Abstract Algebra

Jubayer Ibn Hamid

Contents

Preface

These reading notes are a combination of material from the courses Math 210A by Prof. Ravi Vakil at Stanford University, Dummit and Foote's *"Abstract Algebra"* [1] and Aluffi's *"Algebra Chapter 0"* [2].

There may be major and minor errors throughout these notes. If you find any, please let me know by sending me an email at jubayer@stanford.edu. Oftentimes, I wrote these notes *after* I had already handwritten them elsewhere and I was careless / inefficient in rewriting the proof. I also glossed over various parts of the original texts that the reading notes were trying to follow despite them being pretty important.

1. Introduction to Group Theory

1.1. Definitions and Immediate Properties

Definition 1.1 (Groups)**.** *A **group** is the following data: G is a set and $\bullet$ is a binary operation on G, such that:*

1. *the operation is associative: $(x \bullet y) \bullet z = x \bullet (y \bullet z)$ for all $x, y, z \in G$*
2. *the operation has an identity: there exists an element $1_G \in G$ such that $x \bullet 1_G = 1_G \bullet x = x$ for all $x \in G$*
3. *the operation gives each element an inverse: for all $x \in G$, there exists an inverse $x^{-1} \in G$ such that $x \bullet x^{-1} = x^{-1} \bullet x = 1_G$*

*In particular, the operation $\bullet$ need not be commutative. However, if it is commutative (i.e. $x \bullet y = y \bullet x$ for all $x, y \in G$), then we say that the group is **abelian** or commutative.*

Observe that a group is always non-empty since it must, at the very least, have the identity, $1_G \in G$. We now look at some immediate examples of groups:

Examples 1.2. *The following are all groups:*

1. *The set of integers ($\mathbb{Z}$), the set of rationals ($\mathbb{Q}$), the set of reals ($\mathbb{R}$), and the set of complex numbers ($\mathbb{C}$) are all groups under addition, and they are all abelian. However, they are not all groups under multiplication. For example, $\mathbb{Z}$ is not a group under multiplication since $x > 1$ and $x < -1$ has no inverse. Furthermore, $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are not groups under multiplication since 0 has no inverse.*
2. *The sets $\mathbb{R} - \{0\}, \mathbb{Q} - \{0\}$, and $\mathbb{C} - \{0\}$ are groups under multiplication (but not under addition since there is no additive identity).*
3. *All vector spaces V are groups under addition. In particular, they are abelian groups.*
4. *The set $\mathbb{Z}/n\mathbb{Z}$ where $n \in \mathbb{Z}_{>0}$ is an abelian group under addition. The identity in the group is $\bar{0}$ and the additive inverse of $\bar{x}$ is $\bar{-x}$ for any $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$.*

Note that $\mathbb{Z}/n\mathbb{Z}$ is not guaranteed to be a group under multiplication since, a priori, all elements are not guaranteed to have a multiplicative inverse. First, we define the subset of $\mathbb{Z}/n\mathbb{Z}$ which admits such inverses to be a group:

Example 1.3. The set $(\mathbb{Z}/n\mathbb{Z})^\times \subseteq \mathbb{Z}/n\mathbb{Z}$ is the set of all equivalence classes $\bar{x}$ such that there exists a multiplicative inverse. This is a group under multiplication where the identity is $\bar{1}$.

It should be clear, from the notation itself, that $\mathbb{Z}/n\mathbb{Z}$ is a group under addition and $(\mathbb{Z}/n\mathbb{Z})^\times$ is a group under multiplication.

Definition 1.4 (Direct Product of Groups)**.** *Suppose $(X, \bullet)$ and $(Y, \square)$ are groups. Then, the direct product of these groups is the set $X \times Y = \{(x, y) \mid x \in X, y \in Y\}$ under the componentwise operation:*

$$(x_1, y_1)(x_2, y_2) = (x_1 \bullet x_2, y_1 \square y_2).$$

We now look at some immediate properties that all groups satisfy.

Notation 1.5. *We adopt the shorthand notation where we suppress the group operation $x_1 \bullet x_2$ and write it as $x_1 x_2$. We write multiplicatively even though the group operation need not be.*

Theorem 1.6. *Suppose G is a group. Then,*

1. *the identity 1_G of G is unique*

2. *the inverse x^{-1} of each $x \in G$ is unique*
3. *$(x^{-1})^{-1} = x$ for all $x \in G$*
4. *$(xy)^{-1} = y^{-1}x^{-1}$ for all $x, y \in G$*
5. *If $xy = xz$ for some $x, y, z \in G$, then $y = z$. If $yx = zx$, then $y = z$. In particular, there is a unique solution for $ax = b$ in x and a unique solution for $ya = b$ in y.*

Finally, we define the *order* of an element.

Definition 1.7 (Order of an Element in a Group)**.** *Let G be a group and let $x \in G$. Then, the order of x is denoted by $|x|$ and is defined as the smallest positive integer n such that $x^n = 1_G$. If there is no such n, then we say that the order is infinite.*

Examples 1.8.
1. *The element $1_G \in G$ has order 1. In fact, it is the element with this property, i.e. an element in any group has order 1 if and only if it is the identity.*
2. *In $\mathbb{R} - \{0\}$, or $\mathbb{Q} - \{0\}$, the element -1 has order 2 under the operation of multiplication. All other elements in these groups have infinite order.*

1.2. Symmetric Groups

The symmetric group is an extraordinarily important and ubiquitous construction.

Definition 1.9 (Symmetric Groups)**.** *Let M be a set and the let S_M be the set of all bijections from M to itself i.e. the set of all permutations of M. Then, S_M is a group under composition i.e. if $\sigma_s, \sigma_t \in S_M$, then $\sigma_s\sigma_t = \sigma_s \circ \sigma_t$. The identitiy of the group is 1 which sends every element in M to itself.*

In particular, when the set is $M = \{1, 2, \cdots, n\}$ of size n, the symmetric group is denoted by S_n and called the symmetric group of degree n.

Sometimes, the symmetric group of the set M is denoted by $\mathrm{Sym}(M)$. In these notes, however, we simply denote it by S_M.

Proposition 1.10. *The order of the symmetric group S_n is $n!$, i.e. $|S_n| = n!$.*

Proof. Each permutation in a symmetric group is an injective function from $\{1, \cdots, n\}$ to itself. There are $n!$ such injective functions. □

One can denote the elements of a symmetric group using cycles. A cycle is a string such as $(a_1, a_2, \cdots, a_m)$ which represents a permutation; this cycle represents that the permutation takes a_1 to a_2, a_2 to a_3 and so on until a_m to a_1. The cycle $(3, 4, 1)$ takes 3 to 4, 4 to 1, and 1 to 3. With this notation, we can decompose any $\sigma \in S_n$ as a composition of cycles of the form $(a_1, a_2, \cdots, a_m)(a_p, a_{p+1}, \cdots, a_{p+k})$. The length of a cycle is the number of integers in it. In particular, we have the following method for calculating the order of any element in a symmetric group:

Proposition 1.11. *The order of a permutation in a symmetric group is the l.c.m. of the lengths of the cycles in its cycle decomposition.*

Proposition 1.12. *S_n is a non-abelian group for all $n \geq 3$.*

Proof. Consider the set $\{1, 2, 3, \cdots, n\}$. Then, consider the two permutations σ_s defined by $1 \to 3$ and and the permutation σ_t defined by $1 \to 2$. Then, $\sigma_s\sigma_t \neq \sigma_t\sigma_s$. Since these permutations exists in all symmetric groups S_n for $n \geq 3$, we are done. □

1.3. Dihedral Groups

Dihedral groups are an extremely important class of groups that define *symmetries* of polygons.

Definition 1.13 (Dihedral groups)**.** *For a positive integer $n \geq 3$, the dihedral group D_{2n} is the set of all symmetries of the regular n-gon. A symmetry is defined as any rigid motion on the object such that the objects look exactly the same. More precisely:*

- *A symmetry of an n-gon is the following: label all n vertices of the polygon first. Then, a symmetry is a permutation σ of the set $\{1, 2, \cdots, n\}$ corresponding to the rigid motion that leaves the polygon unchanged. For e.g., consider the 90 degrees clockwise rotation of a square (i.e. 4-gon) whose vertices are labelled sequentially. Then, the rotation can be described as the permutation σ that sends i to $i+1$, for all $i \in \{1, \cdots, n-1=3\}$, and $n=4$ to 1.*

This set D_{2n} is a group under the operation of composition. In other words, if $s, t \in D_{2n}$ (i.e. s is some symmetry and t is another symmetry), then st is the symmetry obtained by first applying t and then applying s. This can also be defined by looking at the permutations each such symmetry corresponds to: if s corresponds to the perutation σ_s and t corresponds to the permutation σ_t, then st corresponds to the permutation $\sigma_s \circ \sigma_t$.

In D_{2n}, the identity is the identity symmetry which leaves al vertices fixed/unchanged and is denoted by 1. The inverse of $s \in D_{2n}$ is the symmetry that reverses all the rigid motions of s i.e. s^{-1} corresponds to the permutation σ^{-1} if s corresponds to σ.

Proposition 1.14. *For any dihedral group D_{2n}, the size of the set is $|D_{2n}| = 2n$. We say the dihedral group D_{2n} is of order $2n$.*

Proof. Consider some sequential numbering of the vertices of the n-gon i.e. 1 is next to 2 which is next to 3 and so on. Now, we can send the vertex number 1 to n possible locations/vertices. Suppose we send 1 to i. Then, we must send 2 to either $i+1$ or $i-1$ because symmetries must be rigid motions. That means we have $n \times 2 = 2n$ possible permutations that define symmetries. □

Definition 1.15 (Rotations and Reflections in D_{2n})**.** *Define $r \in D_{2n}$ to be a clockwise rotation about the origin through $\frac{2\pi}{n}$ radians. Define $s \in D_{2n}$ to be reflection about the line going through the vertex and the origin.*

Proposition 1.16. *The following are satisfied in a dihedral group:*

1. *$1, r, r^2, \cdots, r^{n-1}$ are distinct and $r^n = 1$. In particular, $|r| = n$*
2. *$|s| = 2$*
3. *$s \neq r^i$ for any i*
4. *$sr^i \neq sr^j$ for $i \neq j$ and $0 \leq i, j \leq n-1$*

As such, we can write out the full group as:

$$D_{2n} = \{1, r, r^2, \cdots, r^{n-1}, s, sr, sr^2, \cdots, sr^{n-1}\}$$

and any $x \in D_{2n}$ can be written as $x = s^i r^j$ for $i \in \{0, 1\}$ and $0 \leq j \leq n-1$. Furthermore,

1. *$rs = sr^{-1}$. As such, **the dihedral group is not an abelian group**.*
2. *$r^i s = sr^{-i}$ for all $0 \leq i \leq n$.*

1.4. Homomorphisms and Isomorphisms

A recurring, central question we ask in abstract algebra is whether or not two mathematical objects of interest are, in some sense, the same. To be able to ask this question, we define homomorphisms and isomorphisms that help us understand these questions for groups with respect to their operations.

Definition 1.17 (Homomorphisms and Isomorphisms)**.** *Let $(G, \bullet)$ and $(H, \square)$ be two groups. Then, $\varphi : G \to H$ is a **homomorphism** if*

$$\varphi(x \bullet y) = \varphi(x) \square \varphi(y)$$

*for all $x, y \in G$. In other words, a homomorphism is a mapping that respects the structure of the group G and the group H. In particular, if φ is a bijection, then we call it an **isomorphism**, and we write $G \cong H$.*

We will switch to the more convenient notation and simply write $\varphi(xy) = \varphi(x)\varphi(y)$ by suppressing the group operation.

Recall that S_M is the symmetric group over the set M. We now show that symmetric groups over sets of equal size are isomorphic.

Theorem 1.18. *Let M and M' be two sets. Then, $S_M \cong S_{M'}$ if and only if $|M| = |M'|$.*

Proof Sketch: The forward direction is simple. First, since both the sets have the same cardinality, define some correspondence of the elements between them via θ i.e. $\theta(m) = m'$ for some $m \in M, m' \in M'$ where θ is bijective. This map, θ, is our way of associating each element in M with an element in M' which we can do since they have the same cardinality. Now, suppose $\sigma(x) = y$ for $x, y \in M$, i.e. σ is an element in S_M. Then, we will map this to a symmetry in $S_{M'}$ by looking at how the corresponding elements in M' get permuted. Define $\varphi : S_M \to S_{M'}$ by $\varphi(\sigma)(\theta(x)) = \theta(y)$. In other words, φ takes σ to a permutation in $S_{M'}$ that moves the elements of M' the same way σ moves the elements of M. One can easily show that this is a homomorphism. Furthermore, this is invertible since θ itself is invertible, i.e. given any $\mu \in S_{M'}$, we can find a corresponding $\sigma \in S_M$ using the map θ. The converse direction is easy to prove for the finite group case (we will prove the infinite case later). Since the two groups are isomorphic, it must be that $|S_M| = |S_{M'}|$. now, suppose $|M| = p$ and $|M'| = q$. Then, $|S_M| = p!$ and $|S_{M'}| = q!$. So, $p = q$ and we are done.

Examples 1.19. *The following are examples of isomorphisms:*

1. *$G \cong G$ for any group G via, at least, the identity isomorphism.*
2. *Any non-abelian group of order 6 is isomorphic to S_3. In particular, $D_6 \cong S_3$. We shall prove this later when we study classification theorems.*
3. *$\varphi : \mathbb{R} \to \mathbb{R}_{>0}$ by $\varphi(x) = \exp(x)$ is an isomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}_{>0}, \times)$.*

Proposition 1.20. *If $\varphi : G \to H$ is an isomorphism, then*

1. *$|G| = |H|$*
2. *G is abelian if and only if H is abelian*
3. *$|x| = |\varphi(x)|$ for all $x \in G$.*

Example 1.21. Note that if $\varphi : G \to H$ is an isomorphism, then $|G| = |H|$, but the converse is not true. For example, S_3 is not isomorphic to $\mathbb{Z}/6\mathbb{Z}$, despite their cardinality being the same, because the latter is abelian while the former is not.

1.5. Group Actions

So far, we have seen homomorphisms/isomorphisms which maps a group G to a group H. Now, we will look at a particular mapping from $G \times A$ to A where G is a group and A is an arbitrary set.

Definition 1.22 (Group Action)**.** *A **group action** of a group G on a set A is a mapping $\varphi : G \times A \to A$ such that:*

1. $\varphi(g_1, \varphi(g_2, a)) = \varphi(g_1 g_2, a)$ *for all* $g_1, g_2 \in G, a \in A$
2. $\varphi(1, a) = a$ *for all* $a \in A$

We will usually use notation that suppresses the fact that a group action is a mapping and, instead, write ga to mean $\varphi(g, a)$. As such, the requirements can be written as $g_1(g_2 a) = (g_1 g_2)a$ and $1a = 1$.

Observation. *A group action can be thought of as a permutation of the set. Since each group element maps elements $a \in A$ to $a' \in A$, we can think of each group element as a permutation in the symmetric group, S_A. Concretely, $g \cdot a$ is $g \in G$ is acting on $a \in A$. Now, for each $g \in G$, we can define $\sigma_g : A \to A$ by $\sigma_g(a) = g \cdot a$. Then,*

1. *σ_g is a permutation of A for each g, and*
2. *$\psi : G \to S_A$ via $\psi(g) = \sigma_g$ is a homomorphism. In particular, ψ is called the **permutation representation** associated to the given group action. In other words, for each group action, there exists a permutation representation corresponding to the group action.*

To see the first, one can show that σ_g has an inverse which is $\sigma_{g^{-1}}$; this follows from the first defining property of a group action. To see the second, we can show that $\psi(g_1 g_2)(a) = (\psi(g_1) \cdot \psi(g_2))(a)$. This means, a group action of G on a set A is to be understood as a way of turning every element of G into a permutation on the set A.

Observation. *We saw that, given a group action, there is an associated permutation representation i.e. a homomorphism $G \to S_A$. We can reverse this process. Given a homomorphism $\psi : G \to S_A$, we can construct a group action $G \times A \to G$ by setting $g \cdot a = \psi(g)(a)$.*

Examples 1.23. *We now look at a number of examples of group actions.*

1. *The trivial action is defined by setting $g \cdot a = a$ for all $a \in A$ and all $g \in G$ i.e. all elements of G correspond to the identity permutation in S_A. The associated permutation representation sends every element in G to the identity $1 \in S_A$.*
2. *On the other hand, if each element of G corresponds to a unique permutation in S_A, we say that the group action is **faithful**. The associated permutation representation is injective.*
3. *Let our group be a field F and let V be a vector space defined over F. Then, F acts on V via $\alpha\vec{v} = \alpha(v_1, \cdots, v_n) = (\alpha v_1, \cdots, \alpha v_n) \in V$.*
4. *Let A be a nonempty set. Then, the symmetric group of A, S_A, acts on A via $\sigma \cdot a = \sigma(a)$ for any $a \in A, \sigma \in S_A$. The associated permutation representation,* $\mathrm{id} : S_A \to S_A$*, is identity.*
5. *After fixing some labeling of the vertices of an n-gon, each element of D_{2n} corresponds to a permutation σ in S_n defined by the way the element permutes the corresponding vertices. This gives us a group action $D_{2n} \times \{1, \cdots, n\} \to \{1, \cdots, n\}$ i.e. $\sigma \cdot i = j$ where j is the permutation of i under σ.*

1.6. SUBGROUPS

Definition 1.24 (Subgroups)**.** *Let G be a group and let H be a subset of G. Then, H is called a subgroup if*

1. *H is non-empty, i.e. $H \neq \emptyset$*
2. *H is closed under the group operation and inverses, i.e. $xy, x^{-1} \in H$ for all $x, y \in H$*

In symbols, we write $H \leq G$.

Examples 1.25. *We look at some examples and non-examples of subgroups.*

1. *Any group G has at least two subgroups: $H = G$ and $H = \{1_G\}$.*
2. *$\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R}$.*
3. *Note that the subgroup must be defined with respect to the same operation as that of the group. For example, $(\mathbb{Q} - \{0\}.\times)$ is not a subgroup of $(\mathbb{R}, +)$ even though both are groups.*
4. *D_6 is not a subgroup of D_8 since D_6 is not a subset of D_8 - this is because the symmetries in D_6 are not the same as the symmetries in D_8 (e.g., the rotation is by 60 degrees in D_6 whereas it is by 45 degrees in D_8).*

Alternatively, one can verify whether H is a subgroup of G via the following criterion:

Proposition 1.26 (Subgroup Criterion)**.** *A subet $H \subseteq G$ of a group G is a subgroup if and only if*

1. *$H \neq \emptyset$, and*
2. *$xy^{-1} \in H$ for all $x, y \in H$.*

If H is finite, an equivalent and sufficient criterion is to simply check that

1. *$H \neq \emptyset$*
2. *H is closed under group operation.*

We will now look at some special classes of subgroups.

1.6.1 Centralizers, Normalizers, Centre

Given a subset A of a group G, we can construct some important classes of subgroups of G defined by how they interact with that specific set A. This leads us to the definitions of centralizers and normalizers. The centre of a group is another important subgroup that is defined by considering the subset $A = G$.

Definition 1.27 (Centralizers)**.** *Let G be a group and let A be a subset of G that is non-empty. Then, the centralizer of A in G is defined as*

$$C_G(A) := \{g \in G \mid gag^{-1} = a, \forall a \in A\}.$$

*In other words, the centralizer of A in G are **all the elements in G that elements of A commute with.***

Theorem 1.28. *The centralizer, $C_G(A)$, is a subgroup, i.e. $C_G(A) \leq G$.*

The proof is straightforward using the subgroup criterion.

Observation. *Note that if G is an abelian group, then for any non-empty subset A of G, $C_G(A) = G$.*

The centralizer is a particularly strict criterion in the sense that $a \in A$ must commute with all the elements in $C_G(A)$ i.e. $ag = ga$ for all $g \in C_G(A)$. Next, we look at the normalizer which relaxes the condtion quite a bit.

Definition 1.29 (Normalizer)**.** *let A be a non-empty subset of the group G. Then, the normalizer of A in G is the set*

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

where $gAg^{-1} = \{gag^{-1} \mid a \in A\}$. In other words, the normalizer of A in G are all the elements in G that conjugate elements of A (i.e. gag^{-1}) and return some element in A.

So far, our constructions were with respect to some non-empty subset A of a group G. Next, we look at the centre of a group, which can be seen as the centralizer of the subset G of G.

Theorem 1.30. *The normalizer of a set A in group G is a subgroup, i.e. $N_G(A) \leq G$.*

Definition 1.31 (Centre)**.** *The centre of a group G is defined as the subset of elements that commute with all elements of G, i.e.*

$$Z(G) := \{x \in G \mid xg = gx, \forall g \in G\}.$$

Theorem 1.32. *The centre of a group G is a subgroup, i.e. $Z(G) \leq G$.*

We will soon see an elegant way to understand why the normalizer and the centre are subgroups.

1.6.2 Stabilizers and Kernels

Now, we define some classes of subgroups that are defined with respect to a *group action* of G. In particular, again, we consider some non-empty subset $A \subseteq G$. We will also see that the preceding subgroups (i.e. centralizers, normalizers, and centre) can be defined as special cases of the constructions we will see now.

Recall that a group action is a mapping $G \times A \to A$ such that that the mapping is associative and $1 \cdot a = a$.

Definition 1.33 (Stabilizer)**.** *If G is a group acting on a set A, and $a \in A$ is some fixed element, then the stabilizer of a in G is the set*

$$G_a = \{g \in G \mid g \cdot a = a\}$$

where $g \cdot a$ is the group action of G on A.

Theorem 1.34. *The stabilizer is a subgroup, i.e. for any $a \in A \subseteq A$, $G_a \leq G$*

Definition 1.35 (Kernel of Group Action)**.** *If the group G is acting on a set A, then the kernel of the group action is defined as*

$$\{g \in G \mid g \cdot a = a, \forall a \in A\}.$$

Theorem 1.36. *The kernel of a group action of G on a set A is a subgroup of G.*

Now, we finally come to the main observation where we note that several of these constructions can be unified by the notion of ***conjugation***. Let $X = \mathcal{P}(G)$ be the set of all subsets of the group G. Now, suppose G acts on X by conjugation, i.e. for any $g \in G$ and $M \in X = \mathcal{P}(G)$, we say $g \cdot M = gMg^{-1} = \{gmg^{-1} \mid m \in M\}$. Then, we can note the following:

1. the normalizer, $N_G(A)$, is the stabilizer of A in G, i.e. $N_G(A) = G_A$ where $A \in \mathcal{P}(G)$
2. if the normalizer, $N_G(A)$ acts on the set A by conjugation, i.e. $g \cdot a = gag^{-1}, \forall a \in A$ and $g \cdot a \in A$ since $g \in N_G(A)$, then $C_G(A)$ is the kernel of this action. In other words, **the centralizer is the kernel of the action of $N_G(A)$ on A by conjugation.** As such,

$$C_G(A) \leq N_G(A).$$

3. the center of a group G, $Z(G)$, is the kernel of G acting on G by conjugation. As such,

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

1.7. Cyclic Groups

Definition 1.37 (Cyclic Groups)**.** *A **cyclic group** is a group is a group H that is generated by a single element, i.e.*

$$H = \{x^n \mid n \in \mathbb{Z}\}.$$

Note that n iterates over all integers, including negative integers. In other words, we product x with both itself and its inverse.

Here, we wrote the group operation as multiplication as just a matter of notation; we could have also written the group operation as addition, which would lead us to write $H = \{nx \mid n \in \mathbb{Z}\}$. In either case, we denote a cyclic group as $H = \langle x \rangle$ and say that H is a group that is generated by x.

Observation. *The generator in a cyclic group need not be unique. For example, if $H = \langle x \rangle$, we could also write $H = \langle x^{-1} \rangle$. This is because:*

- *In multiplicative notation where $H = \{x^n \mid n \in \mathbb{Z}\}$, any x^n can be written as $(x^{-1})^{-n}$, so $H = \{x^{-1} \mid n \in \mathbb{Z}\}$.*
- *In additive notation where $H = \{nx \mid n \in \mathbb{Z}\}$, any nx can be written as $(-n)(-x)$, so $H = \{n(-x) \mid n \in \mathbb{Z}\}$.*

Examples 1.38. *We take a look at some examples of cyclic groups. They often appear as subgroups of larger groups that may not be cyclic themselves.*

Consider the dihedral group: $G = D_{2n}$. Now, let H be the group of all rotations. Then, $H = \langle r \rangle = \{r^m \mid m \in \mathbb{Z}\}$. Note that $|H| = n$ since $r^n = 1 = r^0$. Also, $r^{-1} = r^{n-1}$.

The group of integers is cyclic i.e. $\mathbb{Z} = \langle 1 \rangle$.

1.7.1 Cardinality of cyclic group

We immediately note that there is a simple way of figuring out the cardinality of a cyclic group via its generator:

Proposition 1.39. *If H is a cyclic group and $H = \langle x \rangle$. Then, $|H| = |x|$ (note that $|H|$ and $|x|$ are allowed to be infinite).*

- *if $|H| = n < \infty$, then $x^n = 1$ and the distinct elements of H are $\{1, x, \cdots, x^{n-1}\}$.*
- *if $|H| = \infty$, then $x^n \neq 1$ for any $n \neq 0$.*

Proof. First, suppose $|x| = n$. For any arbitrary $x^k \in H$, we can write using the division algorithm that $k = nq + r$ where $0 \leq r < n$. Then, $x^k = x^{nq+r} = (x^n)^q \cdot x^r = x^r \in \{1, x, \cdots, x^{n-1}\}$. One can easily show that $x^a \neq x^b$ is $a, b \in \{1, \cdots, n-1\}$ and $a \neq b$: if not, then, $x^{b-a} = 1$ but we know that n is the smallest positive integer such that $x^n = 1$. The proof for the infinite order is simple: no two x^a and x^b are equal for $a \neq b$ since, otherwise, we have an n such that $x^n = 1$ where $0 < n < \infty$. □

Lemma 1.40. *Let $x \in G$ where G is a group and let $m, n \in \mathbb{Z}$. If $x^m = 1 = x^n$, then*

$$x^d = 1, \quad \text{where } d = (m, n).$$

In particular, if $x^m = 1$, then $|x|$ divides m.

Now, we come to an important result:

Theorem 1.41 (Classification of Cyclic Groups)**.** ***Any two cyclic groups of the same order are isomorphic**.*

1. *Suppose the cyclic groups $\langle x \rangle$ and $\langle y \rangle$ are both of order $n \in \mathbb{Z}_{>0}$. Then, the following is an isomorphism: $\varphi(x^k) = y^k$.*
2. *Suppose $\langle x \rangle$ is a cyclic group, then $\varphi(k) = x^k$ is an isomorphism. This follows from the observation that if $\langle x \rangle$ is of order n, then $\langle x \rangle \cong \mathbb{Z}/n\mathbb{Z}$.*

3. *In particular, for any $n \in \mathbb{Z}_{>0}$, let Z_n be the cyclic group of order n, then*

$$Z_n \cong \mathbb{Z}/n\mathbb{Z}.$$

Proof Sketch: First we show that φ is well-defined. Suppose $x^r = x^s$. Then, we show that $\varphi(x^r) = \varphi(x^s)$. Note that $x^{r-s} = 1$, so $n|(r-s)$ by our previous lemma. Write $(r-s) = nt$. Then, $\varphi(x^r) = \varphi(x^{tn+s}) = y^{tn+s} = y^s = \varphi(x^s)$.

1.8. Formulas for orders and finding generators

In this section, we try to find the generators of a cyclic group.

First, we try to calculate the order of arbitrary powers of x in an arbitrary group. **Note:** the following result applies to an arbitrary group, not necessarily a cyclic group.

Proposition 1.42. *Let G be a group (not necessarily cyclic) and let $x \in G$. Let $a \in \mathbb{Z} - \{0\}$.*

1. *if $|x| = \infty$, then $|x^a| = \infty$*
2. *if $|x| = n < \infty$, then $|x^a| = \frac{n}{(n,a)}$*
3. *if $|x| = n < \infty$ and $a|n$, then $|x^a| = \frac{n}{a}$.*

Now, we use this to understand which elements in a cyclic group are generators of the group.

Proposition 1.43. *Let H be a cyclic group, i.e. $H = \langle x \rangle$. Then,*

1. *If $|x| = \infty$, then $H = \langle x^a \rangle$ if and only if $a = 1$ or $a = -1$.*
2. *If $|x| = n < \infty$, then $H = \langle x^a \rangle$ if and only if $(a, n) = 1$.*

Proof Sketch: we know that $\langle x^a \rangle$ generates a group of order $|x^a|$, so if $\langle x^a \rangle = \langle x \rangle$, we require that $|x^a| = |x|$. By 1.42, this is true if and only if $(a, n) = 1$.

Example 1.44. Consider $\mathbb{Z}/12\mathbb{Z}$. Then, we know that $\bar{1}, \bar{5}, \bar{7}$, and $\bar{11}$ are generators, since for each of these $(a, 12) = 1$.

Theorem 1.45. *Let $H = \langle x \rangle$ be a cyclic group.*

1. *Every subgroup of H is cyclic. More precisely, if $K \leq H$, then either $K = \{1\}$ (i.e. the trivial group) or $K = \langle x^d \rangle$, where d is the smallest positive integer such that $x^d \in K$.*
2. *If $|H| = \infty$, then for any distinct nonnegative integers a and b, $\langle x^a \rangle \neq \langle x^b \rangle$. Furthermore, for every integer m, $\langle x^m \rangle = \langle x^{|m|} \rangle$, where $|m|$ denotes the absolute value of m.* ***In other words, the nontrivial subgroups of H correspond bijectively with the integers*** *$1, 2, 3, \ldots$.*
3. *If $|H| = n < \infty$, then for each positive integer a dividing n there is a unique subgroup of H of order a. This subgroup is the cyclic group $\langle x^d \rangle$, where $d = \frac{n}{a}$.*

   Furthermore, for every integer m, $\langle x^m \rangle = \langle x^{(n,m)} \rangle$, so that ***the subgroups of H correspond bijectively with the positive divisors of n.***

1.9. Subgroups generated by subsets

The next class of subgroups we will look at are subgroups that are generated by subsets of a group. Let G be a group and let A be a subset of a group. We will define the subgroup generated by A to be the intersection of all subgroups of G that contain A. Naturally, this raises the question: is this intersection guaranteed to be a group? We prove this using the following lemma:

Lemma 1.46. *Let $\mathcal{C} \neq \emptyset$ be a collection of subgroups of a group G. Then, the intersection of all elements of $\mathcal{C}$ is a subgroup of G.*

Proof. Define $K = \cap_{X \in \mathcal{C}} X$. Given $1_G \in X$ (since X is defined to be a subgroup for each $X \in \mathcal{C}$), $1_G \in K$. If $x \in K$, then $x \in X$ for all $X \in \mathcal{C}$, which implies $x^{-1} \in X$ for all $X \in \mathcal{C}$, which implies $x^{-1} \in K$. This logic can be used to show that if $x, y \in K$, then $xy^{-1} \in K$. □

Definition 1.47 (Subgroup generated by a Subset)**.** *Let G be a group and let A be a subset of G. The, the subgroup of G generated by A is defined as the intersection of all subgroups of G containing A, i.e.*

$$\langle A \rangle := \cap_{A \subseteq H, H \leq G} H. \tag{1}$$

In particular, for notational clarity, we set the following:

1. *If $A = \{a_1, \cdots, a_n\}$ is a finite set, we write $\langle a_1, \cdots, a_n \rangle = \langle A \rangle$.*
2. *If A and B are two subsets, we write $\langle A, B \rangle = \langle A \cup B \rangle$.*

Observation. *Note that $\langle A \rangle$ is a subgroup by our last lemma if we let $\mathcal{C} = \{H \mid H \leq G, A \subseteq H\}$.*

So far, we have only said that this definition gives us a subgroup that is generated by a subset. However, we do not yet know what the elements of this subgroup look like. We remedy this in the next result.

Definition/Proposition 1.48. *The subgroup of G that is generated by the subset $A \subseteq G$ can be written as:*

$$\langle A \rangle = \{a_1^{\epsilon_1} a_2^{\epsilon_2} \cdots a_t^{\epsilon_t} \mid a_i \in A, \epsilon \in \{\pm 1\}, t \in \mathbb{Z}\} =: \bar{A}. \tag{2}$$

Proof. It is easy to show that $\bar{A}$ is a subgroup. To show that $\langle A \rangle = \bar{A}$, we first note that $\langle A \rangle \subseteq \bar{A}$ since each $a \in$ can be written as $a^1 \in \bar{A}$. To show the reverse direction, we simply note that products and inverses belong to the group, so $\bar{A} \subseteq \langle A \rangle$. □

1.10. Quotient Groups

Definition 1.49 (Fibers)**.** *Given $\varphi : G \to H$ is a group homomorphism, the fibers of φ are the sets of elements of G that φ maps to single elements. In other words, the fiber of φ above $h \in H$, denoted by X_h, is defined as:*

$$X_h = \{g \in G \mid \varphi(g) = h\}.$$

Observation. *Note that there is a natural operation we can do on fibers themselves because of the properties of homomorphisms. Let X_h and $X_{h'}$ be two fibers. Then, $X_h X_{h'}$ is the fiber $X_{hh'}$. This is because for any $\alpha \in X_h, \beta \in X_{h'}$, $\varphi(\alpha\beta) = \varphi(a)\varphi(\beta) = hh'$.*

This will allow us to define the quotient group as the group of fibers of a homomorphism.

Definition 1.50 (Kernel and image of a homomorphism)**.** *Let $\varphi : G \to H$ be a group homomorphism. Then, the kernel of φ is*

$$\ker \varphi := \{g \in G \mid \varphi(g) = 1_H\}.$$

On the other hand, the image of the homomorphism is defined as

$$\operatorname{im} \varphi := \{h \in H \mid \varphi(g) = h \text{ for some } g \in G\}.$$

We look at some immediate properties of kernels and images:

Proposition 1.51. *Let $\varphi : G \to H$ be a group homomorphism. Then,*

1. *$\varphi(1_G) = 1_H$, $\varphi(g^{-1}) = \varphi(g)^{-1}$ and $\varphi(g^n) = \varphi(g)^n$*
2. *$\ker \varphi$ and $\operatorname{im} \varphi$ are subgroups of G and H respectively, i.e. $\ker \varphi \leq G$ and $\operatorname{im} \varphi \leq H$.*

Now, we define the quotient group:

Definition 1.52 (Quotient Group)**.** *Let $\varphi : G \to H$ be a group homomorphism with $K = \ker \varphi$. Then, the quotient group, denoted by G/K, is the group whose elements are fibers X_h for each $h \in H$ and the operation is defined by $X_h X_{h'} = X_{hh'}$. Note that K is also an element in G/K; concretely $K = X_{1_H}$ and K is the identity of the quotient group G/K.*

The odd thing about this definition is that X_h is very opaque. What we will now see is that each fiber is essentially a translate of the kernel K via *some* representative:

Proposition 1.53. *Let $\varphi : G \to H$ be a group homomorphism and let $K := \ker \varphi$ be its kernel. Then, $X_h \in G/K$ can be written as, for any $g' \in X_h$,*

$$X_h = g'K := \{g'k \mid k \in K\}$$

and

$$X_h = Kg' := \{kg' \mid k \in K\}.$$

Proof. It is easy to see that $g'K \subseteq X_h$ because $\varphi(g'k) = h$ for any $k \in K$. To see the reverse inclusion, let $g \in X_h$, i.e. $\varphi(g) = h$. Now, define $k = g'^{-1}g$. Then, $\varphi(k) = \varphi(g'^{-1}g) = \varphi(g')^{-1}\varphi(g) = h^{-1}h = 1$. So, $k \in K$. Therefore, $g = g'k \in g'K$. □

We used a particularly general construction in this definition that is worth noting separately:

Definition 1.54 (Left coset/Right coset and Representatives)**.** *For a subgroup N of G and some element $g \in G$, we will use the notation $gN = \{gn \mid n \in N\}$ which is called a **left coset** of N in G. Similarly, $Ng = \{ng \mid n \in N\}$ which is called a **right coset** of N in G. Any element of a coset is called a **representative** of the coset. In particular, $g = g1 = 1g$ itself is a representative of the coset gN or Ng.*

Note that if G is an additive group, we will write $g + N$ to be the left coset of N in G with representative g (and the equivalent statement for right cosets is true).

Observation. *The quotient group G/K contains of elements that are the left cosets of $K = \ker \varphi$ in G. In other words, the elements of G/K look like gK where g is a representative of a fiber. Furthermore, since different representatives define the same fiber, the choice of the representative does not matter – we will formalize this now:*

Proposition 1.55. *Let G be a grup and let $K = \ker \varphi$ for some group homomorphism φ. Then, consider the set of left cosets of K in G and define the following operation on them: $uK \circ vK = (uv)K$. Then,*

1. *This operation defined a group, called the quotient group, denoted by G/K*
2. *The operation is well-defined, i.e. if $u_1 \in uK$ and $v_1 \in vK$, then $u_1v_1 \in uvK$ and $u_1v_1K = uvK$. In other words, the group operation does not depend on the choice of representative.*
3. *The statements are true after replacing left cosets with right cosets.*

In light of all this, we write the following as the definition of a quotient group:

Definition 1.56 (Quotient Group)**.** *let $\varphi : G \to H$ be a group homomorphism and let $K = \ker \varphi$. Then, the quotient group G/K is defined as the cosets of the kernel $K = \ker \varphi$ in G, i.e.*

$$G/K := \{\bar{g} := gK \mid g \in G\}$$

with the group operation being $\bar{g} \cdot \bar{g'} = \overline{gg'}$, i.e. $gK \cdot g'K = (gg')K$. Note that $\bar{g} = \bar{g'}$ if $g' \in gK$ or $g \in g'K$.

Example 1.57. Let $\varphi : G \to H$ be an isomorphism. Then, the kernel is just 1. In particular, the fibres of φ are singleton subsets of G (since φ is injective and subjective), so $G/1 \cong G$.

Example 1.58. Consider the homomorphism $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. This has the kernel $K = n\mathbb{Z}$. Then, the cosets of K in $\mathbb{Z}$ are $a + K = a + n\mathbb{Z}$ for each $a \in \mathbb{Z}$.

Example 1.59. let $G = \mathbb{R}^2$ and let $H = \mathbb{R}$. Define $\varphi : G \to H$ by $\varphi((x, y)) = x$. Then, one can show that φ is a homomorphism and its kernel is $\ker \varphi = \{(0, y) \mid y \in \mathbb{R}\}$. Then, the quotient group G/K consists of the cosets $\overline{(x, 0)} = (x, 0) + \ker \varphi$ for each $x \in \mathbb{R}$.

1.10.1 Important properties of cosets and representatives

Some of what we have seen so far can be generalized. For example, the fact that a coset can be written using any representative and the choice of the representative does not make a material difference in defining the coset can be generalized to cosets of other subgroups as well alongside cosets of a kernel. On the other hand, we will see that the group operation in the quotient group, i.e. $uK \cdot vK = uvK$, is only defined if K satisfies some properties.

Proposition 1.60. *Let N be any subgroup of G, i.e. $N \leq G$. Then, the set of left cosets of N (sets of the form gN for $g \in G$) partition G, i.e. all elements of G belong to some coset of N in G. In particular, for all $u, v \in G$, $uN = vN$ if and only if $v^{-1}u \in N$. In particular, $uN = vN$ if and only if u and v are representatives of the same coset.*

Proof. Since $1 \in N$ (as N is a subgroup), each element of G can be written as $g = g \cdot 1 \in gN$. As such, g is a representative of the coset gN and, therefore, $G = \cup_{g \in G} gN$. We must now show that distinct cosets have no intersection. In other words, if $uN \cap vN \neq \emptyset$, then $uN = vN$. Let $x \in uN \cap vN$. Then, $x = un = vm$ for some $m, n \in N$. now, $u = vmn^{-1} = vm_1$ where $m_1 := mn^{-1} \in N$. Then, $uN = \{ut \mid t \in N\} = \{vm_1 t \mid t \in N\} = vm_1 N \subseteq vN$. Similarly, $vN \subseteq uN$, which gives us $uN = vN$.

Now, we prove the second statement. We know that $uN = vN$ if and only if $u \in vN$ if and only if $u = vn$ for some $n \in N$ if and only if $v^{-1}u \in N$.

Now, we prove the last statement. Again, $uN = vN$ if and only if $v \in uN$ which is equivalent to saying $v = v \cdot 1_G$ is a representative of uN. Similarly, $uN = vN$ if and only if $u \in vN$ which is equivalent to saying u is a representative of vN. Since $uN = vN$, therefore, u and v are representatives of the same coset. □

Since this makes remembering almost everything so far quite simple, it is worth writing it again: **Two cosets are the same, i.e. $uN = vN$, if and only if u and v are representatives of the same coset. Also, two cosets are the same, i.e. $uN = vN$, if and only if $u \in vN$.**

Note that, in additive notation, we would say that two cosets are the same, i.e. $uN = vN$, if and only if $u \in v + N$

Now, we come to the second part: what are the requirements on the subgroup N that make $uN \circ vN = (uv)N$ a well-defined group operation?

Proposition 1.61. *Let G be a group and let N be a subgroup, $N \leq G$.*

1. *The operation $uN \circ vN = (uv) \circ N$ is well-defined if and only if $gng^{-1} \in N$ for all $g \in G, n \in N$ (as we will soon see - this means, this operation is well-defined if and only if N is a normal subgroup).*
2. *If this condition is satisfied, then the set of left cosets of N in G, i.e. $\{gN \mid g \in G\}$, is a group with the group operation $gN \circ g'N = (gg')N$. In particular, the identity is the coset $1N$ and the inverse of gN is $g^{-1}N$.*

Proof. We sketch the proof of the first part. Assume that the operation is well-defined. Then, suppose $u, u_1 \in uN$ and $v, v_1 \in vN$. We know that $uN \circ vN = (uv)N$. But choosing different representatives of uN and vN, we get that $u_1N \circ v_1N = (u_1v_1)N$ must be the same as $(uv)N$, so $(uv)N = (u_1v_1)N$. Now, let $u = 1$, $u_1 = n$ for some $n \in N$ (clearly, then $u, u_1 \in uN$) and let $v = v_1 = g^{-1}$ for some fixed $g \in G$. Then, $1g^{-1}N = ng^{-1}N$ which implies $g^{-1}N = ng^{-1}N$. Clearly, $ng^{-1} \in ng^{-1}N$, so $ng^{-1} \in g^{-1}N$, so $ng^{-1} = g^{-1}n'$ for some $n' \in N$, which gives us that $gng^{-1} \in n' \in N$. Conversely, suppose $gng^{-1} \in N$ for all $g \in G, n \in N$. Again, let $u, u_1 \in uN$ and $v, v_1 \in vN$. Write $u_1 = un$ and $v_1 = vm$ for some $n, m \in N$. We can show that $u_1v_1 = (uv)(n_1m)$ where $n_1 = v^{-1}nv$ which is in N by assumption. Since N is closed under products, $n_1m \in N$, so $u_1v_1 = (uv)n_2$ for some $n_2 \in N$ (precisely $n_2 = n_1m \in N$. Since $u_1v_1 \in uvN$, $u_1v_1N = uvN$. As such, the operation is well-defined. □

Subgroups that satisfy these properties are extremely important in the study of groups and, as such, are given a separate name.

Definition 1.62 (Normal Groups and conjugates)**.** *Let G be a group and let N be a subgroup of G. The element gng^{-1} is called the conjugate of $n \in N$ by $g \in G$. The set $gNg^{-1} = \{gng^{-1} \mid n \in N\}$ is called the conjugate of N by g.*

*In particular, the element g is said to normalize N if $gNg^{-1} = N$. A subgroup N of a group G is called a **normal subgroup** if $gNg^{-1} = N$ for all $g \in G$, i.e. every element of G normalizes N. If N is a normal subgroup of G, we write $N \trianglelefteq G$.*

Theorem 1.63. *Let N be a subgroup f the group G. Then, the following are equivalent:*

1. *$N \trianglelefteq G$*
2. *$N_G(N) = G$, i.e. the normalizer of N in G is G itself*
3. *$gN = Ng$ for all $g \in G$*
4. *The set of left cosets are a group under the operation $uN \circ vN = (uv)N$*
5. *$gNg^{-1} \subseteq N$ for all $g \in G$.*

Note that the kernel of a homomorphism satisfies both the requirements in lemma 1.61. One can ask whether all subgroups N that satisfy these properties can be shown to be the kernel of some homomorphisms. This is answered in the next proposition:

Proposition 1.64. *A subgroup N of the group G is normal if and only if it is the kernel of some homomorphism.*

Proof. The kernel of a homomorphism is normal as we have already shown. We need to now show that if $N \trianglelefteq G$, then there exists a homomorphism whose kernel is N. Define $\varphi : G \to G/N$ by $\varphi(g) = gN$ for all $g \in G$. Note that this is a homomorphism as $\varphi(g_1g_2) = (g_1g_2)N = g_1N \cdot g_2N = \varphi(g_1)\varphi(g_2)$. Now, it is easy to check that $\ker \varphi = \{g \in G \mid \varphi(g) = 1N\} = \{g \in G \mid gN = 1N\} = \{g \in G \mid g \in N\} = N$. □

Definition 1.65. *Let $N \trianglelefteq G$ be a normal subgroup. The homomorphism $\pi : G \to G/N$ defined by $\pi(g) = gN$ is called the **normal projection/homomorphism** of G onto G/N. If $\bar{H} \leq G/N$ is a subgroup of G/N, the complete preimage of $\bar{H}$ in G is the preimage of $\bar{H}$ under the normal projection homomorphism.*

Example 1.66. For any group G, the subgroups 1 and G are normal in G. In particular, $G/1 \cong G$ and $G/G \cong 1$.

Example 1.67. Let G be an abelian group, then *any* subgroup N of G is a normal subgroup since $gng^{-1} = gg^{-1}n = n \in N$ for all $g \in G, n \in N$.

Example 1.68. Let $G = Z_k$ be the cyclic group of order k. Let x be a generator of G and let $N \leq G$. Then, $N = \langle x^d \rangle$ where d is the smallest integer such that $x^d \in N$. Then,

$$G/N = \{gN \mid g \in G\} = \{x^\alpha N \mid \alpha \in \mathbb{Z}\}.$$

Now, since $x^\alpha N = (xN)^\alpha$, $G/N = \langle xN \rangle$, i.e. G/N is cyclic and its generator is xN. Furthermore, $|G/N| = \frac{|G|}{|N|}$. **In other words, the quotient groups of cyclic groups are cyclic**.

We now prove the following theorem, known as Lagrange's Theorem, which allows us to compute the order of a quotient group.

Theorem 1.69 (Lagrange's Theorem)**.** *If G is a finite group and H is a subgroup of G, then the order of H divides the order of G and the number of left cosets of H in G equals $\frac{|G|}{|H|}$.*

Proof. Let $|H| = n$ and let the number of left cosets of H in G equal k. Now, we claim that for any fixed $g \in G$, $|gH| = n$. This can be seen by noting that the map $H \to gH$ by $h \to gh$ is (a) surjective by definition and (b) injective because (if $gh_1 = gh_2$, then $h_1 = h_2$), and so $|gH| = |H| = n$.

Now, we have proven previously (see Proposition 1.60) the left cosets of H in G partition G, so $|G| = |$ no. of left cosets $| \cdot |$ cardinality of each left coset $| = kn$. As such, number of left cosets of H in G is $k = \frac{|G|}{n} = \frac{|G|}{|H|}$. □

One point to note and remember from this proof is the idea that $|H| = |gH|$ and that $H \to gH$ is a bijection.

Definition 1.70 (Index of a subgroup)**.** *Let G be a group and let H be a subgroup of G. Then, the index of H in G is the number of left cosets of H in G. We denote the index by $|G : H|$.*

Note that if G is a finite group, then by Lagrange's theorem, $|G : H| = \frac{|G|}{|H|}$. However, if G is an infinite group, then this is not true. In particular, a subgroup of an infinite group can have finite index or infinite index. As an example, consider the group $\mathbb{Z}$. Then, the trivial subgroup $\{0\}$ has order 1 but the subgroup $\langle n \rangle$ is of index n (assuming $n > 0$).

Corollary 1.71. *let G be a group. We have the following consequences of Lagrange's theorem:*

1. *If G is a finite group and let $x \in G$. Then, $|x|$ divides the order of G. In particular, $x^{|G|} = 1$ for all $x \in G$.*
2. *If G is a group of order p where p is a prime integer. Then, G is cyclic, hence $G \cong Z_p$. (Recall that Z_p is the cyclic group of order p and $Z_p \cong \mathbb{Z}/p\mathbb{Z}$)*

Example 1.72. Let $H = \langle (1, 2, 3) \rangle \leq S_3$ and let $G = S_3$. We now show that $H \trianglelefteq S_3$ using Lagrange's theorem. First, one can show that $H \leq N_G(H) \leq G$. Now, by Lagrange's theorem, the order of H divides the order of $N_G(H)$ which divides the order of S_3, which is 6. Now, since G has order 6 and H has order 3, the only possibilities for $N_G(H)$ are that $N_G(H)$ is either the same as H or the same as $G = S_3$. Now, one can show that $(1, 2)$ conjugates $(1, 2, 3)$ to $(1, 2, 3)^{-1}$. So, $(1, 2)$ conjugates a generator of H to another generator of H, which allows us to conclude that $(1, 2) \in N_G(H)$. Since $(1, 2) \notin H$, so, $N_G(H) \neq H$ and $N_G(H) = G$, which allows us to conclude that $H \trianglelefteq S_3$.

Definition 1.73 (Simple Groups)**.** *Simple groups are groups whose only normal subgroups are 1 and G.*

Theorem 1.74 (Cauchy's Theorem)**.** *If G is a finite group and p is a prime dividing $|G|$, then G has an element of order p.*

Theorem 1.75 (Sylow)**.** *If G is a finite group of order $p^\alpha m$, where p is a prime and p does not divide m, then G has a subgroup of order p^α.*

Proposition 1.76. *If H and K are finite subgroups of a group, then*

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

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

Proposition 1.77. *If H and K are subgroups of a group, HK is a subgroup if and only if $HK = KH$.*

Corollary 1.78. *If H and K are subgroups of G, and $H \leq N_G(K)$, then $HK \leq G$. In particular, if $K \trianglelefteq G$, then $HK \leq G$ for any $H \leq G$.*

1.11. Group Isomorphism Theorems

Theorem 1.79 (First Isomorphism Theorem)**.** *Let $\varphi : G \to H$ be a group homomorphism. Then, $\ker \varphi \trianglelefteq G$ and $G/\ker \varphi \cong \varphi(G)$.*

Proof. Let $x \in \ker \varphi$. Then, for any $g \in G$, $\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g)^{-1} = \varphi(g)1_H\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = 1_H$, so $gxg^{-1} \in \ker \varphi$. We already know that $\ker \varphi$ is a subgroup, so $\ker \varphi \trianglelefteq G$. To prove the second statement, define $\Psi : G/\ker \varphi \to \varphi(G)$ by $\Psi(g \ker \varphi) = \varphi(g)$. Now, with $K = \ker \varphi$,

- Ψ is well-defined. Suppose $gK = hK$. Then, $h^{-1}g \in K$. Then, $\varphi(h^{-1}g) = 1_H$. But $\varphi(h^{-1}g) = \varphi(h)^{-1}\varphi(g) = 1_H$, which implies $\varphi(h) = \varphi(g)$. So, $\Psi(g) = \Psi(h)$.
- Ψ is a homomorphism since $\Psi(gK \circ hK) = \Psi(ghK) = \varphi(gh) = \varphi(g)\varphi(h) = \Psi(gK)\Psi(hK)$.

- Ψ is injective. This is because $\Psi(gK) = \Psi(hK) \implies \varphi(g) = \varphi(h)$. But then, $\varphi(h)^{-1}\varphi(g) = 1_H$, which implies $\varphi(h^{-1}g) = 1_H$. So $h^{-1}g \in K$, so $gK = hK$.
- Ψ is surjective by definition of the morphism.

□

Corollary 1.80. *Let $\varphi : G \to H$ be a group homomorphism. Then, φ is injective if and only if* $\ker \varphi = 1$. *Furthermore,* $|G : \ker \varphi| = |\varphi(G)|$.

Proof. If φ is injective, then, $\ker \varphi = 1_G$ by definition of an injective map. On the other hand, if $\ker \varphi = 1_G$, then suppose $\varphi(x) = \varphi(y)$. Then, $\varphi(y)^{-1}\varphi(x) = \varphi(y^{-1}x) = 1_H$. Since $y^{-1}x$ is in the kernel and the kernel is simply 1_G, we have that $y^{-1}x = 1_G$, so $x = y$. To prove the second statement, we simply use the first isomorphism theorem (1.79) and Lagrange's theorem (1.69). □

Theorem 1.81 (Second/Diamond Isomorphism Theorem)**.** *Let G be a group and let A and B be subgroups of G. Assume that $A \leq N_G(B)$. Then, $AB \leq G$, $B \trianglelefteq AB$, $A \cap B \trianglelefteq A$, and $AB/B \cong A/A \cap B$.*

Proof. The first statement is the same as 1.78. To show $B \trianglelefteq AB$, we note that $A \leq N_G(B)$ by hypothesis and $B \leq N_G(B)$ trivially, so $AB \leq N_G(B)$. This means, all elements of AB normalize B. As such, B is a normal subgroup of AB considered as a group.

Now, given $B \trianglelefteq AB$, we can define the quotient group AB/B and that allows us to construct the map $\varphi : A \to AB/B$ by $\varphi(a) = aB$. It is straightforward to check that this is well-defined and a homomorphism. From the definition, clearly, φ is surjective. On the other hand, the kernel of φ is $A \cap B$. As such, $\ker \varphi = A \cap B$ which, by the first isomorphism theorem, is a normal subgroup of A. The first isomorphism theorem also allows us to conclude the last statement. □

Theorem 1.82 (Third Isomorphism Theorem)**.** *Let G be a group. Let $H \trianglelefteq G$ and $K \trianglelefteq G$, and let $H \leq K$. Then,*

$$K/H \trianglelefteq G/H$$

and $(G/H)/(K/H) \cong G/K$, which can be equivalently written with the bar notation (i.e. $\bar{J} = J/H$) as:

$$\bar{G}/\bar{K} \cong G/K.$$

Proof. The fact that $K/H \trianglelefteq G/H$ follows from the fact that $K \trianglelefteq G$ and the group operation in quotient group, i.e. $uK \circ vK = (uv)K$. To prove the second statement, construct the following map: $\varphi : G/H \to G/K$ which sends gH to gK. First, φ is well-defined: if $g_1H = g_2H$, then $g_1 = g_2h$ for some $h \in H$, and since $H \leq K$, $g_1K = g_2K$. So $\varphi(g_1H) = \varphi(g_2H)$. On the other hand, φ is, clearly, a surjective homomorphism. Finally, consider its kernel:

$$\begin{aligned}\ker \varphi &= \{gH \in G/H \mid \varphi(gH) = 1K\} \\ &= \{gH \in G/H \mid gK = 1K\} \\ &= \{gH \in G/H \mid g \in K\} \\ &= K/H.\end{aligned}$$

Using the first isomorphism theorem, we get the final statement in the theorem. □

Finally, we come to the fourth isomorphism theorem, which is arguably more important than the last two:

Theorem 1.83 (Fourth or Lattic Isomorphism Theorem / Correspondence Theorem)**.** *Let G be a group and let $N \trianglelefteq G$. Then, there is the following bijection:*

$$\{ \textit{ Subgroups } A \leq G \textit{ s.t. } N \subseteq A\} \leftrightarrow \{ \textit{ Subgroups } \bar{A} = A/N \leq G/N\}.$$

In particular, any subgroup of G/N is of the form A/N for some subgroup A of G containing N.

In particular, the bihection has the following properties: for all $A, B \leq G$ with $N \leq A$ and $N \leq B$:

1. *$A \leq B$ if and only if $\bar{A} \leq \bar{B}$ (recall that $\bar{A} = A/N$)*
2. *if $A \leq B$, then $|B : A| = |\bar{B} : \bar{A}|$*
3. *$\overline{\langle A, B\rangle} = \langle \bar{A}, \bar{B}\rangle$*
4. *$\overline{A \cap B} = \bar{A} \cap \bar{B}$*
5. *$A \trianglelefteq G$ if and only if $\bar{A} \trianglelefteq \bar{G}$.*

Observation. *In all the theorems and examples, we have constructed homomorphisms on quotient groups, i.e. homomorphisms of the form $\varphi : G/N \to H$. In some of these cases, the value of φ on the coset gN is given in terms of the representative g alone. We then had to prove that φ is well-defined (i.e. the value of φ on the coset was independent of the choice of g). Now, we can get a homomorphism Φ from G to H that makes the following diagram commute:*

$$\begin{array}{ccc} G & \xrightarrow{\pi} & G/N \\ & \searrow^{\Phi} & \downarrow{\scriptstyle \varphi} \\ & & H \end{array}$$

In terms of these constructions, we have that

$$\varphi \text{ is well-defined on } G/N \text{ if and only if } N \leq \ker \Phi.$$

1.12. Group Actions

Recall: a **group action** of a group G on a set A is a mapping $G \times A \to A$ such that:

1. $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$ for all $g_1, g_2 \in G, a \in A$
2. $1_G \cdot a = a, \forall a \in A$.

With this, for each $g \in G$, we can define a *permutation* of A by

$$\sigma_g : A \to A, \quad \sigma_g(a) = g \cdot a.$$

We can also define a *permutation representation* associated to a given group action by the following homomorphism:

$$\varphi : G \to S_A, \quad \varphi(g) = \sigma_g.$$

Furthermore, we defined the following:

1. The kernel of a group action of G on A is the set $\{g \in G \mid g \cdot a = a, \forall a \in A\}$. The kernel of the group action is the same as the kernel of the corresponding permutation representation. Therefore, the kernel of a group action is a normal subgroup of G.
2. For each $a \in A$, we have the stabilizer of a in G which is the set $G_a := \{g \in G \mid g \cdot a = a\}$.
3. The group action is called faithful if the kernel is the identity 1_G.

Note:

1. Two group elements g and g' induce the same permutation on A (i.e. $\sigma_g = \sigma_{g'}$) if and only if they are in the same fibre of the permutation representation φ. This happens if and only if they are in the same coset of the kernel.
2. An action of G on A is a faithful action of $G/\ker\varphi$ on A.

Example 1.84. Consider the action of S_n on $A = \{1, 2, \cdots, n\}$ (where $n \in \mathbb{Z}_{>0}$) by $\sigma \cdot i = \sigma(i)$. In this case, the permutation representation is the identity map, i.e. $\varphi : S_A \to S_A$ by $\varphi(\sigma) = \sigma$. The action is faithful and, for each $i \in \{1, \cdots, n\}$, the stabilizer G_i is isomorphic to S_{n-1}.

We saw that given a group action of G on A, we can define a permutation representation, which is a homomorphism $\varphi : G \to S_A$. This can be reversed: if $\varphi : G \to S_A$ is a group homomorphism, we can define a group action of G on A by $g \cdot a = \varphi(g)(a)$. This is summarized in the following:

Proposition 1.85. *For any group G and a non-empty set A, there is the following bijection:*

$$\{ \text{ group actions of } G \text{ on } A\} \leftrightarrow \mathrm{Hom}(G, S_A).$$

Given this result, we can redefine permutation representations as the following:

Definition 1.86 (Permutation Representation)**.** *If G is a group, then a permutation representation of G is a homomorphism*

$$\varphi : G \to S_A$$

where S_A is the symmetric group for some non-empty set A. We say that a given group action of G on A induces a permutation presentation of G.

Note that in the case where A is a finite set of n elements, we can also say that $S_A \cong S_n$.

Proposition 1.87. *Let G be a group acting on a set $A \neq \emptyset$. The relation on A defined by $a \sim b$ if and only if $a = g \cdot b$ for some $g \in G$ is an equivalent relation. For each $a \in A$, the number of elements in the equivalence class containing a is $|G : G_a|$, the index of the stabilizer of a.*

Proof. To show that this is an equivalence relation. First, $a \sim a$ since $a = 1_G \cdot a$ by definition of a group action, i.e. the relation is reflexive. Secondly, if $a \sim b$, i.e. $a = g \cdot b$ for some $g \in G$, then $g^{-1} \cdot a = g^{-1} \cdot (g \cdot b) = 1_G \cdot b = b$, so $b \sim a$, i.e. the relation is symmetric. Finally, if $a \sim b$ and $b \sim c$, then $a = g \cdot b$ and $b = g' \cdot c$ for some $g, g' \in G$. Then, $a = g \cdot b = g \cdot (g' \cdot c) = \tilde{g} \cdot c$ where $\tilde{g} = g \cdot g' \in G$, so $a \sim c$, i.e. the relation is transitive.

To prove the second statement, we construct a bijection between the left cosets of G_a in G and the elements of the equivalence class of a. Denote the equivalence class of a as

$$\mathcal{C}_a = \{g \cdot a \mid g \in G\}.$$

Now, suppose $b = g \cdot a \in \mathcal{C}_a$. Then, gG_a is a left coset of G_a in G. The map $b = g \cdot a \to gG_a$. Then, gG_a is a left coset of $\mathcal{C}_a$ in G. The map $b = g \cdot a \to gG_a$ is a map from $\mathcal{C}_a$ to the set of left cosets of G_a in G. This is surjective since for any $g \in G$, the element $g \cdot a$ is an element of $\mathcal{C}_a$. Since $g \cdot a = h \cdot a$ if and only if $h^{-1}g \in G_a$ if and only if $gG_a = hG_a$, the map is injective, so this is a bijection. □

1.13. Cycle Decompositions

Definition 1.88 (Orbits)**.** *Let G be a group acting on $A \neq \emptyset$. Then, the equivalence class $\{g \cdot a \mid g \in G\}$ is called the orbit of G containing a.*

Proposition 1.89. *Every element of the symmetric group S_n has a unique cycle decomposition. In other words, every element can be uniquely expressed as a product of disjoint cycles.*

Proof. Let $A = \{1, \cdots, n\}$ and let $\sigma \in S_A = S_n$. Now, consider $G = \langle \sigma \rangle$. Then, G acts on A and, so, it partitions A into unique set of disjoint sets, i.e. the orbits.

Now, consider a fixed orbit $\mathcal{O} = \{g \cdot x \mid g \in G\}$ of G containing $x \in \mathcal{O}$. Then, there exists the following bijection:

$$\{ \text{ left cosets of } G_x \text{ in G } \} \leftrightarrow \{ \text{ elements of } \mathcal{O}\}$$

(recall that $G_x = \{g \cdot x \mid g \in G \text{ s.t. } gx = x\}$, so in our case $G_x = \{\sigma^j \mid \sigma^j \in G \text{ s.t. } \sigma^j x = x\}$) by

$$\sigma^i G_x \leftrightarrow \sigma^i x.$$

Since G is cyclic, we know that $G_x \trianglelefteq G$ and G/G_x is cyclic of order d which is the smallest positive integer such that $\sigma^d \in G_x$. On the other hand, because of the bijection, $d = |G : G_x| = |\mathcal{O}|$. Then, there are d distinct cosets of G_x in G which can be written as $\{G_x, \sigma G_x, \sigma^2 G_x, \cdots, \sigma^{d-1} G_x\}$. Using the

bijection, the distinct elements of $\mathcal{O}$ are $\{x, \sigma x, \sigma^2 x, \cdots, \sigma^{d-1}x\}$. Therefore, σ is a d-cycle. This allows us to conclude that each σ has a cycle decomposition.

Now, the ordbits of $\langle\sigma\rangle$ are uniquely determined by σ. Within each orbit, $\mathcal{O}$, we can begin with any element as a representative — edifferent choices simply produces a different cyclic permutation of the original list. As such, the cycle decomposition is unique up to a rearrangement of the cycles and up to a cyclic permutation of the integers within each cycle. □

Definition 1.90 (Permutation Groups)**.** *Subgroups of symmetric groups are called permutation groups.*

For each subgroup G of S_n, the orbits of G will refer to its orbit on $\{1, 2, \cdots, n\}$.

1.14. Cayley's Theorem and the group action of left multiplication

Let G act on itself via left multiplication, i.e. $g \cdot a = ga, \forall g, a \in G$. Note that if G is written additively, then $ga = g + a$. Now, if G is finite, we can label its elements as $\{g_1, \cdots, g_n\}$. Then, each $g \in G$ describes a permutation $\sigma_g \in S_n$ via

$$\sigma_g(i) = j \leftrightarrow gg_i = g_j.$$

This group action, by left multiplication, is both transitive and faithful, as we will see in the next proposition. The stabilizer of any point is the identity subgroup.

Now, let $H \leq G$ be a subgroup. Let

$$A = \{\text{left cosets of } H \text{ in G}\}.$$

Then, G also acts on A by $g \cdot aH = gaH, \forall g \in A, aH \in A$. Note that if $H = \{1\}$, then $aH = \{a\}$ and, so, this action is the same as G acting on itself via left multiplication. Similar to the case for $A\{1, \cdots, n\}$, if H is finite index m, we can label the cosets of H with the integers from 1 to m.

Proposition 1.91. *Let G be a group and let $H \leq G$ be a subgroup. Let G act on $A = \{$ left cosets of H in $G\}$. Let π_H be the permutation representation of this action:*

$$\pi_H : G \to S_A.$$

Then,

1. *G acts transitively on A*
2. *the stabilizer in G of the point $1_H \in A$ is the subgroup H.*
3. *the kernel of the action, i.e. $\ker \pi_H$, is $\cap_{x \in G} xHx^{-1}$.*
4. *$\ker \pi_H$ is the largest normal subgroup of G contained in H.*

Proof. To prove (1), we show that there is only one orbit of this group action. Let $aH, bH \in A$. Then, let $g = ba^{-1}$. Then, $g \cdot aH = bH$, so any two arbitrary elements fall into the same orbit.

To prove (2), we note that the stabilizer of 1_H is $\{g \in G \mid g \cdot 1_H = 1_H\} = \{g \in G \mid gH = H\} = H$.

To prove (3), we calculate as follows:

$$\begin{aligned}
\ker \pi_H &= \{g \in G \mid g \cdot xH = xH, \forall x \in G\} \\
&= \{g \in G \mid (x^{-1}gx)H = H, \forall x \in G\} \\
&= \{g \in G \mid x^{-1}gx \in H, \forall x \in G\} \\
&= \{g \in G \mid g \in xHx^{-1}, \forall x \in G\} \\
&= \cap_{x \in G} xHx^{-1}.
\end{aligned}$$

To prove (4), we know already that $\ker \pi_H \trianglelefteq G$ (by first isomorphism theorem) and $\ker \pi_H \trianglelefteq H$. To see the latter, let $x = 1$ and we get that $\ker \pi_H \subset H$. Now, since $\ker \pi_H \trianglelefteq G$, for any $h \in H$, $hkh^{-1} \in \ker \pi_H$ for any $k \in \ker \pi_H$, so $\ker \pi_H \trianglelefteq H$. Now, let $N \trianglelefteq G$ such that $N \subseteq H$. Then, $N = xNx^{-1} \leq xHx^{-1}$ for any $x \in G$. Then, $N \subseteq \cap_{x \in G} xHx^{-1} = \ker \pi_H$. □

Theorem 1.92 (Cayley's Theorem)**.** *Every group is isomorphic to a subgroup of some symmetric group. In particular, if G is a group of order n, then, G is isomorphic to a subgroup of S_n.*

Proof. Let $H = 1$. Let G act on itself via left multiplication, which can be seen as G acting on $A = \{\text{left cosets of } H \text{ in G}\}$. This gives us a homomorphism $\pi_H : G \to S_G$. Now, by the previous proposition, $\ker \pi_H \trianglelefteq H$, so $\ker \pi_H \subseteq 1_G$. This means, $\ker \pi_H = 1_G$. Therefore, $G \cong \text{im}\pi_H \leq S_G$. □

1.15. Classification of Finitely Generated Abelian Groups

We first recall the definition of a direct product of groups:

Definition 1.93 (Direct Product of Groups)**.** *The direct product $G_1 \times G_2 \times \cdots \times G_n$ of the groups $G_1, \cdots, G_n$ is the set*

$$\{(g_1, \cdots, g_n) \mid g_i \in G_i\}$$

with the component-wise operation:

$$(g_1, \cdots, g_n) \cdot (g_1', \cdots, g_n') = (g_1 g_1', \cdots, g_n g_n').$$

Note that one can take the direct product of infinitely many groups as well.

Example 1.94. Let $G_i = \mathbb{R}$. Then, $\mathbb{R}^\kappa = \mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R}$.

Theorem 1.95. *If $G_1, G_2, \cdots, G_n$ are groups, then*

$$|G_1 \times \cdots \times G_n| = |G_1||G_2| \cdots |G_n|.$$

In particular, the direct product $G_1 \times \cdots \times G_n$ is also a group.

Proposition 1.96. *Let $G_1, G_2, \cdots, G_n$ be groups and let $G = G_1 \times \cdots \times G_n$.*

1. *For each i,*
$$G_i \cong \{(1, \cdots, 1, g_i, 1, \cdots, 1) \mid g_i \in G_i\}.$$
Identifying the right hand side as G_i, we can say that
$$G_i \trianglelefteq G$$
and
$$G/G_i \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n.$$
2. *For each fixed i, define*
$$\pi_i : G \to G_i$$
by
$$\pi_i(g_1, \cdots, g_n) = g_i.$$
Then, π_i is a surjective homomorphism and
$$\ker \pi_i = \{(g_1, \cdots, g_{i-1}, 1, g_{i+1}, \cdots, g_n) \mid g_j \in G_j \forall j \neq i\}.$$
In particular,
$$\ker \pi_i \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n.$$
3. *Under the identifications in part (1), for all $x \in G_i$ and for all $y \in G_j$ with $j \neq i$, $xy = yx$. Here we are viewing G_i and G_j as normal subgroups of G.*

Definition 1.97 (Finitely Generated Groups)**.** *A group G is called finitely generated (f.g.) if there is a finite subset $A \subseteq G$ such that $G = \langle A \rangle$.*

Definition 1.98 (Free Abelian Group)**.** *For each $r \in \mathbb{Z}$ with $r \geq 0$, we let $\mathbb{Z}^r = \mathbb{Z} \times \cdots \times \mathbb{Z}$ (where we define $\mathbb{Z}^0 = 1$). Then, $\mathbb{Z}^r$ is called the free abelian group of rank r.*

Theorem 1.99 (Fundamental Theorem of Finitely Generated Abelian Groups)**.** *Let G be a finitely generated abelian group. Then,*

$$G \cong \mathbb{Z}^r \times Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_s}$$

where $r, n_1, \cdots, n_s \in \mathbb{Z}$ such that:

1. *$r \geq 0$ and $n_j \geq 2$ for all j*
2. *$n_{i+1} \mid n_i$ for all $1 \leq i \leq s-1$.*

In particular, the expression is unique in the following sense: if $G \cong \mathbb{Z}^q \times Z_{u_1} \times \cdots \times Z_{u_t}$ such that the integers satisfy the conditions above, then $r = q$, $s = t$, and $n_i = u_i$.

Definition 1.100 (Free Rank, Invariant Factors)**.** *The integer r in Theorem 1.99 is called the free rank of the group G. The integers $n_1, \cdots, n_s$ are called the invariant factors of G.*

Observation. *Recall that the cardinality of the direct product of a set of groups can be written as $|G_1 \times \cdots \times G_n| = |G_1| \cdot |G_2| \cdots |G_n|$. In light of this, we can see that in Theorem 1.99,*

***G is finite if and only if its free rank is 0, i.e.** $r = 0$.*

.

Observation. *Suppose G is a finite abelian group. Then, we can see that, with the decomposition as in Theorem 1.99,:*

$$|G| = \prod_{i=1}^{s} n_i.$$

Therefore, to classify all finite abelian groups of order n, we must find all sequences $n_1, \cdots, n_s$ of integers such that:

1. *$n_j \geq 2$ for all j*
2. *$n_{i+1} \mid n_i$ for all $i \in \{1, \cdots, s-1\}$*
3. *$n_1 \cdots n_s = n$.*

In particular, we also see that

- *n_1 is the largest invariant factor*
- *each n_i must divide n*
- *if p is a prime factor of n, then it must also divide n_i for some $i \in \{1, \cdots, s\}$*
- *if p divides n_j, then it must also divide all n_i for $i \leq j$*
- ***Every prime divisor of** n **must also divide** n_1.*
- *In particular, if n is a product of **distinct primes**, then $n = n_1$.*

Corollary 1.101. *If G is a finite abelian group of order n such that n is the product of distinct primes, then G is isomorphic to Z_n. In other words, the only abelian group of order n is, up to isomorphism, Z_n.*

Theorem 1.102 (Elementary Divisor Decomposition of f.g. abelian groups)**.** *Let G be a finitely generated abelian group of order $n > 1$ such that the following is the prime factorization of n:*

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}.$$

Then,

1. *$G \cong A_1 \times A_2 \times \cdots \times A_k$ where $|A_i| = p_i^{\alpha_i}$.*

2. *for each* $A \in \{A_1, \cdots, A_k\}$ *such that* $|A| = p^\alpha$*, we can write:*

$$A \cong Z_{p^{\beta_1}} \times Z_{p^{\beta_2}} \times \cdots \times Z_{p^{\beta_k}}$$

where $\beta_1 + \cdots + \beta_k = \alpha$ *and* $\beta_1 \geq \cdots \geq \beta_k \geq 1$.

3. *This decomposition is unique in the sense that if* $G \cong B_1 \times \cdots \times B_s$ *with* $|B_i| = p_i^{\alpha_i}$ *for each* i*, then* $B_i \cong A_i$ *and* $k = s$.

References

[1] D. S. Dummit and R. M. Foote, *Abstract Algebra*, 3rd ed. John Wiley & Sons, 2004.

[2] P. Aluffi, *Algebra: Chapter 0*, ser. Graduate studies in mathematics. American Mathematical Society, 2009. [Online]. Available: https://books.google.com/books?id=deWkZWYbyHQC

A. Euclidean Algorithm, Bézout's Identity

Euclidean Algorithm The Euclidean Algorithm is an algorithm for finding the greatest common divisor of two non-zero integers a and b.

$$
\begin{aligned}
a &= q_0 b + r_0 && (3)\\
b &= q_1 r_0 + r_1 && (4)\\
r_0 &= q_2 r_1 + r_2 && (5)\\
r_1 &= q_3 r_2 + r_3 && (6)\\
&\vdots\\
r_{n-2} &= q_n r_{n-1} + r_n && (7)\\
r_{n-1} &= q_{n+1} r_n. && (8)
\end{aligned}
$$

Here r_n is the last nonzero remainder. Such an r_n must exist since

$$|b| > |r_0| > |r_1| > \cdots > |r_n|$$

is a strictly decreasing sequence of positive integers whenever the remainders are nonzero, and therefore the process cannot continue indefinitely. The final nonzero remainder r_n is the greatest common divisor of a and b, i.e.,

$$\gcd(a, b) = r_n =: (a, b).$$

Bézout's Identity Let $a, b \in \mathbb{Z}$, not both zero. Then there exist integers x and y such that

$$ax + by = \gcd(a, b).$$

In other words, the greatest common divisor of a and b can be written as an integer linear combination of a and b.