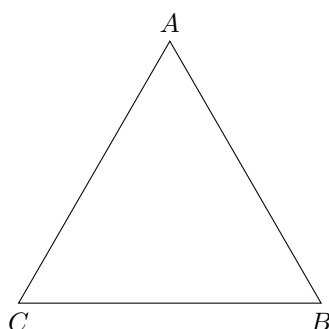


# MAT347 Abstract Algebra

Jonah Chen

## 1 GROUPS

Groups are generally associated with symmetries. Consider the equilateral triangle:



We know that there are six symmetries of the triangle:

- Identity transformation (do nothing) denoted as  $\text{id}$  or  $e$
- Two rotations ( $A \rightarrow B \rightarrow C \rightarrow A$  and  $A \rightarrow C \rightarrow B \rightarrow A$ )
- Three reflections  $A \leftrightarrow B$ ,  $A \leftrightarrow C$ ,  $B \leftrightarrow C$

Note that these symmetries preserve the structure of the triangle, hence the composition of two symmetries must also be a symmetry. Let

- $\rho$  be the rotation  $A \rightarrow B \rightarrow C \rightarrow A$
- $\sigma$  be the reflections  $B \leftrightarrow C$

Note that  $\rho\sigma$  is the  $A \leftrightarrow C$  reflection and  $\sigma\rho$  is the  $A \leftrightarrow B$  reflection. Hence they may not be commutative.

We also know that all symmetries can be reversed.  $\alpha$  has an inverse  $\alpha^{-1}$  such that  $\alpha\alpha^{-1} = \alpha^{-1}\alpha = e$ . These inspires the following definition:

**Definition—:** A **group** is a set  $G$  with a composition

$$G \times G \rightarrow G \tag{1}$$

$$(g, h) \mapsto g \cdot h \tag{2}$$

Satisfying:

- Associativity:  $(g \cdot h) \cdot k = g \cdot (h \cdot k)$

- Identity:  $\exists e \in G$  such that  $g \cdot e = e \cdot g = g$  for all  $g \in G$
- Inverse:  $\forall g \in G, \exists g^{-1} \in G$  such that  $g \cdot g^{-1} = g^{-1} \cdot g = e$

Examples:

- $\mathbb{Z}$  with  $+$  is a group. It is associative,  $e = 0$  and  $g^{-1} = -g$ .
- $\mathbb{Z}/n\mathbb{Z}$  with addition modulo  $n$ .
- If  $F$  is a field, it implicitly has two group structures:
  - Additive group:  $(F, +)$  is a group. It is associative,  $e = 0$  and  $g^{-1} = -g$ .
  - Multiplicative group:  $(F \setminus \{0\}, \times)$  is a group. It is associative,  $e = 1$  and  $g^{-1} = 1/g$ .
- $GL(n, F)$  – “general linear group” contains all invertible  $n \times n$  matrices.
- $SL(n, F)$  – “special linear group” contains all invertible  $n \times n$  matrices with determinant 1.
- $SO(n, F)$  – “special orthogonal group”  $= \{A \in SL(n, F) | A^t = A^{-1}\}$ .

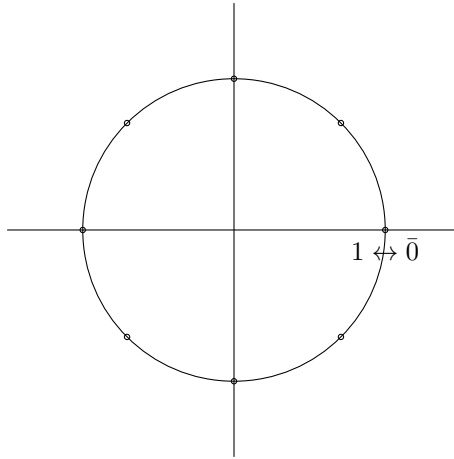
## 1.1 CYCLIC GROUPS

One of the simplest groups is  $\mathbb{Z}/n\mathbb{Z}$  for  $n \in \mathbb{N}$  with the operation addition modulo  $n$ . This is known as the “cyclic group of order  $n$ ” or  $C_n$ . i.e. for  $n = 8$ ,  $5 + 7 = 4 \pmod{8}$ , which we denote  $\bar{5} + \bar{7} = \bar{4}$ .

We know the inverse  $\bar{k}^{-1} = \overline{n - k}$  for nonzero  $k$  or  $\bar{0}^{-1} = \bar{0}$ .

Another way to express the cyclic group is  $\bar{k} \leftrightarrow e^{2\pi i k/n}$  with multiplication operation. Then,

$$\overline{k+n} = e^{2\pi i(k+n)/n} = e^{2\pi i k/n} e^{2\pi i n/n} = e^{2\pi i k/n} = \bar{k}. \quad (3)$$



**Definition–Order:** The **order** of a group  $G$  is its cardinality denoted  $\text{ord}(G)$  or  $|G|$ . It could be a finite or infinite ordinal. In particular,  $|C_n| = n$ .

## 1.2 QUATERNION GROUP

The quaternion group  $\mathbb{H} = \{\pm 1, \pm i, \pm j, \pm k\}$  is a group of order 8 with the multiplication operation. It has

**Definition–Subgroup:** A **subgroup** of a group  $G$  is a subset  $H \subseteq G$  such that  $H$  is a group.

**Definition–Coset:** If  $G$  is a group and  $H \leq G$ , consider sets of the form

$$Hg = \{hg | h \in H\} \quad (4)$$

This is a **right coset** of  $H$ .

**Theorem–Partitioning with Cosets:** Consider  $Hg$  and  $Hg'$  for  $g, g' \in G$ . There are two cases:

- They might be disjoint:  $Hg \cap Hg' = \emptyset$ .
- They might intersect. Suppose  $hg = h'g'$  for some  $h, h' \in H$

$$h^{-1}hg = h^{-1}h'g' \quad (5)$$

$$g = h^{-1}h'g' \in Hg' \quad (6)$$

Similarly,  $g' \in Hg$ . Consider an arbitrary element of  $Hg$  with  $k \in H$ . Then,  $kg = kh^{-1}h'g' \in Hg'$  i.e.  $Hg \leq Hg'$ . Similarly,  $Hg' \leq Hg$ . Thus,  $Hg = Hg'$ .

The right cosets of  $H$  partition  $G$ . In particular,

$$G = \bigsqcup Hg_i \quad (7)$$

For fixed  $g$ , if  $hg = h'g$  for  $h, h' \in H$  then  $hgg^{-1} = h'gg^{-1}$  so  $h = h'$ . So in  $Hg$ , every element can be matched with an element of  $H$ . So,  $|Hg| = |H|$ .

**Theorem–Lagrange:** If  $|G| < \infty$  and  $H \leq G$ , then  $|H| \mid |G|$

**Definition–Index:** For  $H \leq G$ , the **index** of  $H$  in  $G$  is  $[G : H] = |G|/|H|$ .

If  $|G| = 13$ , the only subgroups of  $G$  are  $\{e\}, G$ .

If  $G = \mathbb{Z}$  and  $H = 2\mathbb{Z}$  (even numbers). Then  $H + 0 = H$  is one coset, and  $H + 1$  = the odd integers is another coset. So,  $\mathbb{Z} = (2\mathbb{Z}) \sqcup (2\mathbb{Z} + 1)$ .

Same for Left Cosets Interaction of left and right cosets?

Consider the triangle group with rotations  $e, \rho, \rho^2$  and reflections  $\sigma_A, \sigma_B, \sigma_C$ . Consider the subgroup  $H = \{e, \sigma_A\}$ .

$$He = \{e, \sigma_A\} \quad (8)$$

$$H\rho = \{\rho, \sigma_B\} \quad (9)$$

$$H\rho^2 = \{\rho^2, \sigma_C\} \quad (10)$$

$$eH = \{e, \sigma_A\} \quad (11)$$

$$\rho H = \{\rho, \sigma_C\} \quad (12)$$

$$\rho^2 H = \{\rho^2, \sigma_B\} \quad (13)$$

Note that the left and right cosets are different. They are the same if the group is commutative.

**Definition–Action:** An **action** of a group  $G$  on a set  $X$  is a map

$$G \times X \rightarrow X \quad (14)$$

$$(g, x) \mapsto gx \quad (15)$$

such that

$$(gh)x = g(hx) \quad (16)$$

$$ex = x \quad (17)$$

If  $G$  is a group, it acts on itself. This is called a “left translation” or “left regular action”.

How about the right action  $(g, x) \mapsto xg$ . The second condition may not be true

$$(gh, x) = xgh \quad (18)$$

$$(g, (hx)) = (g, xh) = xhg \quad (19)$$

which is not true. Instead, let  $(g, x) = xg^{-1}$ . Then,

$$(gh, x) = x(gh)^{-1} = xh^{-1}g^{-1} \quad (20)$$

$$(g, (hx)) = (g, xh^{-1}) = xh^{-1}g^{-1} \quad (21)$$

This is the definition of the right action.

There is a third action of  $G$  on itself by  $(g, x) = xgx^{-1}$ . This action is called conjugation.

Take the following example: Let  $G = SO(3)$  and let  $X = S^2$ .  $G$  acts on  $X$  by rotation. Let  $H = \left\{ \begin{pmatrix} \cos \theta & -\sin \theta & 0 \\ \sin \theta & \cos \theta & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\}$  be the subgroup of rotations that fixes the  $z$ -axis.

$H$  also acts on  $X$  ??

**Definition–Orbit:** If  $G$  acts on  $X$ , the **orbit** of  $x \in X$  is the set  $Gx = \{gx | g \in G\}$ . i.e. the set of all points  $x$  is taken to by elements of  $G$ .

The orbits of  $H \approx SO(2)$  on the sphere are the lines of latitude (and the north and south poles).

$H$  fixes the north pole, thus every coset  $gH$  takes the north pole to a point. Suppose  $gH$  and  $g'H$  are cosets such that  $gHN = g'HN \implies gN = g'N \implies (g')^{-1}gN = N \implies (g')^{-1}g \in H \implies gH \dots$  so the points ofn the sphere are in 1-1 correspondence with the left cosets of  $H$ .

**Definition–Stabilizer:** If  $G$  acts on  $X$  and  $x \in X$ , the “stabilizer” of  $x$  in  $G$  is  $\{g \in G | gx = x\}$

**Definition–Centralizer:** If  $A \subset G$ , the **centralizer** of  $A$  in  $G$  is  $C_G(A) = \{g \in G | ga = ag \forall a \in A\}$

- If  $G$  is abelian, then  $C_G(A) = G$  for any  $A$ .
- In the triangle group,  $C_G(\{\rho\}) = \{e, \rho, \rho^2\}$

**Definition–Center:** The **center** of  $G$  is  $Z(G) = \{g \in G | gg' = g'g \forall g' \in G\} = C_G(G)$

**Proposition:** For any  $A \subset G$ ,  $C_G(A) \leq Z(G)$  (is a subgroup).

Consider the regular  $n$ -gon ( $n \geq 3$ ), what are its rigid motion symmetries?

- There are always  $n$  rotations by  $\frac{2\pi}{n}$  about the origin.
- When  $n$  is even, there are  $n/2$  reflections in each pair of edges, and each pair of vertices. When  $n$  is odd, there are  $n$  reflections in each pair of (edge, vertex). There are always  $n$  reflections.
- Write  $\rho$  for clockwise rotation by  $\frac{2\pi}{n}$ . Fix one vertex and let  $\sigma$  be the reflection that fixes that vertex.
- Note that  $\rho\sigma = \sigma\rho^{-1}$ . To show this, it suffices to find where two of the vertices gets mapped.

**Proposition:** The symmetries are  $e, \rho, \rho^2, \dots, \rho^{n-1}, \sigma, \sigma\rho, \sigma\rho^2, \dots, \sigma\rho^{n-1}$

**Definition–dihedral group:** The group of symmetries of the regular  $n$ -gon is  $D_{2n}$ , the **dihedral group** of order  $2n$ .

Given  $H \leq G$  we write  $G/H$  as the set of left cosets

$$G/H = \{gH | g \in G\} \quad (22)$$

$$H \setminus G = \{Hg | g \in G\} \quad (23)$$

Both of these are called “ $G \bmod H$ ”. In general, the two are different.

Now we want to ask, is  $H \setminus G$  a group?

- The most naive idea is to reuse multiplication in  $G$ , i.e.  $Hg \cdot Hg' = Hgg'$ , but it only sometimes works.
- This formula means:  $hg \cdot h'g' = h''gg'$ . For any  $h, h' \in H, \exists h''$  s.t. this holds.
- Trick:  $hg \cdot h'g' = hgh'e'g' = hgh'(g^{-1}g)g' = h(ghg^{-1})gg'$ . Now we can ask if  $ghg^{-1} \in H$  (for every  $h' \in H$ )

**Definition–Normal Subgroup:** A subgroup  $H \leq G$  is **normal** if  $ghg^{-1} \in H \forall g \in G, h \in H$ , which is abbreviated as  $gHg^{-1} = H$ .  $H \trianglelefteq G$  means  $H$  is a normal subgroup of  $G$

- Notice that if  $gHg^{-1} = H$  then  $gH = Hg$ . So  $H$  is normal, the left and right cosets must be the same.

**Definition–Quotient Group:** If  $H \trianglelefteq G$ , then  $G/H$  is called the quotient group.

### 1.3 HOMOMORPHISMS

**Definition–Homomorphism:** If  $G, K$  are groups, a **homomorphism** is a map  $\varphi : G \rightarrow K$  such that  $\varphi(gg') = \varphi(g)\varphi(g') \forall g, g' \in G$ .

Observations: IF  $\varphi : G \rightarrow K$  is a homomorphism and  $g \in G$ , then

1.  $\varphi(g) = \varphi(eg) = \varphi(e)\varphi(g)$ , so  $\varphi(e) = e$  (the identity element of  $K$ )
2.  $e = \varphi(e) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1})$ , so  $\varphi(g^{-1}) = \varphi(g)^{-1}$

#### Examples

- $G = \mathbb{Z}$  and  $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}, \varphi(n) = 2n$  is a homomorphism, as  $\varphi(n+m) = 2(n+m) = 2n+2m = \varphi(n) + \varphi(m)$
- $G = \mathbb{Z}, K = \mathbb{R}$  and  $\varphi : \mathbb{Z} \rightarrow \mathbb{R}, \varphi(n) = n$ . This mapping is called an **inclusion** as  $\mathbb{Z} \subset \mathbb{R}$ .
- If  $G$  is a group and  $g_0 \in G$ , then  $C_{g_0} : G \rightarrow G, g \mapsto g_0 g g_0^{-1}$  is a homomorphism.
- A linear transformation  $T : V \rightarrow W$  if  $V, W$  are vector spaces (the additive group).
- Note that  $\varphi : g \mapsto g^{-1}$  is **only** a homomorphism if  $G$  is abelian.

**Definition–Kernel/Image:** If  $\varphi : G \rightarrow G'$  is a homomorphism, then the **kernel** of  $\varphi$  is

$$\ker(\varphi) = \{g \in G \mid \varphi(g) = e\}. \quad (24)$$

The **image** of  $\varphi$  is

$$\text{im}(\varphi) = \{\varphi(g) \mid g \in G\} \subseteq G' \quad (25)$$

**Theorem–:**  $\ker(\varphi) \leq G$  and  $\text{im}(\varphi) \leq G' \quad \ker(\varphi) \leq G$

*Proof.* Since  $\varphi(e) = e$ ,  $e \in \ker(\varphi)$ , and  $e \in \text{im}(\varphi)$ . So both are nonempty. Suppose  $g, h \in \ker(\varphi)$ ,  $e = \varphi(e) = \varphi(hh^{-1}) = \varphi(h)\varphi(h^{-1}) \dots$  □

- Suppose  $N \leq G$  and then define  $G \rightarrow G/N, g \mapsto Ng$ . We claim this is a homomorphism. Proof is simple  $\varphi(gg') = Ng g', \varphi(g)\varphi(g') = NgNg' = NgN(g^{-1}gg') = N(gNg^{-1})gg' = NNgg' = Ng g'$
- This map is called the (natural) **projection** of  $G$  onto  $G/N$ . Sometimes written  $\Pi_{G/N}$  or  $\text{proj}_{G/N}$ .
- $\text{im}(\Pi_{G/N}) = G/N$  and  $\ker(\Pi_{G/N}) = N$ .
- Any homomorphism is related to this one, so this could be considered as the “generic homomorphism”.

**Definition–Isomorphism:** If  $\varphi : G \rightarrow H$  is a homomorphism, and  $\ker(\varphi) = \{e\}$  then  $\varphi$  is injective. If  $\varphi(G) = H$  then  $\varphi$  is surjective. Thinking of  $G$  and  $H$  as sets, there is an inverse  $\varphi^{-1} : H \rightarrow G$  such that  $\varphi^{-1} \circ \varphi = 1_G$  and  $\varphi \circ \varphi^{-1} = 1_H$ . It is easy to check that  $\varphi^{-1}$  is also a homomorphism. In this case,  $\varphi$  is an **isomorphism**

- Suppose we have an injective homomorphism  $\varphi : G \rightarrow H$  where  $\ker(\varphi) = \{e\}$ . Then, we can consider  $\varphi : G \rightarrow \text{im}(\varphi) < H$ . Sometimes we say  $\varphi : G \rightarrow H$  is an **isomorphism into**  $H$ , as opposed to an isomorphism **onto**  $H$  or between  $G$  and  $H$ .

**Definition–Automorphism:** If  $G$  is a group, an **automorphism** of  $G$  is an isomorphism  $\varphi : G \rightarrow G$ .

#### Examples:

- If  $G = \mathbb{Z}$ ,  $n \mapsto -n$  is the only automorphism apart from the identity.
- If  $G$  is abelian,  $g \mapsto g^{-1}$  is an automorphism.
- If  $F$  is a field, and  $G = GL(n, F)$  then  $g \mapsto (g^t)^{-1}$  (transposed inverse) is an automorphism.
- If we fix  $g_0 \in G$  then the conjugation  $C_{g_0} : G \rightarrow G$  where  $C_{g_0}(g) = g_0 g g_0^{-1}$  is an automorphism.

**Definition—Automorphism Group:**  $\text{Alt}(G)$  is the **group** of automorphisms of  $G$ .

**Definition—Inner/Outer Automorphisms:** The **inner automorphisms** of  $G$  are

$$\text{Inn}(G) = \{\varphi \in \text{Alt}(G) \mid \varphi = C_{g_0} \text{ for some } g_0 \in G\}. \quad (26)$$

If an element of  $\text{Alt}(G)$  that is not inner is **outer**.

- It is easy to show that  $\text{Inn}(G) \leq \text{Alt}(G)$ .
- Observe that if  $G$  is abelian, then  $\text{Inn}(G) = \{\text{id}\}$
- In general,  $\{\text{id}\} \leq \text{Inn}(G) \leq \text{Alt}(G)$ .
- The map

$$G \rightarrow \text{Alt}(G) \quad (27)$$

$$g \mapsto C_g \quad (28)$$

is a homomorphism. Its image is  $\text{Inn}(G)$  and its kernel is  $Z_G$  (the center).

**Definition—Fiber:** If  $p$  is a projection, then  $p^{-1}(x)$  is the **fiber** over  $x$

- If  $N \triangleleft G$ , the projection  $\pi : G \rightarrow G/N$  is a homomorphism. The fibers of  $\pi$  is the cosets  $gN = Ng$ , and they are all the same size.
- Suppose  $\varphi : G \rightarrow H$  is a homomorphism, and  $N = \ker(\varphi) \trianglelefteq G$ . The fibers of  $\varphi$  is the cosets of  $G/N$ .
- We have  $\varphi : G \rightarrow H$  and  $\pi : G \rightarrow G/N$ . Wouldn't it be nice if  $G/N \rightarrow H$  "induced by  $\varphi$ " were a homomorphism? Well, it is.

**Theorem—(First) Isomorphism:** If  $\varphi : G \rightarrow H$  is a homomorphism, and  $N = \ker(\varphi)$ , then there is a homomorphism  $\bar{\varphi} : G/N \rightarrow H$  such that  $\bar{\varphi} \circ \pi = \varphi$ . Moreover,  $\ker(\bar{\varphi}) = \{eN\}$ , the trivial subgroup of  $G/N$ , so  $\bar{\varphi}$  is injective. So,  $\bar{\varphi} : G/N \rightarrow \text{im}(\varphi)$  is an **isomorphism**.

- This theorem suggests that you can construct an isomorphism from an arbitrary homomorphism. First,  $\varphi$  factors through  $G/N$ , then we can include it into  $H$ .

$$G \xrightarrow{\pi} G/N \xrightarrow{\bar{\varphi}} \text{im}(\varphi) \xrightarrow{\text{inclusion}} H \quad (29)$$

**Theorem—(Third) Isomorphism:**  $N \trianglelefteq G$  and  $H \leq G$ , then  $N \leq H \implies N \trianglelefteq G$ .

*Proof.* ????

□

**Theorem—:**

$$G/H \cong G/N \big/ H/N \quad (30)$$

*Proof.* Define  $\varphi : G \rightarrow G/N \big/ H/N$  by

$$\varphi(g) = (gN)H/N \quad (31)$$

We need to show  $\varphi$  is a homomorphism. Let

$$\varphi(gg') = gg'N H/N \quad (32)$$

$$= gNg'N H/N \quad (33)$$

$$= gN H/N \cdot g'N H/N \quad (34)$$

$$= \varphi(g)\varphi(g') \quad (35)$$

$$(36)$$

□

We will then ask what is  $\ker(\varphi)$ . Suppose  $\varphi(g) = H/N$ , so  $gN H/N = H/N$ . But  $g$  is a representation for  $gN$ , so  $gH/N$  for this to be in  $H/N$  we want  $g \in H$  so  $\ker(\varphi) = H$ . An arbitrary element of  $G/N \big/ H/N$  is  $gN H/N$  for some  $g \in G$ , so  $\text{im}(\varphi) = G/N \big/ H/N$ .

- $G = \mathbb{Z}, H = 3\mathbb{Z}, K = 4\mathbb{Z}$ . By the second isomorphism theorem,  $\mathbb{Z}/3\mathbb{Z} \cong 4\mathbb{Z}/12\mathbb{Z}$ , and also  $\mathbb{Z}/4\mathbb{Z} \cong 3\mathbb{Z}/12\mathbb{Z}$ .

**Definition—Equivalence Class:** Being in the same coset of a subgroup  $H$  is an equivalence relation. So, the large group is a disjoint union of equivalence classes (cosets) of  $H$ .

- The cosets of  $\mathbb{Z}$  in  $\mathbb{R}$  is  $r + \mathbb{Z}$  for  $r \in [0, 1)$ .
- Homomorphism  $\varphi : \mathbb{R} \rightarrow \mathbb{C}^\times, t \mapsto e^{2\pi it}$ . Then,  $\ker(\varphi) = \mathbb{Z}$ . Observe that  $\varphi$  is **onto** the unit circle, by the first isomorphism theorem,  $\mathbb{R}/\ker(\varphi) = \mathbb{R}/\mathbb{Z} \cong S^1$ .
- $\mathbb{Z}^2 \triangleleft \mathbb{R}^2$

**Theorem—Fourth Isomorphism Theorem/Lattice Theorem:** Consider a lattice of subgroups with  $N \trianglelefteq G$ . In  $G/N$ , the subgroup lattice has the same structure as the subgroup lattice of  $G$  that contains  $N$ .

Specifically, if  $N \trianglelefteq G$ , and  $N \trianglelefteq H < G$ , we write  $\bar{H} = H/N$ . Including  $\bar{G} = G/N$  and  $\bar{N} = \bar{e} = N/N$ . Then, the lattice of  $\bar{H}$ s in  $\bar{G}$  has the same lattice structures as the part of the lattice for  $G$  consisting



of subgroups that are intermediate between  $N$  and  $G$ . Moreover,

$$H \leq K \iff \bar{H} \leq \bar{K} \quad (37)$$

$$H \trianglelefteq K \iff \bar{H} \trianglelefteq \bar{K} \quad (38)$$

$$[H : K] = [\bar{H} : \bar{K}] \text{ if } K \leq H \quad (39)$$

$$\overline{H \cap K} = \bar{H} \cap \bar{K} \quad (40)$$

$$\overline{\langle H, K \rangle} = \langle \bar{H}, \bar{K} \rangle \quad (41)$$

If  $G, G'$  are groups, consider the cartesian product  $G \times G' = \{(g, g') | g \in G, g' \in G'\}$ . Note that  $|G \times G'| = |G||G'|$ . There is an obvious way to turn this into a group by

$$(g, g')(h, h') = (gh, g'h') \quad (42)$$

$$(g, g')^{-1} = (g^{-1}, g'^{-1})e = (e, e) \quad (43)$$

In  $G \times G'$ , the subset  $G_0 = \{(g, e) | g \in G\} \cong G$  is a subgroup. Likewise,  $G'_0 = \{(e, g') | g' \in G'\} \cong G'$ . Also notice that  $G_0$  and  $G'_0$  commute. So,  $(G \times G')/G_0 \cong G'$ .

## 1.4 SYMMETRIC GROUPS

**Definition–Symmetric Group:** The symmetric group  $S_n$  is the group of permutation of  $n$  elements, with composition as the operation.

- $|S_n| = n!$
- A cycle is a permutation that cycles through some subset of  $\{1, \dots, n\}$ , denoted as

$$(a_1 a_2 \dots a_k), \quad k \leq n \text{ and } a_i \text{ are distinct.} \quad (44)$$

Represents the permutation  $a_1 \rightarrow a_2 \rightarrow \dots \rightarrow a_k \rightarrow a_1$ .

- Note that these are ambiguous, as  $(a_1 a_2 \dots a_k)$  is the same as  $(a_2 a_3 \dots a_k a_1)$ . So by convention, we often start with the smallest number first so they are unique.
- $k$  is the length of the cycle, it is also called a  **$k$ -cycle**.
- Every permutation can be written as a product of disjoint cycles. If given a permutation, we will start from 1 and write a cycle until we get back to 1. Then, we will start from the next number that hasn't been included yet and repeat until we get to the end.
- If  $\sigma = (136)(45)$ , then  $\sigma^{-1} = (45)^{-1}(136)^{-1} = (45)(163) = (163)(45)$ . We will order the cycles by their first element, and omit 1-cycles.
- Two **disjoint cycles** (i.e. without any numbers in common) will commute.
- If cycles are not disjoint, like  $\sigma = (142)(235)(347) \in S_7$  will not commute.

- $1 \rightarrow 4$
- $4 \rightarrow 7$
- $7 \rightarrow 3 \rightarrow 5$
- $5 \rightarrow 2 \rightarrow 1$
- $2 \rightarrow 3$
- $3 \rightarrow 4 \rightarrow 2$

So  $\sigma = (1475)(23)$ .

- Any  $k$ -cycle is a product of 2-cycles. Thus, every element in the symmetric group can be written as a product of 2-cycles so  $S_n$  is generated by 2-cycles. For example, if  $k = 4$  and  $\sigma = (a b c d)$ , then  $\sigma = (a d)(a c)(a b)$ .
- We can ask what is the minimum number of 2-cycles needed to generate any  $\sigma \in S_n$ . In general, this is a very difficult question to answer. However, the **parity** of the number of 2-cycles in a product equalling  $\sigma$  is well-defined.
- If  $\sigma = (a_1 b_1)(a_2 b_2) \dots (a_k b_k)$  is a product of 2-cycles, then  $\sigma$  is **even** if  $k$  is even, and **odd** if  $k$  is odd.
- **Warning: a  $k$ -cycle is even if  $k$  is odd, and odd if  $k$  is even.**
- To make odd and even well defined, we need to know that the parity of a permutation is independent of the way we write the cycles.

*Proof.* Given  $\sigma \in S_n$  is a  $k$ -cycle. Define  $\Delta = \prod_{1 \leq i < j \leq n} (j - i)$ . If  $\tau \in S_n$ , it acts on  $\Delta$  with

$$\tau \cdot \Delta = \prod_{1 \leq i < j \leq n} (\tau(j) - \tau(i)). \quad (45)$$

These two products are the same up to a factor of  $\pm 1$ , you have to multiply by  $-1$  for each pair  $i < j$  for which  $\tau(i) > \tau(j)$ .

We will consider how  $(a b)$  with  $a < b$  affect  $\Delta$ . If neither  $i$  nor  $j$  is equal to  $a$  or  $b$ , the term is unaffected. Note that

- If  $i < a$ , then  $i < \tau(a) = b$  and  $i < \tau(b) = a$ . So  $(i a)$  or  $(i b)$  are unaffected.
- Likewise, for  $j > b$  then  $(a j)$  or  $(b j)$  are unaffected.

The only pairs that will be affected are ones  $(a i)$ ,  $(i b)$  with  $a < i < b$  and  $(a b)$ . If  $a < i < b$ , then both  $(a i)$  and  $(i b)$  will change sign, so the product will be unaffected.  $(a b)$  will change sign, so  $\Delta$  will change sign under a transposition.

If  $\sigma \in S_n$ , write it as any product of  $k$  transpositions. If  $\sigma \cdot \Delta = \Delta$  then there must be an even number of transpositions. If  $\sigma \cdot \Delta = -\Delta$  then there must be an odd number of transpositions. Thus, the parity of  $\sigma$  is independent of the way we write it.  $\square$

**Definition–Sign:** The sign of  $\sigma \in S_n$  is

$$\text{sgn}(\sigma) = (-1)^k, \quad (46)$$

if  $\sigma$  is a product of  $k$  transpositions.

- Note that  $\text{sgn}(\sigma\tau) = (-1)^k(-1)^l = (-1)^{k+l} = \text{sgn}(\sigma)\text{sgn}(\tau)$ .
- Thus,  $\text{sgn} : S_n \rightarrow \{\pm 1\}$  is a homomorphism.
- $\ker(\text{sgn}) = A_n \trianglelefteq S_n$  is the alternating group of  $n$  elements which contains all the even permutations. Note that

$$S_n/A_n \cong \{\pm 1\} \quad [S_n : A_n] = 2 \quad |A_n| = \frac{n!}{2} \quad (47)$$

- for  $n > 5$ ,  $A_n$  has no normal subgroups. What are the possible cycle types in  $A_5$ ? There is  $(a b c d e)$ ,  $(a b)(c d)$ ,  $(a b c)$
- Let  $\sigma \in S_n$  with  $a \rightarrow b \rightarrow c \rightarrow \dots$ , and suppose  $\tau \in S_n$  takes  $a \rightarrow a'$ ,  $b \rightarrow b'$ ,  $c \rightarrow c'$ ,  $\dots$ . Consider the conjugation  $\tau\sigma\tau^{-1}$ .

$$\tau\sigma\tau^{-1}(a') = \tau\sigma(a) = \tau(b) = b' \quad (48)$$

$$\tau\sigma\tau^{-1}(b') = \tau\sigma(b) = \tau(c) = c' \quad (49)$$

$$(50)$$

So  $\tau\sigma\tau^{-1}$  takes  $a' \rightarrow b' \rightarrow c' \rightarrow \dots$ . Conjugating by  $\tau$  “relabels” what  $\sigma$  by replacing  $a$  with  $a'$ ,  $\dots$

## 1.5 SIMPLE GROUP

One way we study groups is to write it as a chain of normal subgroups  $G_0 = \{e\} \triangleleft G_1 \triangleleft G_2 \triangleleft \cdots \triangleleft G_r = G$ , where  $G_{i+1}/G_i$  is a simple group  $\forall i = 0, \dots, r-1$ . A decomposition like this is called a **Jordan-Holder Series** (composition series), and the quotients are called the **composition factors**. However, the same  $G$  may have different composition series.

**Theorem–Jordan-Holder:** Any two Jordan-Holder series for  $G$  have the same length. Moreover, the composition factors are the same (but perhaps in different orders).

Example: Suppose  $H, K$  are both normal subgroups of  $G$ . Apply 2nd isomorphism theorem. Note,  $H \subseteq \text{Norm}_G(K) = G$  and  $K \subseteq \text{Norm}_G(H) = G$ . Thus,  $HK/K \cong H/H \cap K$  and  $HK/H \cong K/H \cap K$ . In this example there are two composition series

$$\{e\} \triangleleft H \cap K \triangleleft H \triangleleft HK \triangleleft G \quad (51)$$

$$\{e\} \triangleleft H \cap K \triangleleft K \triangleleft HK \triangleleft G \quad (52)$$

Every group has a Jordan-Holder series. In genera, a group  $G$  is not determined by its Jordan-Holder series. However, if  $G$  is simple, then its Jordan-Holder series is  $\{e\} \triangleleft G$ .

**Definition–Solvable:** If the composition factor  $G_{i+1}/G_i$  of  $G$  are all **abelian**, we say  $G$  is **solvable**.

If  $G$  acts on a set  $X$ , then each  $g \in G$  permutes the element of  $X$ . So there is a map  $G \rightarrow S_X$  (the symmetric group of  $X$ ). It is easy to show that this map is a homomorphism. So, we will allow ourselves to go between group actions and Homomorphisms into  $S_X$ .

Suppose  $H \leq G$  and let  $X = G/H$  be the coset space. So,  $G$  acts on  $X$  by left multiplication  $g(xH) \mapsto gxH$ . If  $n = [G : H] = |X|$ , the action amounts to a homomorphism  $\varphi : G \rightarrow S_n$ .

Our first observation is that  $G$  acts **transitively**. For any  $x, y \in X$ ,  $\exists g \in G$  s.t.  $gx = y$ . i.e. the orbit of any  $x \in X$  is  $X$ .

What is  $\ker \varphi$ ? We know that if  $h \in \ker \varphi$ , that  $hxH = xH$ . Then consider  $h', h'' \in H$  then

$$h x h' = x h'' \quad (53)$$

$$h x = x h'' h'^{-1} \quad (54)$$

$$h = x h'' h'^{-1} x^{-1} \quad (55)$$

$$\ker \varphi = \bigcap_{x \in G} x H x^{-1} \quad (56)$$

If  $H = \{e\}$ , then  $G/H = G$ , so  $\ker \varphi = \{e\}$ . then  $\varphi$  is injective. By the first isomorphism theorem,  $G \cong \text{im } \varphi = S_n$ .

**Theorem–Cayley:** Any group  $G$  with  $|G| = n$  is isomorphic to a subgroup of  $S_n$ .

*Proof.* We already proved it! □

Another example is to let  $G$  act on itself by conjugation. In this case,  $\varphi$  with  $g \cdot x = gxg^{-1} = C_g(x)$ . This is not a transitive action unless  $G$  is trivial. The orbits of conjugation are the **conjugacy classes** of  $G$ . They are disjoint (because conjugacy is an equivalence relation).

Note that  $geg^{-1} = e$ ,  $\forall g$ . If  $z \in Z(G)$ , then  $gzt^{-1} = zg g^{-1} = z \forall g$ , then the conjugacy classes contain a single element.

If  $G$  is abelian,  $Z(G) = G$  and every element is its own conjugacy class.

Because conjugacy is an equivalence relation,  $G$  is a disjoint union of all conjugacy classes.

If  $Z(G) = \{e, z_1, \dots, z_k\}$  and  $g_1, \dots, g_m$  are representatives from the non-central conjugacy classes. Let's write  $C(g_i) = \{gg_i g^{-1} | g \in G\}$ . So,

$$G = Z(G) \sqcup \left( \bigsqcup C(g_i) \right) \quad (57)$$

so

$$|G| = |Z(G)| + \sum_i |C(g_i)| \quad (58)$$

This is called the **Class Equation**.

**Theorem—Orbit-Stabilizer:** If  $G$  acts on  $X$ , for each  $x \in X$ , write  $G \cdot x$  for its orbit. Then,

$$|G \cdot x| = [G : G_x] = [G : \text{Stab}(x)] \quad (59)$$

The point is that two things in the same coset of  $G_x$  has the same effect on  $x$ .

Under conjugation,

$$\text{Stab}(x) = G_x = \{g \in G | gxg^{-1} = x\} = Z(x), \quad (60)$$

the centralizer of  $x$ . So the class equation can be rewritten as

$$|G| = |Z(G)| + \sum_i [G : Z(g_i)] \quad (61)$$

**Definition— $p$ -group:** Suppose  $p$  is prime,  $G$  is a  **$p$ -group** if  $|G| = p^k$  for some  $k \geq 1$ .

**Theorem—:** If  $G$  is a non-trivial  $p$ -group, then it has a non-trivial center.

*Proof.* Suppose  $|G| = 1$ . Then

$$|G| = |Z(G)| + \sum_i [G : Z(g_i)] \quad (62)$$

Claim  $Z(g_i) < G$ , otherwise  $g_i \in Z(G)$ . By Lagrange's theorem  $|Z(g_i)| \mid |G| = p^k$ . So  $|Z(g_i)| = p^l$  for some  $l < k$ . Then,

$$p^k = |G| = |Z| + \sum_i [G : Z(g_i)] \quad (63)$$

$$(64)$$

Since  $|Z| = 1$ , the RHS is not divisible by  $p$  so this is a contradiction.  $\square$

**Corollary:** Suppose  $p$  is prime. If  $|G| = p^2$ , then  $G$  is abelian.

*Proof.* We know  $Z(G)$  is a non-trivial subgroup so  $1 \neq |Z(G)| \mid p^2$ . So  $|Z(G)| = p$  or  $p^2$ . If  $|Z(G)| = p^2$ , then  $G$  is abelian by definition. If  $|Z(G)| = p$ , then  $|G/Z(G)| = p$  hence  $G/Z(G) \cong C_p$ . So  $x \notin Z(G)$ , then  $G/Z(G) = \{\bar{e}, \bar{x}, \bar{x}^2, \dots, \bar{x}^{p-1}\}$  where  $\bar{x} =: xZ(G)$ . Also,  $\bar{x}^p = \bar{e} \in G/Z(G)$ . Note that  $\text{ord}(x)$  is either  $p$  or  $p^2$ .

- If  $|\langle x \rangle| = p^2$  so  $\langle x \rangle = G$  and  $G$  is cyclic hence abelian.
- If  $\text{ord}(p)$ , then  $G = \bigcup_{k=0}^{p-1} x^k Z(G)$ . Recall  $|Z(G)| = p$ , so  $Z(G)$  is cyclic. Then,

$$Z(G) = \{e, z, z^2, \dots, z^{p-1}\} \quad (65)$$

so

$$G = \{x^i z^j \mid 0 \leq i, j < p\} \quad (66)$$

These elements commute.  $x^i z^j x^m z^n = x^i x^m z^j z^n = x^{i+m} z^{j+n}$

□

Note we need to be careful with the steps in this proof. Just because  $\bar{x}^p = \bar{e}$  doesn't mean there is a representative  $x \in \bar{x}$  that is order  $p$ .

- Now we consider the rotations of a tetrahedron. A easy way to think about this is to identify a "top" vertex, which is well defined (4 possibilities). Then, we fix the top and we have 3 rotations (like of the triangle). So, there are 12 rotations.
- Apart from  $e$ , there are two non-trivial rotations that fix any particular vertex. This only accounts for 8 rotations, and  $e$ , so we are missing 3 rotations.
- The other rotations does not fix any vertices and are like  $(1\ 2)(3\ 4)$ . Then, 2, 3, 4 goes with 1 so we have 3 rotations. This accounts for all 12.
- In summary, we have  $e$ , and 8 rotations in the form  $(a\ b\ c)$  and 3 rotations in the form  $(a\ b)(c\ d)$ . This is  $A_4$ .
- The rigid motions are  $S_4$ .

**Proposition:**  $A_5$  is simple.  $A_5 \triangleleft S_5$  with index 2, so  $|A_5| = 60$ .

*Proof.* We will enumerate the conjugacy classes of  $S_5$

- $(a\ b\ c\ d\ e) \in A_5$
- $(a\ b\ c\ d) \notin A_5$
- $(a\ b\ c) \in A_5$
- $(a\ b\ c)(d\ e) \notin A_5$
- $(a\ b)(c\ d) \in A_5$
- $(a\ b) \notin A_5$
- $e \in A_5$

There are 24 elements in the conjugacy class of  $(a\ b\ c\ d\ e)$ . However, 24 does not divide 60 so it is not a conjugacy class of  $A_5$ .

Consider the centralizer  $Z_{A_5}(abcde) \geq \langle(abcde)\rangle$  which has order 5. But  $Z_{A_5}(abcde) \leq Z_{S_5}(abcde)$  so  $Z_{A_5}(abcde) = \langle(abcde)\rangle$

So there are two  $A_5$  conjugate classes of 5-cycles, each with 12 elements.

There are 20 3-cycles in  $S_5$ . Are they all conjugate in  $A_5$ ? If  $(abc)$  is conjugate to  $(xyz)$  by  $\sigma \in S_5$ , then it is also conjugate by  $\sigma(de)$ . If  $\sigma \notin A_5$  then  $\sigma(de) \in A_5$  so there is one conjugate class of 20 3-cycles.

There are 15 double transpositions.

**If we have a normal subgroup, it is a union of the conjugacy classes**, so if  $A_5$  has a normal subgroup it must be a combination of 1 + 15, 20, 12, 12 but there is no combination (apart from 1) that divides 60. Hence,  $A_5$  is simple.  $\square$

## 2 SYLOW THEOREMS

**Theorem—** Suppose  $|G| = p^\alpha n$  where  $p \nmid n$ . Then, a subgroup  $P \leq G$  is a Sylow  $p$ -subgroup if  $|P| = p^\alpha$ . We'll write  $n_p(G)$  for the number of Sylow  $p$ -subgroups of  $G$ .

1. Sylow  $p$ -subgroups exist.
2. Suppose  $P$  is a Sylow  $p$ -subgroup of  $G$  and  $Q \leq G$  s.t.  $|Q| = p^r$  for some  $r > 0$ . Then,  $\exists g \in G$  s.t.  $gQg^{-1} \subseteq P$ . In particular, all Sylow  $p$ -subgroups of  $G$  are conjugate.
3.  $n_p(G) \equiv 1 \pmod{p}$  and  $n_p(G) = [G : \text{Norm}_G(P)]$  for any Sylow  $p$ -subgroup. Hence  $n_p(G) \mid |G|$ . It actually also divides  $n = |G|/|P|$ .

Before proving the theorem we will consider the following example: Let  $G = S_3$ . The Sylow 2 subgroups are  $\{e, (12)\}, \{e, (13)\}, \{e, (23)\}$  we know  $n_2(S_3) = 3 \equiv 1 \pmod{2}$ . The only Sylow 3 subgroup is  $A_3$ , so  $n_3(S_3) = 1$ .

**Lemma 1:** If  $G$  is abelian and  $p \mid |G|$ , then  $G$  contains an element of order  $p$ .

*Proof.* If  $|G| = p$  then  $G$  is cyclic and every non-trivial element has order  $p$ .

If  $|G| > p$ , and  $x \in G$  with order  $p^r m$  where  $p \nmid m$ . If  $r \neq 0$ , then  $x^{p^{r-1}m}$  has order  $p$ . This reduces us to the case where  $p \nmid \text{ord}(x), \forall x \in G$ . We will use induction.

- Assume the result is true for all groups smaller than  $G$ .
- If  $p \nmid \text{ord}(x) = |\langle x \rangle| < |G|$ . As  $G$  is abelian, then  $N =: \langle x \rangle \triangleleft G$ .
- By induction  $G/N$  contains an element of order  $p$ .
- i.e.  $\exists y = y_0 N \in G/N$  s.t.  $y^p = e = N$ . so  $y_0^p \in N$
- We claim that  $\langle y_0^p \rangle < \langle y_0 \rangle$  since otherwise  $y_0 \in N$  which has order 1.
- This means  $p \mid |y_0|$  otherwise  $\langle y_0^p \rangle = \langle y_0 \rangle$ . This is a contradiction.
- This means a suitable power of  $y_0$  must have order  $p$ .

$\square$

**Lemma 2:** If  $P \in \text{Syl}_p(G)$  and  $Q$  is a non-trivial  $p$ -subgroup of  $G$ . Then,  $Q \cap \text{Norm}_G(P) = Q \cap P$ .

*Proof.* Let  $H = Q \cap \text{Norm}_G(P) \geq Q \cap P$ . We need to show that  $H \leq Q \cap P$ . But  $H \leq Q$  so we only need to show that  $H \leq P$ .

$H \leq N_G(P) \implies HP$  is a subgroup. The result will follow if we can argue that  $HP$  is a  $p$ -group. We know that

$$|HP| = \frac{|H||P|}{|H \cap P|} \quad (67)$$

Since  $|H|, |P|, |H \cap P|$  are all powers of  $P$ . So  $HP \geq P$  but  $|HP|$  can't be bigger than  $|P|$ .  $\square$

Proof that Sylow  $p$ -subgroup exists. We will use induction on  $|G|$ .

If  $p \mid |Z(G)|$ , we know by the lemma that  $\exists z \in Z(G)$  with  $|z| = p$ . Let  $N = \langle z \rangle$  is a normal subgroup as  $N \leq Z(G)$ . Then,  $G/N$  is a smaller group than  $G$ . By the induction hypothesis say  $G/N$  has a Sylow  $p$ -subgroup.

If  $|G| = p^\alpha m, p \nmid m$  then  $G/N = p^{\alpha-1}m$ . So, it has a Sylow  $p$ -subgroup of order  $p^{\alpha-1}$ . By the lattice isomorphism theorem, the preimage of this group in  $G$  has order  $p^\alpha$ , as required.

Assume  $p \nmid |Z(G)|$ . Let  $g_1, \dots, g_k$  be representatives of the non-central conjugacy classes of  $G$ . So,

$$|Z(G)| + \sum_{i=1}^k [G : C_G(g_i)] = |G|. \quad (68)$$

We know that  $p \mid |G|$  but  $p \nmid |Z(G)|$  meaning for some  $i$ , we know  $p \nmid [G : C_G(g_i)]$ . As  $g_i$  represents a non-central conjugacy class, then  $C_G(g_i) < G$ . We will use the induction hypothesis. Note that since  $p \nmid [G : C_G(g_i)]$ , then  $p^\alpha \mid |C_G(g_i)|$ . By the induction hypothesis,  $C_G(g_i)$  has a Sylow  $p$ -subgroup of order  $p^\alpha$ , it is also a Sylow  $p$ -subgroup of  $G$ . Thus, Sylow  $p$ -subgroups exist.

Fix a Sylow  $p$ -subgroup  $P_1$  of  $G$  and enumerate all its distinct conjugates as  $P_1, \dots, P_r$ . Let  $Q$  be any  $p$ -subgroup.

$G$  acts on  $S = \{P_1, \dots, P_r\}$ , and  $Q$  also act on  $S$ , but it may not have a single orbit. Decompose  $S$  into  $Q$  orbits,

$$S = \mathcal{O}_1 \sqcup \mathcal{O}_2 \sqcup \dots \sqcup \mathcal{O}_s. \quad (69)$$

How big is  $\mathcal{O}_k$ ? Relabel  $P_1, \dots, P_k$  s.t.  $\mathcal{O}_k = \{qP_kq^{-1} \mid q \in Q\}$ . We know how to find the size of a conjugacy class.  $|\mathcal{O}_k| = [Q : N_Q(P_k)]$ . Note that  $N_Q(P_k) = N_G(P_k) \cap Q$ . The second lemma states  $N_G(P_k) \cap Q = P_k \cap Q$ .

For now, let  $Q = P_1$ . So,  $\mathcal{O}_1 = \{qP_1q^{-1} \mid q \in P_1\} = P_1$ .

$$|S| = r = \underbrace{|\mathcal{O}_1|}_1 + \underbrace{\sum_{i=2}^s [P_1 : P_1 \cap P_i]}_{\text{divisible by } p} \quad (70)$$

If we know that if all Sylow  $p$ -subgroup are conjugate, then we know the number of Sylow  $p$ -subgroup is  $1 \pmod p$ .

Let  $Q$  be any  $p$ -subgroup of  $G$  and suppose  $Q$  is not contained in any of the  $P_1, \dots, P_r$ . Then,  $Q \cap P_i$  is a proper subgroup of  $Q$ . Then,

$$|\mathcal{O}_k| = [Q : P_k \cap Q] \quad (71)$$

is divisible by  $P$ . So,  $p \mid |S|$  so  $p \mid |r|$  but  $r \equiv 1 \pmod p$  so this is a contradiction.

Suppose  $|G| = pq$ , and  $p < q$  prime. We know  $n_q(G) = 1$ , i.e.  $\text{Syl}(G) = \{Q\}$ , then  $Q \triangleleft G$ . One possibilities is that  $G$  is cyclic. Often,  $n_p(G) = 0$  unless  $p \mid (q-1)$ , then it is more complicated.

The significance of  $q - 1 = \text{the number of units mod } q$ , which turns out to be the number of automorphisms of  $C_q$ . (multiply each element of  $C_q$  by a unit  $u = (\mathbb{Z}/q\mathbb{Z})^x$ ).

So this is a homomorphism  $C_p \rightarrow \text{Aut}(C_q)$ . We can use this homomorphism to make a group that is not abelian.

**Definition–Finitely Generated:** An abelian group  $G$  is **finitely generated** if there exists a finite set  $S$  such that  $G = \langle S \rangle$ .

Examples of finitely generated abelian groups are finite abelian groups,  $\mathbb{Z}, \mathbb{Z}^r$  but not  $\mathbb{R}, S^1, \mathbb{Q}$ .

**Theorem–Fundamental Theorem of Abelian Groups:** If  $G$  is a finitely generated abelian group, then  $G$  is isomorphic to a product

$$G \cong \mathbb{Z}^r \times \prod_{i=1}^s C_{r_i} \quad (72)$$

where  $r \in \mathbb{N}_0, n_i \in \mathbb{N}^{>1}$ , and  $n_{i+1} \mid n_i \forall i = 1, \dots, s-1$ . Note the following:

- $r = 0 \iff G$  is finite.
- $G$  is cyclic  $\iff r = 0 \wedge s = 1$

Moreover, this decomposition is unique up to isomorphism.

*Proof.* The proof will come easily from another theorem later. □

**Definition–:** In this decomposition,  $r$  is called the **free rank** of  $G$  or the **Betti number** of  $G$ . The  $n_i$ 's are called the **invariant factors** of  $G$ .

Another version. Any finitely generated abelian group  $G$  can be written as

$$G = \mathbb{Z}^r \times \prod_{i=1}^k P_{p_i} \quad (73)$$

where  $|G/\mathbb{Z}^r| = \prod_i p_i^{\alpha_i}$ . Moreover, for each  $i$ ,

$$P_{p_i} = C_{p_i^{\beta_1^i}} \times C_{p_i^{\beta_2^i}} \times \dots \times C_{p_i^{\beta_{\alpha_i}^i}} \quad (74)$$

where  $\beta_1^i \geq \beta_2^i \geq \dots \geq \beta_{\alpha_i}^i$  and  $\beta_1^i + \beta_2^i + \dots + \beta_{\alpha_i}^i = \alpha_i$ . The notation is awful, but idea is we can decompose  $G$  into its Sylow  $p$ -subgroups and then decompose each Sylow  $p$ -subgroup into its cyclic factors. This decomposition is unique up to isomorphism.

**Definition–Elementary Divisors:** The subgroups  $C_{p_i^{\beta_1^i}}, \dots, C_{p_i^{\beta_{\alpha_i}^i}}$  or sometimes their orders are called the **elementary divisors** of  $G$ .