication:

$$q \cdot \overline{g} = \overline{qg}$$

A fixed point $\bar{g}$ under this action means $\overline{qg} = \bar{g}$ for all $q \in Q$. This implies for each $q \in Q$ there is a $p_q \in P$ such that $qg = gp_q$, or in other words, $q = gp_qg^{-1}$. This implies $Q \subset gPg^{-1}$, which further implies $Q = gPg^{-1}$ since Q and gPg^{-1} have the same size. So a fixed point under this action corresponds with an element g which conjugates Q to P. So we just need to show that there exists a fixed point in G/P. Since Q is a finite p-group,

$$|G/P| \equiv |\text{Fix}_Q(G/P)| \bmod p$$

The left side is nonzero modulo p since P is a p-Sylow subgroup: If $|G| = p^k m$ and $|P| = p^k$ then $|G/P| = m$. Thus $|\text{Fix}_Q(G/P)|$ can't be 0, so there is a fixed point in G/P. □

If g conjugates P to Q, then so too does gh, for any $h \in N(P)$:

$$ghPh^{-1}g^{-1} = gPg^{-1} = Q$$

It's natural to wonder if the number of p-Sylow subgroups of G equals $[G : N(P)]$. This is indeed true, but before we tackle that, we prove the third Sylow theorem.

Theorem 2.11. *(Sylow III). For each prime p, let n_p be the number of p-Sylow subgroups of G. Write $|G| = p^k m$, where p doesn't divide m. Then*

$$n_p \equiv 1 \bmod p \qquad \text{and} \qquad n_p | m.$$

Proof. We will prove $n_p \equiv 1 \bmod p$ and then $n_p | m$. To show $n_p \equiv 1 \bmod p$, consider the action of P on the set $Syl_p(G)$ by conjugation

$$P \cdot Q = PQP^{-1}.$$

The size of $Syl_p(G)$ is n_p. Since P is a finite p-group

$$n_p \equiv |\text{Fix}_P(Syl_p(G)| \bmod p$$

Fixed points for P acting by conjugation on $Syl_p(G)$ are $Q \in Syl_p(G)$ such that $gQg^{-1} = Q$ for all $g \in P$. One choice for Q is P. For any such Q, $P \subset N_G(Q)$. Also $Q \subset N_G(Q)$, so P and Q are p-Sylow subgroups in $N_G(Q)$. Applying Sylow II to the group $N_G(Q)$, P and Q are conjugate in $N_G(Q)$. Since $Q \lhd N_G(Q)$, the only subgroup of $N_G(Q)$ conjugate to Q is Q, so $P = Q$. Thus P is the only fixed point when P acts on $Syl_p(G)$, so $n_p \equiv 1 \bmod p$. To show $n_p | m$, consider the action of G by conjugation on $Syl_p(G)$. Since the p-Sylow subgroups are conjugate to each other, there is one orbit. A set on which a group acts with one orbit has size dividing the size of the group, so $n_p || G|$. From $n_p \equiv 1 \bmod p$, the number n_p is relatively prime to p, so $n_p | m$. □

Theorem 2.12. *(Sylow III*). For each prime p, let n_p be the number of p-Sylow subgroups of G. Then $n_p = [G : N_G(P)]$, where P is any p-Sylow subgroup.*

Proof. Let P be a p-Sylow subgroup of G and let G act on $Syl_p(G)$ by conjugation. By the orbit-stabilizer formula,

$$n_p = [G : \text{Stab}_{\{P\}}] = [G : N_G(P)].$$

□

2.5 Sylow Applications

Theorem 2.13. *For a prime p, any element of $GL_2(\mathbb{Z}/(p))$ with order p is conjugate to a strictly upper-triangular matrix $e_{12}(a)$. The number of p-Sylow subgroups is $p + 1$.*

Proof. The size of $GL_2(\mathbb{Z}/(p))$ is $(p^2 - 1)(p^2 - p) = p(p - 1)(p^2 - 1)$. Therefore a p-Sylow subgroup has size p. The matrix $e_{12}(1)$ has order p, so it generates a p-Sylow subgroup $P = \{e_{12}(*)\}$. Since all p-Sylow subgroups are conjugate, any matrix with order p is conjugate to some power $e_{12}(1)$. The number of p-Sylow subgroups is

$$n_p = [GL_2(\mathbb{Z}/(p)) : N(P)]$$

by Sylow III*. For $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ to lie in $N(P)$ means it conjugates $e_{12}(1)$ to some power $e_{12}(*)$. Since

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{\Delta} \begin{pmatrix} 1 - ac & a^2 \\ -c^2 & 1 + ac \end{pmatrix}$$

where $\Delta = ad - bc \neq 0$, $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in N(P)$ precisely when $c = 0$. Therefore $N(P) = \{\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)\}$ in $GL_2(\mathbb{Z}/(p))$. The size of $N(P)$ is $(p-1)^2 p$, thus

$$n_p = [GL_2(\mathbb{Z}/(p)) : N(P)] = p + 1$$

□

Corollary 5. *The number of elements of order p in $GL_2(\mathbb{Z}/(p))$ is $p^2 - 1$.*

Proof. Each p-Sylow subgroup has $p - 1$ elements of order p. Different p-Sylow subgroups intersect trivially, so the number of elements of order p is $(p-1)n_p = p^2 - 1$.

□

Theorem 2.14. *There is a unique p-Sylow subgroup of $Aff(\mathbb{Z}/(p^2))$.*

Proof. $Aff(\mathbb{Z}/(p^2))$ has size $p^2\varphi(p^2) = p^3(p-1)$, so a p-Sylow subgroup has order p^3. Letting n_p be the number of p-Sylow subgroups, Sylow III says $n_p | (p-1)$ and $n_p \equiv 1 \mod p$. Therefore $n_p = 1$.

□

Theorem 2.15. *For any prime p, $Heis(\mathbb{Z}/(p))$ is the unique p-Sylow subgroup of the group of invertible upper-triangular matrices*

$$\begin{pmatrix} d_1 & a & b \\ 0 & d_2 & c \\ 0 & 0 & d_3 \end{pmatrix}$$

in $GL_3(\mathbb{Z}/(3))$.

Proof. This matrix group, call it U, has size $(p-1)^3 p^3$, so $Heis(\mathbb{Z}/(p))$ is a p-Sylow subgroup of U. Sylow III tells us $n_p | (p-1)^3$ and $n_p \equiv 1 \mod p$, but it does not follow from this that n_p must be 1. Let's prove $Heis(\mathbb{Z}/(p)) \lhd U$ by showing it is in the kernel of a map out of U: Project a matrix in U to the 3-fold product $(\mathbb{Z}/(p))^\times \times (\mathbb{Z}/(p))^\times \times (\mathbb{Z}/(p))^\times$.

$$\begin{pmatrix} d_1 & a & b \\ 0 & d_2 & c \\ 0 & 0 & d_3 \end{pmatrix} \mapsto (d_1, d_2, d_3)$$

The kernel of this map is $Heis(\mathbb{Z}/(p))$.

□

2.6 Cayley's Theorem

Theorem 2.16. *(Cayley's Theorem) Let G be a finite group of order n. Then G is isomorphic to a subgroup of S_n.*

Proof. We write S_G for the group of all permutations of G as a set. We have $S_G \cong S_n$, so we just need to show that G is isomorphic to a subgroup of S_G. Define a map $\pi \colon G \to S_G$, denoted $\pi \mapsto \pi_g$, where $\pi_g \colon G \to G$ is given by

$$\pi_g(x) = gx$$

for all $x \in G$. We claim that π is an injective group homomorphism. Indeed, first let us show that it is a group homomorphism. Let $g_1, g_2 \in G$. Then observe that

$$\begin{aligned} \pi_{g_1 g_2}(x) &= g_1 g_2 x \\ &= \pi_{g_1}(g_2 x) \\ &= \pi_{g_1} \pi_{g_2}(x) \end{aligned}$$

for all $x \in G$. It follows that $\pi_{g_1 g_2} = \pi_{g_1} \pi_{g_2}$, and hence π is a group homomorphism. Now let us show that it is injective. Suppose $g \in \ker \pi$. Thus $gx = x$ for all $x \in G$. In particular, $g^2 = g$. Multiplying both sides by g^{-1} implies $g = 1$. Thus $\ker \pi = \{1\}$, which implies π is injective. Finally, by the first isomorphism theorem for groups, we find that $\operatorname{im} \pi$ is a subgroup of S_G, and moreover,

$$\operatorname{im} \pi \cong G / \ker \pi \cong G.$$

It follows that G is isomorphic to a subgroup of S_G which implies G is isomorphic to a subgroup of S_n.

□

2.7 Composition Series and the Hölder program

Definition 2.2. A group G is said to be **simple** if $|G| > 1$ and if its only normal subgroups are $\{e\}$ and G itself.

Example 2.8. Let p be a prime. Then $\mathbb{Z}/p\mathbb{Z}$ is simple. By lagrange's theorem, the order of any subgroup of $\mathbb{Z}/p\mathbb{Z}$ must divide p. So we only have two options for subgroups of $\mathbb{Z}/p\mathbb{Z}$: $\{e\}$ and $\mathbb{Z}/p\mathbb{Z}$.

The Hölder program innitiated the classification all finite simple groups, which was accomplished in the 1980s.

Theorem 2.17. *There are* 18 *families of finite simples groups, and* 26 *sporadic finite simple groups.*

Example 2.9. $\{\mathbb{Z}_p \mid p \text{ prime}\}$ and $\{\mathrm{PSL}_m(\mathbb{F}_p) \mid m \geq 2\}$

Definition 2.3. In a group G a sequence of subgroups

$$1 = H_0 \leq H_1 \leq \cdots \leq H_r = G$$

is called a **composition series** if $H_i \trianglelefteq H_{i+1}$ and H_{i+1}/H_i is simple for all $i \in \{0, \ldots, r-1\}$. The groups H_{i+1}/H_i are called the **composition factors**.

Example 2.10. A composition series for S_3 is

$$1 \trianglelefteq \langle (1,2,3) \rangle \trianglelefteq S_3,$$

with composition factors $\mathbb{Z}_3$ and $\mathbb{Z}_2$.

Example 2.11. A composition series for S_4 is

$$\{(1)\} \trianglelefteq U \trianglelefteq V \trianglelefteq A_4 \trianglelefteq S_4,$$

where $V = \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ and $U = \{(1), (1,2)(3,4)\}$, and three factors being C_2 and one factor being C_3.

Theorem 2.18. *Let G be a finite group. Then G has a composition series*

$$1 = H_0 \leq H_1 \leq \cdots \leq H_r = G,$$

and the composition factors are unique up to isomorphism, i.e. if

$$1 = G_0 \leq G_1 \leq \cdots \leq G_s = G$$

is another composition series of G, then $r = s$ and there exists $\pi \in S_r$ such that $G_{i+1}/G_i \cong H_{\pi(i)+1}/H_{\pi(i)}$.

Proof. We can always construct a normal series of G. Let r be the length of the longest such sequence. We need to check that this is a composition series (i.e. H_{i+1}/H_i is simple for all i). Suppose not: there is a some i such that H_{i+1}/H_i is not simple. Then there exists $N \trianglelefteq H_{i+1}/H_i$ such that $N \neq H_i/H_i$ and $N \neq H_{i+1}/H_i$. But then $N = A/H_i$ with $H_i \trianglelefteq A \trianglelefteq H_{i+1}$. So we have a sequence of subgroups of G

$$1 = H_0 \leq H_1 \leq \cdots \leq H_i \leq A \leq H_{i+1} \cdots \leq H_r = G.$$

which is a contradiction because this has length $r + 1$.

Lemma: Let G be a finite group. If $M \trianglelefteq G$, $N \trianglelefteq G$, with $M \neq N$ and both G/M and G/N are simple groups, then $G/M \cong N/M \cap N$ and $G/N \cong M/M \cap N$. Now we prove the second part of the theorem using induction on $|G|$. If $|G| = 1$ then $G = \{1\}$. Assume the statement is true for all groups of order less than $|G|$. Let $M = G_{s-1}$ and $N = H_{r-1}$. If $M = N$, then use the induction hypothesis to show $r - 1 = s - 1$ $(H_1/H_0, \cdots, H_{r-1}/H_{r-2}) \sim (G_1/G_0, \cdots, G_{s-1}/G_{s-2})$. So assume $M \neq N$, then use the lemma. Let $K = M \cap N$. Consider a composition series for K:

$$1 = K_0 \leq K_1 \leq \cdots \leq K_{t-1} \leq K_t = K$$

Composition series for M

$$1 = G_0 \leq G_1 \leq \cdots \leq G_{s-3} \leq G_{s-2} \leq M$$

$$1 = K_0 \leq K_1 \leq \cdots \leq K_{t-1} \leq K \leq M$$

So $(G_1/G_0, \cdots, G_{s-2}/G_{s-3}, M/G_{s-2}) \sim (K_1/K_0, \cdots, K/K_{t-1}, M/K)$ and

□

Serre

Definition 2.4. Let G be a group.

1. A **filtration** of G is a finite sequence of subgroups $(G_i)_{0\leq i\leq n}$ of G such that

$$G_0 = G \supset G_1 \supset \cdots \supset G_n = 1 \tag{11}$$

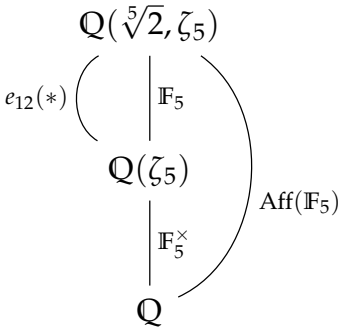
   with G_{i+1} normal in G_i for $0 \leq i \leq n-1$. Given a filtration $(G_i)_{0\leq i\leq n}$, the successive quotients G_i/G_{i+1} are denoted $\mathrm{gr}_i(G)$. The sequence of the $\mathrm{gr}_i(G)$ is denoted by $\mathrm{gr}(G)$.

2. A filtration $(G_i)_{0\leq i\leq n}$ of G is called a **Joran-Hölder filtration** (or a **Joran-Hölder series** or a **composition series**) if $\mathrm{gr}_i(G)$ is simple all $0 \leq i < n$. The number n is called the **length** of the filtration.

Example 2.12. Let F be a field. A filtration for the group $\mathrm{Aff}(F)$ is given by

$$\mathrm{Aff}(F) \trianglerighteq \{e_{12}(*)\} \trianglerighteq \{1\},$$

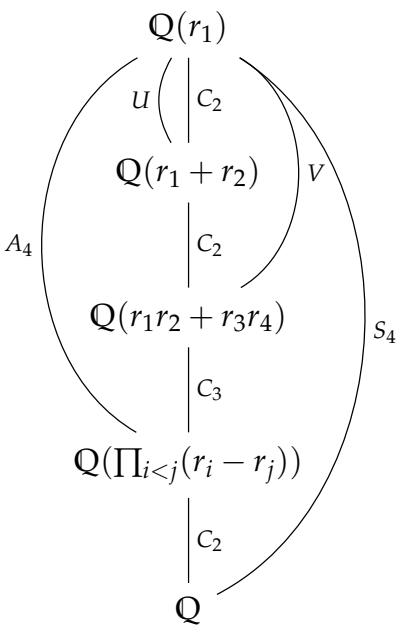
with factors isomorphic to F and $F^\times$. Compare this with the following sequence of field extensions:



Example 2.13. A composition series for S_4 is

$$S_4 \trianglerighteq A_4 \trianglerighteq V \trianglerighteq U \trianglerighteq \{(1)\},$$

where $V = \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ and $U = \{(1), (1,2)(3,4)\}$, with three factors being C_2 and one factor being C_3. Compare this with the following sequence of field extensions:



where r_1, r_2, r_3 and r_4 are roots of the polynomial $f(x) = x^4 - x - 1$.

Example 2.14. A composition series for D_4 is

$$D_4 \trianglerighteq \langle r^2, s\rangle \trianglerighteq \langle s\rangle \trianglerighteq \langle 1\rangle,$$

with all three factors being C_2.

2.7.1 Every Finite Group has a Jordan-Hölder Filtration

A group need not have a Jordan-Hölder filtration. Indeed, consider the group of integers $\mathbb{Z}$. It turns out that however, that finite groups always have Jordan-Hölder filtrations.

Proposition 2.2. *Let G be a finite group. Then there exists a Jordan-Hölder filtration of G.*

Proof. If $G = 1$, take the trivial Jordan-Hölder filtration with $n = 0$ in (11). If G is simple, take $n = 1$ in (11). Suppose G is neither 1 nor simple. Use induction on the order of G. Let N be a normal subgroup of G , distinct from G, and of maximal order. Then G/N is simple. Since $|N| < |G|$, we apply the induction hypothesis to N and we obtain a Jordan-Hölder filtration $(N_i)_{0\leq i\leq n}$ for N. Then $(G_i)_{0\leq i\leq n+1}$ is a Jordan-Hölder filtration for G, where $G_0 = G$ and $G_i = N_{i-1}$ for all $1 \leq i \leq n+1$. □

2.7.2 Uniqueness of $\mathrm{gr}_i(G)$

Theorem 2.19. *(Jordan-Hölder). Let $(G_i)_{0\leq i\leq n}$ be a Jordan-Hölder filtration of a group G. Then the $gr_i(G)$ do not depend on the choice of filtration, up to the permutation of the indices. In particular, the length of the filtration is independent of the filtration.*

Remark 13. The length of the filtration is called the **length** of G, and is denoted $\ell(G)$; when G has no Jordan-Hölder filtration, we write $\ell(G) = \infty$.

Proof. Let S be a simple group, and let $n(G, (G_i), S)$ be the number of j such that G_j/G_{j+1} is isomorphic to S. What we have to prove is that $n(G, (G_i), S)$ does not depend on the chosen filtration (G_i).

Note first that, if H is a subgroup of G, a filtration (G_i) of G incudes a filtration (H_i) of H by putting $H_i = G_i \cap H$. Similarly, if N is a normal subgroup of G, we obtain a filtration of G/N by putting $(G/N)_i = G_i/(G_i \cap N) = G_iN/N$. The exact sequence

$$1 \longrightarrow N \longrightarrow G \longrightarrow G/N \longrightarrow 1$$

gives an exact sequence

$$1 \longrightarrow N_i/N_{i+1} \longrightarrow G_i/G_{i+1} \longrightarrow (G/N)_i/(G/N)_{i+1} \longrightarrow 1$$

i.e.

$$1 \longrightarrow \mathrm{gr}_i(N) \longrightarrow \mathrm{gr}_i(G) \longrightarrow \mathrm{gr}_i(G/N) \longrightarrow 1$$

If (G_i) is a Jordan-Hölder filtration, all the $\mathrm{gr}_i(G)$ are simple; thus, $\mathrm{gr}_i(N)$ is either 1 or $\mathrm{gr}_i(G)$. Let us partition $I = \{1, \ldots, n\}$ into two sets:

$$I_1 = \{i \in I \mid \mathrm{gr}_i(N) = \mathrm{gr}_i(G)\} \quad \text{and} \quad I_2 = \{i \in I \mid \mathrm{gr}_i(N) = 1\}.$$

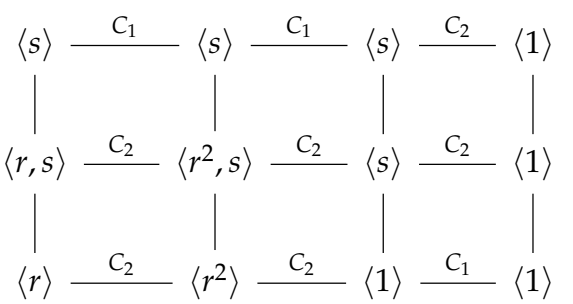
By reindexing I_1 (resp. I_2) we obtain a Jordan-Hölder filtration of N (resp. of G/N) of length $|I_1|$ (resp. of length $|I_2|$); note that $|I_1| + |I_2| = n$.

We now prove the theorem by induction on the length n of the filtration (G_i). If $n = 0$, then $G = 1$, and if $n = 1$, then G is simple and only one filtration is possible. Assume $n \geq 2$. Choose a normal subgroup N of G distinct from 1 and G. The sets I_1 and I_2 defined above are non-empty, hence their number of elements is $< n$, and we can apply the induction hypothesis to N and G/N; it shows that $n(N, (N_i)_{i\in I_1}, S)$ and $n(G/N, ((G/N)_i)_{i\in I_2}, S)$ are independent of the filtrations since

$$n(G, (G)_{ii\in I}, S) = n(N, (N_i)_{i\in I_2}, S) + n(G/N, ((G/N)_i)_{i\in I_2}, S),$$

this implies that $n(G, (G_i)_{i\in I}, S)$ is independent of the choice of filtration, as wanted. □

Example 2.15. Illustration of proof for $D_4 = \langle r, s\rangle$.



3 Group Actions

3.1 Definition of Group Action

Definition 3.1. Let G be a group and let X be a set. An **action of** G **on** X is the choice, for each $g \in G$, of a permutation $\pi_g \colon X \to X$ such that the following two conditions hold:

1. If e is the identity element in G, then $\pi_e(x) = x$ for all $x \in X$.
2. We have $\pi_{g_1} \circ \pi_{g_2} = \pi_{g_1 g_2}$ for all $g_1, g_2 \in G$.

Remark 14. In practice, one dispenses with the notation π_g and writes $\pi_g(x)$ simply as $g(x)$ or $g \cdot x$ or even just gx. This is *not* meant to be an actual multiplication of elements from two possibly different sets G and X. It is just the notation for the effect permutation associated to g on the element x. In this notation, the axioms for a group action take the following form:

1. $ex = x$ for all $x \in X$.
2. $g_1(g_2 x) = (g_1 g_2)x$ for all $g_1, g_2 \in G$ and $x \in X$.

The basic idea in any group action is that the elements of a group are viewed as permutations of a set in such a way that composition of the corresponding permutations matches multilpication in the original group.

3.2 Examples of Group Actions

3.2.1 Permutation Action

Example 3.1. Let S_n act on $X = \{1, 2, \ldots, n\}$ in the usual way. Here $\pi_\sigma(i) = \sigma(i)$ in the usual notation.

Example 3.2. Any group G acts on itself ($X = G$) by left multilpication functions. That is, we set $\pi_g \colon G \to G$ by

$$\pi_g(h) = gh$$

for all $g, h \in G$. Then the conditions for π being a group action are satisfied since e is the identity and multiplication in G is associative.

Example 3.3. The group S_n acts on polynomials $f(T_1, \ldots, T_n)$, by permuting variables:

$$(\sigma \cdot f)(T_1, \ldots, T_n) = f(T_{\sigma(1)}, \ldots, T_{\sigma(n)}).$$

This is a change of variables $T_i \mapsto T_{\sigma(i)}$ in $f(T_1, \ldots, T_n)$. For example, $(12)(23) = (123)$ in S_3 and

$$\begin{aligned}(12) \cdot ((23) \cdot (T_2 + T_3^2)) &= (12) \cdot (T_3 + T_2^2) \\ &= T_3 + T_1^2 \\ &= (123) \cdot (T_2 + T_3^2)\end{aligned}$$

giving the same result both ways. It's also obvious that $(1) \cdot f = f$. To check $\sigma \cdot (\sigma' \cdot f) = (\sigma\sigma') \cdot f$ for all $\sigma, \sigma' \in S_n$, we compute

$$\begin{aligned}(\sigma \cdot (\sigma' \cdot f))(T_1, \ldots, T_n) &= (\sigma \cdot f)(T_{\sigma'(1)}, \ldots, T_{\sigma'(n)}) \\ &= f(T_{\sigma(\sigma'(1))}, \ldots, T_{\sigma(\sigma'(n))}) \\ &= f(T_{(\sigma\sigma')(1)}, \ldots, T_{(\sigma\sigma')(n)}) \\ &= ((\sigma\sigma') \cdot f)(T_1, \ldots, T_n)\end{aligned}$$

Lagranges study of this group action marked the first systematic use of symmetric groups in algebra. Lagrange wanted to understand why nobody had found an analogue of the quadratic formula for roots of a polynomial in degree greater than four.

Example 3.4. Here is a tricky example, so pay atttenion. Let S_n act on $\mathbb{R}^n$ by permuting coordinates: for $\sigma \in S_n$ and $v = (c_1, \ldots, c_n) \in \mathbb{R}^n$, set $\sigma \cdot v = (c_{\sigma(1)}, \ldots, c_{\sigma(n)})$. Is this a group action? No. The reason is because $c_{\sigma(i)}$ is treated as the i'th position, whereas in conrast to the previous example, $T_{\sigma(i)}$ is treated as the $\sigma(i)$'th position.

3.2.2 Conjugation Action

Example 3.5. Let G be a group and let N be a normal subgroup. Then G acts on N by conjugation: let $x \in G$ and $y \in N$. We set

$$x \cdot y = xyx^{-1}. \tag{12}$$

To see that this is in fact an action, first note that (12) lands in N since N is normal in G. Next, let $x_1, x_2 \in G$ and let $y \in N$. Then

$$\begin{aligned} x_1 \cdot (x_2 \cdot y) &= x_1 \cdot (x_2 y x_2^{-1}) \\ &= x_1 (x_2 y x_2^{-1}) x_1^{-1} \\ &= (x_1 x_2) y (x_1 x_2)^{-1} \\ &= (x_1 x_2) \cdot y. \end{aligned}$$

Also if $e \in G$ is the identity, then

$$\begin{aligned} e \cdot y &= eye^{-1} \\ &= y. \end{aligned}$$

It follows that (12) gives an action of G on N.

3.3 Orbit-Stabilizer Theorem

An action of a group G on a set X gives rise to an equivalence relation on X. Namely, for $x, y \in X$ we say $x \sim y$ if there exists $g \in G$ such that $gx = y$. One readily checks that this is indeed an equivalence relation. The equivalence classes are called G**-orbits** (or more simply just **orbits** if G is understood). Let us make the following definitions.

Definition 3.2. Let G be a group and suppose G acts on a set X. For each $x \in X$, we define

1. The **orbit of** x, denoted $\mathrm{Orb}_G(x)$, is the subset of X given by

$$\mathrm{Orb}_G(x) = \{gx \in X \mid g \in G\}$$

2. The **stabilizer of** x, denoted $\mathrm{Stab}_G(x)$, is the subgroup of G given by

$$\mathrm{Stab}_G(x) = \{g \in G \mid gx = x\}.$$

Exercise 3. Verify that $\mathrm{Stab}_G(x)$ is a subgroup of G.

Theorem 3.1. *(Orbit-Stabilizer Theorem) Let G be a group and suppose G acts on a set X. Then for each $x \in X$, we have*

$$|\mathrm{Orb}_G(x)| = [G : \mathrm{Stab}_G(x)].$$

Proof. Define $\varphi \colon G \to \mathrm{Orb}_G(x)$ be given by

$$\varphi(g) = gx$$

for all $g \in G$. The map φ induces a map $\overline{\varphi} \colon G/\mathrm{Stab}_G(x) \to \mathrm{Orb}_G(x)$, given by

$$\overline{\varphi}(\overline{g}) = gx$$

for all $\overline{g} \in \mathrm{Stab}_G(x)$. We claim that $\overline{\varphi}$ is a bijection. Indeed, it is surjective since φ is surjective. To see that it is injective, suppose $\overline{\varphi}(\overline{g}) = \overline{\varphi}(\overline{h})$ for some $\overline{g}, \overline{h} \in G/\mathrm{Stab}_G(x)$. Then $gx = hx$ implies $g^{-1}h \in \mathrm{Stab}_G(x)$. Therefore

$$\begin{aligned} \overline{g} &= \overline{gg^{-1}h} \\ &= \overline{h}. \end{aligned}$$

This implies $\overline{\varphi}$ is injective. □

3.3.1 Stabilizers and Conjugate Subgroups

Proposition 3.1. *Let G be a group and suppose G acts on a set X. Let $g \in G$ and $x \in X$. Then*

$$gStab_G(x)g^{-1} = Stab_G(g(x))$$

Proof. Suppose $h \in \text{Stab}_G(x)$. Then

$$\begin{aligned} ghg^{-1}(g(x)) &= gh(g^{-1}g)(x) \\ &= gh(x) \\ &= g(x). \end{aligned}$$

Therefore $g\text{Stab}_G(x)g^{-1} \subseteq \text{Stab}_G(g(x))$. Converesely, if $h \in \text{Stab}_G(g(x))$, then $h = g(g^{-1}hg)g^{-1}$, where $g^{-1}hg \in \text{Stab}_G(x)$ since

$$\begin{aligned} g^{-1}hg(x) &= g^{-1}h(g(x)) \\ &= g^{-1}(g(x)) \\ &= (g^{-1}g)(x) \\ &= x. \end{aligned}$$

Therefore $g\text{Stab}_G(x)g^{-1} \supseteq \text{Stab}_G(g(x))$. □

3.4 Fixed-Point Congruence

The fixed-point congruence theorem is very useful when dealing with p-groups. To state this theorem, we first need the following definition.

Definition 3.3. Let G be a finite p-group and suppose G acts on a finite set X. We define

$$\text{Fix}_G(X) := \{x \in X \mid g \cdot x = x \text{ for all } g \in G\}.$$

Theorem 3.2. *Let G be a finite p-group and suppose G acts on a finite set X. Then*

$$|X| \equiv \text{Fix}_G(X) \ mod\ p.$$

Proof. After partitioning X into its G-orbit classes. We have

$$|X| = |\text{Fix}_G(X)| + |\text{Orb}_G(x_1)| + \cdots + |\text{Orb}_G(x_n)|. \tag{13}$$

where $x_1, \ldots, x_n$ are representatives whose G-orbit classes have size ≥ 2. By the orbit-stabilizer theorem, we have $\text{Orb}_G(x_i) = [G : \text{Stab}_G(x_i)]$ for all $i = 1, \ldots, n$. Since $x_i \notin \text{Fix}_G(X)$, we must have $\text{Stab}_G(x_i)$ is a *proper* subgroup of G. In particular, this implies p divides $\text{Orb}_G(x_i)$. Thus, we obtain our desired reults after reduce both sides of (13) modulo p. □

Theorem 3.3. *If G acts on X and H is a subgroup of G, then the following are equivalent:*

1. *H acts transtivitely on X*
2. *G acts transitively on X and $G = HStab_x$ for every $x \in X$.*

Proof. If H is transitive, then clearly G is transitive too. For $g \in G$, $gx = hx$ for some $h \in H$, so $h^{-1}g \in \text{Stab}_x$. Thus $g = h\left(h^{-1}g\right) \in H\text{Stab}_x$, so $G = H\text{Stab}_x$. Conversely, given $x, y \in X$, choose $g \in G$ such that $gx = y$. Write $g = hs$, where $h \in H$ and $s \in \text{Stab}_x$. Then $hx = y$, so H acts transitively on X.

□

If G is a group that acts on A then the action defines an equivalence relation on A: $a \sim b$ if there exists $g \in G$ such that $ga = b$. The equivalence class of $a \in A$ is $C_a = \{ga \mid g \in G\}$. We say C_a is the **orbit** of G containing a. Recall $|C_a| = |G : G_a|$ where $G_a = \{g \in G \mid ga = a\}$.

Definition 3.4. The action of G on A is **transitive** if there is exactly one orbit, i.e. $C_a = A$ for any $a \in A$.

Example 3.6. Let $n \geq 2$. S_n acts transitively on $A = \{1, 2, \ldots, n\}$ by $\sigma \cdot i = \sigma(i)$ for all $\sigma \in S_n$ and for all $i \in \{1, 2, \ldots, n\}$.

Example 3.7. Let G be a group and let A be a nonempty set. Consider the trivial action of G on A : $ga = a$ for all $g \in G$ and for all $a \in A$. This action is transitive if and only if A has exactly one element since $C_a = \{a\}$ for all $a \in A$.

3.5 Groups Acting by Left Multiplication

Let G be a group with identity 1. Recall that G acts on itself by left multiplication by $g \cdot h = gh$ for all $g, h \in G$. The associated permutation representation $\varphi : G \to S_G$ given by $\varphi(g) = \sigma_g$ where $\sigma_g : G \to G$ given by $\sigma_g(a) = ga$ for all $a \in G$. So $\text{Ker}\varphi = \{g \in G \mid \sigma_g = 1_g\} = \{g \in G \mid ga = a, \forall a \in G\} = \{1\}$.

Theorem 3.4. *(Cayley) Every group is isomorphic to a subgroup of a group of permutations.*

Proof. G acts on G by left multiplication. This gives a homomorphism $\varphi : G \to S_G$ with $\text{Ker}\varphi = \{1\}$. By the first isomorphism theorem, $G \cong G/\text{Ker}\varphi \cong \varphi(G) \leq S_G$. □

Proposition 3.2. *Let G be a group, let $H \leq G$, and let $A = \{aH \mid a \in G\}$. Then*

1. *G acts transitively on A by left multiplication: $g \cdot aH = gaH$ for all $g \in G$, $aH \in A$.*
2. *$Ker = \bigcap_{x \in G} xHx^{-1}$ and $Ker \leq H$.*

Proof. (1) : We have

$$\begin{aligned} g_1 \cdot (g_2 \cdot aH) &= g_1 \cdot (g_2 a)H) \\ &= g_1(g_2 a)H \\ &= (g_1 g_2)aH \\ &= g_1 g_2 \cdot aH \end{aligned}$$

for all $g_1, g_2 \in G$ and $aH \in A$. We also have $1 \cdot aH = aH$ for all $aH \in A$. Therefore this is a group action. Now we check that the action is transitive. Let aH and bH be two elements in A. Then $ba^{-1} \cdot aH = bH$. Therefore this action is transitive.

(2) : By definition, $\text{Ker} = \{g \in G \mid g \cdot xH = xH, \forall x \in G\}$. This means $g = xh_x x^{-1}$ for all $x \in G$ where $h_x \in H$. □

Proposition 3.3. *Let G be a group of finite order. If p is the smallest prime dividing $|G|$, then any subgroup of index p is normal.*

Proof. Let $H \leq G$ such that $[G : H] = p$ and let $A = \{aH \mid a \in G\}$. Then $|A| = p$. We've just shown G acts on A. Let $\pi : G \to S_A$ be the permutation representation and let $K = \text{Ker}\pi$. We know that K is a normal subgroup of G and that $K \leq H$. We show that $K = H$. By the first isomorphism theorem, $G/K \cong \pi(G) \leq S_A$. So $|\pi(G)|$ divides $|S_A| = p!$, and $|\pi(G)| = [G : K]$. Since $K \leq H \leq G$ we have $[G : K] = [G : H][H : K] = p[H : K]$. Suppose $[H : K] > 1$. Then $[H : K]$ divides $(p-1)!$, and this implies any prime dividing $[H : K] < p$. But $[H : K]$ divides $|H|$ which implies $[H : K]$ divides $|G|$. By hypothesis, any prime dividing $[H : K]$ is greater than or equal to p. Contradiction. So $[H : K] = 1$. Then $H = K = \text{Ker}\pi \trianglelefteq G$. □

3.6 Groups Acting on Themselves by Conjugation and the Class Equation

Let G act on itself by conjugation, i.e. $g \cdot a = gag^{-1}$ for all $g, a \in G$. The equivalence relation induced on G is: $a \sim b$ if there exists $g \in G$ such that $b = gag^{-1}$. In this case, a and b are **conjugate**. The orbit containing $a \in G$ is $C_a = \{gag^{-1} \mid g \in G\}$ and the stabilizer of a is $G_a = \{g \in G \mid gag^{-1} = a\} = C_G(a)$. So $|C_a| = [G : C_G(a)]$.

Lemma 3.5. *$C_a = \{a\}$ if and only if $a \in Z(G)$.*

Proof. $C_a = \{a\}$ if and only if $gag^{-1} = a$ for all $g \in G$. This implies $a \in Z(G)$. Conversely, if $a \in Z(G)$, then $gag^{-1} = a$ for all $g \in G$. This implies $C_a = \{a\}$. □

Theorem 3.6. *(The Class Equation) Let G be a group. Let $g_1, \ldots, g_k$ be representatives of all distinct conjugacy classes not contained in $Z(G)$. Then*

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

Proof. Let $Z(G) = \{1 = z_1, z_2, \ldots, z_\ell\}$. By the lemma, $C_{z_\ell} = \{z_\ell\}$. The distinct conjugacy classes of G are

$$C_{z_1}, \ldots, C_{z_\ell}, C_{g_1}, \ldots, C_{g_k}.$$

Then

$$G = C_{z_1} \cup \cdots \cup C_{z_\ell} \cup C_{g_1} \cup \cdots \cup C_{g_k}$$

is a disjoint union of these conjugacy classes. So

$$\begin{aligned}|G| &= |C_{z_1}| \cup \cdots \cup |C_{z_\ell}| \cup |C_{g_1}| \cup \cdots \cup |C_{g_k}| \\ &= |Z(G)| + \sum_{i=1}^{k} [G : C_G(g_i)].\end{aligned}$$

□

Example 3.8. In S_3, the class equation says

$$\begin{aligned}|S_3| &= |Z(S_3)| + [S_3 : C_{S_3}((1,2))] + [S_3 : C_{S_3}((1,2,3))] \\ &= 1 + 3 + 2\end{aligned}$$

Theorem 3.7. *Let p be a prime and let G be a p-group. Then $Z(G) \neq \{1\}$.*

Proof. Let $g_1, \ldots, g_k$ be representatives of all distinct conjugacy classes which are not contained in $Z(G)$. Then

$$|G| = |Z(G)| + \sum_{i=1}^{k} [G : C_G(g_i)]. \tag{14}$$

First note that $C_G(g_i)$ is a proper subgroup of G since $g_i \notin Z(G)$ for each $i = 1, \ldots, k$. Therefore, reducing both sides of (14) mod p, we see that $|Z(G)| \equiv 0 \bmod p$, which implies the theorem. □

Corollary 6. *Any group G of order p^2 is abelian.*

Proof. By the previous theorem, we have $|Z(G)| \in \{p, p^2\}$. If $|Z(G)| = p^2$, then G is abelian. If $|Z(G)| = p$, then $|G/Z(G)| = p$, which implies $G/Z(G)$ is cyclic. This implies G is abelian. □

Proposition 3.4. *Let G be a group. If $H \trianglelefteq G$ and if K is a conjugacy class of G, then either $H \cap K = \emptyset$ or $K \subseteq H$.*

Proof. If $H \cap K = \emptyset$ we're done. If $H \cap K \neq \emptyset$ then there exists an a in $H \cap K$. This implies $K = C_a = \{gag^{-1} \mid g \in G\} \subseteq H$ since H is normal in G. □

Corollary 7. *If $H \trianglelefteq G$ then H is a union of conjugacy classes ($H = \cup_{a \in H} C_a$).*

Example 3.9. We list all conjugacy classes and their sizes in S_4 in the table below

Representative	Size
(1)	1
$(1,2)$	6
$(1,2,3)$	8
$(1,2)(3,4)$	3
$(1,2,3,4)$	6

Suppose $H \trianglelefteq S_4$. By Lagrange's Theorem, $|H|$ divides $|S_4| = 2^3 \cdot 3$. Therefore $|H| = \{1, 2, 3, 4, 6, 8, 12, 24\}$. Since $H \trianglelefteq S_4$, it must be a union of conjugacy classes. This implies $|H| = 1 + \ell_1 + \cdots + \ell_k$ with $\ell_i \in \{6, 8, 3, 6\}$. From this we see that $|H| \in \{1, 4, 12, 24\}$. Clearly there are normal subgroups of S_4 with orders $1, 12$, and 24, namely the trivial group, A_4, and S_4. There is also a normal subgroup of S_4 with size 4: $V = \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$.

Example 3.10. We list all conjugacy classes and their sizes in A_5 in the table below

Representative	Size
(1)	1
$(1,2,3)$	20
$(1,2,3,4,5)$	12
$(2,1,3,4,5)$	12
$(1,2)(3,4)$	15

Suppose $H \trianglelefteq S_4$. By Lagrange's Theorem, $|H|$ divides $|S_4| = 2^3 \cdot 3$. Therefore $|H| = \{1, 2, 3, 4, 6, 8, 12, 24\}$. Since $H \trianglelefteq S_4$, it must be a union of conjugacy classes. This implies $|H| = 1 + \ell_1 + \cdots + \ell_k$ with $\ell_i \in \{6, 8, 3, 6\}$. From this we see that $|H| \in \{1, 4, 12, 24\}$. Clearly there are normal subgroups of S_4 with orders $1, 12$, and 24, namely the trivial group, A_4, and S_4. There is also a normal subgroup of S_4 with size 4: $V = \{(1), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$.

Sylow's Theorem

In this section, let p be a prime and let G be a group of order $p^\alpha m$ where $\alpha \geq 0$ and $p \not| m$.

Definition 3.5. Let p be a prime. A p-**group** is a group of order p^m for some $m \geq 0$. A **Sylow** p-**subgroup** of G is a subgroup P of G with $|P| = p^\alpha$. We use the notation $\text{Syl}_p(G) = \{P \leq G \mid |P| = p^\alpha\}$ to denote the set of all Sylow p-subgroups of G and we also use the notation $n_p = |\text{Syl}_p(G)|$ to denote the number of Sylow p-subgroups of G.

Theorem 3.8. *Let p be a prime and let G be a group of order $p^\alpha m$ where $\alpha \geq 0$ and $p \not| m$. Then*

1. *$Syl_p(G) \neq \emptyset$.*
2. *If Q is a p-subgroup of G and if $P \in Syl_p(G)$, then $Q \leq gPg^{-1}$ for some $g \in G$.*
3. *For all $P \in Syl_p(G)$, we have $n_p \equiv 1$ mod p, $n_p \mid m$, and $n_p = [G : N_G(P)]$.*

Corollary 8. *The following are equivalent.*

1. *$n_p = 1$.*
2. *P is a characteristic subgroup of G.*
3. *$P \trianglelefteq G$.*

Example 3.11. We show that any group of order 15 is cyclic. Let G be a group of order 15. We have $n_5 \mid 3$ and $n_5 \equiv 1$ mod 5, thus $n_5 = 1$. Similarly $n_3 = 1$. This implies $\text{Syl}_3(G) = \{P\}$ where $|P| = 3$. Thus, $P = \langle x \rangle$ where $\text{ord}(x) = 3$. Similarly $\text{Syl}_5(G) = \{Q\}$ and $Q = \langle y \rangle$ where $\text{ord}(y) = 5$. Since P and Q are normal subgroups of G and $P \cap Q = \{e\}$, we have $xy = y^k x$ and $xy = yx^\ell$ for some k and ℓ. So $y^k x = yx^\ell$ or $y^{k-1}x^{1-\ell} = 1$, which implies $k = \ell = 1$. So x commutes with y and this implies $\text{ord}(xy) = \text{ord}(x)\text{ord}(y) = 15$.

Lemma 3.9. *If Q is a p-subgroup of G and if $P \in Syl_p(G)$, then $Q \cap N_G(P) = Q \cap P$.*

Example 3.12. We show that any group of order 105 is not simple. Let G be a group such that $|G| = 105 = 3 \cdot 5 \cdot 7$. Suppose G is simple. Then $n_3, n_5, n_7 > 1$. Since $n_p \mid m$, we have $n_3 \in \{1, 5, 7, 35\}$, $n_5 \in \{1, 3, 7, 21\}$, and $n_7 \in \{1, 3, 5, 15\}$. Since $n_p \equiv 1$ mod p, we have $n_3 \in \{1, 7\}$, $n_5 \in \{1, 21\}$, and $n_7 \in \{1, 15\}$. Since $n_p > 1$, we have $n_3 = 7$, $n_5 = 21$, and $n_7 = 15$. This is a contradiction though because this would imply there are $2 \cdot 7$ elements of order 3, $4 \cdot 21$ elements of order 5, $6 \cdot 15$ elements of order 7, and $2 \cdot 7 + 4 \cdot 21 + 6 \cdot 15 = 188 > 105$.

Example 3.13. Let G be a group of order $30 = 2 \cdot 3 \cdot 5$. We show that G has a normal subgroup of order 15. Since $n_p \mid m$ and $n_p \equiv 1$ mod p, we have $n_2 \in \{1, 3, 5, 15\}$, $n_3 \in \{1, 10\}$, $n_5 \in \{1, 6\}$. We want to show that one of n_3, n_5 has to be 1. If $n_3, n_5 > 1$, then $n_3 = 10$ and $n_5 = 6$. This is a contradiction though since $2 \cdot 10 + 4 \cdot 6 = 44 > 30$. So either n_3 or n_5 is equal to 1. Assume $n_3 = 1$. Let P be the 3-Sylow Subgroup and let Q be a 5-Sylow Subgroup. Then since P is normal, PQ is a subgroup of G. Since $|P \cap Q| = 1$, $|PQ| = |P| \cdot |Q|$. So PQ is a group of order 15, hence it is cyclic. So $\text{Syl}_5(PQ) = \{Q\}$ and Q is a characteristic subgroup of PQ, and $PQ \trianglelefteq G$ because $[G : PQ] = 2$, so $Q \trianglelefteq G$. The same idea works when $n_5 = 1$.

Sylows's Theorem Applications

Recall, if $|G| = 15$ then G is cyclic. In particular, $n_5 = 1$. If $|G| = 30$, then $n_3 = n_5 = 1$.

Example 3.14. If G is a group of order 6 then $n_3 = 1$.

Example 3.15. If G is a group of order 20 then $n_5 = 1$.

Proposition 3.5. *Any group of order* 12 *has either $n_2 = 1$ or $n_3 = 1$.*

Proof. Let G be a group of order $12 = 3 \cdot 2^2$. If $n_3 = 1$ then we are done. So assume $n_3 > 1$. Then by Sylow's Theorems, $n_3 = 4$. So $\text{Syl}_3(G) = \{P_1, P_2, P_3, P_4\}$ with $|P_i| = 3$. Each P_i is cyclic of order 3 and $P_i \cap P_j = \{e\}$ for $i \neq j$, so there are 8 elements of order 3 in G. Now G acts on $\text{Syl}_3(G)$ by conjugation: $g \cdot P_i = gP_ig^{-1}$. This gives a homomorphism $\varphi : G \to S_4$ with

$$\text{Ker}\varphi = \{g \in G \mid gP_ig^{-1} = P_i, \quad 1 \leq i \leq 4\} = \bigcap_{i=1,2,3,4} \text{N}_G(P_i).$$

Since

$$\begin{aligned} 4 &= n_3 \\ &= [G : \mathrm{N}_G(P_i)] \\ &= \frac{|G|}{\mathrm{N}_G(P_i)} \\ &= \frac{12}{\mathrm{N}_G(P_i)}. \end{aligned}$$

$\mathrm{N}_G(P_i) = 3$. So $P_i \leq \mathrm{N}_G(P_i)$ and $|P_i| = |\mathrm{N}_G(P_i)|$ implies $P_i = \mathrm{N}_G(P_i)$. So

$$\mathrm{Ker}\varphi == \bigcap_{i=1,2,3,4} P_i = \{e\}.$$

Then $G \cong \varphi(G) \leq S_4$. Since G has 8 elements of order 3, $\varphi(G)$ also has 8 elements of order 3. So $|\varphi(G) \cap A_4| \geq 8$ and $\varphi(G) \cap A_4 \leq \varphi(G)$ implies $|\varphi(G) \cap A_4| = 12 = \varphi(G)$. So if $n_3 = 4$, then $\varphi(G) \cong A_4$ and $n_2(A_4) = 1$. □

Proposition 3.6. *If G is a group of order 60 and $n_5 > 1$, then G is simple.*

Proof. To obtain a contradiction, suppose G is a group of order $60 = 2^2 \cdot 3 \cdot 5$ such that G is not simple. By Sylow's Theorems, we have $n_5 \in \{1, 6\}$. Since G is not simple, we must have $n_5 = 6$. So $\mathrm{Syl}_6(G) = \{P_1, P_2, P_3, P_4, P_5, P_6\}$ with $|P_i| = 5$. Each P_i is cyclic of order 5 and $P_i \cap P_j = \{e\}$ for $i \neq j$, so there are 24 elements of order 5 in G. Since G is not simple, there exists $H \trianglelefteq G$ such that $H \neq 1, G$. Now

$$|H| \mid 60 \implies |H| \in \{2, 3, 4, 5, 6, 10, 12, 15, 20, 30\}.$$

If $5 \mid |H|$, then H contains a subgroup of order 5. Thus there is some P_i such that $P_i \leq H$. For any other $P_j \in \mathrm{Syl}_5(G)$, we have $P_j = gP_ig^{-1}$ for some $g \in G$. So $P_j = gP_ig^{-1} \leq gHg^{-1} = H$. So H contains all the Sylow 5-subgroups of G. Thus $|H| \geq 1 + 24 = 25$, this implies $|H| = 30$. But if $|H| = 30$, then $n_5(H) = 1$, which is a contradiction. So

$$|H| \in \{2, 3, 4, 6, 12\}.$$

If $|H| \in \{6, 12\}$, then there exists K char H with $K \in \mathrm{Syl}_3(H)$ or $K \in \mathrm{Syl}_2(H)$. Since K is characteristic in H and H is normal in G, K is normal in G. So there is a normal subgroup K of G with $|K| \in \{2, 3, 4\}$. So it suffices to assume

$$|H| \in \{2, 3, 4\}$$

leads to a contradiction. Then $|G/H| \in \{30, 20, 15\}$. Now $n_5(G/H) = 1$ implies there exists $H \trianglelefteq T \trianglelefteq G$ such that $T/H \trianglelefteq G/H$ with $|T/H| = 5$. So there exists $T \trianglelefteq G$ such that $|T|/|H| = 5$ implies $|T| = 5 \cdot |H|$. But this leads to the first case where $5 \mid |T|$ and T is normal. This leads to a contradiction.

□

Corollary 9. *A_5 is simple in S_5.*

Proof. We have $|A_5| = 60$ and $n_5 > 1$ since $\langle (1, 2, 3, 4, 5) \rangle \neq \langle (2, 1, 3, 4, 5) \rangle$. □

Proposition 3.7. *If G is a simple group of order 60 then $G \cong A_5$.*

Theorem 3.10. *A_n is a simple group for all $n \geq 5$.*

Example 3.16. Let G be a group of order $231 = 3 \cdot 7 \cdot 11$. We will show $Z(G)$ contains a Sylow 11-sybgroup and $n_7 = 1$. From the Sylow theorems, we obtain $n_{11} = 1$ and $n_7 = 1$. Let P be the Sylow 11 -subgroup of G. Consider the action of G on P by conjugation $\varphi : G \to \mathrm{Aut}(P)$, $\varphi(g) = \sigma_g$ where $\sigma_g(x) = gxg^{-1}$ for $x \in P$. The kernel of φ is $C_G(P)$. By the Isomorphism theorems, we have $G/C_G(P) \cong \varphi(G) \leq \mathrm{Aut}(P)$. Since $|\mathrm{Aut}(P)| = 10$, we must have $|G/C_G(P)| \mid 10$. The only possibility is when $|G/C_G(P)| = 1$, so $C_G(P) = G$. That is, P is contained in $Z(G)$.

Example 3.17. Let G be a group of order $105 = 3 \cdot 5 \cdot 7$ and suppose $n_3 = 1$. We will show G is abelian. Let P be the Sylow 3-subgroup and consider the action of G on P by conjugation. Again, we find that $|G/C_G(P)|$ divides $|\mathrm{Aut}(P)| = 2$. The only possibility is $|G/C_G(P)| = 1$, so $G = C_G(P)$.

Direct Products of Abelian Groups

Proposition 3.8. *Let $G_1, G_2, \ldots, G_n$ be groups and let $G = \{(a_1, \ldots, a_n) \mid a_i \in G_i,\ 1 \leq i \leq n\}$. Then G is a group with multiplication defined by*

$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n).$$

Proof. The multiplicaiton operation is clearly an associative binary operation. We also have an identity element $(e_1, \ldots, e_n)$ where e_i is the identity element in G_i. And the inverse of an element $(a_1, \ldots, a_n) \in G$ is $(a_1^{-1}, \ldots, a_n^{-1})$. □

Definition 3.6. A group G is **finitely generated** if $G = \langle A \rangle$ for some $\emptyset \neq A \subset G$ such that $|A| < \infty$.

The Fundamental Theorem of Finitely Generated Abelian Groups

Let G be a finitely generated abelian group. Then

1. $G \cong \mathbb{Z}^r \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \cdots \times \mathbb{Z}_{n_k}$ for $r \geq 0$, $n_i \geq 2$ such that $n_{i+1} \mid n_i$ for all $1 \leq i \leq k-1$. We say n_i are the **invariant factors** of G and r is the **Betti number** of G.

2. The decomposition in (1) is unique i.e. if $G \cong \mathbb{Z}^\ell \times \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \cdots \times \mathbb{Z}_{m_t}$ with $\ell \geq 0$, $m_j \geq 2$ such that $m_{j+1} \mid m_j$ for all $1 \leq j \leq t-1$, then $r = \ell$, $k = t$, and $n_i = m_i$ for all $1 \leq i \leq k$.

Remark 15. If $|G| < \infty$ then $r = 0$. So $G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$ with $n_i \geq 2$ and such that $n_{i+1} \mid n_i$ for all $1 \leq i \leq k-1$. In this case, $|G| = n_1 n_2 \cdots n_k$.

Remark 16. If G is a finite abelian group, then every prime divisor of $|G|$ must divide n_1. This is because $p \mid n_1 n_2 \cdots n_k$ implies $p \mid n_i \mid n_{i-1} \mid \cdots \mid n_2 \mid n_1$.

Example 3.18. We find (up to isomorphism) all abelian groups of order 180. Let G be a group of order $180 = 2^2 \cdot 3^2 \cdot 5$. Then $G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$ with $n_i \geq 2$ and such that $n_{i+1} \mid n_i$ for all $1 \leq i \leq k-1$. So we have by the second remark, $2, 3, 5 \mid n_1$ implies n_1 equals $2 \cdot 3 \cdot 5$, or $2^2 \cdot 3 \cdot 5$, or $2 \cdot 3^2 \cdot 5$, or $2^2 \cdot 3^2 \cdot 5$.

In the case $n_1 = 2 \cdot 3 \cdot 5$,

$$n_2 \mid n_1 \qquad \text{and} \qquad n_1 n_2 \mid 2^2 \cdot 3^2 \cdot 5 \qquad \Longrightarrow \qquad n_2 \in \{2, 3, 2 \cdot 3\}.$$

Suppose $n_2 = 2$. Then $n_1 n_2 = 2^2 \cdot 3 \cdot 5 < |G|$. So $n_3 \mid n_2$ and $n_1 n_2 n_3 \mid 180$ implies $n_3 = 3$ which is a contradiction. So $n_2 \neq 2$. Again we get a contradiction if we assume $n_2 = 3$. So for $n_1 = 2 \cdot 3 \cdot 5$, the only possibility is for $n_2 = 2 \cdot 3$. Then $n_1 n_2 = 2^2 \cdot 3^2 \cdot 5$ and $n_3 = 1$. So $G \cong \mathbb{Z}_{30} \times \mathbb{Z}_6$.

In the case $n_2 = 2^2 \cdot 3 \cdot 5$,

$$n_2 \mid n_1 \qquad \text{and} \qquad n_1 n_2 \mid 2^2 \cdot 3^2 \cdot 5 \qquad \Longrightarrow \qquad n_2 = 3.$$

So $G \cong \mathbb{Z}_{60} \times \mathbb{Z}_3$.

In the case $n_1 = 2 \cdot 3^2 \cdot 5$,

$$n_2 \mid n_1 \qquad \text{and} \qquad n_1 n_2 \mid 2^2 \cdot 3^2 \cdot 5 \qquad \Longrightarrow \qquad n_2 = 2.$$

So $G \cong \mathbb{Z}_{90} \times \mathbb{Z}_2$.

The last case to consider is $n_1 = 180$. In this case, $G \cong \mathbb{Z}_{180}$.

Theorem 3.11. *Let G be a finite abelian group of order n. Write the prime factorization of n as $n = p_1^{e_1} \cdots p_k^{e_k}$. Then*

1. *$G \cong A_1 \times A_2 \times \cdots \times A_k$ with $|A_i| = p_i^{e_i}$ for all $1 \leq i \leq k$.*

2. *If $A \in \{A_1, \ldots, A_k\}$ and $|A| = p^e$, then $A \cong \mathbb{Z}_{p^{f_1}} \times \cdots \times \mathbb{Z}_{p^{f_\ell}}$ where $f_1 \geq f_2 \geq \cdots \geq f_\ell \geq 1$. The $p_i^{f_i}$ are called the **elementary divisors** of G.*

3. *The decomposition of G is unique.*

Example 3.19. We find all abelian groups (up to isomorphism) of order 8.

Partitions of 3	Abelian Groups of order 2^3
3	$\mathbb{Z}_{2^3}$
$2+1$	$\mathbb{Z}_{2^2} \times \mathbb{Z}_2$
$1+1+1$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

Theorem 3.12. *Let $m, k \in \mathbb{Z}$. Then $\mathbb{Z}_m \times \mathbb{Z}_k \cong \mathbb{Z}_{mk}$ if and only if $gcd(m,k) = 1$.*

We list all abelian groups of order 180 in the table below

Abelian Groups of Order 180	Isomorphic Group
$\mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$	$\mathbb{Z}_{36} \times \mathbb{Z}_5$
$\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$	$\mathbb{Z}_{60} \times \mathbb{Z}_3$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$	$\mathbb{Z}_{90} \times \mathbb{Z}_2$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$	$\mathbb{Z}_{180}$

3.7 Class Equation of a Group Action

Suppose G is a group and X is a finite set. Suppose we are given a group action of G on X. Let X_0 denote the set of those points in S that are fixed under the action of all elements of G. Let $O_1, O_2, \ldots, O_r$ be the orbits of size greater than one under this action. For each orbit O_i, let x_i be an element of O_i and let G_i denote the stabilizer of x_i in G. The class equation for this action is given as follows:

$$|X| = |X_0| + \sum_{i=1}^{r} [G : G_i]$$

This follows from Orbit-Stabilizer.

4 Group Cohomology

4.1 Basic Terminology

Throughout this subsection, let G be a group.

4.1.1 Group Rings

Definition 4.1. The **group ring** $\mathbb{Z}[G]$ corresponding to G is defined as follows: the underlying set of $\mathbb{Z}[G]$ is given by

$$\mathbb{Z}[G] = \left\{ \sum_{g \in G} n_g g \mid n_g \in \mathbb{Z} \text{ and } n_g = 0 \text{ for all but finitely many } g \in G \right\}.$$

Addition in $\mathbb{Z}[G]$ is given by

$$\sum_{g \in G} m_g g + \sum_{g \in G} n_g g = \sum_{g \in G} (m_g + n_g) g$$

and multiplication in $\mathbb{Z}[G]$ is given by

$$\left(\sum_{g \in G} m_g g \right) \left(\sum_{g \in G} n_g g \right) = \sum_{g \in G} \left(\sum_{h \in G} m_h n_{h^{-1}g} \right) g$$

for all $\sum_{g \in G} m_g g$ and $\sum_{g \in G} n_g g$ in $\mathbb{Z}[G]$. To simplify notation, whenever we write $\sum_{g \in G} n_g g$, it will be understood that this is an element in $\mathbb{Z}[G]$. It is straightforward to check that addition and multiplication defined above gives $\mathbb{Z}[G]$ the structure of a ring, with e being the unit (where e is the usual identity element in G).

4.1.2 G-Modules

Definition 4.2. A **G-module** A is just a $\mathbb{Z}[G]$-module in the usual sense. In particular, A is abelian group (written additively) on which $\mathbb{Z}[G]$ acts by additive maps, so

$$\begin{aligned} (gh)a &= g(ha) \\ ea &= a \\ g(a+b) &= ga + gb \end{aligned}$$

for all $g, h \in G$ and $a, b \in A$.

Example 4.1. For each $n \in \mathbb{N}$, we define the following $\mathbb{Z}[G]$-modules: as a set, we have

$$\mathbb{Z}[G^{n+1}] = \left\{ \sum_{g_0, \ldots, g_n \in G} n_{g_0, \ldots, g_n} (g_0, \ldots, g_n) \mid n_{g_0, \ldots, g_n} \in \mathbb{Z} \text{ and } n_{g_0, \ldots, g_n} = 0 \text{ for all but finitely many tuples } (g_0, \ldots, g_n) \in G^n \right\}.$$

Addition in $\mathbb{Z}[G^{n+1}]$ is defined pointwise as in $\mathbb{Z}[G]$ and scalar multiplication is uniquely determined by

$$g(g_0, \dots, g_n) = (gg_0, \dots, gg_n)$$

for all $g \in G$ and $(g_0, \dots, g_n) \in G^n$. We write $\mathbb{Z}[[G]]$ to be the graded module whose component in degree $n \in \mathbb{Z}$ is

$$\mathbb{Z}[[G]]_n = \mathbb{Z}[G^{n+1}]$$

Here, we view $\mathbb{Z}[G]$ as a trivially graded ring which sits in the degree 0 component of $\mathbb{Z}[[G]]$. In particular, we have

$$\mathbb{Z}[[G]] = \bigoplus_{n \geq 0} \mathbb{Z}[G^{n+1}].$$

We give $\mathbb{Z}[[G]]$ the structure of a $\mathbb{Z}[G]$-complex by defining the differential $\mathrm{d} \colon \mathbb{Z}[[G]] \to \mathbb{Z}[[G]]$ by

$$\mathrm{d}_{n+1}(g_0, \dots, g_n) = \sum_{i=0}^{n} (-1)^i (g_0, \dots, \widehat{g_i}, \dots, g_n)$$

for all $n \geq 0$ and $(g_0, \dots, g_n) \in \mathbb{Z}[[G]]$, and extending it $\mathbb{Z}[G]$-linearly. It is easy to check that d is graded of degree -1 and satisfies $\mathrm{d}^2 = 0$, making it a differential.

4.1.3 Viewing $\mathbb{Z}[G^{n+1}]$ as a Free $\mathbb{Z}[G]$-Module

By definition, $\mathbb{Z}[G^{n+1}]$ is a free $\mathbb{Z}$-module with basis given by

$$\{(g_0, \dots, g_n) \mid g_0, \dots, g_n \in G\}.$$

In fact, let us now show that $\mathbb{Z}[G^{n+1}]$ is a free $\mathbb{Z}[G]$-module, with basis

$$\{(1, g_1, \dots, g_n) \mid g_1, \dots, g_n \in G\} \tag{15}$$

where 1 is the identity in G.

Proposition 4.1. *$\mathbb{Z}[G^n]$ is a free $\mathbb{Z}[G]$-module with basis given by (15).*

Proof. First note that

$$\sum_{g_0, \dots, g_n \in G} n_{g_0, \dots, g_n}(g_0, \dots, g_n) = \sum_{g_0, \dots, g_n \in G} n_{g_0, \dots, g_n} g_0 (1, g_0^{-1} g_1 \dots, g_0^{-1} g_n)$$

shows

$$\operatorname{span}_{\mathbb{Z}[G]} \{(1, g_1, \dots, g_n) \mid g_1, \dots, g_n \in G\} = \mathbb{Z}[G^n].$$

It remains to show that $\{(1, g_1, \dots, g_n) \mid g_1, \dots, g_n \in G\}$ is linearly independent over $\mathbb{Z}[G]$. Suppose

$$\sum_{i=1}^{k} \left(\sum_{g \in G} n_{g,i} g \right) (1, g_{1,i}, \dots, g_{n,i}) = 0,$$

where $\sum_{g \in G} n_{g,i} g \in \mathbb{Z}[G]$ for each $1 \leq i \leq k$ and $(1, g_{1,i}, \dots, g_{n,i}) \neq (1, g_{1,j}, \dots, g_{n,j})$ whenever $i \neq j$ (so $g_{m,i} \neq g_{m,j}$ for some $1 \leq m \leq n$). Then

$$\begin{aligned} 0 &= \sum_{i=1}^{k} \left(\sum_{g \in G} n_{g,i} g \right) (1, g_{1,i}, \dots, g_{n,i}) \\ &= \sum_{i=1}^{k} \sum_{g \in G} n_{g,i} (g, gg_{1,i}, \dots, gg_{n,i}) \\ &= \sum_{\substack{g \in G \\ 1 \leq i \leq k}} n_{g,i} (g, gg_{1,i}, \dots, gg_{n,i}) \end{aligned}$$

implies $n_{g,i} = 0$ for all $g \in G$ and $1 \leq i \leq k$ since

$$\{(g, gg_{1,i}, \dots, gg_{n,i}) \mid g \in G \text{ and } 1 \leq i \leq k\}$$

is linearly independent over $\mathbb{Z}$. Here we are using the fact that $(g, gg_{1,i}, \dots, gg_{n,i}) \neq (h, hg_{1,j}, \dots, hg_{n,j})$ whenever $g \neq h$ or $i \neq j$. To see why this is the case, first note that if $g \neq h$, then clearly $(g, gg_{1,i}, \dots, gg_{n,i}) \neq (h, hg_{1,j}, \dots, hg_{n,j})$ since they do not agree in the first component, so assume $g = h$. If $i \neq j$, then there exists an $1 \leq m \leq n$ such that $g_{m,i} \neq g_{m,j}$, in which case $gg_{m,i} \neq gg_{m,j}$. □

4.1.4 Differential on $\mathbb{Z}[[G]]$

We want to give $\mathbb{Z}[[G]]$ a $\mathbb{Z}[G]$-complex structure as follows. We define $\mathrm{d}\colon \mathbb{Z}[[G]] \to \mathbb{Z}[[G]]$ in terms of the $\mathbb{Z}$-basis $\{(g_0, \dots, g_n) \mid n \in \mathbb{N}\}$ and then extend it $\mathbb{Z}$-linearly. We will then show that it is in fact $\mathbb{Z}[G]$-linear. The reason we define it on the $\mathbb{Z}$-basis first is because it will be easy to show that $\mathrm{d}^2 = 0$. So for any $\mathbb{Z}$-basis element $(g_0, \dots, g_n)$ in $\mathbb{Z}[[G]]$, we set

$$\mathrm{d}((g_0, \dots, g_n)) = \sum_{i=0}^{n} (-1)^i (g_0, \dots, \widehat{g_i}, \dots, g_n).$$

It is easy to check that $\mathrm{d}^2 = 0$ and is homogeneous of degree -1. Let us show that d is $\mathbb{Z}[G]$-linear. First note that d is additive since it is $\mathbb{Z}$-linear, so we just need to show that is preserves $\mathbb{Z}[G]$-scalar multiplication. Since d is already additive, we just need ot check this on the $\mathbb{Z}[G]$-basis elements, so let $g \in G$ and let $(1, g_1 \dots, g_n)$ be any $\mathbb{Z}[G]$-basis element. We have

$$\begin{aligned}
\mathrm{d}\left(g(1, g_1 \dots, g_n)\right) &= \mathrm{d}(g, gg_1 \dots, gg_n) \\
&= (gg_1 \dots, gg_n) + \sum_{i=1}^{n} (-1)^i (g, gg_1, \dots, \widehat{gg_i}, \dots, gg_n) \\
&= g\left((g_1 \dots, g_n) + \sum_{i=1}^{n} (-1)^i (1, g_1, \dots, \widehat{g_i}, \dots, g_n)\right) \\
&= g\mathrm{d}(1, g_1 \dots, g_n).
\end{aligned}$$

It follows that d is $\mathbb{Z}[G]$-linear, and since already $\mathrm{d}^2 = 0$ and is graded of degree -1, we see that d is a $\mathbb{Z}[G]$-differential.

4.1.5 Free Resolution of $\mathbb{Z}$ Over $\mathbb{Z}[G]$

So far we've shown that $\mathbb{Z}[[G]]$ can be given a nice $\mathbb{Z}[G]$-complex structure. We will now show that $\mathbb{Z}[[G]]$ can be the structure of a free resolution of $\mathbb{Z}$ over $\mathbb{Z}[G]$. In particular, we view $\mathbb{Z}$ as a trivial $\mathbb{Z}[G]$-complex and we define a chain map $\varepsilon\colon \mathbb{Z}[[G]] \to \mathbb{Z}$ as follows: in homological degree $i > 0$ we set $\varepsilon_i\colon \mathbb{Z}[G^{i+1}] \to 0$ to be the zero map, and in homological degree 0 we define $\varepsilon_0\colon \mathbb{Z}[G] \to \mathbb{Z}$ by

$$\varepsilon_0\left(\sum_{g \in G} n_g g\right) = \sum_{g \in G} n_g.$$

for all $\sum_{g \in G} n_g g \in \mathbb{Z}[G]$.

To show that the pair $(\mathbb{Z}[[G]], \varepsilon)$ really is a free resolution of $\mathbb{Z}$ over $\mathbb{Z}[G]$, we need to check that the augmented $\mathbb{Z}[G]$-complex $\mathbb{Z}[[G]]_\varepsilon$ is exact. Here, $\mathbb{Z}[[G]]_\varepsilon$ is defined as follows: as a graded module, the homogeneous component in homological degree i is

$$\mathbb{Z}[[G]]_{\varepsilon,i} = \begin{cases} \mathbb{Z}[[G]]_i & \text{if } i \geq 0 \\ \mathbb{Z} & \text{if } i = -1 \\ 0 & \text{if } i < -1 \end{cases}$$

and the differential $\mathrm{d}_\varepsilon\colon \mathbb{Z}[[G]]_\varepsilon \to \mathbb{Z}[[G]]_\varepsilon$ in homological degree i is defined by

$$\mathrm{d}_{\varepsilon,i} = \begin{cases} \mathrm{d}_i & \text{if } i > 0 \\ \varepsilon & \text{if } i = 0 \\ 0 & \text{if } i < 0 \end{cases}$$

It is easy to check that $\mathbb{Z}[[G]]_\varepsilon$ is a $\mathbb{Z}[G]$-complex. Now we will show that it is exact.

Proposition 4.2. *The complex $\mathbb{Z}[[G]]_\varepsilon$ is exact.*

Proof. Define a $\mathbb{Z}$-graded homomorphism $\mathrm{h}\colon \mathbb{Z}[[G]]_\varepsilon \to \mathbb{Z}[[G]]_\varepsilon$ of degree 1 as follows: if $i \geq 1$ we define $\mathrm{h}_{i-1}\colon \mathbb{Z}[G^i] \to \mathbb{Z}[G^{i+1}]$ on the $\mathbb{Z}$-basis by

$$\mathrm{h}_{i-1}(g_1, \dots, g_i) = (e, g_1, \dots, g_i)$$

and extend $\mathbb{Z}$-linearly. In homological degree -1, we define $\mathrm{h}_{-1}\colon \mathbb{Z} \to \mathbb{Z}[G]$ by

$$\mathrm{h}_{-1}(n) = ne$$

for all $n \in \mathbb{Z}$. One check thats $\mathrm{h}\colon \mathbb{Z}[[G]]_\varepsilon \to \mathbb{Z}[[G]]_\varepsilon$ is in fact a $\mathbb{Z}[G]$-graded homomorphism of degree 1 and furthermore satisfies

$$\mathrm{d}_\varepsilon \mathrm{h} + \mathrm{h}\mathrm{d}_\varepsilon = 1.$$

In particular, the identity map $1\colon \mathbb{Z}[[G]] \to \mathbb{Z}[[G]]$ is null homotopic. □

4.1.6 Definition of Group Cohomology

Let us now define cohomology groups.

Definition 4.3. Let G be a group and let A be a G-module. We define the **cohomology group of** G **with coefficients in** A by

$$\mathrm{H}(G, A) := \mathrm{Ext}_{\mathbb{Z}[G]}(\mathbb{Z}, A).$$

We can explicitely compute $\mathrm{H}(G, A)$ using the fact that $\mathbb{Z}[[G]]$ is a free resolutions of $\mathbb{Z}$ over $\mathbb{Z}[G]$. Namely

$$\mathrm{H}(G, A) = \mathrm{H}(\mathrm{Hom}^{\star}_{\mathbb{Z}[G]}(\mathbb{Z}[[G]], A)).$$

We can explicitely compute $\mathrm{H}(G, A)$ using the fact that $\mathbb{Z}[[G]]$ is a free resolutions of $\mathbb{Z}$ over $\mathbb{Z}[G]$. Namely

$$\mathrm{H}(G, A)$$

$\mathrm{Ext}_{\mathbb{Z}[G]}(\mathbb{Z}, A)$ can be computed as follows: we c

4.1.7 Alternative Description

Definition 4.4. Let n be an integer ≥ 0. An n**-cochain**, or a **cochain of degree** n, on G with values in A is a function $\varphi\colon G^n \to A$. The set of all n-cochains on G with values in A, denoted $\mathrm{C}^n(G, A)$, forms an abelian group with addition induced from A. In particular, if $\varphi, \psi \in \mathrm{C}^n(G, A)$, then we define $\varphi + \psi \in \mathrm{C}^n(G, A)$ by

$$(\varphi + \psi)(g_1, \ldots, g_n) := \varphi(g_1, \ldots, g_n) + \psi(g_1, \ldots, g_n)$$

for all $(g_1, \ldots, g_n) \in G^n$.

Definition 4.5. Let $\varphi \in \mathrm{C}^n(G, A)$. The **coboundary** of φ, denoted by $\delta\varphi$, is an element in $\mathrm{C}^{n+1}(G, A)$ defined by the following formula:

$$(\delta\varphi)(g_1, \ldots, g_n, g_{n+1}) = g_1\varphi(g_2, \ldots, g_{n+1}) + \sum_{i=1}^{n}(-1)^i\varphi(g_1, \ldots, g_{i-1}, g_ig_{i+1}, g_{i+2}, \ldots, g_{n+1}) + (-1)^{n+1}\varphi(g_1, \ldots, g_n)$$

for all $(g_1, \ldots, g_n, g_{n+1}) \in G^{n+1}$.

Definition 4.6. Let $\varphi \in \mathrm{C}^n(G, A)$.

1. We say φ is an n**-cocycle** if $\delta\varphi = 0$. The set of all n-cocycles forms a subgroup of $\mathrm{C}^n(G, A)$ and is denoted by $\mathrm{Z}^n(G, A)$.
2. We say φ is an n**-coboundary** if if there exists an $(n-1)$-cochain ψ such that $\varphi = \delta\psi$. The set of all n-coboundaries form a subgroup of $\mathrm{Z}^n(G, A)$ and is denoted by $\mathrm{B}^n(G, A)$.
3. The quotient group $\mathrm{Z}^n(G, A)/\mathrm{B}^n(G, A)$ is denoted by $\mathrm{H}^n(G, A)$ and is called the n**th cohomology group of** G **with values in** A. Two n-cocycles are said to be **cohomologous** if they define the same cohomology class in $\mathrm{H}^n(G, A)$.

4.1.8 Isomorphism of Complexes

Recall that $\mathrm{Hom}^{\star}_{\mathbb{Z}[G]}(\mathbb{Z}[[G]], A)$ is a $\mathbb{Z}[G]$-complex. Indeed, as a graded module, it's ith homogeneous component is

$$\mathrm{Hom}^{\star}_{\mathbb{Z}[G]}(\mathbb{Z}[[G]], A)_i := \begin{cases} \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G^{i+1}], A) & \text{if } i \end{cases}.$$

Its differential is denoted $\mathrm{d}^{\star}$ and is defined by

Proposition 4.3. *Define* $\Psi\colon \mathrm{Hom}^{\star}_{\mathbb{Z}[G]}(\mathbb{Z}[[G]], A) \to \mathrm{C}(G, A)$ *as folows:*

4.2 Group Extensions

Definition 4.7. Let G and A be groups. An **extension** of G by A is a group E, together with an exact sequence:

$$1 \longrightarrow A \xrightarrow{\alpha} E \xrightarrow{\beta} G \longrightarrow 1$$

We shall denote such an extension by (E, α, β). If A is a normal subgroup of E and $G = E/A$, then we will denote the extension simply by E. In this case α must be the inclusion map and π must be the quotient map.

Definition 4.8. Let (E, α, β) and (E', α', β') are two extensions of G by A, then we say they are **isomorphic** if there exists an isomorphism $\varphi\colon E \to E'$ such that the following diagram is commutative

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \xrightarrow{\alpha} & E & \xrightarrow{\beta} & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle 1_A} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle 1_G} & & \\ 1 & \longrightarrow & A & \xrightarrow{\alpha'} & E' & \xrightarrow{\beta'} & G & \longrightarrow & 1 \end{array}$$

where 1_A and 1_G denote the identity maps on A and G respectively. The set of all extensions of G by A which are isomorphic to (E, α, β) is called the **isomorphism class** of (E, α, β) and is denoted by $[E, \alpha, \beta]$. If A is a normal subgroup of E and $G = E/A$, then the isomorphism class of the extension E is denoted by $[E]$.

Remark 17. Let (E, α, β) and (E, α', β') be extensions of G by A. If $\varphi\colon (E, \alpha, \beta) \to (E, \alpha', \beta')$ is an isomorphism of extensions, then it induces an isomorphism $\varphi\colon E \to E'$ of groups. On the other hand, if $\varphi\colon E \to E'$ is an isomorphism of extensions, then it does not necessarily give rise to an isomorphism between the extensions (E, α, β) and (E, α', β'). Indeed, we need φ to satisfy extra constraints, namely $\alpha\varphi = \alpha'$ and $\beta'\varphi = \beta$. However, φ does give rise to an isomorphism of extensions between (E, α, β) and $(E, \varphi\alpha, \pi\varphi^{-1})$.

Proposition 4.4. *Let (E, α, β) be an extension of G by A. Then we have a bijection of isomorphism classes*

$$[E, \alpha, \beta] \cong [E]$$

Proof. The first thing we need to do is to translate the short exact sequence

$$1 \longrightarrow A \xrightarrow{\alpha} E \xrightarrow{\beta} G \longrightarrow 1$$

to the short exact sequence

$$1 \longrightarrow \alpha(A) \xrightarrow{\iota} E \xrightarrow{\pi} E/\alpha(A) \longrightarrow 1$$

where ι is the inclusion map and π is the is the quotient map. Define a map $\gamma\colon G \to E/\alpha(A)$ as follows: for each $g \in G$ choose a lift $e_g \in E$ of g with respect to β (so $\beta(e_g) = g$) and set

$$\gamma(g) = \pi(e_g). \tag{16}$$

We must check that γ is well-defined. Suppose for each $g \in G$ we choose a different lift of g with respect to β, say $\alpha(a_g)e_g$ where $a_g \in A$ (every lift of g with respect to β has this form!). Then

$$\begin{aligned} \pi(\alpha(a_g)e_g) &= \pi(\alpha(a_g))\pi(e_g) \\ &= \pi(e_g) \\ &= \gamma(g). \end{aligned}$$

where we used the fact that $\alpha(a_g) \in \ker\pi$. It follows that γ is well-defined.

Next we check that γ is a group homomorphism. Let $g, h \in G$. First note that $e_{gh}e_{h^{-1}}e_{g^{-1}} \in \ker\beta$. Indeed,

$$\begin{aligned} \beta(e_{gh}e_{h^{-1}}e_{g^{-1}}) &= \beta(e_{gh})\beta(e_{h^{-1}})\beta(e_{g^{-1}}) \\ &= ghh^{-1}g^{-1} \\ &= e. \end{aligned}$$

Thus there exists a unique $a_{g,h} \in A$ such that $(a_{g,h}) = e_{gh}e_{h^{-1}}e_{g^{-1}}$ or in other words

$$\alpha(a_{g,h})e_ge_h = e_{gh}.$$

Therefore we have

$$\begin{aligned}\gamma(gh) &= \pi(e_{gh}) \\ &= \pi(\alpha(a_{g,h})e_g e_h) \\ &= \pi(\alpha(a_{g,h}))\pi(e_g)\pi(e_h) \\ &= \gamma(g)\gamma(h)\end{aligned}$$

where we used the fact that $\alpha(a_{g,h}) \in \ker \pi$. Thus γ is a group homomorphism. The reader can verify that it is in fact an isomorphism and the following diagram commutes

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \xrightarrow{\alpha} & E & \xrightarrow{\beta} & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle 1_E} & & \downarrow{\scriptstyle \gamma} & & \\ 1 & \longrightarrow & \alpha(A) & \xrightarrow{\iota} & E & \xrightarrow{\pi} & E/\alpha(A) & \longrightarrow & 1 \end{array}$$

Now let (E', α', β') be an extensions of G by A and let $\varphi\colon (E, \alpha, \beta) \to (E', \alpha', \beta')$ be an isomorphism. Then φ induces an isomorphism between the extensions E and $(E, \alpha'\alpha^{-1}, \gamma\beta')$ of $E/\alpha(A)$ by $\alpha(A)$. Indeed, since $\gamma\colon G \to E/\alpha(A)$ and and $\alpha^{-1}\colon \alpha(A) \to A$ are isomorphisms, we see that $\alpha'\alpha^{-1}$ is injective and $\gamma\beta'$ is surjective, moreover $\operatorname{im}(\gamma\beta') \subseteq \ker(\alpha'\alpha^{-1})$. It follows that

$$1 \longrightarrow \alpha(A) \xrightarrow{\alpha'\alpha^{-1}} E \xrightarrow{\gamma\beta'} G \longrightarrow 1$$

is a short exact sequence. Furthemore, we have $\gamma\beta'\varphi = \gamma\beta = \pi$ and $\alpha'\alpha^{-1} = \varphi\alpha\alpha^{-1} = \varphi\iota$.

Conversely, let $(E', \delta, \varepsilon)$ be an extension of $E/\alpha(A)$ by $\alpha(A)$ and let $\psi\colon E \to (E', \delta, \varepsilon)$ be an isomorphism. Then ψ induces an isomoprhism between the extensions (E, α, β) and $(E', \delta\alpha, \gamma^{-1}\varepsilon)$. This construction is easily checked to be the inverse to the consturction above, and thus we have a bijection of isomorphism classes. □

The proposition above simplifies our notation a bit. Given an extension (E, α, β) of E by A, we are often interested in the set $[E, \alpha, \beta]$ up to *bijection*. The proposition above gives us a canonical bijection between $[E, \alpha, \beta]$ and $[E]$. Thus there is no harm if we identify A and G with $\alpha(A)$ and $E/\alpha(A)$ respectively.

4.3 Sections

Definition 4.9. Let (E, α, β) be an extension of G by A.

1. A **right section** of (E, α, β) is a function $\widetilde{\beta}\colon G \to E$ such that $\beta\widetilde{\beta} = 1_G$. In other words, we have

   $$\beta(\widetilde{\beta}(g)) = g$$

   for all $g \in G$. If $\widetilde{\beta}$ is a homomorphism, then we say $\widetilde{\beta}$ is a **right splitting section** and that it **splits** (E, α, β) **to the right**.

2. A **left section** of (E, α, β) is a function $\widetilde{\alpha}\colon E \to A$ such that $\widetilde{\alpha}\alpha = 1_A$. In other words, we have

   $$\widetilde{\alpha}(\alpha(a)) = a$$

   for all $a \in A$. If $\widetilde{\alpha}$ is a homomorphism, then we say $\widetilde{\alpha}$ is a **left splitting section** and that it **splits** (E, α, β) **to the left**.

4.3.1 Right Splitting Sections

Proposition 4.5. *Let (E, α, β) be be an extension of G by A. Then there exists a right splitting section of (E, α, β) if and only if there exists a homomorphism $\rho\colon G \to \operatorname{Aut}(A)$ such that $(E, \alpha, \beta) \cong (A \rtimes_\rho G, \iota_1, \pi_2)$.*

Proof. To keep notation clean we identify A with $\alpha(A)$. In particular, we assume that A is a normal subgroup of E and that α is the inclusion map. Let $\widetilde{\beta}\colon G \to E$ be a right splitting section of (E, α, β). Define $\rho\colon G \to \operatorname{Aut}(A)$ by $\rho(g) = \mathrm{c}_{\widetilde{\beta}(g)}$ for all $g \in G$, where $\mathrm{c}_{\widetilde{\beta}(g)}$ is conjugation map given by

$$\mathrm{c}_{\widetilde{\beta}(g)}(a) = \widetilde{\beta}(g)a\widetilde{\beta}(g)^{-1}$$

for all $a \in A$. Note that $\mathrm{c}_{\widetilde{\beta}(g)}$ lands in A since A is a normal subgroup. Since conjugation and $\widetilde{\beta}$ are both homomorphisms, it follows that ρ is a homomorphism. Now define $\varphi\colon (E, \alpha, \beta) \to (A \rtimes G, \iota_1, \pi_2)$ by

$$\varphi(x) = (x\widetilde{\beta}\beta(x)^{-1}, \beta(x))$$

for all $x \in E$. Observe that $x\widetilde{\beta}\beta(x)^{-1}$ really does belong to A since

$$\begin{aligned}\beta(x\widetilde{\beta}\beta(x)^{-1}) &= \beta(x)\beta\widetilde{\beta}\beta(x)^{-1}\\ &= \beta(x)\beta(x)^{-1}\\ &= e\end{aligned}$$

and $A = \ker\beta$. Also φ is a group homomorphism. Indeed, let $x, y \in E$. Then we have

$$\begin{aligned}\varphi(x)\varphi(y) &= (x\widetilde{\beta}\beta(x)^{-1}, \beta(x)) \cdot (y\widetilde{\beta}\beta(y)^{-1}, \beta(y))\\ &= (x\widetilde{\beta}\beta(x)^{-1}\mathrm{c}_{\widetilde{\beta}\beta(x)}(y\widetilde{\beta}\beta(y)^{-1}), \beta(x)\beta(y))\\ &= (x\widetilde{\beta}\beta(x)^{-1}\widetilde{\beta}\beta(x)y\widetilde{\beta}\beta(y)^{-1}\widetilde{\beta}\beta(x)^{-1}, \beta(xy))\\ &= (xy\widetilde{\beta}\beta(y)^{-1}\widetilde{\beta}\beta(x)^{-1}, \beta(xy))\\ &= (xy\widetilde{\beta}\beta(xy)^{-1}, \beta(xy))\\ &= \varphi(xy).\end{aligned}$$

It is straightforward to check that the map $\psi\colon A \rtimes G \to E$, defined by

$$\psi(a, g) = a\widetilde{\beta}(g)$$

for all $a \in A$ and $g \in G$, is the inverse to φ. In particular, this implies φ is an isomorphism. It is also straightforward to check that φ is an isomorphism of extensions, that is, $\varphi\alpha = \iota_1$ and $\pi_2\varphi = \beta$. We leave the details as an exercise. □

4.3.2 Left Splitting Sections

Proposition 4.6. *Let (E, α, β) be be an extension of G by A. Then there exists a left splitting section of (E, α, β) if and only if $(E, \alpha, \beta) \cong (A \times G, \iota_1, \pi_2)$ where $\iota_1\colon A \to A \times G$ and $\pi_2\colon A \times G$ are defined by*

$$\iota_1(a) = (a, e) \quad \textit{and} \quad \pi_2(a, g) = g$$

for all $a \in A$ and $g \in G$.

Proof. The proof is similar in nature to the one above. □

4.4 Conjugation Action of G on $\mathrm{Z}(A)$

Let (E, α, β) be a group extension of G by A. To simplify notation in what follows, assume that A is a normal subgroup of G (so α is just the inclusion map). We define an action of G on $\mathrm{Z}(A)$ as follows: for each element $g \in G$, we choose a lift $e_g \in E$ with respect to β (so $\beta(e_g) = g$). Thus the map $g \mapsto e_g$ is a right splitting section of (E, α, β). Furthermore, every element in E can be expressed uniquely in the form ae_g where $a \in A$ and $g \in G$ both uniquely determine that element. In other words, if $x, y \in E$ are expressed as $x = ae_{\beta(x)}$ and $y = be_{\beta(y)}$ for some $a, b \in A$, Then $x = y$ if and only if $\beta(x) = \beta(y)$ and $a = b$.

Now, for each $g \in G$ and $x \in \mathrm{Z}(A)$, we define

$$g \cdot x = e_g x e_g^{-1}. \tag{17}$$

In a moment, we will need to show that (17) is well-defined, but first let us note that $e_g x e_g^{-1} \in \mathrm{Z}(A)$. Indeed, suppose $a \in A$. Then since A is normal in E, we have $e_g^{-1} a e_g = a_g$ for some $a_g \in A$. Therefore

$$\begin{aligned}ae_g x e_g^{-1} &= e_g a_g x e_g^{-1}\\ &= e_g x a_g e_g\\ &= e_g x e_g a.\end{aligned}$$

It follows that $e_g x e_g^{-1} \in \mathrm{Z}(A)$. Thus (17) at least lands in $\mathrm{Z}(A)$. Now let us show that it is well-defined. Let ae_g be another lift of g with respect to β, where $a \in A$. Then we have

$$\begin{aligned}ae_g x (ae_g)^{-1} &= ae_g x e_g^{-1} a^{-1}\\ &= e_g x e_g^{-1} a a^{-1}\\ &= e_g x e_g^{-1},\end{aligned}$$

where the last equality follows since $e_g x e_g^{-1} \in \mathrm{Z}(A)$. Thus (17) is well-defined.

Finally, let us show that this map is a group action of G on $\mathrm{Z}(A)$. Clearly the identity element e in G fixes all of $\mathrm{Z}(A)$. Let $g, h \in G$ and $x \in \mathrm{Z}(A)$. Then there exists a unique $a_{g,h} \in A$ such that

$$e_g e_h = a_{g,h} e_{gh}.$$

Thus we have

$$\begin{aligned} g \cdot (h \cdot x) &= g \cdot e_h x e_h^{-1} \\ &= e_g e_h x e_h^{-1} e_g^{-1} \\ &= e_g e_h x (e_g e_h)^{-1} \\ &= a_{g,h} e_{gh} x (a_{g,h} e_{gh})^{-1} \\ &= a_{g,h} e_{gh} x e_{gh}^{-1} a_{g,h}^{-1} \\ &= e_{gh} x e_{gh}^{-1} \\ &= gh \cdot x \end{aligned}$$

where the last equality follows from the fact that $gh \cdot x \in \mathrm{Z}(A)$.

4.5 $\mathbf{H}^2(G, A)$

Now we assume A is abelian (so $A = Z(A)$) and suppose the section mapping g to e_g was actually a group theoretic section, i.e. a set theoretic section that is also a homomorphism. Then we would have:

$$e_g e_h = e_{gh}.$$

In general this isn't necessarily true, but since π is a homomorphism, we know that

$$e_g e_h = \alpha_{g,h} e_{gh}$$

for some unique $\alpha_{g,h} \in A$. What can we say about $\alpha_{g,h}$? Well since E is a group, the associativity law tells us that on the one hand, we have

$$\begin{aligned} (e_g e_h) e_k &= \alpha_{g,h} e_{gh} e_k \\ &= \alpha_{g,h} \alpha_{gh,k} e_{ghk}, \end{aligned}$$

and on the other hand, we have

$$\begin{aligned} e_g (e_h e_k) &= e_g \alpha_{h,k} e_{hk} \\ &= e_g \alpha_{h,k} e_g^{-1} e_g e_{hk} \\ &= g \cdot \alpha_{h,k} \alpha_{g,hk} e_{ghk}, \end{aligned}$$

and so equating the two sides gives us the 2-cocycle condition:

$$g \cdot \alpha_{h,k} \alpha_{g,hk} = \alpha_{g,h} \alpha_{gh,k}.$$

Thus, we can think of α as a map $\alpha : G \times G \to A$, denoted $(g, h) \mapsto \alpha_{g,h}$, which satisfies the 2-cocycle condition $\delta\alpha = 0$. If we had chosen a differenent section, say $g \mapsto \beta_g e_g$, then

$$\begin{aligned} \beta_g e_g \beta_h e_h &= \beta_g (g \cdot \beta_h) e_g e_h \\ &= \beta_g (g \cdot \beta_h) \alpha_{g,h} e_{gh}, \end{aligned}$$

or in other words

$$e_g e_h = (\delta\beta)_{g,h} \alpha_{g,h} e_{gh}.$$

Proposition 4.7. *An automorphism $\varphi : E \to E$ which induces the identity on A and on E/A is of the form*

$$a e_g \mapsto a \beta_g e_g$$

where β is a 1-cocycle. It is an inner automorphism if and only if β is a coboundary.

Since φ induces the identity on E/A, it must map e_g to $\beta_g e_g$, where $\beta_g \in A$. Since φ induces the identity on A, we must have

$$\varphi(a e_g) = \varphi(a)\varphi(e_g) = a \beta_g e_g$$

We need to check that α is a 1-cocycle, i.e.

$$\beta_{gh} = \beta_g(g \cdot \beta_h)$$

We compute $\varphi(e_{gh})$ in two ways.

$$\varphi(e_{gh}) = \beta_{gh}e_{gh} = \beta_{gh}\alpha_{g,h}e_g e_h$$

Let G and A be groups. An **extension** of G by A is a group E, together with an exact sequence:

$$1 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1$$

An extension E' of G by A is said to be **isomorphic** to E if there exists an isomorphism $\varphi : E \to E'$ such that the following diagram is commutative

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle id} & & \\ 1 & \longrightarrow & A & \longrightarrow & E' & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

If E is an extension of G by A, a **section** of E is a map $s : G \to E$, such that the composite map $G \to E \to G$ is the identity. If π denotes the projection $E \to G$, this means that $\pi \circ s = id_G$. A section s which is a homomorphism is called a **splitting** of E; if such a section exists, we say E **splits**. If s is a splitting, its image is a subgroup C of E, with $C \cap A = 1$ and $AC = E$. The projection $E \to G$ gives an isomorphism $C \to G$, and C is called a **lifting of** G **in E**. If we identify C with G, then every element of E can be written uniquely as ag with $a \in A$ and $g \in G$. The group E is said to be a **semidirect product** of G and A

4.6 Conjugation Action on $Z(A)$

Let E be a group extension of G by A. We define an action of G on $Z(A)$ as follows: for each element $g \in G$, choose a lift $e_g \in E$ (so $\pi(e_g) = g$). The map $g \mapsto e_g$ is a *set-theoretic* splitting, and thus every element of E can be decomposed as ae_g, for unique $a \in A$ and unique $g \in G$. For $x \in Z(A)$ and $g \in G$, we set

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

First note that $e_g x e_g^{-1} \in Z(A)$. Indeed, if $a \in A$, then since A is normal in E, we have $e_g^{-1} a e_g = a_g$, where $a_g \in A$. Thus,

$$\begin{aligned} ae_g x e_g^{-1} &= e_g a_g x e_g^{-1} \\ &= e_g x a_g e_g^{-1} \\ &= e_g x e_g^{-1} a. \end{aligned}$$

Next, we note that this map is well-defined since if ae_g is another lift of g, where $a \in A$, then

$$\begin{aligned} g \cdot x &= ae_g x (ae_g)^{-1} \\ &= ae_g x e_g^{-1} a^{-1} \\ &= e_g x e_g^{-1}, \end{aligned}$$

where the last equality follows since $e_g x e_g^{-1} \in Z(A)$. Finally, we note that this map is a group action of G on $Z(A)$. Indeed, let $g, h \in G$ and $x \in Z(A)$. Then there exists a unique $\alpha_{g,h} \in A$ such that $e_{g,h} = e_{gh}$, and hence

$$\begin{aligned} g \cdot (h \cdot x) &= g \cdot e_h x e_h^{-1} \\ &= e_g e_h x e_h^{-1} e_g^{-1} \\ &= e_g e_h x \left(e_g e_h\right)^{-1} \\ &= \alpha_{g,h} e_{gh} x \left(\alpha_{g,h} e_{gh}\right)^{-1} \\ &= \alpha_{g,h} e_{gh} x e_{gh}^{-1} \alpha_{g,h}^{-1} \\ &= \alpha_{g,h} \left(gh \cdot x\right) \alpha_{g,h}^{-1} \\ &= gh \cdot x, \end{aligned}$$

where the last equality follows from the fact that $gh \cdot x \in Z(A)$.

4.7 $\mathbf{H}^2(G, A)$

Now we assume A is abelian (so $A = Z(A)$Suppose the section mapping g to e_g was actually a group theoretic section, i.e. a set theoretic section that is also a homomorphism. Then we would have:

$$e_g e_h = e_{gh}.$$

In general this isn't necessarily true, but since π is a homomorphism, we know that

$$e_g e_h = \alpha_{g,h} e_{gh}$$

for some unique $\alpha_{g,h} \in A$. What can we say about $\alpha_{g,h}$? Well since E is a group, the associativity law tells us that on the one hand, we have

$$\begin{aligned}(e_g e_h)e_k &= \alpha_{g,h} e_{gh} e_k \\ &= \alpha_{g,h}\alpha_{gh,k} e_{ghk},\end{aligned}$$

and on the other hand, we have

$$\begin{aligned}e_g(e_h e_k) &= e_g \alpha_{h,k} e_{hk} \\ &= e_g \alpha_{h,k} e_g^{-1} e_g e_{hk} \\ &= g \cdot \alpha_{h,k}\alpha_{g,hk} e_{ghk},\end{aligned}$$

and so equating the two sides gives us the 2-cocycle condition:

$$g \cdot \alpha_{h,k}\alpha_{g,hk} = \alpha_{g,h}\alpha_{gh,k}.$$

Thus, we can think of α as a map $\alpha : G \times G \to A$, denoted $(g, h) \mapsto \alpha_{g,h}$, which satisfies the 2-cocycle condition $\delta\alpha = 0$. If we had chosen a differenent section, say $g \mapsto \beta_g e_g$, then

$$\begin{aligned}\beta_g e_g \beta_h e_h &= \beta_g (g \cdot \beta_h) e_g e_h \\ &= \beta_g (g \cdot \beta_h)\alpha_{g,h} e_{gh},\end{aligned}$$

or in other words

$$e_g e_h = (\delta\beta)_{g,h}\alpha_{g,h} e_{gh}.$$

Proposition 4.8. *An automorphism $\varphi : E \to E$ which induces the identity on A and on E/A is of the form*

$$a e_g \mapsto a\beta_g e_g$$

where β is a 1-cocycle. It is an inner automorphism if and only if β is a coboundary.

Proof. Since φ induces the identity on E/A, it must map e_g to $\beta_g e_g$, where $\beta_g \in A$. Since φ induces the identity on A, we must have

$$\varphi(a e_g) = \varphi(a)\varphi(e_g) = a\beta_g e_g$$

$$\varphi(e_{gh}) = \varphi(\alpha_{g,h} e_g e_h) = \alpha_{g,h}\beta_g e_g \beta_h e_h = \alpha_{g,h}\beta_g (g \cdot \beta_h) e_g e_h$$

And so we have

$$\beta_{gh}\alpha_{g,h} = \alpha_{g,h}\beta_g (g \cdot \beta_h)$$

$$\beta_{gh} = \beta_g (g \cdot \beta_h)$$

Now suppose β_g is a coboundary:

$$\beta_g = b(g \cdot b)^{-1}$$

Then

$$\varphi(a e_g) = a\beta_g e_g = ab(g \cdot b)^{-1} e_g = abe_g b^{-1} e_g^{-1} e_g = bae_g b^{-1}$$

□

We said earlier that this action is well defined because A is abelian. If A is not abelian, then the action is well defined only up to conjugation. If we restrict the action to the center of A, $Z(A)$, then we get a well defined action again. When A is abelian, $Z(A) = A$, so we may as well consider cohomology with coefficients in $Z(A)$.

4.8 The existence problem and its obstruction in $H^3(G, Z(A))$

Let $\psi\colon G \to \mathrm{Out}(A)$ be a group homomorphism. For each $g \in G$, let ψ_g be a representative of the coset $\psi(g) = \overline{\psi_g}$ in $\mathrm{Out}(A)$. Also for each $a \in A$, let $\mathrm{c}_a\colon A \to A$ denote the conjugation homomorpism, given by

$$\mathrm{c}_a(x) = a^{-1}xa$$

for all $x \in A$. Note that if $g \in G$ and $a \in A$, then

$$\begin{aligned}\psi_g \mathrm{c}_a(x) &= \psi_g(a^{-1}xa)\\ &= \psi_g(a^{-1})\psi_g(x)\psi_g(a)\\ &= \mathrm{c}_{\psi_g(a)}\psi_g(x)\end{aligned}$$

for all $x \in A$ implies $\psi_g \mathrm{c}_a = \mathrm{c}_{\psi_g(a)}\psi_g$. Thus ψ being a group homomorphism means for each $g, h \in G$, we have

$$\overline{\psi_g\psi_h} = \overline{\psi_{gh}}.$$

In other words, for each $g, h \in G$ there exists $\alpha_{g,h} \in A$ such that

$$\psi_g\psi_h = \psi_{gh}\mathrm{c}_{\alpha_{g,h}}.$$

Notice what happens if we choose different coset representatives of the coset $\overline{\psi_g}$ for each $g \in G$: a different coset representative of $\overline{\psi_g}$ has the form $\psi_g \mathrm{c}_{\beta_g}$ for some $\beta_g \in A$. Using these different coset representatives for each $g \in G$, we find that for each $g, h \in G$ we have

$$\begin{aligned}(\psi_g \mathrm{c}_{\beta_g})(\psi_h \mathrm{c}_{\beta_h}) &= \psi_g \mathrm{c}_{\beta_g}\psi_h \mathrm{c}_{\beta_h}\\ &= \psi_g\psi_h \mathrm{c}_{\psi_g^{-1}(\beta_g)}\mathrm{c}_{\beta_h}\\ &= \psi_{gh}\mathrm{c}_{\psi_g^{-1}(\beta_g)\beta_h}.\end{aligned}$$

Thus
a homomorphism $\psi : G \to \mathrm{Out}(A)$. This means to each $g \in G$, we assign a coset of automorphisms of A:

$$g \mapsto \{s_g(\cdot), as_g(\cdot)a^{-1}\dots\}$$

The fact that s_g is an automorphism of A means $s_g xx' = s_g x s_g x'$ for all $x, x' \in A$. The fact that ψ is a homomorphism means $s_g s_h x = s_{g,h}s_{gh}xs_{g,h}^{-1}$ for some $s_{g,h} \in A$ and for all $x \in A$. Notice what happens if we choose different coset representatives: $bs_g as_h xa^{-1}s_g^{-1}b^{-1} = bs_g as_{g,h}s_{gh}xs_{g,h}^{-1}a^{-1}s_g^{-1}b^{-1}$, so this is well defined with $s_{g,h}$ being replaced with $bs_g as_{g,h}$. The question we ask now is, does there exist an extension E of G by A corresponding to ψ? In other words, can we turn s_g into e_g? What Eilenberg and Mac Lane did is to associate to ψ and element $c(\psi)$ of $H^3(G, Z(A))$ and to prove:

Theorem 4.1. *There exists an extension of G by A corresponding to ψ if and only if $c(\psi) = 0$.*

For every $g, h \in G$, choose $s_{g,h} \in A$ such that $s_{g,h}xs_{g,h}^{-1} = s_g s_h s_{gh}^{-1}x$. We can think of this equations like this: We can switch $s_{g,h}$ and x, where $s_{g,h}$ is to the left of x, at the cost of $s_g s_h s_{gh}^{-1}x$.

$$s_{g,h}x = s_g s_h s_{gh}^{-1}xs_{g,h}$$

Now define a 3-cocycle as follows

$$s_{g,h,k} = s_g s_{h,k}s_{g,hk}s_{gh,k}^{-1}s_{g,h}^{-1}$$

Let's show that $s_{g,h,k}$ is an element of $Z(A)$. We do this by showing the associated conjugation map by $s_{g,h,k}$ is trivial.

$$\begin{aligned}s_{g,h,k}xs_{g,h,k}^{-1} &= s_g s_{h,k}s_{g,hk}s_{gh,k}^{-1}s_{g,h}^{-1}xs_{g,h}s_{gh,k}s_{g,hk}^{-1}s_g s_{h,k}^{-1}\\ &= s_g s_{h,k}s_{g,hk}s_{gh,k}^{-1}s_{gh}s_h^{-1}s_g^{-1}xs_{gh,k}s_{g,hk}^{-1}s_g s_{h,k}^{-1}\\ &= s_g s_{h,k}s_{g,hk}s_{ghk}s_k^{-1}s_{gh}^{-1}s_{gh}s_h^{-1}s_g^{-1}xs_{g,hk}^{-1}s_g s_{h,k}^{-1}\\ &= s_g s_{h,k}s_{ghk}s_k^{-1}s_{gh}^{-1}s_{gh}s_h^{-1}s_g^{-1}xs_g s_{h,k}^{-1}\\ &= s_g s_{hk}s_{ghk}^{-1}s_{ghk}s_k^{-1}s_{gh}^{-1}s_{gh}s_h^{-1}s_g^{-1}xs_{h,k}^{-1}\\ &= s_g s_h s_k s_{hk}^{-1}s_{hk}s_{ghk}^{-1}s_{ghk}s_k^{-1}s_{gh}^{-1}s_{gh}s_h^{-1}s_g^{-1}x\\ &= x\end{aligned}$$

4.9 Examples

Example 4.2. We have $\mathrm{Ext}(\mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_2) \cong H^2(\mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_2) \cong \mathbb{Z}_8$.
The quaternion group Q_8 fits in the short exact sequence

$$1 \longrightarrow \{\pm 1\} \longrightarrow Q_8 \longrightarrow Q_8/\{\pm 1\} \longrightarrow 1$$

a corresponding 2-cocycle is given by

f_2	$(1,1)$	$(1,-1)$	$(-1,1)$	$(-1,-1)$
$(1,1)$	1	1	1	1
$(1,-1)$	1	-1	1	-1
$(-1,1)$	1	-1	-1	1
$(-1,-1)$	1	1	-1	-1

Suppose

f_1	$(1,1)$	$(1,-1)$	$(-1,1)$	$(-1,-1)$
$f_1(g)$	1	1	1	-1

Then $f_2 d f_1$ would be

$f_2 d f_1$	$(1,1)$	$(1,-1)$	$(-1,1)$	$(-1,-1)$
$(1,1)$	1	1	1	1
$(1,-1)$	1	-1	-1	1
$(-1,1)$	1	1	-1	-1
$(-1,-1)$	1	-1	1	-1

However, all we did here was switch columns up. The dihedral group D_4 fits in the short exact sequence

$$1 \longrightarrow \langle r^2 \rangle \longrightarrow D_4 \longrightarrow D_4/\langle r^2 \rangle \longrightarrow 1$$

The corresponding 2-cocycle is given by

f_2	$(1,1)$	$(1,-1)$	$(-1,1)$	$(-1,-1)$
$(1,1)$	1	1	1	1
$r=(1,-1)$	1	-1	1	-1
$s=(-1,1)$	1	-1	1	-1
$rs=(-1,-1)$	1	1	1	1

The dihedral group $(\mathbb{Z}/2\mathbb{Z})^2/\mathbb{Z}/2\mathbb{Z}$ fits in the short exact sequence

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2 \longrightarrow (\mathbb{Z}/2\mathbb{Z})^2 \longrightarrow 0$$

The corresponding 2-cocycle is given by

f_2	$(1,1)$	$(1,-1)$	$(-1,1)$	$(-1,-1)$
$(1,1)$	1	1	1	1
$r=(1,-1)$	1	1	1	1
$s=(-1,1)$	1	1	1	1
$rs=(-1,-1)$	1	1	1	1

Example 4.3. The group $H^2(S_n, \{\pm 1\})$ is well-known, with the action of S_n on $\{\pm 1\}$ being necessarily the trivial one. Since the action is trivial, the signature homomorphism $S_n \to \{\pm 1\}$ gives rise to an element $\epsilon_n \in H^1(S_n, \{\pm 1\})$. For example, ϵ_3 looks like:

e	(23)	(12)	(123)	(321)	(13)
1	-1	-1	1	1	-1

Now consider the cup product $\epsilon_n \cup \epsilon_n$ induced by the $\mathbb{Z}$-bilinear map:

$B(\cdot,\cdot)$	1	-1
1	1	1
-1	1	-1

For ϵ_3 the resulting cup product looks like:

$B(a_g, g \cdot a_h)$	e	(23)	(12)	(123)	(321)	(13)
e	1	1	1	1	1	1
(23)	1	-1	-1	1	1	-1
(12)	1	-1	-1	1	1	-1
(123)	1	1	1	1	1	1
(321)	1	1	1	1	1	1
(13)	1	-1	-1	1	1	-1

If $n = 2, 3$, then $H^2(S_n, \{\pm 1\}) \simeq \mathbb{Z}/2\mathbb{Z}$ and it is generated by $\epsilon_n \cup \epsilon_n$. If $n \geq 4$, then $H^2(S_n, \{\pm 1\}) \simeq (\mathbb{Z}/2\mathbb{Z})^2$ and it is generated by $\epsilon_n \cup \epsilon_n$ and another class t_n. Here is part of it, which you can be completed as an exercise:

$(t_4)_{g,h}$	e	(12)	(23)	(34)	(123)	$(12)(34)$	$(13)(24)$	$(14)(23)$	...
e	1	1	1	1	1	1	1	1	
(12)	1	1	1	1	1				
(23)	1	1	1	1	1				
(34)	1	-1	1	1	1				
$(12)(34)$	1	-1	-1	1	1	-1	1	1	
$(13)(24)$	1					-1	-1	1	
$(14)(23)$	1					1	-1	-1	
...									

Notice the corresponding extension will have identities like:

$$e_{(12)(34)} = -e_{(34)(12)} \qquad \text{and} \qquad e_{(123)(23)} = -e_{(23)(123)}$$

More formally, the extension corresponding to t_n is denoted by $\tilde{S}_n$. Here is a presentation of this group:

$$\tilde{S}_n = < s_i, z \mid s_i^2 = 1,\ z^2 = 1,\ s_i z = z s_i,\ (s_i s_{i+1})^3 = 1,\ s_i s_j = z s_j s_i \text{ if } |j - i| \geq 2 >$$

Now $(\epsilon_n \cup \epsilon_n)(t_n)$ will correspond to another extension which we denote $2 \cdot S_n^-$. Here is its presentation (why?):

$$2 \cdot S_n^- = < s_i, z \mid s_i^2 = z,\ z^2 = 1,\ s_i z = z s_i,\ (s_i s_{i+1})^3 = z,\ s_i s_j = z s_j s_i \text{ if } |j - i| \geq 2 >$$

Now, if G is a subgroup of S_n, we can construct central extensions of G by $\{\pm 1\}$ using the restriction map

$$\text{Res: } H^2(S_n, \{\pm 1\}) \to H^2(G, \{\pm 1\})$$

In particular, we can define the extension $\tilde{G}$ corresponding to $\text{Res}(t_n)$. It is then easy to see that we have the following commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \pm 1 & \longrightarrow & \tilde{G} & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \pm 1 & \longrightarrow & \tilde{S}_n & \longrightarrow & S_n & \longrightarrow & 1 \end{array}$$

For example, identify the group $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ with the subgroup V of S_4 where

$$V = \{(),\ (12)(34),\ (13)(24),\ (14)(23)\}$$

Then $\tilde{G} = Q_8$. Can you see it in the table above?

Part II
Extra

5 Quaternion Group

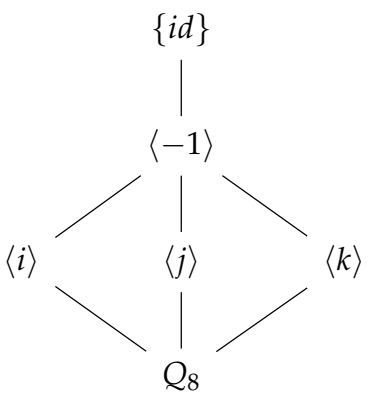
Example 5.1. The quaternion group Q_8 is given by the group presentation

$$Q_8 = < -1, i, j, k \mid (-1)^2 = 1, i^2 = j^2 = (ij)^2 = -1 >$$

Below, is the multiplication table for Q_8

$\cdot$	1	i	j	$k=ij$
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
$k=ij$	k	j	$-i$	-1

Below is the diagram of all subgroups of Q_8, written upside down.



Richard Dean showed in 1981, the quaternion group can be presented as the Galois group $Gal(K/\mathbb{Q})$ where K is the splitting field, over $\mathbb{Q}$, of the polynomial $x^8 - 72x^6 + 180x^4 - 144x^2 + 36$. The development uses the fundamental theorem of Galois theory in specifying four intermediate fields between $\mathbb{Q}$ and K and their Galois groups, as well as two theorems on cyclic extension of degree four over a field.

6 Symmetric Groups

6.1 Transpositions

Proposition 6.1. *S_n is generated by transpositions.*

Proof. We shall prove this in two steps.

Step 1: First we show that any element in S_n can be expressed as a product of disjoint cycles. Let $\sigma \in S_n$. We shall describe an algorithm which expresses σ as a product of disjoint cycles. In the first step of the algorithm, choose any $a_{1,1} \in [n]$. Let k_1 be the least nonnegative integer such that $\sigma^{k_1}(a_{1,1}) = a_{1,1}$. We denote $a_{1,i_1} = \sigma^{i_1-1}(a_{1,1})$ for each $1 \leq i_1 \leq k_1$. Observe that $1 \leq k_1 \leq n$ by the pigeonhole principle. Also observe that $a_{1,i_1} \neq a_{1,i_1'}$ whenever $i_1 \neq i_1'$. Indeed, if $a_{1,i_1} = a_{1,i_1'}$ for some $1 \leq i_1 < i_1' \leq k_1$, then

$$\begin{aligned}
\sigma^{i_1'-i_1}(a_{1,1}) &= \sigma^{i_1'}\sigma^{-i_1}(a_{1,1}) \\
&= \sigma^{-i_1}\sigma^{i_1'}(a_{1,1}) \\
&= \sigma^{-i_1}(a_{1,i_1'}) \\
&= \sigma^{-i_1}(a_{1,i_1}) \\
&= a_{1,1},
\end{aligned}$$

which would contradict the minimality of k_1 since $i_1' - i_1 < k_1$. So if we denote $\tau_1 = (a_{1,1} \cdots a_{1,k_1})$ and $\sigma_1 = \tau_1^{-1}\sigma$, then we can express σ as

$$\sigma = \tau_1\sigma_1.$$

where τ_1 is a cycle of length k_1 and where σ_1 fixes $\{a_{1,i_1} \mid 1 \leq i_1 \leq k_1\}$. Indeed, we have

$$\begin{aligned}
\sigma_1(a_{1,i}) &= \tau_1^{-1}\sigma(a_{1,i_1}) \\
&= \tau_1^{-1}(a_{1,i_1+1}) \\
&= a_{1,i_1},
\end{aligned}$$

where a_{1,i_1+1} is understood to be $a_{1,1}$ if $i_1 = k_1$.

Now we proceed to the second step of the algorithm. If $\{a_{1,i_1} \mid 1 \leq i_1 \leq k_1\} = [n]$, then the algorithm terminates and we are done. Indeed, in this case, σ_1 is the identity element since it fixes all of $[n]$. Then $\sigma = \tau_1$ shows that σ is a cycle itself. If $\{a_{1,i_1} \mid 1 \leq i_1 \leq k_1\} \subset n$, where the inclusion is proper, then we choose any $a_{2,1} \in [n]\backslash\{a_{1,i_1} \mid 1 \leq i_1 \leq k_1\}$. Let k_2 be the least nonnegative integer such that $\sigma^{k_2}(a_{2,1}) = a_{2,1}$. We denote

$a_{2,i_2} = \sigma^{i_2-1}(a_{2,1})$ for each $1 \leq i_2 \leq k_2$. As in the case of the first step of the algorithm, we observe that $1 \leq k_2 \leq n - k_1$ and we also observe that $a_{2,i_2} \neq a_{2,i_2'}$ whenever $i_2 \neq i_2'$. The proof for these two observations is nearly identical to the ones we did above. We denote $\tau_2 = (a_{2,1} \cdots a_{2,k_2})$ and $\sigma_2 = \tau_2^{-1}\sigma_1$. Then we can express σ_1 as

$$\sigma_1 = \tau_2\sigma_2,$$

where τ_2 is a cycle of length k_2 and where σ_2 fixes $\{a_{1,i_1}, a_{1,i_2} \mid 1 \leq i_1 \leq k_1 \text{ and } 1 \leq i_2 \leq k_2\}$. Indeed, the proof that σ_2 fixes a_{1,i_2} is nearly identical to the proof that σ_1 fixes a_{1,i_1}, and the reason that σ_2 fixes a_{1,i_1} is because both τ_2 and σ_1 fix a_{1,i_1}.

Now we describe the algorithm at the sth step where $s \geq 2$. If $\{a_{1,i_r} \mid 1 \leq r < s \text{ and } 1 \leq i_r \leq k_r\} = [n]$, then the algorithm terminates and we are done. Indeed, in this case, σ_{s-1} is the identity element since it fixes all of $[n]$. Then

$$\begin{aligned}
\sigma &= \tau_1\sigma_1 \\
&= \tau_1\tau_2\sigma_2 \\
&\vdots \\
&= \tau_1\tau_2 \cdots \tau_{s-1}\sigma_{s-1} \\
&= \tau_1\tau_2 \cdots \tau_{s-1}
\end{aligned}$$

shows that σ is a product of distinct cycles. If $\{a_{1,i_r} \mid 1 \leq r < s \text{ and } 1 \leq i_r \leq k_r\} \subset [n]$, where the inclusion is proper, then we choose any $a_{s,1} \in [n] \backslash \{a_{1,i_r} \mid 1 \leq r < s \text{ and } 1 \leq i_r \leq k_r\}$. Let k_s be the least nonnegative integer such that $\sigma^{k_s}(a_{s,1}) = a_{s,1}$. We denote $a_{s,i_s} = \sigma^{i_s-1}(a_{s,1})$ for each $1 \leq i_s \leq k_s$. As in the case of the first and second step of the algorithm, we observe that $1 \leq k_s \leq n - k_1 - \cdots - k_{s-1}$ and we also observe that that $a_{s,i_s} \neq a_{s,i_s'}$ whenever $i_s \neq i_s'$. We denote $\tau_s = (a_{s,1} \cdots a_{s,k_s})$ and $\sigma_s = \tau_s^{-1}\sigma_{s-1}$. Then we can express σ_{s-1} as

$$\sigma_{s-1} = \tau_s\sigma_s,$$

where τ_s is a cycle of length k_s and where σ_s fixes $\{a_{1,i_r} \mid 1 \leq r < s \text{ and } 1 \leq i_r \leq k_r\}$.

This algorithm must terminate since $[n]$ is finite and since after the sth step, we produce a strictly increasing sequence of sets

$$(\{a_{1,i_r} \mid 1 \leq r < s \text{ and } 1 \leq i_r \leq k_r\})$$

each of which is contianed in $[n]$.

Step 2: Now we show that any cycle in S_n can be expressed as a product of transposition. Let $(a_1a_2 \cdots a_k)$ be any in S_n. We claim that

$$(a_1a_2 \cdots a_k) = \prod_{i=1}^{k-1}(a_ia_{i+1}). \tag{18}$$

Indeed, let $a \in [n]$. If $a \neq a_j$ for any $1 \leq j \leq k$, then applying a to both $(a_1a_2 \cdots a_k)$ and $\prod_{i=1}^{k-1}(a_ia_{i+1})$ results in a again. In other words, both $(a_1a_2 \cdots a_k)$ and $\prod_{i=1}^{k-1}(a_ia_{i+1})$ fix a. If $a = a_j$ for some $1 \leq j \leq k$, then applying a_j to $(a_1a_2 \cdots a_k)$ results in a_{j+1}, where a_{j+1} is understood to be a_1 if $j = k$. Applying a_j to $\prod_{i=1}^{k-1}(a_ia_{i+1})$ also results in a_{j+1}, where a_{j+1} is understood to be a_1 if $j = k$. Indeed,

$$\begin{aligned}
\prod_{i=1}^{k-1}(a_ia_{i+1})(a_j) &= (a_1a_2) \cdots (a_{j-1}a_j)(a_ja_{j+1}) \cdots (a_ka_{k-1})(a_j) \\
&= (a_1a_2) \cdots (a_{j-1}a_j)(a_ja_{j+1})(a_j) \\
&= (a_1a_2) \cdots (a_{j-1}a_j)(a_{j+1}) \\
&= a_{j+1}.
\end{aligned}$$

Combining step 1 with step 2 shows that any permutation can be expressed as a product of transpositions. □

6.1.1 Order of Permutation

In the proof that every permutation can be expressed as a product of transpositions, we also showed that every permutation can be expressed as a product of disjoint cycles.

Proposition 6.2. *Let $\sigma \in S_n$. Express σ as a product of disjoint cycles, say $\sigma = \tau_1 \cdots \tau_k$. Let m denote the order of σ and let m_i denote the order of τ_i for each $1 \leq i \leq k$. Then*

$$m = \operatorname{lcm}(m_1, \ldots, m_k)$$

Proof. First we show that m is a common multiple of $m_1, \ldots, m_k$. In other words, we first show that $m_i \mid m$ for each $1 \leq i \leq k$. Indeed, first note that $\tau_1, \ldots, \tau_k$ all commute with each other since they are all disjoint from each other. Thus

$$\begin{aligned} 1 &= \sigma^m \\ &= (\tau_1 \cdots \tau_k)^m \\ &= \tau_1^m \cdots \tau_k^m. \end{aligned}$$

Again since $\tau_1, \ldots, \tau_k$ are all disjoint from each other, it follows that $\tau_i^m = 1$ for all $1 \leq i \leq k$: if $\tau_i^m(a) \neq a$ for some $a \in [n]$ and $1 \leq i \leq k$, then

$$\begin{aligned} a &= 1(a) \\ &= \tau_1^m \cdots \tau_i^m \cdots \tau_k^m(a) \\ &= \tau_1^m \cdots \tau_i^m(a) \\ &= \tau_i^m(a) \end{aligned}$$

would be a contradiction. It follows that $m_i \mid m$ for each $1 \leq i \leq k$. To see that m is the *least* common multiple, we just need to show that if $n \in \mathbb{N}$ such that $m_i \mid n$ for all $1 \leq i \leq k$, then $m \mid n$. Indeed, in this case, we have

$$\begin{aligned} \sigma^n &= (\tau_1 \cdots \tau_k)^n \\ &= \tau_1^n \cdots \tau_k^n \\ &= 1^n \cdots 1^n \\ &= 1, \end{aligned}$$

which implies $m \mid n$. □

Definition 6.1. A **transposition** is a 2-cycle $(a, b) \in S_n$

Lemma 6.1. *Every cycle from S_n can be written as a product of transpositions.*

Proof. $(a_1, a_2, \ldots, a_k) = (a_1, a_2)(a_2, a_3) \cdots (a_{k-1}, a_k)$ □

Example 6.1. Write $(1, 2, 3) \in S_3$ as a product of transpositions: $(1, 2, 3) = (1, 2)(2, 3) = (1, 3)(1, 2)$

Proposition 6.3. *Every $\sigma \in S_n$ $(n \geq 2)$ can be written as a product of transpositions.*

Proof. Write σ as a product of disjoint cycles

$$\sigma = \tau_1 \cdots \tau_k$$

Now write τ_i as a product of transpositions for all $1 \leq i \leq k$. □

6.2 Conjugacy Classes in S_n

Lemma 6.2. *For any cycle $(i_1, \ldots, i_k)$ in S_n and any $\sigma \in S_n$,*

$$\sigma(i_1, \ldots, i_k)\sigma^{-1} = (\sigma(i_1), \ldots, \sigma(i_k)).$$

Proof. Let $\pi = \sigma(i_1, \ldots, i_k)\sigma^{-1}$. First we show π and takes $\sigma(i_j)$ to $\sigma(i_{j+1})$ for all $1 \leq j \leq k$.

$$\begin{aligned} \pi(\sigma(i_j)) &= (\sigma(i_1, \ldots, i_k)\sigma^{-1})(\sigma(i_j)) \\ &= (\sigma(i_1, \ldots, i_k)\sigma^{-1}\sigma)(i_j) \\ &= (\sigma(i_1, \ldots, i_k))(i_j) \\ &= \sigma(i_{j+1}) \end{aligned}$$

Next we show π fixes everything else. So pick $x \in \{1, \ldots, n\} \setminus \{\sigma(i_1), \ldots, \sigma(i_k)\}$. Since $x \neq \sigma(i_j)$ for any $1 \leq j \leq k$, $\sigma^{-1}(x)$ is not i_j for any $1 \leq j \leq k$. Therefore, the cycle $(i_1, \ldots, i_k)$ does not move $\sigma^{-1}(x)$. So we have

$$\begin{aligned} \pi(x) &= (\sigma(i_1, \ldots, i_k)\sigma^{-1})(x) \\ &= \sigma((i_1, \ldots, i_k))(\sigma^{-1}(x))) \\ &= \sigma(\sigma^{-1}(x)) \\ &= x \end{aligned}$$

□

We show that all cycles of the same length in S_n are conjugate. Pick any two k-cycles, say $(a_1, \ldots, a_k)$ and $(b_1, \ldots, b_k)$. Choose $\sigma \in S_n$ such that $\sigma(a_i) = b_i$ for all $1 \leq i \leq k$. Then by Lemma (6.2), we see that conjugation by σ carries the first k-cycle to the second.

Definition 6.2. Let $\sigma \in S_m$. Write σ as a product of disjoint cycles $\sigma = \pi_1 \pi_2 \cdots \pi_k$. The **cycle type** of σ is the sequence $(1^{e_1}, 2^{e_2}, \ldots, m^{e_m})$ where e_i is the number of i-cycles in the product factorization of σ.

Example 6.2. Let $\sigma = (1,3,5)(2,7)(9,8,13)(4,6,10,11,12)$. Then the cycle type of σ is $(2, 3^2, 5)$.

For $\sigma, \tau \in S_m$, denote $\sigma^\tau = \tau\sigma\tau^{-1}$. Now write σ as a product of disjoint cycles $\sigma = \pi_1 \pi_2 \cdots \pi_k$. Then

$$\begin{aligned}
\sigma^\tau &= \tau\sigma\tau^{-1} \\
&= \tau\pi_1\pi_2 \cdots \pi_k\tau^{-1} \\
&= \tau\pi_1\tau^{-1}\tau\pi_2\tau^{-1} \cdots \tau\pi_k\tau^{-1} \\
&= \pi_1^\tau \pi_2^\tau \cdots \pi_k^\tau.
\end{aligned}$$

So σ^τ has the same cycle type as σ.

Proposition 6.4. *Let $\sigma, \tau \in S_m$. Then σ and τ are conjugate if and only if they have the same cycle type.*

6.3 The Alternating Group

Definition 6.3. A permutation $\sigma \in S_n$ is **even** if σ can be written as a product of an even number of transpositions. A permutation $\tau \in S_n$ is **odd** if τ is a product of an odd number of transpositions. We denote A_n to be the set of all even permutations.

Example 6.3. Any 3-cycle $(a,b,c) = (a,b)(b,c)$ is even. Any 4-cycle $(a,b,c,d) = (a,b)(b,c)(c,d)$ is odd.

Lemma 6.3. *The identity cannot be written as product of an odd number of transpositions.*

Proof. Write the identity as some product of transpositions:

$$(1) = (a_1, b_1)(a_2, b_2) \cdots (a_k, b_k), \tag{19}$$

where $k \geq 1$ and $a_i \neq b_i$ for all i. We will prove k is even.

The product on the right side of (19) can't have $k = 1$ since it is the identity. Suppose by induction that $k \geq 3$ and we know any product of fewer than k transpositions that equals the identity involves an even number of transpositions.

One of the $a_i's$ or $b_i's$ in the transpositions (a_i, b_i) for $i = 2, 3, \ldots, k$ has to be a_1, otherwise the permutation $(a_1, b_1)(a_2, b_2) \cdots (a_k, b_k)$ would map a_1 to b_1, and hence wouldn't be the identity permutation. Since $(a,b) = (b,a)$, we can one of the $a_i's$ in the transpositions (a_i, b_i) for $i = 2, 3, \ldots, k$ has to be a_1. Using different letters to denote different numbers, the formulas

$$(c,d)(a,b) = (a,b)(c,d), \quad (b,c)(a,b) = (a,c)(b,c)$$

show any product of two transpositions in which the second factor moves a and the first factor does not move a can be written as a product of two transpositions in which the first factor moves a and the second factor does not move a. Therefore, without changing the number of transpositions in (19), we can push the position of the second most left transposition in (19) that moves a_1 to the position right after (a_1, b_1), and thus we can assume $a_2 = a_1$.

If $b_2 = b_1$, then the product $(a_1, b_1)(a_2, b_2)$ in (19) is the identity and we can remove it. This reduces (19) to a product of $k - 2$ transpositions. By induction, $k - 2$ is even so k is even.

If instead $b_2 \neq b_1$, then the product $(a_1, b_1)(a_2, b_2)$ is equal to $(a_1, b_2)(b_1, b_2)$. Therefore (19) can be rewritten as

$$(1) = (a_1, b_2)(b_1, b_2)(a_3, b_3) \cdots (a_k, b_k), \tag{20}$$

where only the first two factors on the right have been changed. Now run through the argument again with (20) in place of (19). It involves the same number k of transpositions, but there are fewer transpositions in the product that move a_1 since we used to have (a_1, b_1) and (a_1, b_2) in the product and now we have (a_1, b_2) and (b_1, b_2).[1]

Some transposition other than (a_1, b_2) in the new product (20) must move a_1, so by the same argument as before either we will be able to reduce the number of transpositions by 2 and be done by induction or we will be able

[1] Since (a_1, b_1) and (a_1, b_2) were assumed all along to be honest transpositions, b_1 and b_2 do not equal a_1, so (b_1, b_2) doesn't move a_1.

to rewrite the product to have the same total number of transpositions but drop by 1 the number of them that move a_1. This rewriting process eventually has to fall into the case where the first two transpositions cancel out, since we can't wind up with (1) as a product of transpositions where only the first one move a_1. Thus we will be able to see that k is even.

□

Proposition 6.5. *A permutation $\sigma \in S_n$ is either even or odd, but not both.*

Proof. Suppose we can write $\sigma = \tau_1 \cdots \tau_k$ and $\sigma = \tau_1' \cdots \tau_m'$ where k is even and m is odd. Then this implies (1) is odd.:$(1) = \tau_1 \cdots \tau_k \tau_1' \cdots \tau_m'$. □

Proposition 6.6. *$A_n \trianglelefteq S_n$ and $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$.*

Proof. Let $\varepsilon : S_n \to \{\pm 1\}$ be the map which sends an even permutation to 1 and an odd permutation to -1. First we show this is a homomorphism. Suppose $\sigma, \tau \in S_n$. If both σ, τ are even, then $\sigma\tau$ is even. If σ is even and τ is odd, then $\sigma\tau$ is odd. If σ, τ are both odd, then $\sigma\tau$ is odd. In all cases, we can see that ε is indeed a homomorphism. Now we have $A_n = \text{Ker}\varepsilon = \{\sigma \in S_n \mid \sigma \text{ is even}\}$. By the first isomorphism theorem, we have $S_n / A_n \cong \{\pm 1\}$. This implies $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$. □

Example 6.4. In S_3, we have $A_3 = \{(), (1,2,3), (3,2,1)\}$.

Simplicity of A_n

Lemma 6.4. *For $n \geq 3$, A_n is generated by 3-cycles. For $n \geq 5$, A_n is generated by permutations of type $(2,2)$.*

Proof. The identity is $(1,2,3)^3$, a product of 3-cycles. Any even permutation σ has the form

$$\sigma = \prod_{k=1}^{m} (i_k, i_{k+1})(i_{k+2}, i_{k+3}),$$

where $i_k \in \{1, \ldots, n\}$ such that $i_k < i_{k+1}$ and $i_{k+2} < i_{k+3}$. r is even. If $i_{k+1} = i_{k+2}$, then $(i_k, i_{k+1})(i_{k+2}, i_{k+3}) = (i_k, i_{k+1}, i_{k+3})$, so

$$\sigma = \prod_{k=1}^{m} (i_k, i_{k+1}, i_{k+3}).$$

If $i_{k+1} \neq i_k$, then

$$\begin{aligned}(i_k, i_{k+1})(i_{k+2}, i_{k+3}) &= (i_k, i_{k+1})(i_{k+1}, i_{k+2})(i_{k+1}, i_{k+2})(i_{k+2}, i_{k+3}) \\ &= (i_k, i_{k+1}, i_{k+2})(i_{k+1}, i_{k+2}, i_{k+3}).\end{aligned}$$

So

$$\sigma = \prod_{k=1}^{m} (i_k, i_{k+1}, i_{k+2})(i_{k+1}, i_{k+2}, i_{k+3}).$$

In either case, we can write σ as a product of 3-cycles. To show permutations of type $(2,2)$ generate A_n for $n \geq 5$, it suffices to write any 3-cycle (a,b,c) in terms of such permutations. Pick $d, e \notin \{a,b,c\}$. Then note

$$(a,b,c) = (a,b)(d,e)(d,e)(b,c).$$

□

The 3-cycles in S_n are all conjugate in S_n, since permutations of the same cycle type in S_n are conjugate. Are 3-cycles conjugate in A_n? Not when $n = 4$: (123) and (132) are not conjugate in A_4. But for $n \geq 5$ we do have conjugacy in A_n.

Lemma 6.5. *For $n \geq 5$, any two 3-cycles in A_n are conjugate in A_n.*

Proof. We show every 3-cycle in A_n is conjugate within A_n to $(1,2,3)$. Let σ be a 3-cycle in A_n. It can be conjugated to $(1,2,3)$ in S_n:

$$(1,2,3) = \pi\sigma\pi^{-1}$$

for some $\pi \in S_n$. If $\pi \in A_n$, we're done. Otherwise, let $\pi' = (45)\pi$, so $\pi' \in A_n$ and

$$\pi'\sigma\pi'^{-1} = (1,2,3)$$

□

The basic argument to show that the groups A_n is simple for $n \geq 5$ is to show any non-trivial normal subgroup $N \trianglelefteq A_n$ contains a 3-cycle, so N contains every 3-cycle by Lemma (6.5), and therefore N is A_n by Lemma (6.4).

Theorem 6.6. *A_5 is simple.*

Proof. Suppose N is a normal subgroup of A_5. Pick $\sigma \in N$ with $\sigma \neq (1)$. The cycle structure of σ is (a,b,c), $(a,b)(c,d)$, or (a,b,c,d,e), where different letters represent different numbers. Since we want to show N contains a 3-cycle, we may suppose σ has the second or third cycle type. In the second case, N contains

$$((a,b,e)(a,b)(c,d)(a,b,e)^{-1})(a,b)(c,d) = (b,e)(c,d)(a,b)(c,d) = (a,e,b).$$

In the third case, N contains

$$((a,b,c)(a,b,c,d,e)(a,b,c)^{-1})(a,b,c,d,e)^{-1} = (b,c,a,d,e)(e,d,c,b,a) = (a,b,d).$$

Therefore N contains a 3-cycle, so $N = A_5$.

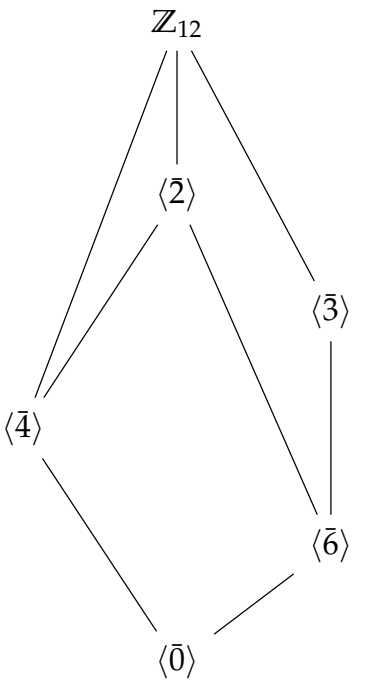
□

7 The Lattice of Subgroups of a Finite Group

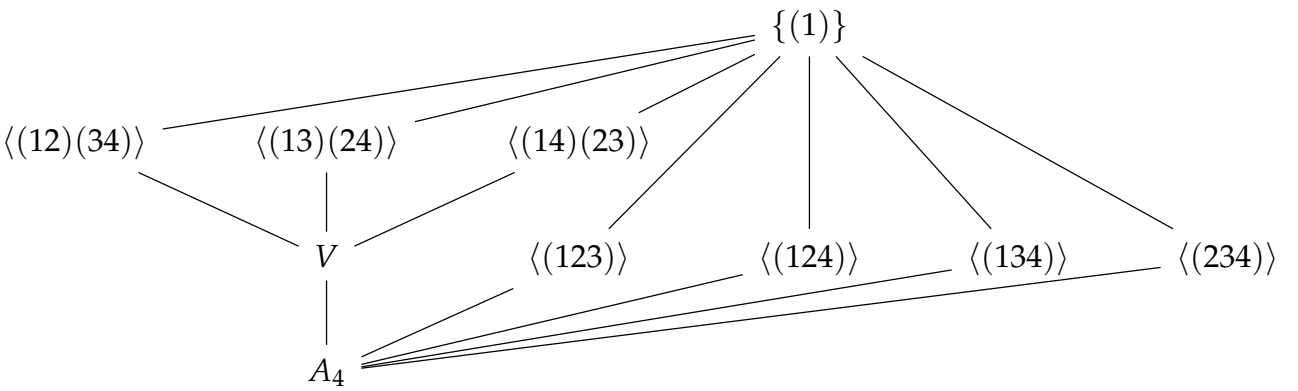
Let G be a group and A and B be subgroups of G. If $|A| > |B|$, then A is placed higher than B. If $B \leq A$ and there is no subgroup C such that $B \leq C \leq A$, then we draw a line from B to A.

Example 7.1. The lattice of subgroups of $\mathbb{Z}_8$ looks like this

Example 7.2. The lattice of subgroups of $\mathbb{Z}_{12}$ looks like this



Example 7.3. The lattice of subgroups of A_4 upside down looks like this



8 Finite Groups of Order ≤ 100

8.1 Groups of Order p^2

For each prime p, we will show that every group of order p^2 is abelian. In particular, it will then follow from the fundamental theorem of finite abelian groups that every group of order p^2 is isomorphic to one of the two possibilities, namely C_{p^2} or $C_p \times C_p$. First we begin with an important lemma.

Lemma 8.1. *Any p-group has nontrivial center.*

Proof. Suppose G is a p-group, say $|G| = p^n$, and assume for a contradiction that $|\mathrm{Z}(G)| = 1$. Let $x_1, \ldots, x_k$ represent the nontrivial conjugacy classes of G: so $|\mathrm{K}_{x_i}| > 1$ and $\mathrm{K}_{x_i} \cap \mathrm{K}_{x_j}$ for each $1 \leq i < j \leq k$ and

$$G = \mathrm{Z}(G) \cup \mathrm{K}_{x_1} \cup \cdots \cup \mathrm{K}_{x_k}.$$

Then the class equation gives us

$$|G| = |\mathrm{Z}(G)| + \sum_{i=1}^{k} [G : \mathrm{Z}(x_i)]. \tag{21}$$

Note that $p \mid [G : \mathrm{Z}(x_i)]$ for each $1 \leq i \leq k$. Indeed, $\mathrm{Z}(x_i)$ is a proper subgroup (otherwise x_i would not represent a nontrivial conjugacy class). Its order must divide the order of G by Lagrange's Theorem, thus $|\mathrm{Z}(x_i)| = p^{m_i}$ for some $m_i < n$. It follows that $[G : \mathrm{Z}(x_i)] = p^{n-m_i}$. With this understood, we now reduce (21) modulo p to get

$$0 \equiv 1 \bmod p,$$

which is a contradiction. □

Proposition 8.1. *Every group of order p^2 is abelian.*

Proof. Assume for a contradiction that $G \neq \mathrm{Z}(G)$. Since G is a p-group, $\mathrm{Z}(G)$ must be a nontrivial subgroup of G by Lemma (8.1). In particular, we must have $|\mathrm{Z}(G)| = p$. But then $|G/\mathrm{Z}(G)| = p$, which implies $G/\mathrm{Z}(G)$ is cyclic. It follows that G is abelian, which implies $G = \mathrm{Z}(G)$, a contradiction. So our assumption that $G \neq \mathrm{Z}(G)$ leads to a contradiction, which means we must in fact have $G = \mathrm{Z}(G)$. □

8.2 Groups of Order p^3

Let p be a prime. In this subsection, we classify all groups of order p^3. From the cyclic decomposition of finite abelian groups, there are three abelian groups of order p^3 up to isomorphism, namely C_{p^3}, $C_p \times C_{p^2}$, and C_p^3. These are nonisomorphic since they have different maximal orders for their elements: p^3, p^2, and p. We will show that there are two nonabelian groups of order p^3 up to isomorphism. The descriptions of these two groups will be different for $p = 2$ and $p \neq 2$, so we will treat these cases separately. First we need a lemma.

Lemma 8.2. *Let G be a nonabelian group of order p^3. Then*

1. $|\mathrm{Z}(G)| = p$;
2. $G/\mathrm{Z}(G) \cong C_p \times C_p$ *and;*
3. $[G, G] = \mathrm{Z}(G)$

Proof. 1. Since G is a p-group, $Z(G)$ must be a nontrivial subgroup of G by Lemma (8.1). Also since G is nonabelian, $Z(G)$ must be a proper subgroup of G. It follows that $|Z(G)| = p$ or $|Z(G)| = p^2$. Assume for a contradiction that $|Z(G)| = p^2$. Then $|G/Z(G)| = p$, which implies $G/Z(G)$ is cyclic, which is implies G is abelian, a contradiction. Thus $|Z(G)| = p$.

2. Since $|Z(G)| = p$, we have $|G/Z(G)| = p^2$. From the classification of groups of order p^2, we see that either $G/Z(G) \cong C_{p^2}$ or $G/Z(G) \cong C_p \times C_p$. If $G/Z(G) \cong C_{p^2}$, then $G/Z(G)$ is cyclic, which implies G is abelian, a contradiction. Thus $G/Z(G) \cong C_p \times C_p$.

3. Since $G/Z(G)$ is abelian, we see that $Z(G) \supseteq [G,G]$. Thus $|[G,G]| \mid p$, which means either $|[G,G]| = 1$ or $|[G,G]| = p$. We cannot have $|[G,G]| = 1$ since G is nonabelian, and so $|[G,G]| = p$. Thus we have $Z(G) \supseteq [G,G]$ and $|Z(G)| = |[G,G]|$ which implies This implies $Z(G) = [G,G]$. □

8.2.1 Case $p = 2$

Theorem 8.3. *A nonabelian group of order 8 is isomorphic to D_4 or Q_8.*

Proof. Let G be a nonabelian group of order 8. The nonidentity elements in G have order 2 or 4. If $g^2 = 1$ for all $g \in G$, then G is abelian, so some $x \in G$ must have order 4. Let $y \in G \backslash \langle x \rangle$. The subgroup $\langle x, y \rangle$ properly contains $\langle x \rangle$, so $\langle x, y \rangle = G$. Since G is nonabelian, x and y do not commute.

Since $\langle x \rangle$ has index 2 in G, it is a normal subgroup. Therefore $yxy^{-1} \in \langle x \rangle$, that is

$$yxy^{-1} \in \{1, x, x^2, x^3\}.$$

Since yxy^{-1} has order 4, we must have $yxy^{-1} = x$ or $yxy^{-1} = x^3 = x^{-1}$. Since x and y do not commute, we cannot have $yxy^{-1} = x$. Thus

$$yxy^{-1} = x^{-1}.$$

The group $G/\langle x \rangle$ has order 2. Therefore $y^2 \in \langle x \rangle$, that is

$$y^2 \in \{1, x, x^2, x^3\}.$$

Since y has order 2 or 4, we see that y^2 has order 1 or 2. Thus either $y^2 = 1$ or $y^2 = x^2$. Combining everything together, we see that either

$$G = \langle x, y \mid x^4 = 1, y^2 = 1, yxy^{-1} = x^{-1} \rangle$$

in which case $G \cong D_4$, or

$$G = \langle x, y \mid x^4 = 1, y^2 = x^2, yxy^{-1} = x^{-1} \rangle$$

in which case $G \cong Q_8$. □

8.2.2 Case $p \neq 2$

Now assume $p \neq 2$. The two nonabelian groups of order p^3, up to isomorphism, will turn out to be

$$\mathrm{Heis}(\mathbb{Z}/\langle p \rangle) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{Z}/\langle p \rangle \right\} \quad \text{and} \quad G_p = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a, b \in \mathbb{Z}/\langle p^2 \rangle,\ a \equiv 1 \bmod p \right\}.$$

These two constructions make sense if $p = 2$, but they turn out to be isomorphic to each other in that case. If $p \neq 2$, we can distinguish $\mathrm{Heis}(\mathbb{Z}/\langle p \rangle)$ from G_p by counting elements of order p. In $\mathrm{Heis}(\mathbb{Z}/\langle p \rangle)$, we have

$$\begin{aligned} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^p &= \begin{pmatrix} 1 & na & nb + \frac{p(p-1)}{2}ac \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & \frac{p(p-1)}{2}ac \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \end{aligned}$$

where the last equality follows since $p \neq 2$. Thus every nonidentity element in $\mathrm{Heis}(\mathbb{Z}/\langle p \rangle)$ has order p. On the other hand, $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in G_p$ has order p^2 since $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)^n = \left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$ for all $n \in \mathbb{Z}$. So $G_p \neq \mathrm{Heis}(\mathbb{Z}/\langle p \rangle)$. At the prime

$p = 2$, $\mathrm{Heis}(\mathbb{Z}/\langle p\rangle)$ and G_2 each contain more than one element of order 2, so both $\mathrm{Heis}(\mathbb{Z}/\langle p\rangle)$ and G_2 are isomorphic to D_4.

Let's perform some calculations. First we see what matrix multiplication in $\mathrm{Heis}(\mathbb{Z}/\langle p\rangle)$ looks like. We have

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+a' & b+b'+ac' \\ 0 & 1 & c+c' \\ 0 & 0 & 1 \end{pmatrix}$$

We can decompose any matrix in $\mathrm{Heis}(\mathbb{Z}/\langle p\rangle)$ as

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

and a particular commutator is

$$\left[\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \right] = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Thus we have

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = e_{23}^c e_{12}^a [e_{12}, e_{23}]^b$$

where e_{ij} denotes the matrix with 1 along the diagonal and at the (i,j)th spot and zero everywhere else where $1 \leq i < j \leq 3$.

Matrix multiplication in G_p looks like

$$\begin{pmatrix} 1+pm & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1+pm' & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1+p(m+m') & b+b'+pmb' \\ 0 & 1 \end{pmatrix}.$$

We can decompose any matrix in G_p as

$$\begin{pmatrix} 1+pm & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^b \begin{pmatrix} 1+p & 0 \\ 0 & 1 \end{pmatrix}^m$$

and a particular commutator is

$$\left[\begin{pmatrix} 1+p & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right] = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^p.$$

Thus we have

$$\begin{pmatrix} 1+pm & b \\ 0 & 1 \end{pmatrix} = e_{12}^p x^m$$

where $x = \left(\begin{smallmatrix} 1+p & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

Lemma 8.4. *Let G be a group and let $g, h \in G$. Suppose g and h commute with $[g,h]$. Then for all m and n in $\mathbb{Z}$, we have*

1. $[g^m, h^n] = [g,h]^{mn}$ *and;*
2. $g^n h^n = (gh)^n [g,h]^{\binom{n}{2}}$.

Proof. 1. We just need to show that for all $k \in \mathbb{N}$, we have

$$[g,h]^k = [g^k, h] = [g, h^k]. \tag{22}$$

We shall prove this by induction on k. The base case $k = 1$ is trivial, so assume that we have shown (22) for all $k < n$ for some $n \in \mathbb{Z}_{>1}$. Then we have

$$\begin{aligned}
[g,h]^n &= (ghg^{-1}h^{-1})^n \\
&= (ghg^{-1}h^{-1})(ghg^{-1}h^{-1})[g,h]^{n-2} \\
&= (g^2hg^{-1}h^{-1})(hg^{-1}h^{-1})[g,h]^{n-2} \\
&= (g^2hg^{-2}h^{-1})[g,h]^{n-2} \\
&= (g^2hg^{-2}h^{-1})[g^{n-2},h] \\
&= (g^2hg^{-2}h^{-1})(g^{n-2}hg^{-(n-2)}h^{-1}) \\
&= (g^nhg^{-2}h^{-1})(hg^{-(n-2)}h^{-1}) \\
&= g^nhg^{-n}h^{-1} \\
&= [g^n, h],
\end{aligned}$$

where we used the fact that g^{n-2} commutes with $[g,h]$ (which follows since g commutes with $[g,h]$). A similar computation also shows $[g,h]^n = [g,h^n]$.

2. We prove

$$g^k h^k = (gh)^k [g,h]^{\binom{k}{2}} \tag{23}$$

by induction on $k \in \mathbb{Z}_{\geq 2}$. Let us first work out the base case $k = 2$. We have

$$\begin{aligned} g^2h^2 &= gghh \\ &= ggh(g^{-1}h^{-1}hg)h \\ &= g[g,h]hgh \\ &= (gh)^2[g,h]. \end{aligned}$$

Now assume that we have shown (**??**) for all $k < n$ for some $n \in \mathbb{Z}_{>2}$. We have

$$\begin{aligned} (gh)^n[g,h]^{\binom{n}{2}} &= (gh)^n[g,h]^{\binom{n-1}{2}}[g,h]^{n-1} \\ &= gh(gh)^{n-1}[g,h]^{\binom{n-1}{2}}[g,h]^{n-1} \\ &= gh(g^{n-1}h^{n-1})[g,h]^{n-1} \\ &= gh[g,h]^{n-1}g^{n-1}h^{n-1} \\ &= [g,h]hg[g,h]^{n-1}g^{n-1}h^{n-1} \\ &= [g,h]^n hg^n h^{n-1} \\ &= [g^n,h]hg^n h^{n-1} \\ &= g^n hg^{-n}h^{-1}hg^n h^{n-1} \\ &= g^n hg^{-n}g^n h^{n-1} \\ &= g^n hh^{n-1} \\ &= g^n h^n. \end{aligned}$$

□

Theorem 8.5. *For primes $p \neq 2$, a nonabelian group of order p^3 is isomorphic to* $\mathrm{Heis}(\mathbb{Z}/\langle p\rangle)$ *or* G_p.

Proof. Let G be a nonabelian group of order p^3. Each $g \neq 1$ in G has order p or p^2. By Lemma (8.2), we can write $G/\mathrm{Z}(G) = \langle \overline{x}, \overline{y}\rangle$ and $\mathrm{Z}(G) = \langle z\rangle$. For $g \in G$, we have $g \equiv x^i y^j \bmod \mathrm{Z}(G)$ for some integers i and j, so

$$\begin{aligned} g &= x^i y^j z^k \\ &= z^k x^i y^j \end{aligned}$$

for some $k \in \mathbb{Z}$. If x and y commute, then G is abelian, which is a contradiction. Thus x and y do not commute. Therefore $[x,y] = xyx^{-1}y^{-1} \in \mathrm{Z}(G)$ is nontrivial, so $\mathrm{Z}(G) = \langle [x,y]\rangle$. Therefore we can use $[x,y]$ for z, showing $G = \langle x, y\rangle$.

Let's see what the product of two elements of G looks like. Using Lemma (8.4), we have

$$x^i y^j = y^j x^i [x,y]^{ij} \quad \text{and} \quad y^j x^i = x^i y^j [x,y]^{-ij}.$$

This shows we can move every power of y past every power of x on either side, at the cost of introducing a (commuting) power of $[x,y]$. So every element of $G = \langle x, y\rangle$ has the form $y^j x^i [x,y]^k$. A product of two such terms is

$$\begin{aligned} y^c x^a [x,y]^b \cdot y^{c'} x^{a'} [x,y]^{b'} &= y^c (x^a y^{c'}) x^{a'} [x,y]^{b+b'} \\ &= y^c (y^{c'} x^a [x,y]^{ac'}) x^{a'} [x,y]^{b+b'} \\ &= y^{c+c'} x^{a+a'} [x,y]^{b+b'+ac'}. \end{aligned}$$

Here the exponents are all integers. It appears that we have a homomorphism $\mathrm{Heis}(\mathbb{Z}/\langle p\rangle) \to G$ by

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mapsto y^c x^a [x,y]^b. \tag{24}$$

After all, we just showed multiplication of such triples $y^c x^a [x,y]^b$ behaves like multiplication in $\mathrm{Heis}(\mathbb{Z}/\langle p\rangle)$. But there is a catch: the matrix entries a, b, and c in $\mathrm{Heis}(\mathbb{Z}/\langle p\rangle)$ are integers modulo p, so the "function" (24) from $\mathrm{Heis}(\mathbb{Z}/\langle p\rangle)$ to G is only well-defined if x, y, and $[x,y]$ all have pth power 1 (so exponents on them only matter modulo p). Since $[x,y]$ is in the center of G, a subgroup of order p, its exponents only matter modulo p. But maybe x or y could have order p^2.

Well if x and y have both order p, then there is no problem with (24). It is a well-defined function from $\mathrm{Heis}(\mathbb{Z}/\langle p\rangle)$ to G that is a homomorphism. Since its image contains x and y, the image contains $\langle x,y\rangle = G$, so the function is onto. Both $\mathrm{Heis}(\mathbb{Z}/\langle p\rangle)$ and G have order p^3, so our surjective homomorphism is an isomorphism: $G \cong \mathrm{Heis}(\mathbb{Z}/\langle p\rangle)$.

What happens if x or y has order p^2? In this case we anticipate that $G \cong G_p$. In G_p two generators are $g = \left(\begin{smallmatrix} 1+p & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $h = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, where g has order p, h has order p^2, and $[g,h] = h^p$. We want to show our abstract G also has a pair of generators like this.

Starting with $G = \langle x,y\rangle$ where x or y has order p^2, without loss of generality let y have order p^2. It may or may not be the case that x has order p. To show we can change generators to make x have order p, we will look at the pth power function on G. For all $g \in G$, we have $g^p \in \mathrm{Z}(G)$ since $G/\mathrm{Z}(G) \cong C_p^2$. Moreover, the pth power function on G is a homomorphism: by Lemma (8.4), we have $(gh)^p = g^p h^p [g,h]^{p(p-1)/2}$ and $[g,h]^p = 1$ since $[G,G] = \mathrm{Z}(G)$ has order p, so

$$(gh)^p = g^p h^p.$$

Since y^p has order p and $y^p \in \mathrm{Z}(G)$, we have $\mathrm{Z}(G) = \langle y^p\rangle$. Therefore $x^p = (y^p)^r$ for some $r \in \mathbb{Z}$ and since the pth power function on G is a homomorphism we get $(xy^{-r})^p = 1$ with $xy^{-r} \neq 1$ since $x \notin \langle y\rangle$. So xy^{-r} has order p and $G = \langle x,y\rangle = \langle xy^{-r}, y\rangle$. We now rename xy^{-r} as x, so $G = \langle x,y\rangle$ where x has order p and y has order p^2.

We are not guaranteed that $[x,y] = y^p$, which is one of the relations for the two generators of G_p. How can we force this relation to occur? Well, since $[x,y]$ is a nontrivial element of $[G,G] = \mathrm{Z}(G)$, we have $\mathrm{Z}(G) = \langle [x,y]\rangle = \langle y^p\rangle$, so

$$[x,y] = (y^p)^k \tag{25}$$

where $k \not\equiv 0 \bmod p$. Let ℓ be a multiplicative inverse for k mod p and raise both sides of (25) to the ℓth power: using Lemma (8.4), $[x,y]^\ell = (y^{pk})^\ell$ implies $[x^\ell, y] = y^p$. Since $\ell \not\equiv 0 \bmod p$, we have $\langle x\rangle = \langle x^\ell\rangle$, so we can rename x^ℓ as x: now $G = \langle x,y\rangle$ where x has order p, y has order p^2, and $[x,y] = y^p$.

Because $[x,y]$ commutes with x and y and $G = \langle x,y\rangle$, every element of G has the form

$$y^j x^i [x,y]^k = [x,y]^k y^j x^i = y^{pk+j} x^i.$$

Let's see how such products multiply:

$$\begin{aligned} y^b x^m \cdot y^{b'} x^{m'} &= y^b (x^m y^{b'}) x^{m'} \\ &= y^b (y^{b'} x^m [x,y]^{mb'}) x^{m'} \\ &= y^{b+b'} x^m (y^p)^{mb'} x^{m'} \\ &= y^{b+b'+pmb'} x^{m+m'}. \end{aligned}$$

So we get a homomorphism $G_p \to G$ by

$$\begin{pmatrix} 1+pm & b \\ 0 & 1 \end{pmatrix} \mapsto y^b x^m.$$

This function is well-defined since on the left side m matters modulo p and b matters modulo p^2 which $x^p = 1$ and $y^{p^2} = 1$. This homomorphism is onto since x and y are in the image, so it is an isomorphism since G_p and G have equal order: $G \cong G_p$. □

8.3 Finite Groups of Order 24

Theorem 8.6. *If $|G| = 24$, then G has a normal subgroup of size 4 or 8.*

Proof. Let P be a 2-Sylow subgroup, so $|P| = 8$. Consider the left multiplication map $\ell\colon G \to \mathrm{Sym}(G/P) \cong S_3$, given by $g \mapsto \ell_g$, where

$$\ell_g(\overline{x}) = \overline{gx}$$

for all $\overline{x} \in G/P$. Set K to be the kernel of ℓ. Then $K \subseteq P$, which implies $|K| \mid 8$. Also G/K embeds into S_3, which implies $[G:K] \mid 6$, that is, $4 \mid K$. Thus we have either $|K| = 4$ or $|K| = 8$. Since K is the kernel of ℓ, we see that K is a normal subgroup. □

Example 8.1. Consider the group $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$. The order of this group is

$$\#\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) = (3^2-1)(3^2-3) = 48.$$

It has as a normal subgroup $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$. Indeed, $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ is the kernel of the determinant map

$$\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) \to (\mathbb{Z}/3\mathbb{Z})^\times.$$

Also, since $\#(\mathbb{Z}/3\mathbb{Z})^\times = 2$, we have

$$\#\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z}) = 48/2 = 24.$$

It follows from Theorem (8.6) that $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ contains a normal subgroup of size 4 or 8.