Indian Institute of Technology, Guwahati

Pre-Final Year : 6^{th} Semester

Abstract Algebra

Animesh Renanse

Self-Study Notes

January 22, 2021

Contents

[1] *From this section onward, all rings are rings with identity & all homomorphisms of rings are homomorphisms of rings with identity.*

Target : *Reach Field Extensions.*

1 Groups

1.1 Semigroups

We'll go over definitions and properties of semgroups, groups, subgroups, homomorphisms, free groups and presentations.

PRODUCTS

⋆ **Definition 1.** (**Binary Operation**) It is mapping of a set S of the Cartesian product $S \times S$ into S.

⋆ **Definition 2.** (**1-term products and empty products**) Let S be set with a binary operation, written multiplicatively. Let $n \geq 1$($n \geq 0$ if an identity element exists) and let $x_1, x_2, \ldots, x_n \in S$.

1. If $n = 1$, then $x \in S$ is a product of $x_1, x_2, \ldots, x_n$ (in that order) if and only if $x = x_1$.
2. If S has an identity element 1 and $n = 0$, then $x \in S$ is a product of $x_1, x_2, \ldots, x_n$ (in that order) if and only if $x = 1$.
3. If $n \geq 2$, then $x \in S$ is a product of $x_1, x_2, \ldots, x_n$ (in that order) if and only if, for some $1 \leq k < n$, x is a product $x = yz$ of a product y of $x_1, \ldots, x_k$ (in that order) and a product z of $x_{k+1}, \ldots, x_n$ (in that order).

Remark. Note that the notation of addition can be used here too.

ASSOCIATIVITY

⋆ **Definition 3.** (**Associative operation**) A binary operation on a set S is associative when $(xy)z = x(yz)$ for all $x, y, z \in S$.

⋆ **Definition 4.** (**Commutative operation**) A binary operation on a set S is commutative when $xy = yx$ for all $x, y \in S$.

⋆ **Definition 5.** (**Semigroup**) is an ordered pair of a set S, the underlying set of the semigroup, and one *associative binary operation* on S.

1. A semigroup with an *identity element* is a **monoid** (Associative & Identity).
2. A semigroup or monoid is **commutative** when it's operation is *commutative*.

POWERS

⋆ **Definition 6.** (n^{th} **power**) Let S be a semigroup (written multiplicatively). Let $a \in S$ and let $n \geq 1$ be an integer ($n \geq 0$ if an identity element exists). The n^{th} power a^n of a is the product

$$x_1 x_2 \ldots x_n$$

such that $x_1 = x_2 = \cdots = x_n = a$.

SUBSET MULTIPLICATION

⋆ **Definition 7.** (**Subset product**) In a set S with a multiplication, the product of two subsets A and B of S is

$$AB = \{ab \mid a \in A,\ b \in B\}.$$

That is, $x \in AB$ if and only if $x = ab$ for some $a \in A$ and $b \in B$.

FREE SEMIGROUP

⋆ **Definition 8.** (**Free Semigroup and Monoid**) The free semigroup on a set X is the semigroup of all *finite non-empty sequences* of elements of X.

The free monoid on a set X is the semigroup of all finite (possibly empty) sequences of elements of X.

1. The multiplication here is concatenation of two sequences. For $x_1, x_2, \ldots, x_n$ and $y_1, y_2, \ldots, y_m$ in X

$$(x_1, x_2, \ldots, x_n) \cdot (y_1, y_2, \ldots, y_m) = (x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m)$$

2. The identity element (for monoids) would hence the empty sequence $()$.

Remark. Note that we can write the sequence $(x_1, x_2, \ldots, x_n)$ compactly as $x_1 x_2 \ldots x_n$ as a *word*.

FREE COMMUTATIVE SEMIGROUP

★ **Definition 9.** (**Free Commutative Monoid & Semigroup**) The free commutative monoid on a finite set $X = \{x_1, x_2, \ldots, x_n\}$ is the semigroup of all monomials $x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n}$ where $a_i \in 0, 1, 2, \ldots \quad \forall \quad i$.

The free commutative semigroup on $X = \{x_1, x_2, \ldots, x_n\}$ is the semigroup of all monomials $x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n}$ with positive degree $a_1 + a_2 + \cdots + a_n$.

1.2 Groups

★ **Definition 10.** (**Group**) A group is an *ordered pair of a set* G and *one binary operation* $(\cdot)$ on that set G such that

1. The operation is *Associative*.
2. There exists an *Identity* element in G represented by $1 \in G$.
3. Each element $x \in G$ has an unique *Inverse* $y \in G$ so that $x \cdot y = y \cdot x = 1$.

★ **Definition 11.** (**Dihedral Groups**) The dihedral group D_n of a regular polygon with $n \geq 2$ vertices is the group of rotations & symmetries of that polygon.

PROPERTIES

✓ **Proposition 1.** In a group, written multiplicatively, the *cancellation law* holds, that is,

$$x \cdot y = x \cdot z \implies y = z$$

and

$$y \cdot x = z \cdot x \implies y = z$$

Moreover, the following equations have unique solution

$$a \cdot x = b \implies x = a^{-1} \cdot b$$
$$y \cdot a = b \implies y = b \cdot a^{-1}$$

✓ **Proposition 2.** In a group, written multiplicatively, $(x^{-1})^{-1} = x$ and $(x_1 \cdot x_2 \cdot \ \ldots \ \cdot x_n)^{-1} = x_n^{-1} \cdot \ \ldots \ \cdot x_2^{-1} \cdot x_1^{-1}$.

Proof. We have that $x^{-1} \cdot x = 1 \implies x = (x^{-1})^{-1}$.
For $n = 2$, we have that $(x_1 \cdot x_2) \cdot (x_1 \cdot x_2)^{-1} = 1 \implies x_2 \cdot (x_1 \cdot x_2)^{-1} = x_1^{-1} \implies (x_1 \cdot x_2)^{-1} = x_2^{-1} \cdot x_1^{-1}$. ■

★ **Definition 12.** (n^{th} **power**) Let G be a group. Let $a \in G$ and let n be an *arbitrary* integer. The n^{th} power a^n of a is defined as follows:

1. If $n \geq 0$, then a^n is the product
$$a^n = \underbrace{a \cdot a \cdot \ \ldots \ \cdot a}_{n \text{ times}}$$
in particular, $a^0 = 1$ and $a^1 = 1$.
2. If $n \leq 0$ and $n = -m$ for some $m \geq 0$, then
$$a^n = (a^m)^{-1}$$

✓ **Proposition 3.** In a group G, the following properties hold for all $a \in G$ and all integers m, n:

1. $a^0 = 1$, $a^1 = a$
2. $a^m \cdot a^n = a^{m+n}$
3. $(a^m)^n = a^{mn}$
4. $(a^n)^{-1} = a^{-n} = (a^{-1})^n$

→ **Corollary 1.** In a **finite group** G, the inverse of any element is a positive power of that element.

Proof. Let $x \in G$, then there exists the inverse $y \in G$ such that $x \cdot y = y \cdot x = 1$. Since G is finite, then the powers $x^n \ \forall n \in \mathbb{Z}$ cannot be all distinct. Hence, for certain $n, m \in \mathbb{Z}$, $x^n = x^m \implies x^{n-m} = 1 = y \cdot x \implies y = x^{n-m-1}$ where we assume, WLOG, that $n > m$. ■

ABELIAN GROUP

A group G with additional *commutative* property is known as *Abelian*. The additive notion $(+)$ is usually reserved for Abelian groups.

✓ **Proposition 4.** In an Abelian group G (written additively), we have

1. $-(-x) = x$
2. $-(x_1 + x_2 + \cdots + x_m) = (-x_1) + (-x_2) + \cdots + (-x_m)$

✓ **Proposition 5.** In an Abelian group G the following properties hold for all $a, b \in G$ and all integers m, n:

1. $ma + na = (m + n)a$
2. $m(na) = (mn)a$
3. $0a = n0 = 0$
4. $-(na) = (-n)a = n(-a)$
5. $n(a + b) = na + nb$

Remark. Note that the operation and power symbols are the only things that have changed in here, the proof still remains quite trivial.

1.3 Subgroups

⋆ **Definition 13.** (**Subgroup**) A subgroup of a group G is a subset H of G such that

1. $1 \in H$
2. $x \in H$ implies $x^{-1} \in H$
3. $x, y \in H$ implies $x \cdot y \in H$

We denote that H *is a subgroup of* G by

$$H \leq G$$

✓ **Proposition 6.** A subset H of a group G is a subgroup **if and only if** $H \neq \Phi$ and $x, y \in H$ implies $x \cdot y^{-1} \in H$.

Proof. Let $H \leq G$. Since $1 \in H$ therefore $H \neq \Phi$. Moreover, for $x, y \in H$ we have $y^{-1} \in H$ therefore $x \cdot y^{-1} \in H$.
For converse, let $H \neq \Phi$ and $x, y \in H$ implies $x \cdot y^{-1} \in H$. Let $x = y$, therefore $x \cdot x^{-1} = 1 \in H$. Next, let $x \to 1$ and $y \to x$ to get $1 \cdot x^{-1} = x^{-1} \in H$. Finally, for $x, y \in H$, we have that $y^{-1} \in H$ from previous line. Thus $x \cdot (y^{-1})^{-1} \in H \implies x \cdot y \in H$. ■

✓ **Proposition 7.** A subset H of a **finite group** G is a subgroup **if and only if** $H \neq \Phi$ and $x, y \in H$ implies $x \cdot y \in H$.

Proof. If $H \leq G$ then it is trivial. For the converse, suppose $H \neq \Phi$ and $x, y \in H \implies x \cdot y \in H$. Then $x^n \in H$ for all $n > 0$. This implies that $x^{-1} \in H$ by Corollary 1. Finally, if $x \in H$, then $x^{-1} \in H$, hence $x \cdot x^{-1} = 1 \in H$. ■

GENERATORS

✓ **Proposition 8.** Let G be a group and let X be a subset of G. The set of all products in G (including the empty and 1-term products) of elements of X and inverses of elements of X is a subgroup of G. In-fact it is the smallest subgroup of G which contains X.

⋆ **Definition 14.** (**Generator**) The subgroup $\langle X \rangle$ of a group G *generated* by a subset X of G is the set of all products in G (including the empty product and 1-term products) of elements of X and inverses of elements of X.

A group G is generated by a subset X when $\langle X \rangle = G$.

Remark. Thus $G = \langle X \rangle$ when every element of G is a product of elements of X and inverses of elements of X.

→ **Corollary 2.** In a **finite group** G, the subgroup $\langle X \rangle$ of G generated by a subset X of G is the set of all products in G of elements of X.

Proof. This comes trivially from the Corollary 1 and Proposition 8. ■

✓ **Proposition 9.** Let G be a group and let $a \in G$. The set of all powers of a is a subgroup of G. In-fact, it is the subgroup generated by $\{a\}$.

Proof. Let $a \in G$. Then the set of all powers of a would mean that it consists of $a^0 = 1$, $a^{-n} = (a^n)^{-1}$ and $a^m \cdot a^n = a^{m+n}$. ■

⋆ **Definition 15.** (**Cyclic Subgroup**) The *cyclic subgroup generated by an element* a of a group is the set $\langle a \rangle$ of all powers of a.

A group or subgroup is cyclic when it is generated by a single element.

PROPERTIES

✓ **Proposition 10.** In a group G, a subgroup of a subgroup of G is a subgroup of G. Moreover, every intersection of subgroups of a group G is a subgroup of G.

Remark. This is not true in general for unions. However, some unions yield subgroups, as we will see now.

⋆ **Definition 16.** (**Chain of Subsets**) A chain of subsets of a set S is a family $(C_i)_{i\in I}$ of subsets of S such that, for every $i, j \in I$, $C_i \subseteq C_j$ or $C_j \subseteq C_i$.

⋆ **Definition 17.** (**Directed Family of Subsets**) A directed family of subsets of a set S is a family $(D_i)_{i\in I}$ of subsets of subsets of S such that, for every $i, j \in I$, there is some $k \in I$ such that $D_i \subseteq D_k$ and $D_j \subseteq D_k$.

Remark. Every chain is a directed family.

✓ **Proposition 11.** The union of a nonempty directed family of subgroups of a group G is a subgroup of G. In particular, the union of a non-empty chain of subgroups of a group G is a subgroup of G.

COSETS

Now we explore some individual properties of subgroups.

✓ **Proposition 12.** If H is a subgroup of a group, then $H \cdot H = H \cdot a = a \cdot H = H$ for every $a \in H$.

Note that $a \cdot H$ and $H \cdot a$ are products of subsets.

⋆ **Definition 18.** (**Left/Right Coset**) Relative to a subgroup H of a group G, the left coset of an element x of G is the subset $x \cdot H$ of G. Similarly, the right coset of an element x of G is the subset $H \cdot x$ of G. These sets are also called left and right cosets of H.

✓ **Proposition 13.** Let H be a subgroup of a group G. Then both the left and the right cosets of H constitute a partition of G.

Proof. Clearly, we need to find the relation which partitions G. Define the relation R on group G as "xRy iff $x \cdot y^{-1} \in H$". It's trivial to see that this relation is equivalence. Hence R partitions the group G. Note that xRy if and only if $x \in H \cdot y$. Hence right coset of y forms an equivalence class. Therefore, the right cosets of H forms a partition of G. ■

✓ **Proposition 14.** The number of left cosets of a subgroup is equal to the number of it's right cosets.

Proof. The proof is built upon the fact that if we can show that a certain structure A is derived from another structure B and B is derived from A, then the number of A's and B's is same. Let G be a group with $H \leq G$. We will show that for each right coset, you can make a unique left coset and vice-versa. For $a \in G$, if $y \in a \cdot H$, then $y = a \cdot x$ for some $x \in H$. Hence, $y^{-1} = x^{-1} \cdot a^{-1}$ or $y^{-1} \in H \cdot a^{-1}$. That is, for left coset $a \cdot H$, we can create a right coset $\{y^{-1} | y \in a \cdot H\} = H \cdot a^{-1}$. Similarly, we can, from a right coset, create a unique left coset. Hence the proof. ■

Remark. We call this number the *index of the subgroup*.

⋆ **Definition 19.** (**Index of Subgroup**) The index $[G : H]$ of a subgroup H of group G is the number of it's left cosets (equivalently, it's right cosets).

⋆ **Definition 20.** (**Order of Group**) The order of a group G is the number $|G|$ of it's elements.

✓ **Proposition 15.** If H is a subgroup of a group G, then,

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

→ **Corollary 3.** (***Lagrange's Theorem***) In a **finite group** G, the order and index of a subgroup divide the order of G.

Remark. Corollary 3's importance becomes visible through an example : A group of order 9 has no subgroup of order 2(!) That is, a group of order 9 cannot be divided into two parts.

1.4 Homomorphisms

★ **Definition 21.** (**Homomorphism**) A homomorphism of a group A into a group B is a mapping $\varphi : A \longrightarrow B$ such that

$$\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$$

for all $x, y \in A$.

PROPERTIES

✓ **Proposition 16.** If $\varphi : A \to B$ and $\psi : B \to C$ are homomorphisms of groups, then so is $\varphi \circ \psi : A \to C$. Moreover, the identity mapping 1_G on a group G is a homomorphism.

✓ **Proposition 17.** If $\varphi : A \to B$ is a homomorphism of groups, then

1. $\varphi(1) = 1$.
2. $\varphi(x^{-1}) = (\varphi(x))^{-1}$.
3. $\varphi(x^n) = (\varphi(x))^n$.

for all $x \in A$ and $n \in \mathbb{Z}$.

✓ **Proposition 18.** Let $\varphi : A \to B$ be a homomorphism of groups. If H is a subgroup of A, then

$$\varphi(H) = \{\varphi(x) \mid x \in H\} \text{ is a subgroup of } B.$$

Also, if J is a subgroup of B, then

$$\varphi^{-1}(J) = \{x \in A \mid \varphi(x) \in J\} \text{ is a subgroup of } A$$

Remark. This proposition motivates the following definitions.

★ **Definition 22.** (**Image/Range of a Homomorphism**) Let $\varphi : A \to B$ be a homomorphism of groups. The image or range of φ is

$$\text{Im } \varphi = \{\varphi(x) \mid x \in A\}$$

★ **Definition 23.** (**Kernel of a Homomorphism**) The kernel of homomorphism $\varphi : A \to B$ is

$$\text{Ker } \varphi = \{x \in A \mid \varphi(x) = 1\}$$

Remark. Clearly, Im $\varphi = \varphi(A)$ and Ker $\varphi = \varphi^{-1}(1)$ are subgroups of B and A respectively.

★ **Definition 24.** (**Normal Subgroup**) A subgroup N of a group G is normal when $x \cdot N = N \cdot x$ for all $x \in G$. That is, the left cosets and the right cosets of N coincide hence they are simply called *cosets*.

Remark. Clearly, all subgroups of an Abelian group are normal. We denote the relation that N *is a normal subgroup of* G by

$$N \trianglelefteq G$$

✓ **Proposition 19.** Let $\varphi : A \to B$ be a homomorphism of groups. Then the Ker φ is a normal subgroup of A. Moreover, $\varphi(x) = \varphi(y)$ if and only if $y \in x \cdot (\text{Ker } \varphi) = (\text{Ker } \varphi) \cdot x$.

✓ **Proposition 20.** A subgroup N of a group G is normal **if and only if** $x \cdot N \cdot x^{-1} \subseteq N$ for all $x \in G$.

Proof. Let G be a group and $N \trianglelefteq G$. For N, we know that $N \cdot x = x \cdot N$ for every $x \in G$. Hence $N = x \cdot N \cdot x^{-1}$, that is $x \cdot N \cdot x^{-1} \subseteq N$. Conversely, $x \cdot N \cdot x^{-1} \cdot x = x \cdot N \subseteq N \cdot x$ and $x^{-1} \cdot x \cdot N \cdot x^{-1} \subseteq x^{-1} \cdot N \implies N \cdot x^{-1} \subseteq x^{-1} \cdot N$. Since $x^{-1} \in G$, hence we have our result. ■

SPECIAL KINDS OF HOMOMORPHISMS

✓ **Proposition 21.** If φ is a bijective homomorphism of groups, then the inverse bijection φ^{-1} is also a homomorphism of groups.

Proof. Let $\varphi : A \to B$ be a bijective homomorphisms on groups A and B. If $C \subseteq B$, then $\varphi^{-1}(C) = \{x \in A \mid \varphi(x) \in C\}$. Let $a_1, a_2, a_3 \in A$ so that $a_1 \cdot a_2 = a_3$. Since φ is bijective, we can write $\varphi \circ \varphi^{-1} = \mathrm{Id}$. Thus,

$$\begin{aligned} \varphi(a_1 \cdot a_2) = \varphi(a_3) &= \varphi(a_1) \cdot \varphi(a_2) \\ \varphi^{-1} \circ \varphi(a_1 \cdot a_2) &= \varphi^{-1}\left(\varphi(a_1) \cdot \varphi(a_2)\right) \\ a_1 \cdot a_2 &= \varphi^{-1}\left(\varphi(a_1) \cdot \varphi(a_2)\right). \end{aligned}$$

Hence proved. ■

⋆ **Definition 25.** (**Isomorphism**) An isomorphism of groups is a bijective homomorphism of groups. Two groups A and B are isomorphic when there exists an isomorphism of A onto B. This relation is denoted by

$$A \cong B$$

⋆ **Definition 26.** (**Endomorphism**) An endomorphism of a group G is a *homomorphism* of G into G.

⋆ **Definition 27.** (**Automorphism**) An automorphism of a group G is an *isomorphism* of G onto G.

✓ **Proposition 22.** The endomorphisms of a group G constitute a *monoid* $\mathbf{End}(G)$ under composition and the automorphisms of group G constitute a *group* $\mathbf{Aut}(G)$ under composition.

Proof. Consider the set of all endomorphisms $\mathbf{End}(G)$ of group G. Moreover, let $\mathbf{End}(G)$ be endowed with composition $(\circ)$ operation. $\mathbf{End}(G)$ is associative due to a associativity of composition. Now by Proposition 16, we have $1_G \in \mathbf{End}(G)$. Hence $\mathbf{End}(G)$ is a monoid. Now, consider the set of all automorphisms $\mathbf{Aut}(G)$ and endow it with composition operation. Clearly it is associative. Since the identity map 1_G is a bijective homomorphism from G to G, so $1_G \in \mathbf{Aut}(G)$. Let $f \in \mathbf{Aut}(G)$. That means that f is a bijective homomorphism from G to G. By Proposition 21, we have that f^{-1} is also a bijective homomorphism from G to G. Hence $\mathbf{Aut}(G)$ is a group. ■

QUOTIENT GROUPS

This is another special kind of homomorphisms constructed from normal subgroups. We first see the following result.

✓ **Proposition 23.** Let N be a normal subgroup of a group G. Then the set of all cosets of N constitute a *group* under the multiplication of subsets and the mapping $x \longrightarrow x \cdot N = N \cdot x$ is a surjective homomorphism, whose kernel is N.

Proof. Let S be the set of all cosets of normal subgroup N and be it endowed with the binary operation of subset multiplication. Clearly, $x \cdot N,\ y \cdot N \in S$ where $x, y \in G$. Now note that $x \cdot N \cdot y \cdot N = x \cdot y \cdot N \cdot N = x \cdot y \cdot N$, therefore, S is associative. Identity element is clearly $1 \cdot N = N$. For the inverse element of $x \cdot N$, we need $y \cdot N \in S$ for $y \in G$ such that $x \cdot N \cdot y \cdot N = x \cdot y \cdot N = N$(identity is N) which implies that $x \cdot y = 1 \implies y = x^{-1}$. Therefore, the set of all cosets of normal subgroup N is a group.
Consider $y \in x \cdot N = N \cdot x$. Then for some $n \in N$, $y = x \cdot n = n \cdot x$. Since there is atleast one $x \in G$ for each $y \in x \cdot N$, hence $x \longrightarrow x \cdot N$ is surjective. Moreover, if we write $x = y \cdot z$ for $x, y, z \in G$, we see that under this map, we have that $(y \cdot z) \cdot N = y \cdot N \cdot z \cdot N$, so we have a homomorphism. The identity of the group of cosets of N is N. Hence, Ker $(x \to x \cdot N) = N$. ■

⋆ **Definition 28.** (**Quotient Group**) Let N be a normal subgroup of a group G. Then the group of all cosets of N is called the Quotient group G/N of G by N.

⋆ **Definition 29.** (**Canonical Projection**) The homomorphism $x \longrightarrow x \cdot N = N \cdot x$ is called the canonical projection of G into G/N.

⋆ **Definition 30.** (**Integers modulo n**) For every positive integer n, the additive group $\mathbb{Z}_n$ of the integers modulo n is the quotient group $\mathbb{Z}/(\mathbb{Z} \cdot n)$.

Remark. Note that for $\overline{x} \in \mathbb{Z}_n$, we have $\overline{x} = \{x + q \cdot n \mid q \in \mathbb{Z}\}$ for any $x \in \mathbb{Z}$.

✓ **Proposition 24.** $\mathbb{Z}_n$ is a cyclic group of order n with elements $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ and addition operation

$$\overline{i} + \overline{j} = \begin{cases} \overline{i+j} & \text{if } i+j < n \\ \overline{i+j-n} & \text{if } i+j \geq n \end{cases}$$

Proof. Note that for every coset $\overline{x} \in \mathbb{Z}_n$, we have $\overline{x} = x + \mathbb{Z} \cdot n$. Since for any $p \in \overline{x}$ we have that $p \mod n = x \mod n$ therefore we represent every $\overline{x}$ by $x \mod n$ which clearly is $\{0, 1, \ldots, n-1\}$. Hence $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ with addition operation as above. Moreover, we have that $r \cdot \overline{1} = \overline{r}$, hence $\mathbb{Z}_n$ is a cyclic group. ■

✓ **Proposition 25.** Let N be a normal subgroup of a group G. Then every subgroup of the quotient group G/N is the quotient group H/N of a unique subgroup H of G that contains N $(N \subseteq H)$.

Proof. Consider the canonical projection $\pi : G \to G/N$ with $N \trianglelefteq G$ and let $B \leq G/N$. Taking the inverse map over B gives

$$A = \pi^{-1}(B) = \{x \in G \mid \pi(x) = x \cdot N \in B\}.$$

By Proposition 18, we have that A is a subgroup of G $(A \leq G)$. Moreover, $\pi^{-1}(1) = \text{Ker } \pi = N$. Clearly, N is also a normal subgroup of A as $a \cdot N = N \cdot a$ for $a \in A$ $(N \trianglelefteq A)$. Now the quotient group A/N is a subset of B $(A/N \subseteq B)$. Conversely, let $x \cdot N \in B$, then $x \in A$ as shown in the equation above, hence $x \cdot A \in A/N$ which implies $B \subseteq A/N$ which further means that $B = A/N$.
Let $H \leq G$ and $A \leq G$ such that $B = A/N$ and $B = H/N$. For $h \in H$, we have that $h \cdot N \in B$. Since B is also A/N, there is an $a \in A$ such that $a \cdot N = h \cdot N$. Since $A/N = B$ so $h \in A$ which implies $H \subseteq A$. Conversely, for $a \in A$, $a \cdot N \in A/N = H/N$, hence $a \in H$ which implies $A \subseteq A$. Hence we have proved that subgroups of quotient group G/N are quotient groups of subgroups of G. ■

✓ **Proposition 26.** Let N be a normal subgroup of a group G. Then the *direct* and *inverse* image under the canonical projection $G \longrightarrow G/N$ induce a one-to-one correspondence (bijection) which preserves inclusion & normality between subgroups of G that contain N and subgroups of G/N.

Proof. Let N be a normal subgroup and $\pi : G \longrightarrow G/N$ be the canonical projection. Moreover, let A to be the set of all subgroups of G containing N and B be the set of all subgroups of G/N. From Proposition 25, we have for every element in B, a corresponding unique element of A. Hence π forms a bijection from A to B. Since π is a homomorphism, then from Proposition 21, we have that π^{-1} is also a bijection from B to A. For inclusion, consider $A_1, A_2 \in A$ such that $A_1 \subseteq A_2$. It's trivial to see that $A_1/N \subseteq A_2/N$. For normality, consider $A_n \in A$ to be a normal subgroup of G. Then we need to show that $\pi(A_n) = A_n/N = \{a \cdot N \mid a \in A_n\}$ is a normal subgroup of G/N.Let $x \cdot N \in G/N$. Since A_n is a normal subgroup, so $C = x \cdot A_n \cdot x^{-1} = \{x \cdot a \cdot x^{-1} \mid a \in A_n\} \subseteq A_n$ (Proposition 20). In a similar way,

$$\begin{aligned} x \cdot N \cdot (A_n/N) \cdot (x \cdot N)^{-1} &= x \cdot N \cdot (A_n/N) \cdot N \cdot x^{-1} \\ &= x \cdot (A_n/N) \cdot x^{-1} \\ &= \{x \cdot a \cdot N \cdot x^{-1} \mid a \in A_n\} \\ &= \{x \cdot a \cdot x^{-1} \cdot N \mid a \in A_n\} \\ &= C \cdot N \\ &\subseteq A_n/N \end{aligned}$$

Hence, by Proposition 20, we finally get that canonical map forms a bijection over set of subgroups of G and subgroups of G/N which preserves inclusion and normality. ■

1.5 The Isomorphism Theorems

FACTORIZATION

Quotient Groups provide our first example of a *Universal Property*.

⊛ **Theorem 1.** (**Factorization Theorem**) Let N be a normal subgroup of a group G. Then every homomorphism of groups $\varphi : G \longrightarrow H$ whose kernel contains N, factors uniquely through the canonical projection $\pi : G \longrightarrow G/N$. That is, there exists a unique homomorphism $\psi : G/N \longrightarrow H$ such that $\varphi = \psi \circ \pi$.

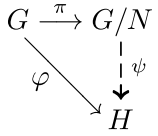

Figure 1: If $N \trianglelefteq G$ and φ is any homomorphism such that $N \subseteq \text{Ker } \varphi$, then above is true.

Proof. Consider the definition of a map $\psi : A \to B$ as a set of ordered pairs (a, b). We need to show that for every $a \in A$, there exists a $b \in B$ such that $(a, b) \in \psi$ and also that if $(a_1, b_1), (a_2, b_2) \in \psi$ and $a_1 = a_2$, it implies that $b_1 = b_2$.
Consider now $x, y \in G$. If $x^{-1} \cdot y \in N$ and since Ker $\varphi = N$, so $\varphi(x^{-1} \cdot y) = \varphi(x^{-1}) \cdot \varphi(y) = (\varphi(x))^{-1} \cdot \varphi(y) = 1$. Hence $x \cdot N = y \cdot N$ implies that $\varphi(x) = \varphi(y)$. In the form of the set of ordered pair, we can write,

$$\psi = \{(x \cdot N, \varphi(x)) \mid x \in G\}.$$

Now for ψ to be a map form G/N to H, we already have that for every $x \cdot N \in G/N$, there exists a $\varphi(x) \in H$ and the second condition is proved as above. Hence $\psi : G/N \to H$ is a map. Moreover, since $\psi(x \cdot N) = \varphi(x)$, hence $\varphi = \psi \circ \pi$.
Uniqueness of ψ can be seen by assuming $\xi : G/N \to H$ be another such homomorphism such that $\xi \circ \pi = \varphi$. But then $\xi(x \cdot N) = \varphi(x) = \psi(x \cdot N)$ for each $x \cdot N \in G/N$ for each $x \in G$. Hence $\xi = \psi$. ∎

THE HOMOMORPHISM THEOREM

⊛ **Theorem 2.** (**Homomorphism Theorem**) If $\varphi : A \longrightarrow B$ is a homomorphism of groups, then

$$A/\text{Ker } \varphi \cong \text{Im } \varphi.$$

That is, there is a unique isomorphism $\theta : A/\text{Ker } \varphi \to \text{Im } \varphi$ such that $\varphi = \iota \circ \theta \circ \pi$ where $\iota : \text{Im } f \to B$ is the inclusion homomorphism and $\pi : A \to A/\text{Ker } f$ is the canonical projection.

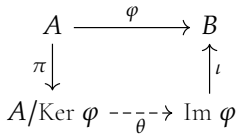

Figure 2: If φ is any homomorphism, then above is true.

Proof. Consider the homomorphism $\psi : A \to \text{Im } \varphi$ to be equal to the map φ. We have that Ker ψ = Ker φ, moreover, from Theorem 1, we have that $\psi = \theta \circ \pi$ for some unique homomorphism $\theta : A/\text{Ker } \varphi \to \text{Im } \varphi$. Denoting $K = \text{Ker } \varphi$, we get that $\theta(a \cdot K) = \theta(a) \cdot \theta(K) = \psi(a) = \varphi(a)$ for all $a \in A$. Hence $\varphi = \iota \cdot \theta \cdot \pi$. We can also see that θ is a surjection (Proposition 23) and since $\theta(a \cdot K) = 1 \implies \varphi(a) = 1 \implies a \in \text{Ker } \varphi \in A/\text{Ker } \varphi$, so θ is injective, hence bijective. Theorem 1 also proves the uniqueness of θ. ∎

→ **Corollary 4.** If $\varphi : A \to B$ is injective, then $A \cong \text{Im } \varphi$ and if φ is surjective, then $A/\text{Ker } \varphi \cong B$.

Proof. If φ is injective, then Ker $\varphi = 1$ and if φ is surjective, then $B = \text{Im } \varphi$. ∎

Remark. Homomorphism theorem tells us that *every homomorphism is a composition of an inclusion homomorphism of subgroups, an isomorphism and the canonical projection to quotient groups.*

✓ **Proposition 27.** Let G be a group and let $a \in G$. If $a^m \neq 1$ for all $m \neq 0$, then $\langle a \rangle \cong \mathbb{Z}$ and $\langle a \rangle$ is infinite.

Conversely, if there is a smallest positive integer n such that $a^n = 1$, then $a^m = 1$ if and only if n divides m and $\langle a \rangle \cong \mathbb{Z}_n$ and order of $\langle a \rangle$ is n.

Proof. Consider the homomorphism $f : m \to a^m$ from $\mathbb{Z}$ to G. By Theorem 2, we have that $\mathbb{Z}/\text{Ker } f \cong \text{Im } f = \langle a \rangle$. Since Ker f is a subgroup of $\mathbb{Z}$ and since every subgroup of $\mathbb{Z}$ is cyclic, hence Ker f is cyclic. Let $n \in \text{Ker } f$, therefore $a^n = 1$ and hence Ker $f = \mathbb{Z} \cdot n$ for some n. If $n = 0$, then $\mathbb{Z} \cong \mathbb{Z}/0 \cong \langle a \rangle$. If $n > 0$, we have that $\langle a \rangle \cong \mathbb{Z}/\mathbb{Z} \cdot n = \mathbb{Z}_n$. Hence $a^m = 1$ if and only if m is a multiple of n (Proposition 24). ■

⋆ **Definition 31.** (**Order of an element of a group**) The order of an element a of a group G is infinite if $a^m \neq 1$ for all $m \neq 0$. Otherwise, the order of element a is the smallest positive integer n such that $a^n = 1$.

→ **Corollary 5.** Any two cyclic groups of order n are isomorphic.

Proof. By Proposition 27, we have that any cyclic group of order n is isomorphic to $\mathbb{Z}_n$, hence they are isomorphic to each other too (Proposition 16). ■

→ **Corollary 6.** Every subgroup of a cyclic group is cyclic.

Proof. Let G be a cyclic group, therefore $G = \langle a \rangle$ for some $a \in G$. Let $H \leq \langle a \rangle$. This implies that $a^m \in H$ for the smallest positive integer $m \in \mathbb{Z}$. Now consider $b \in H$, therefore $b = a^n$ for some $n \in \mathbb{Z}$. By division theorem, we can write $n = mq + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r < m$. Hence $a^n = a^{mq+r} = a^{mq}a^r = (a^m)^q a^r$ which implies that $a^r = (a^m)^{-q}a^n$. Since $a^m \in H$, then $(a^m)^{-1} \in H$ and so on, $(a^m)^{-q} \in H$. Since $a^n \in H$ too and H is a subgroup, hence $a^r = (a^m)^{-q}a^n \in H$. But since $r < m$ and $a^r \in H$, it implies that $r = 0$, hence $a^n = (a^m)^q$, that is, $H = \langle a^m \rangle$. ■

Remark. We denote the *cyclic group of order* n by C_n.

1.6 Generators of a Cyclic Group

*ADD **BLANK** TO EACH PROPOSITION FROM THIS SECTION ONWARDS.*

✓ **Proposition 28.** Let G be a cyclic group of order n. Then, $x \in G$ is a generator of G if and only if $|x| = n$.

Proof. First, assume that $x \in G$ is a generator of G. Therefore, $G = \langle x \rangle$, hence $|G| = |\langle x \rangle| = |x|$. To show the converse, assume $|x| = n$. Then we know that $\langle x \rangle \leq G$. But since $|x| = n$, hence $\langle x \rangle = G$. ■

✓ **Proposition 29.** If $G = \langle a \rangle = \{1_G, a, a^2, \ldots, a^{n-1}\}$ is a cyclic group of order n, then a^m is a generator if and only if $\gcd(n, m) = 1$, that is m and n are relatively prime.

Proof. First assume that a^m is a generator. We know that the order of a^m is given by the following relation[2]:

$$|a^m| = \frac{|a|}{\gcd(m, |a|)}.$$

Now since a^m is a generator of G, therefore $|a^m| = |G|$, hence $\gcd(|a|, m) = 1$. Now assume that $\gcd(|a|, m) = 1$, then by the same relation, we see that $|G| = |a| = |a^m|$, hence a^m is a generator of G. ■

✓ **Proposition 30.** Let G be an **infinite** cyclic group. If $G = \langle a \rangle$ for some $a \in G$, then $G = \langle a^{-1} \rangle$.

Proof. Consider G to be a infinite cyclic group. We are given that $G = \langle a \rangle$. Therefore $|a| = |G|$ (Proposition 28). But, $|a^{-1}| = k$ such that $(a^{-1})^k = 1$ for least such k. This implies that $(a^{-1})^k = 1 \implies (a^k)^{-1} = 1 \implies a^k = 1$. Hence $k = |a|$. Therefore $|G| = |a^{-1}|$ so that $G = \langle a^{-1} \rangle$. ■

Remark. Therefore, if G is an infinite cyclic group, then there are two generators.

✓ **Proposition 31.** If G is a cyclic group with $|G| = n$, then G has $\phi(n) = |\{m \mid 1 \leq m \leq n,\ \gcd(n, m) = 1\}|$ number of generators. Hence, the set of generators of $G = \langle a \rangle = \{1_G, a, a^2, \ldots, a^{n-1}\}$ is $\{a^m \mid \gcd(n, m) = 1\}$.

Proof. Trivial from the basic property of Euler's ϕ function. ■

EXAMPLE : Roots of Unity

$S^1 = \{z \in \mathbb{C}^\times \mid |z| = 1\}$ **is a group** : Note here that $\mathbb{C}^\times = \mathbb{C} - \{0\}$, that is $\mathbb{C}^\times$ is the set of non-zero complex numbers and hence S^1 is the unit circle in complex plane. It's trivial to see that S^1 would be a group. But now, define the following:

Let $n \geq 1$ and $\mu_n = \{z \in \mathbb{C}^\times \mid z^n = 1\}$ = the set of all $n-$th roots of unity. It's easy to see that μ_n is also a group under multiplication. Note that for any $z \in \mu_n$, $z^n = 1$, hence $|z| = 1$, so $z \in S^1$. Hence,

$$\mu_n \leq S^1.$$

But we know that $|\mu_n| = n$ because there are only n roots of $z^n = 1$.

Structure of μ_n.

Consider $\xi_n = e^{\frac{2\pi i}{n}} = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$. Since $\xi_n^n = 1$, therefore $\xi_n \in \mu_n$. But since $\xi_n^n = 1$, hence $|\xi_n| = n$. In summary, $\exists\ \xi_n \in \mu_n$ such that $|\xi_n| = |\mu_n| = n$, hence,

$$\mu_n = \langle \xi_n \rangle.$$

Therefore, μ_n **is cyclic** and by Proposition 31, **the set of generators of cyclic group μ_n is**:

$$\{\xi_n^k \mid 1 \leq k \leq n\ ,\ \gcd(n, k) = 1\}.$$

Now, consider the group

$$\mu_\infty = \{z \in \mathbb{Z}^\times \mid z^n = 1 \text{ for some } n \geq 1\} = \bigcup_{n \geq 1} \mu_n.$$

Again, $\mu_\infty \leq S^1$. But now, μ_∞ is an infinite subgroup of S^1 in which every element has finite order because for any $z \in \mu_\infty$, $\exists n \in \mathbb{N}$ such that $z^n = 1$, hence order of z is n. We hence conclude the following:

$$\mu_\infty \textbf{ cannot be cyclic}.$$

This is because if μ_∞ is cyclic, then $\exists z \in \mu_\infty$ such that for any $a \in \mu_\infty$, we would have $a = z^l$ for some $l \in \mathbb{Z}$. Since there are infinitely many such $a \neq 1_{\mu_\infty}$, therefore $|z| = \infty$, which is a contradiction.

[2] Proof would be nice.

NUMBER OF SUBGROUPS IN A CYCLIC GROUP

✓ **Proposition 32.** Let G be a finite cyclic group of order n. For each positive divisor m of n, G has a unique subgroup of order m.

Proof. Suppose $G = \langle a \rangle$. Let's first show that a subgroup of order m **exists.** Consider that m divides n. So, take the element $a^{\frac{n}{m}} \in G$. Clearly, $(a^{\frac{n}{m}})^m$, hence $\left|a^{\frac{n}{m}}\right| = m$ because $|G| = n$. Hence there exists a subgroup of G with order m. Now, we need to show that this subgroup is **unique**. For this, consider another subgroup $\langle a^k \rangle \leq G$ for some $k \in \mathbb{N}$ which has order m, that is $\left|a^k\right| = m$. This implies that m is the least number such that $(a^k)^m = a^{km} = 1$. But since the order of a is n, hence n divides km. We also know that $\left|a^k\right| = \frac{|a|}{\gcd(|a|,k)}$ which would imply that $m = n/\gcd(n,k)$, that is, $\gcd(n,k) = \frac{n}{m}$. This further implies that $k = \frac{n}{m}d$ for some $d \in \mathbb{N}$. Hence, $a^k = a^{\frac{n}{m}d} = (a^{\frac{n}{m}})^d \in \langle a^{\frac{n}{m}} \rangle$. This means that $\langle a^k \rangle \leq \langle a^{\frac{n}{m}} \rangle$. But order of a^k and $a^{\frac{n}{m}}$ are same and equal to m. Hence $\langle a^k \rangle = \langle a^{\frac{n}{m}} \rangle$. ■

1.7 Isomorphism Theorems

THE ISOMORPHISM THEOREMS

We now discuss the next isomorphism theorems.

Theorem 3. (**The First Isomorphism Theorem**) Let A be a group and let B, C be normal subgroups of A. If $C \subseteq B$, then C is a normal subgroup of B, B/C is a normal subgroup of A/C and

$$A/B \cong (A/C)/(B/C).$$

In particular, there is a unique isomorphism $\theta : A/B \to (A/C)/(B/C)$ such that $\theta \circ \rho = \tau \circ \pi$ where $\rho : A \to A/B$, $\tau : A/C \to (A/C)/(B/C)$ and $\pi : A \to A/C$.

The following commutative diagram explains the situation in detail (note that we have also used the Theorem 1 to draw $\sigma : A/C \to A/B$).

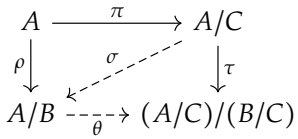

Figure 3: Let $B, C \trianglelefteq A$ with $C \subseteq B$. Then $C \trianglelefteq B$, $B/C \trianglelefteq A/C$ and the above is true.

Proof. Since, $C \trianglelefteq A$ and since $C \subseteq B$, therefore $C \trianglelefteq B$. By Theorem 1, we can factor ρ via a unique homomorphism $\sigma : A/C \to A/B$ such that $\rho = \sigma \circ \pi$. Therefore, for any $b \cdot C \in A/C$ for $b \in B$, we get $\sigma(b \cdot C) = b \cdot B = B \in A/B$ (Proposition 12). Moreover, if $\sigma(a \cdot C) = 1 = B$, then (Proposition 17, 1.) $a \cdot B = B \implies a \in B$. Therefore, Ker $\sigma = \{b \cdot C \mid b \in B\} = B/C$. Also, since Ker $\sigma \trianglelefteq A/C$ (Proposition 19), thus, $B/C \trianglelefteq A/C$. By Theorem 2, we now have that $(A/C)/(B/C) \cong$ Im σ, but since for any $a \cdot B \in A/B$, we have a $a \cdot C \in A/C$ as $C \subseteq B$, therefore Im $\sigma = A/B$ and hence $(A/C)/(B/C) \cong A/B$. Theorem 2 also proves the uniqueness of this isomorphism. ∎

Theorem 4. (**The Second Isomorphism Theorem**) Let A be a subgroup of a group G and let N be a normal subgroup of G. Then $A \cdot N$ is a subgroup of G, N is a normal subgroup of $A \cdot N$, $A \cap N$ is a normal subgroup of A and

$$(A \cdot N)/N \cong A/(A \cap N).$$

In particular, there is a unique isomorphism $\theta : A/(A \cap N) \to (A \cdot N)/N$ such that $\theta \circ \rho = \pi \circ \iota$ where $\rho : A \to A/(A \cap N)$, $\pi : A \cdot N \to (A \cdot N)/N$ are the canonical projections and $\iota : A \to A \cdot N$ is the inclusion homomorphism.

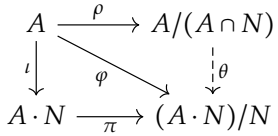

Figure 4: Let $A \leq G$, $N \trianglelefteq G$. Then $N \trianglelefteq A \cdot N \leq G$, $A \cap N \trianglelefteq A$ and the above is true.

Proof. First, note that $A \cdot N = \{a \cdot n \mid a \in A,\ n \in N\}$ (Definition 7). Since $1 \in A$ and $1 \in N$, hence $1 \in A \cdot N$. For $x \in A \cdot N \implies x = a \cdot n$ for some $a \in A,\ n \in N$. Note that $a^{-1} \in A$ and $n^{-1} \in N$ which implies that $n^{-1} \cdot a^{-1} \in N \cdot A = N \cdot A$ (N is normal). Hence $x^{-1} = (a \cdot n)^{-1} = n^{-1} \cdot a^{-1} \in A \cdot N$. Also, for $a_1, a_2 \in A$ and $n_1, n_2 \in N$, we get that $a_1 \cdot n_1, a_2 \cdot n_2 \in N$, hence $a_1 \cdot n_1 \cdot a_2 \cdot n_2 = (a_1 \cdot a_2) \cdot n_1 \cdot n_2 = (a_1 \cdot a_2) \cdot n_3 \in A \cdot N$ for some $n_3 = n_1 \cdot n_2 \in N$. Hence $A \cdot N \leq G$.
Clearly, $1 \in N$ as $N \trianglelefteq G$ and by Proposition 10 we get $N \trianglelefteq A \cdot N$.
So far, we have that $N \trianglelefteq A \cdot N \leq G$ and trivially, $N \subseteq A \cdot N$. Also, from Proposition 10, $N \leq G$. Consider now the homomorphism $\varphi = \pi \circ \iota$ (Theorem 1). Now, for some $a \in A$, we get $\varphi(a) = (a \cdot N)/N = N \cdot a \cdot N = a \cdot N$. Hence, if $a \in A \cap N$, then $a \cdot N = N = 1\varphi(a)$. Conversely, $\varphi(A \cap N) = ((A \cap N) \cdot N)/N = (A \cdot N \cap N)/N = (A \cdot N)/N$. Hence Ker $\varphi = A \cap N$. Now using Theorem 2, we get that $A/\text{Ker}\ \varphi = A/(A \cap N) \cong$ Im φ. Since Im $\varphi = \varphi(A) = (A \cdot N)/N$, hence $A/(A \cap N) \cong (A \cdot N)/N$ uniquely. ∎

1.8 The Direct Products

These are an easy way to construct larger groups from smaller ones. *This construction yields all* ***finite abelian groups***.

[⋆] **Definition 32.** (**Direct Product**) The direct product of two groups G_1 and G_2 is their Cartesian Product $G_1 \times G_2$ also denoted by $G_1 \oplus G_2$, together with the component-wise operation $(\cdot)$. That is, for $x_1, y_1 \in G_1$ and $x_2, y_2 \in G_2$, we have $(x_1, x_2), (y_1, y_2) \in G_1 \oplus G_2$ and

$$(x_1, x_2) \cdot (y_1, y_2) = (x_1 \cdot y_1, x_2 \cdot y_2) \in G_1 \oplus G_2.$$

Remark. Note that $G_1 \oplus G_2$ is also a group.

- Associativity of $G_1 \oplus G_2$ can be seen by the associativity of G_1 and G_2:

$$\begin{aligned}(x_1, x_2) \cdot ((y_1, y_2) \cdot (z_1, z_2)) = (x_1, x_2) \cdot (y_1 \cdot z_1, y_2 \cdot z_2) &= (x_1 \cdot y_1 \cdot z_1, x_2 \cdot y_2 \cdot z_2) \\ &= ((x_1 \cdot y_1) \cdot z_1, (x_2 \cdot y_2) \cdot z_2) \\ &= ((x_1, x_2) \cdot (y_1, y_2)) \cdot (z_1, z_2)\end{aligned}$$

- Since $(1_{G_1}, 1_{G_2}) \in G_1 \oplus G_2$, hence, for any $(x, y) \in G_1 \oplus G_2$, we see the following:

$$(1_{G_1}, 1_{G_2}) \cdot (x, y) = (1_{G_1} \cdot x, 1_{G_2} \cdot y) = (x \cdot 1_{G_1}, y \cdot 1_{G_2}) = (x, y) \cdot (1_{G_1}, 1_{G_2}) = (x, y)$$

  Hence, $(1_{G_1}, 1_{G_2})$ is the Identity of $G_1 \oplus G_2$ under $(\cdot)$.

- For any $(x, y) \in G_1 \oplus G_2$, we have $(x^{-1}, y^{-1}) \in G_1 \oplus G_2$ because G_1 and G_2 are also groups and they contain inverse of each element. Hence,

$$(x, y) \cdot (x^{-1}, y^{-1}) = (x \cdot x^{-1}, y \cdot y^{-1}) = (1_{G_1}, 1_{G_2}).$$

DIRECT SUMS

The conditions under which a group splits into a direct product.

✓ **Proposition 33.** A group G is isomorphic to the direct product $G_1 \oplus G_2$ of two groups G_1 and G_2 if and only if it contains normal subgroups $A \cong G_1$ and $B \cong G_2$ such that $A \cap B = 1$ and $A \cdot B = G$.

[⋆] **Definition 33.** (**Direct Sum**) A group G is the internal direct sum $G = A \oplus B$ of two subgroups A and B when $A, B \trianglelefteq G$, $A \cap B = 1$ and $A \cdot B = G$.

Remark. Note that the conditions for a group G to be broken down into direct products is rather stringent. This however leads to easier results in Abelian Groups as shown next.

[⊛] **Theorem 5.** Every finite abelian group is isomorphic to the direct product of cyclic groups whose orders are positive powers of prime numbers and these cyclic groups are unique, up to order of appearance and isomorphism.

Remark. This theorem implies that any abelian p-group of order p^k is hence isomorphic to the direct product of cyclic groups as $C_{p^{k_1}} \oplus C_{p^{k_2}} \oplus \cdots \oplus C_{p^{k_r}}$ where $k_1 + \cdots + k_r = k$.
We also have the following easy corollary.

→ **Corollary 7.** Let $p_1, \ldots, p_r$ be distinct primes. An abelian group of order $p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ is a direct sum of subgroups of orders $p_1^{k_1}, p_2^{k_2}, \ldots, p_r^{k_r}$

All Abelian Groups of order n

We can now find all abelian groups of order n as follows.

1. Write n as a product of positive powers p^k of distinct primes.
2. For each p, find all abelian p-groups of order p^k from the partitions of k.
3. The abelian groups of order n are the direct products of these p-groups, one for each prime divisor p of n.

Consider example of $n = 200 = 2^3 \cdot 5^2$. We need to find now the partitions of 3 and 2. There are three partitions of 3 : $1+1+1, 2+1, 3+0$. There are two partitions of 2 : $1+1, 2+0$. Hence there are three cyclic groups of order 8 : $C_2 \oplus C_2 \oplus C_2$; $C_4 \oplus C_2$; C_8 and there are 2 cyclic groups of order 25 : $C_5 \oplus C_5$; C_{25}. Finally, there would be $3 \times 2 = 6$ abelian groups of order 200, each of which would be a combination of the two sets of the groups above.

✓ **Proposition 34.** If m and n are relatively prime, then

$$C_{mn} \cong C_m \oplus C_n$$

Remark. Hence $C_2 \oplus C_2 \oplus C_2 = C_2 \oplus C_4 = C_8$ and similarly for others in the above example.

EULER'S ϕ FUNCTION

$\boxed{\star}$ **Definition 34.** (**Euler's function**) Euler's function $\phi(n)$ is the number of integers $1 \leq k \leq n$ that are relatively prime to n. That is, it is the cardinality of the set

$$\phi(n) = |\{a \mid 1 \leq a \leq n,\ \gcd(a,n) = 1\}|$$

Remark. We have:

- If p is prime, then $\phi(p) = p - 1$.
- If $n = p^m$, then $\phi(p^m) = p^m - (p^m/p) = p^m\left(1 - \frac{1}{p}\right)$ since every p^{th} number is a multiple of p^m.

✓ **Proposition 35.** A cyclic group of order n has exactly $\phi(n)$ elements of order n.

Proof. Let $G = \langle c \rangle$ be a cyclic group of order n. Let $1 \leq k \leq n$ and then $c^k \in \langle c \rangle$. Clearly, the order of the element c^k divides n, by Lagrange's Theorem. Now, assume that $\gcd(n,k) = d > 1$. Then $(c^k)^{n/d} = 1$. But then, this implies that order of c^k is atmost $n/d < n$. Whereas, if $\gcd(n,k) = 1$, then $(c^k)^m = 1$ implies that order of c is km, but since order of c is n, hence n divides km and since n and k are relatively prime, therefore n divides m. Hence c^k has order n only when $\gcd(n,k) = 1$, so that there are $\phi(n)$ such elements of order n. ■

ADD TWO PROPOSITIONS, ONE COROLLARY & ONE DEFINITION FROM EVERY REF. BELOW.

1.9 Group Actions

[⋆] **Definition 35.** (**Group Action**) A left group action of a group G on a set X is a mapping $G \times X \to X$ or $(g, x) \to g \cdot x$ such that

1. $1 \cdot x = x$.
2. $g \cdot (h \cdot x) = (g \cdot h) \cdot x$ for all $g, h \in G$ and $x \in X$.

Then G is said to be *acting on the left of* X.

Remark. We can similarly define the *right group action.*

PROPERTIES

✓ **Proposition 36.** In a left group action of a group G on a set X, the action $\sigma_g : x \to g \cdot x$ of $g \in G$ is a permutation of X. Moreover, $g \to \sigma_g$ is a homomorphism of G into the symmetric group S_X.

Proof. First note that $\sigma_g \circ \sigma_h : x \to (g \cdot h) \cdot x$ and hence $\sigma_g \circ \sigma_{g^{-1}} = 1_X = \sigma_{g^{-1}} \circ \sigma_g$ which implies that σ_g is a bijection from X to X. Now since $\sigma_{g \cdot h} = \sigma_g \circ \sigma_h$, hence $g \to \sigma_g$ is a homomorphism. ■

Remark. The symmetric group on a finite set X is the group whose elements are all bijective functions from X to X and whose group operation is that of function composition.

✓ **Proposition 37.** There is a one-to-one correspondence between left actions of G on X and homomorphisms $G \to S_X$.

Proof. The left actions of G on X are the action maps $\sigma_g : x \to g \cdot x$ for all $g \in G$. Also, the homomorphisms from $G \to S_X$ are maps $\rho_g : g \to \sigma_g$. Now for each unique $g \in G$, we have a corresponding σ_g and hence the corresponding ρ_g. Similarly, for each ρ_g, we have a unique σ_g. Hence the bijection between left actions and homomorphisms $G \to S_X$. ■

[⊛] **Theorem 6.** (**Cayley's Theorem**) Every group G is isomorphic to a subgroup of the symmetric group S_G.

Proof. Let G act on G itself by left group action. Therefore $\sigma : G \to S_G$ is a permutation of G and hence an injection (Proposition 29). Moreover, σ is also a surjection from G to $\operatorname{Im} \sigma$. Hence $G \cong \operatorname{Im} \sigma \leq S_G$. ■

✓ **Proposition 38.** Let the group G act on the left of a set X. The relation

$$x \equiv y \text{ if and only if } y = g \cdot x \text{ for some } g \in G$$

is an equivalence relation on X.

Proof. Since G acts on set X hence for $1 \in G$, we have $1 \cdot x = x$, hence $x \equiv x$. For $y \equiv x$, we have $y = g \cdot x \implies x = g^{-1} \cdot x$ and since $g^{-1} \in G$ hence $x \equiv y$. Let $x \equiv y$ and $y \equiv z$, hence $x = g_1 \cdot y$ and $y = g_2 \cdot z$ for some $g_1, g_2 \in G$. We hence get $x = g_1 \cdot (g_2 \cdot z) = (g_1 \cdot g_2) \cdot z$ due to the property of Group Action, and since $g_1 \cdot g_2 \in G$ too, therefore, $x \equiv z$. Hence $\equiv$ is an equivalence relation on X. ■

[⋆] **Definition 36.** (**Orbit**) In a left group action of a group G on a set X, the orbit of $x \in X$ is

$$\{y \in X \mid y = g \cdot x \text{ for some } g \in G\}$$

Remark. Therefore *the orbit of $x \in X$ are all those elements in X to which x can be moved to by the group action of G.*
Also, by virtue of Proposition 31, *the different orbits of the elements of X constitute a partition of X.*

We now look at the size of the orbits.

[⋆] **Definition 37.** (**Stabilizer**) In a left group action of a group G on a set X, the stabilizer $S(x)$ of $x \in X$ is the following subgroup of G:

$$S(x) = \{g \in G \mid g \cdot x = x\}$$

✓ **Proposition 39.** The order of the orbit of an element is equal to the index of it's stabilizer.

Proof. Let G be a group acting on a set X. For some $x \in X$, consider the map $g \to g \cdot x$ from G to orbit of X. Clearly, this is a surjection. Moreover, notice that this map induces a bijection between the elements of orbit of x and the equivalence classes of group G induced by this map. Note that equivalence class of G by this map is $g \cdot x = h \cdot x \implies x = g^{-1} \cdot h \cdot x$ and hence $g^{-1} \cdot h \in S(x)$, hence the equivalence class here is the left cosets of $S(x)$. Hence we have a bijection from left cosets of $S(x)$ and the orbit of an element of X. ■

ACTION BY INNER AUTOMORPHISMS

✓ **Proposition 40.** For every element g of a group G, the mapping $\alpha_g : x \to g \cdot x \cdot g^{-1}$ for any $x \in G$ is an automorphism of G. Moreover, $g \to \alpha_g$ is a homomorphism of G into $\mathbf{Aut}(G)$.

Proof. Remember that an automorphism is a bijective homomorphism from G to G. First note that for $x, y \in G$, we have $\alpha_g(x \cdot y) = g \cdot (x \cdot y) \cdot g^{-1} = g \cdot (x \cdot g^{-1} \cdot g \cdot y) \cdot g^{-1} = (g \cdot x \cdot g^{-1}) \cdot (g \cdot y \cdot g^{-1})$ hence α_g is an endomorphism. For injection, consider $\alpha_g(x) = \alpha_g(y)$ for $x, y \in G$. We get that $g \cdot x \cdot g^{-1} = g \cdot y \cdot g^{-1} \implies x = y$ by cancellation law (Proposition 1). For surjection, note that $\alpha_g \circ \alpha_{g^{-1}} = \mathrm{Id}_G = \alpha_{g^{-1}} \circ \alpha_g$, that is, we have α_g and $\alpha_{g^{-1}}$ as mutually bijective inverses of each other. Hence α_G is an automorphism. Also since under the map $g \to \alpha_g$, we have that $g \cdot h \to \alpha_{g \cdot h} = \alpha_g \circ \alpha_h$, hence $g \to \alpha_g$ is a homomorphism from G to $\mathbf{Aut}(G)$. ■

⋆ **Definition 38.** (**Inner Automorphism**) An inner automorphism of a group G is an automorphism $x \to g \cdot x \cdot g^{-1}$ for some $g \in G$.

⋆ **Definition 39.** (**Action by Inner Automorphism**) The action of a group G on itself by inner automorphism is defined by:

$$g \bullet x = g \cdot x \cdot g^{-1} \quad \text{for all } g, x \in G$$

and we denote $g \cdot x \cdot g^{-1}$ by ${}^g x$.

Remark. $g \bullet x = g \cdot x \cdot g^{-1}$ is indeed a group action.

⋆ **Definition 40.** (**Conjugacy Class**) In the action of a group G on itself by inner automorphisms, the orbits are the conjugacy classes of G. Moreover, two elements are conjugate when they belong to the same conjugacy class.

Remark. More simply, two $x, y \in G$ are said to be *conjugate* in G when $y = g \cdot x \cdot g^{-1}$ for some $g \in G$.
By Proposition 31, *conjugacy is an equivalence relation.*

⋆ **Definition 41.** (**Center of a Group**) The center of a group G is

$$Z(G) = \{g \in G \mid g \cdot x \cdot g^{-1} = x \text{ for all } x \in G\}.$$

Remark. Hence, the conjugacy class of x is said to be ***trivial***, that is $g \cdot x \cdot g^{-1} = x$ for all $x \in G$, if and only if x lies in the center of G. We can see this by noticing that $Z(G) = \{g \in G \mid g = x \cdot g \cdot x^{-1} \text{ for all } x \in G\}$.

✓ **Proposition 41.** $Z(G)$ and all of it's subgroups are normal subgroups of G.

Proof. Consider $z \in Z(G)$. This implies that $z \cdot x \cdot z^{-1} = x \implies z \cdot x = x \cdot z$ for all $x \in G$. Now for any $g \in G$, we hence have $g \cdot z = z \cdot g$. Therefore $g \cdot H = H \cdot g$ for all g and $H \leq Z$, that is $H \trianglelefteq G$. ■

⋆ **Definition 42.** (**Centralizer of an Element**) The centralizer in G of an element x of a group G is

$$C_G(x) = \{g \in G \mid g \cdot x \cdot g^{-1} = x\}.$$

✓ **Proposition 42.** The number of conjugates of an element of a group G is the index of it's centralizer in G.

Proof. Note that the number of conjugates of an element is the order of it's conjugacy class. Since the conjugacy class of an element in G is just it's orbit when G acts by inner automorphism, hence the order of conjugacy class is equal to the index of stabilizer of that element (Proposition 32). But the stabilizer in the case of inner automorphism is just the centralizer. Hence number of conjugates of an element in G is the number of left cosets of it's centralizer. ■

CLASS EQUATION

✓ **Proposition 43.** (**The Class Equation**) In a **finite group** G, we have the following,

$$\boxed{|G| = \sum |C| = |Z(G)| + \sum_{|C|>1} |C|} \tag{1}$$

The first sum has one term for each conjugacy class C and the second sum has one term for each non-trivial conjugacy class C.

Proof. Since the conjugacy classes forms a partition of G by Proposition 31, hence $|G| = \sum |C|$. But there are certain trivial conjugacy classes (whose order is 1) and they are the classes of members of center of the group G. Hence we have $|Z(G)|$ number of trivial conjugacy classes. Therefore the order of the group can be written as the sum of these $|Z(G)|$ trivial classes and all other non-trivial classes. ■

★ **Definition 43.** (p**-groups**) A p-group is a group whose order is a power of a prime p.

Remark. The class equation yields interesting properties of these groups.

✓ **Proposition 44.** Every non-trivial p-group has a non-trivial center.

Proof. Consider G to be a p-group so that $|G| = p^k$ for some $k > 0$. Now assume that G has a trivial center ($Z(g) = \{1_G\}$). Therefore by Class Equation (Proposition 36), we have that $p^k = \sum |C| = 1 + \sum_{|C|>1} |C|$. Now by Lagrange's Theorem (Proposition 15), Proposition 35 and the observation that centralizer of an element in G is a subgroup of G, we can say that $|C|$ divides $|G| = p^k$ apart from the case when $|C| = 1$. Hence we can write class equation as

$$p^k = 1 + p \times (n_1 + n_2 + \dots) = 1 + pn \text{ for some } n > 0$$

which implies that $p^{k-1} = \frac{1}{p} + n$, and since p is a prime, we have a contradiction. Hence every non-trivial p-group has a non-trivial center. ■

✓ **Proposition 45.** Every group of order p^2 where p is prime is abelian.

Proof. Consider a group G of order p^2. Proposition 37 yields that $|Z(G)| > 1$ and Class Equation yields (or for that matter, Lagrange's Theorem) that $|Z(G)| = p$ or $|Z(G)| = p^2$. For $|Z(p)| = p^2$, we would from Class Equation and Proposition 31 have that $G = Z(G)$ and since $Z(G)$ is commutative, hence G would also be commutative.
Next, if $|Z(G)| = p$, then the quotient group $G/Z(G)$ would also have order p by Lagrange's Theorem. Since any group of order p is cyclic (Lagrange's theorem implies that any subgroup has to be trivial), which further implies that if $G/Z(G)$ is cyclic, then for some $g_1 \cdot Z(G) \in G/Z(G)$ and for any $g_2 \cdot Z(G) \in G/Z(G)$ it is true that $g_2 \cdot Z(G) = (g_1 \cdot Z(G))^m$ for some $m > 0$. Expanding this yields us,

$$\begin{aligned} g_2 \cdot Z(G) &= g_1 \cdot Z(G) \cdot g_1 \cdot Z(G) \ \dots \ g_1 \cdot Z(G) \\ &= g_1^m \cdot Z(G)^m \quad \text{(Since } Z(G) \text{ is Normal, Proposition 34)} \\ &= g_1^m \cdot Z(G) \quad \text{(Since } Z(G) \text{ is the set of commuting elements of } G) \end{aligned}$$

which implies by cancellation law of groups that $g_2 = g_1^m$ for any $g_2 \in G$ and for some $g_1 \in G$ and corresponding $m > 0$. Similarly, for $g_3 \in G$, we would have $g_3 = g_1^n$. Hence $g_3 \cdot g_2 = g_1^n \cdot g_1^m = g_1^{n+m} = g_1^{m+n} = g_1^m \cdot g_1^n = g_2 \cdot g_3$. Hence G is commutative in this case too. ■

1.10 The Sylow Theorems

These are a basic tool in finite Group Theory. They are existence theorems of certain subgroups.

First theorem is a *partial converse of Lagrange's Theorem.*

⊛ **Theorem 7.** (**First Sylow Theorem**) Let G be a **finite group** and let p be a prime number. If p^k divides the order of G, then G has a subgroup of order p^k.

Proof. We first prove that *If G is abelian and p divides $|G|$, then G has a subgroup of order p.*

For this, first consider that $|G| = p$, then $G \trianglelefteq G$ will do. Next, for $|G| > p$, we proceed by induction on $|G|$. Let $a \in G$ such that $a \neq 1$. Now if order of a is a multiple of p, as mp, then we have a subgroup $\langle a \rangle$ whose order is divided by p and then we would be done. But if we have order of a not a multiple of p, then it should be true that index of $\langle a \rangle$, equivalently, the order of G/A must be divisible by p. By induction, there would be an element of G/A whose order would be divisible by p, let that element be $b \cdot A$ for some $b \in G$. Notice that order of $b \cdot A$ would be k such that $(b \cdot A)^k = b^k \cdot A^k = b^k \cdot A = A$ in G/A. This implies that k must be a multiple of order of b. But since k is divided by p, hence order of b is divided by p. Therefore, $\langle b \rangle \leq G$ is a subgroup whose order is divisible by p, hence, by induction, G has a subgroup of order p.
Note that we used abelian nature of G in interpreting G/A, as any subgroup of an abelian group is normal.

Now let G be any finite group. We would still proceed by induction. If $|G| = 1$, then this theorem is trivial. For $|G| > 1$, we will prove by induction on $|G|$ that if p^k divides $|G|$, then there is a subgroup of G with order p^k.

Consider the order of the center of G, that is $|Z(G)|$. First consider the case : If p divides $|Z(G)|$, then $Z(G)$ has a subgroup A of order p because $Z(G)$ is by definition abelian. Therefore $A \trianglelefteq G$ is a subgroup of order p. Now, if it is the case that p^k divides $|G|$ hence p^{k-1} divided $|G|$, then clearly, p^{k-1} divides $|G/A| < |G|$ by Lagrange's Theorem. By Induction, there is a subgroup $B/A \leq G/A$ whose order is p^{k-1} and B has order p^k where $B \leq A \leq G$ and then we are done.
Now for the second case : If p does not divide $|Z(G)|$. But since $|G|$ is divided by p^k, then by Class Equation we get that $\sum_{|C|>1} |C|$ cannot be divided by p. That is, there is a atleast one non-trivial conjugacy class C such that p does not divide $|C|$. Now, by Proposition 35, we have that the order of the conjugacy class C is the index of centralizer in G of any element of C. That is, $|C| = [G : C_G(x)]$ for any $x \in C$. Hence we have $|C| = [G : C_G(x)] \leq |Z(G)|$ because $C_G(x) \leq Z(G)$. But since p does not divide $|Z(G)|$, therefore atleast one $|C|$ cannot be divided by p, but $|Z(G)| + |C|$ is surely divided by p. We then have that $|C| = |G| / |C_G(x)|$ is not divided by p but since $|G|$ is divided by p^k, hence $|C_G(x)| < |G|$ is divided by p^k. By induction, there is a subgroup of $C_G(x)$ which has order p^k. ∎

Remark. Because being divisible by p^k means it is divisible by p^j for $0 \leq j \leq k$, hence G also has atleast one subgroup each of order p^j for all $0 \leq j \leq k$.

→ **Corollary 8.** (**Cauchy's Theorem**) A finite group whose order is divisible by a prime p contains an element of order p.

→ **Corollary 9.** Let p be a prime number. The order of a finite group G is a power of p if and only if the order of every element of G is a power of p.

NORMALIZERS

Next Sylow Theorems are proved by allowing G act on it's subgroups by inner automorphisms.

⋆ **Definition 44.** (**Conjugacy Classes of Subgroups**) In the action by inner automorphisms of a group G on it's subgroups, the orbits are the conjugacy classes of subgroups of G. That is, two subgroups of G are conjugate when the belong to the same conjugacy class.

Remark. Thus, two subgroups H and K are *conjugate* when $K = g \cdot H \cdot g^{-1}$ for some $g \in G$.
Also, by extension of Proposition 32, *the number of conjugates of a subgroup is the index of it's stabilizer.*

⋆ **Definition 45.** (**Normalizer of a Subgroup**) The normalizer in G of a subgroup H of G is the *extension of centralizers but for subgroups* as shown:

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

✓ **Proposition 46.** The number of conjugates of a subgroup of a group G is the index of it's normalizer in G.

IInd and IIIrd THEOREMS

These theorems give *properties of p-subgroups of maximal order.*

⋆ **Definition 46.** (**Sylow p-subgroup**) Let p be prime. A Sylow p-subgroup of a **finite group** G is a subgroup of order p^k, where p^k divides $|G|$ and p^{k+1} does not divide $|G|$.

Remark. Note that First Sylow Theorem guarantees the existence of Sylow p-subgroup.

✓ **Proposition 47.** If a Sylow p-subgroup of a finite group G is normal in G, then it is the largest p-subgroup of G and the only Sylow p-subgroup of G.

Proof. Consider $S \trianglelefteq G$ to be the normal Sylow p-subgroup of G of order p^{k_1}. Now assume that T is a p-subgroup of G of order p^{k_2} such that $S \leq T$. Clearly, we have that $|S| = p^{k_1} \leq p^{k_2} = |T|$ so that $|T \cap S| = |S| = p^{k_1}$. By Theorem 4, $S \trianglelefteq T \cdot S$, $T \cap S \trianglelefteq T$ and $T/(T \cap S) \cong (T \cdot S)/S$. Therefore, $|T|/|T \cap S| = |T \cdot S|/|S| \implies |T| = |T \cdot S| \geq |S|$. Now, by the choice of S, we have that $|T \cdot S| = |S|$ which implies that $T \subseteq T \cdot S = S$.**HELP!** ■

⊛ **Theorem 8.** (**Second Sylow Theorem**) Let p be a prime number. The number of Sylow p-subgroups of a finite group G divides the order of G and is congruent to 1 *modulo* p.

⊛ **Theorem 9.** (**Third Sylow Theorem**) Let p be a prime number. All Sylow p-subgroups of a finite group are conjugate.

Proof. To Prove : Number of Sylow p-subgroups is congruent to 1 $(\mod p)$.

1. Let S be a Sylow p-subgroup.
2. Clearly, the conjugates of S are also Sylow p-subgroups by definition.
3. Hence S acts on the set $\mathcal{S}$ of all Sylow p-subgroups by inner automorphisms.
4. Under the action of S by inner automorphisms on $\mathcal{S}$, the set $\{S\}$ is the orbit of S because $a \cdot S \cdot a^{-1} = S$ for all $a \in S$ (Definitions 34 & 35).
5. Conversely, assume $\{T\}$ is the trivial orbit of S under inner automorphism of S on $\mathcal{S}$. This means that $T = a \cdot T \cdot a^{-1}$ for all $a \in S$.
6. This implies that $S \subseteq N_G(T)$.
7. But then it means that S is normal in $N_G(T)$.
8. Hence, by Proposition 40, S is the largest and only Sylow p-subgroup in $N_G(T)$.
9. But T is the trivial orbit, then it is also a Sylow p-subgroup, hence $S = T$.
10. Therefore we proved that under the action of S on $\mathcal{S}$ by inner automorphisms, the only orbit is the trivial orbit is $\{S\}$.
11. Now by Proposition 32, we have that order of the orbit of $S \in \mathcal{S}$ is equal to $|\mathcal{S}|/|S(S)|$ where $S(.)$ is the stabilizer.
12. Since $S(S) = S$, hence $|\{S\}| = 1 = |\mathcal{S}|/|S|$ and due to $|S| = p^k$, therefore $|\mathcal{S}| \equiv 1 (\mod p)$.

Next,
To Prove : The number of total Sylow p-subgroups divides the order of G and all Sylow p-subgroups are conjugate.

1. We would prove that the set of all Sylow p-subgroups $\mathcal{S}$ is a conjugacy class.
2. Let us assume that $\mathcal{S}$ contains two disjoint conjugacy classes C_1 and C_2 of subgroups.
3. Note that C_1 and C_2 are conjugate classes which are also subsets of $\mathcal{S}$, hence they consists of Sylow p-subgroups of G. Therefore for $S \in C_1$ acts on C_1 by inner automorphism.
4. In this case, the trivial orbit is $\{S\}$ and hence $|C_1| \equiv 1 (\mod p)$.
5. Similarly, S also acts on $C_2 \subseteq \mathcal{S}$ by inner automorphism. But $S \notin C_2$, hence trivial orbit is $\{\}$ so that $|C_2| \equiv 0 (\mod p)$.
6. Now let $T \in C_2$ act on C_2 by inner automorphism. We then similarly get that $|C_2| = 1 (\mod p)$ whereas $|C_1| = 0 (\mod p)$. Hence a contradiction.
7. Therefore $\mathcal{S}$ cannot contain two disjoint conjugacy classes, hence it is a conjugacy class.
8. Note that conjugacy class of subgroups is the orbit of any subgroup in it and since order of the orbit divides $|G|$, hence $|\mathcal{S}|$ divides $|G|$.

■

→ **Corollary 10.** A Sylow p-subgroup is normal if and only if it is the only Sylow p-subgroup.

FURTHER RESULTS

✓ **Proposition 48.** In a finite group, every p-subgroup is contained in a Sylow p-subgroup.

Proof. Let H be a p-subgroup of a finite group G and S be the set of all Sylow p-subgroups of G. We have that $|S| \equiv 1(\mod p)$ (Theorem 8). Now suppose H acts on S by inner automorphisms. Note that we have atleast one Sylow p-subgroup S_1 in S. **If it so happens that** $h \cdot S_1 \cdot h^{-1} = S_1$ for all $h \in H$, then that would imply that $H \subseteq N_G(S_1)$. Now note that $S_1 \trianglelefteq N_G(S_1)$, hence by Proposition 40, $H \subseteq S_1$. ■

? **Doubt 1.** Let H be a p-subgroup and S be a Sylow p-subgroup of group G. Then is it true that $H \subseteq N_G(S)$?

Attempt. *We have that* $N_G(S) = \{g \in G \mid g \cdot S \cdot g^{-1} = S\}$. *Cleary,* $S \trianglelefteq N_G(S)$. *Since* S *is a normal Sylow* p*-subgroup of* $N_G(S)$*, hence any other* p*-subgroup of* $N_G(S)$ *would be subset of* S *(Proposition 40). Now note that for any* $h \in H$,$h \cdot S = S$ *because of Corollary 8, we have that* $h \cdot S$ *is another* p*-subgroup and by Definition 45 and Theorem 9,* $h \cdot S = S$. *Similarly for* $S \cdot h^{-1} = S$. *Hence* $h \cdot S \cdot h^{-1} = S$, *so that* $H \subseteq N_G(S)$.

✓ **Proposition 49.** In a finite group, a subgroup that contains the normalizer of a Sylow p-subgroup is it's own normalizer.

Proof. Let G be a finite group and S be a Sylow p-subgroup of G and let $H \leq G$ be a subgroup such that $N_G(S) \subseteq H$. Consider now the normalizer of H as

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

Note that $S \trianglelefteq N_G(S) \subseteq H \trianglelefteq N_G(H)$. Now for any $a \in N_G(H)$, we have $a \cdot H \cdot a^{-1} = H$, so we also have $a \cdot S \cdot a^{-1} = S$. Hence, $a \cdot S \cdot a^{-1}$ and S are Sylow p-subgroups of H. By Theorem 9, $a \cdot S \cdot a^{-1}$ and S are conjugates in H. Therefore, $\exists h \in H$ such that $h \cdot (a \cdot S \cdot a^{-1}) \cdot h^{-1} = S$. This implies that for any $a \in N_G(H)$ and for some $h \in H$ we have $h \cdot a \in N_G(S) \subseteq H$. In other words, $N_G(H) \subseteq H$. But since $H \trianglelefteq N_G(H)$, hence $H = N_G(H)$ when H contains the normalizer of a Sylow p-subgroup. ■

✓ **Proposition 50.** A p-subgroup of a finite group that is not a Sylow p-subgroup is not it's own normalizer.

→ **Corollary 11.** In a finite p-group, every subgroup of index p is normal.

Answers to exercises on applications to follow soon.

2 Rings

Rings are the next algebraic structure we discuss. They combine the complexity of semigroups and algebraic properties of abelian groups.

⋆ **Definition 47.** (**Ring**) A ring is an ordered triple $(R, +, \cdot)$ of a set R and two binary operations on R, an addition and a multiplication, such that

1. $(R, +)$ is an **abelian group**.
2. $(R, \cdot)$ is a **semigroup**.
3. The multiplication $(\cdot)$ is **distributive**:

$$x \cdot (y + z) = x \cdot y + x \cdot z \text{ and } (y + z) \cdot x = y \cdot x = z \cdot x$$

⋆ **Definition 48.** (**Ring with Identity**) A ring with identity is a ring whose multiplicative semigroup $(R, \cdot)$ has an additional identity element, so $(R, \cdot)$ becomes a **monoid**.

Remark. Generally in a ring with identity, the identity element of monoid $(R, \cdot)$ is denoted as 1 and the identity element of abelian group $(R, +)$ is the *zero* element denoted 0.

✓ **Proposition 51.** The set $\mathbf{End}(A)$ of all endomorphisms of an abelian group A is a ring with identity with pointwise addition and functional composition as multiplication.

Proof. By Proposition 22, $\mathbf{End}(A)$ is a monoid under composition. For any $f, g \in \mathbf{End}(A)$, we have that pointwise addition $f + g$ is commutative as $(f + g)(a) = f(a) + g(a) = g(a) + f(a)$ is possible because A is abelian. Associativity follows trivially to show $(\mathbf{End}(A), +)$ is an abelian group. For $(\mathbf{End}(A), \circ)$ where $\circ$ is composition, associativity follows trivially from functional composition and since $\mathrm{Id}_A \in \mathbf{End}(A)$ which implies that $f \circ \mathrm{Id}_A = \mathrm{Id}_A \circ f = f$, therefore existence of identity follows too to show $(\mathbf{End}(A), \circ)$ is a monoid. Finally, $f \circ (g + h) = f \circ g + f \circ h$ and the other case follows trivially from properties of functional composition. ■

PROPERTIES

✓ **Proposition 52.** In a ring $(R, +, \cdot)$, following properties hold:

1. For all **finite** $x_1, x_2, \ldots, x_m, y_1, y_2 \ldots, y_n \in R$ we have,

$$\left(\sum_i x_i\right) \cdot \left(\sum_i y_i\right) = \sum_{i,j} x_i \cdot y_j.$$

2. For all $m, n \in \mathbb{Z}$ and $x, y \in R$ we have,

$$(mx) \cdot (ny) = (mn)(x \cdot y).$$

   Moreover, if R is a ring with identity, then

$$nx = (n1)x.$$

   for all $n \in \mathbb{Z}$ and $x \in R$.

3. For all $x, y, z \in R$ we have,

$$x \cdot (y - z) = x \cdot y - x \cdot z \text{ and } (y - z) \cdot x = y \cdot x - z \cdot x.$$

   In particular,

$$x \cdot 0 = 0 \cdot x = 0$$

   for all $x \in R$.

Proof. Since $(R, +)$ is an abelian group, hence $x = x_1 + x_2 + \cdots + x_m \in R$. Similarly, $y = y_1 + y_2 + \cdots + y_n \in R$. Since $(\cdot)$ is distributive, therefore $(x_1 + \cdots + x_m) \cdot y_1 = x_1 \cdot y_1 + \ldots x_m \cdot y_1 \in R$ and we can proceed similarly for all y_i's. Now since $x_i \cdot y_j \in R$ for all i, j, hence their sum would be too in R so we get first result.

We mean by $mx = \underbrace{x + x + \cdots + x}_{m-\text{times}}$. Therefore by part 1, we have $\underbrace{(x + \cdots + x)}_{m-\text{times}} \cdot \underbrace{(y + \cdots + y)}_{n-\text{times}} = \underbrace{x \cdot y + \cdots + x \cdot y}_{mn-\text{times}} = (mn) \cdot (x \cdot y)$.

Define $-x$ as the inverse of x in abelian group $(R, +)$, therefore $-x \in R$. By distributive property of rings, $x \cdot (y + (-z)) = x \cdot y + x \cdot (-z)$ for any $x, y, z \in R$. Now for $x \cdot (-z)$, note that $z + (-z) = 0 \implies x \cdot z + x \cdot (-z) = 0$, hence inverse of $x \cdot z$ is $x \cdot (-z)$, that is, $x \cdot (-z) = -(x \cdot z)$. Therefore we have the third result. ■

⋆ **Definition 49.** (**Commutative Ring**) A ring is commutative when it's multiplication is commutative.

✓ **Proposition 53.** (**Binomial Theorem**) In a commutative ring R,

$$(x+y)^n = \sum_{0\le i\le n} \binom{n}{i} x^i y^{n-i}, \text{where } \binom{n}{i} = \frac{n!}{i!(n-i)!}.$$

Remark. Binomial theorem is in-fact true for elements x, y of any ring, as long as $x \cdot y = y \cdot x$.

INFINITE SUM IN ABELIAN GROUPS

⋆ **Definition 50.** (**Property holds for *almost all* elements**) A property P holds for almost all elements i of a set I when the set

$$\{i \in I \mid P \text{ does not hold}\} \text{ is } \textbf{finite.}$$

⋆ **Definition 51.** (**Arbitrary Defined Sum**) The sum $\sum_{i\in I} x_i$ of elements $(x_i)_{i\in I}$ of an abelian group A is defined in A when $x_i = 0$ for almost all $i \in I$. If that's the case, then we can write the arbitrary sum as the following finite sum:

$$\sum_{i\in I} x_i = \sum_{i\in I, x_i\neq 0} x_i$$

Remark. Therefore an *arbitrary sum* is in-fact a finite sum to which an arbitrary amount of zeros is added.

✓ **Proposition 54.** In a ring, $\left(\sum_i x_i\right) \cdot \left(\sum_j y_j\right) = \sum_{i,j} x_i \cdot y_j$, whenever $x_i = 0$ for **almost all** $i \in I$ and $y_j = 0$ for **almost all** $j \in J$.

Proof. Follows trivially from Definition 50 (since $(R, +)$ is abelian) & Proposition 45, 1. ■

RING HOMOMORPHISMS

⋆ **Definition 52.** (**Ring Homomorphism**) A homomorphism of a ring R into a ring S is a mapping $\varphi : R \to S$ that preserves sums and products. That is,

- $\varphi(x+y) = \varphi(x) + \varphi(y)$ for all $x, y \in R$.
- $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$ for all $x, y \in R$.

Moreover, if R and S are rings with identity, then the homomorphism of rings with identity from R onto S is a map which additionally also preserves the identity element :

$$\varphi(1_R) = 1_S.$$

✓ **Proposition 55.** Consider the rings R and S and a homomorphism $\varphi : R \to S$ between them. Then the following are true:

- $\varphi(0_R) = 0_S$.
- $\varphi(nx) = n\varphi(x)$ for all $x \in R$ and $n \in \mathbb{Z}_+$.
- For arbitrary $(x_i)_{i\in I} \in R$,
$$\varphi\left(\sum_{i\in I} x_i\right) = \sum_{i\in I} \varphi(x_i).$$
- $\varphi(x^n) = (\varphi(x))^n$ for all $x \in R$.
- If $\varphi : R \to S$ and $\psi : S \to T$ are ring homomorphisms, then they are composable and
$$\psi \circ \varphi : R \to T \text{ is another homomorphism between rings } R \text{ onto } T.$$
- Identity map $\mathrm{Id}_R : R \to R$ is a ring homomorphism.

Remark. Usually, an injective homomorphism is called a *monomorphism* and an surjective homomorphism is called a *epimorphism.*

⋆ **Definition 53.** (**Ring Isomorphism**) An isomorphism of rings $(\cong)$ is a bijective homomorphism of rings.

ADJOINING AN IDENTITY

Any ring R can be embedded into a ring with identity(!)

✓ **Proposition 56.** For every ring R, the set $R^1 = R \times \mathbb{Z}$ with operations

- $(x,m) + (y,n) = (x+y, m+n)$.
- $(x,m) \cdot (y,n) = (x \cdot y + nx + my, mn)$

is a **ring with identity**. Moreover, $\iota : x \to (x,0)$ is an injective homomorphism of R into R^1.

Proof. In $(R^1,+)$, we see that $(x,m)+(y,n) = (x+y,m+n) = (y+x,n+m) = (y,n)+(x,m)$ because R and $\mathbf{Z}$ are rings, hence this is commutative. Similarly we can show associativity. Inverse of any (x,m) is $(-x,-m)$. Identity is $(0_R,0)$. Hence $(R^1,+)$ is an abelian group.

In $(R^1,\cdot)$, we see that $((x,m)\cdot(y,n))\cdot(z,l) = (x\cdot y+nx+my,mn)\cdot(z,l) = ((x\cdot y+nx+my)\cdot z + lx\cdot y + lnx + lmy + mnz, mnl) = (x\cdot y\cdot z + nx\cdot z + my\cdot z + lx\cdot y + lnx + lmy + mnz, mnl)$. Similarly, $(x,m)\cdot((y,n)\cdot(z,l)) = (x,m)\cdot(y\cdot z + ly + nz, nl) = (x\cdot y\cdot z + lx\cdot y + nx\cdot z + my\cdot z + mly + mnz + nlx, mnl)$ which is same as previous, so it is associative. For identity, consider any element $(x,m) \in R^1$ and a particular $(y,n) \in R^1$ such that

$$\begin{aligned} (x,m)\cdot(y,n) &= (x,m) \\ (x\cdot y + nx + my, mn) &= (x,m) \\ \implies \quad x\cdot y + nx + my &= x \text{ and } mn = m (\implies n = 1) \\ (x + m1_R)\cdot y &= -(n-1)x \in R \\ &= 0_R \ \forall\ x \in R \ \&\ \forall\ m \in \mathbb{Z} \end{aligned}$$

Now if $(x+m1_R)\cdot y \in R$ with $y \in R$ already, then $m1_R \in R$ for all $m \in \mathbb{Z}$ and hence $x + m1_R \in R$ for all $x \in R$. This implies that $y = 0_R$ so that $(0_R,1)$ is the identity. Hence $(R^1,\cdot)$ is a monoid.

Finally, $(x,m)\cdot[(y,n)+(z,l)] = (x,m)\cdot(y+z,n+l) = (x\cdot(y+z) + (n+l)x + m(y+z), m(n+l)) = (x\cdot y + nx + my + x\cdot z + lx + mz, mn + nl) = (x,m)\cdot(y,n) + (x,m)\cdot(z,l)$, so $(R,+,\cdot)$ is distributive with $(\cdot)$ over $+$, hence a ring. ■

The ring R^1 has a *Universal Property*, similar to Factorization Theorem (1).

✓ **Proposition 57.** Every homomorphism φ of ring R into a ring S with identity, factors uniquely through $\iota : R \to R^1$. That is, there is a unique homomorphism $\psi : R^1 \to S$ where S is a ring with identity, such that $\varphi = \psi \circ \iota$.

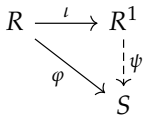

Figure 5: Let $\varphi : R \to S$ be any ring homomorphism and S be a ring with identity, then above commutes.

Proof. Proposition 51 shows that $1_{R^1} = (0_R,1)$. Moreover, we can see that for any $(x,n) \in R^1$, $(x,n) = (x,0) + n(0_R,1) = n1_{R^1}$. Since $\varphi(x) \in S$, $\iota(x) = (x,0) \in R^1$, then if we define $\psi((x,n)) = \varphi(x) + n1_S$ (as S contains identity), it gives us a ring homomorphism from R^1 onto S. Uniqueness of φ can be seen if we take $\xi : R^1 \to S$ as another ring homomorphism so that $\varphi = \xi \circ \iota$. Then $\xi((x,n)) = \xi((x,0) + n1_{R^1}) = \xi((x,0)) + n\xi(1_{R^1})$. Since ξ is a homomorphism, hence $\xi(1_{R^1}) = 1_S$, therefore $\xi((x,n)) = \xi((x,0)) + n1_S$ which is same as the definition of ψ. ■

2.1 Subrings and Ideals[3]

SUBRINGS

★ **Definition 54.** (**Subring**) A subring of a ring R with identity is a subset S of R such that :

- S is a subgroup of $(R,+)$: $S \leq (R,+)$.
- S is closed under multiplication : $x, y \in S$ implies $x \cdot y \in S$.
- S contains the identity element : $1_R \in S$.

✓ **Proposition 58.** Every intersection of subrings of a ring R is a subring of R.

Proof. Consider $(S_i)_{i\in I}$ be a collection of subrings of ring R (with identity). Denote $S = \bigcap_{i\in I} S_i$. Since $0_R \in S_i$ for all $i \in I$, hence $1_R \in S$. For any $x, y, z \in S$, we have $0_R \in S$; $x \in S \implies x \in S_i$ for all i, therefore $-x \in S_i$ for all i and therefore $-x \in S$; $x + y \in S_i$ for all i as x and y are in every S_i. Hence $S \leq (R,+)$. For any $x, y \in S$ implies $x, y \in S_i \ \forall\ i \in I$, so that $x \cdot y \in S_i \ \forall\ i \in I$. Hence S is a subring of R. ■

IDEALS

★ **Definition 55.** (**Ideal**) An ideal of a ring R is a subgroup I of $(R,+)$ such that :

- $I \leq (R,+)$.
- $x \in I \implies x \cdot y \in I$ and $y \cdot x \in I$ for all $y \in R$.

A **Proper** Ideal additionally satisfies that $I \neq R$.

PROPERTIES

✓ **Proposition 59.** Every intersection of ideals of a ring R is an ideal of R.

★ **Definition 56.** (**Ideal Generated from Subset**) The ideal (S) of a ring R generated by a subset S of R is the smallest ideal that contains S.

Remark. The smallest ideal that contains S is constructed by taking intersection of all the ideals of R that contain S.

★ **Definition 57.** (**Principal Ideal**) A principal ideal is an ideal generated by a single element. That is, an ideal I is principal if $\exists\ a \in R$ such that

$$I = \{a \cdot r \mid r \in R\}.$$

Or, $\exists\ a \in R$ such that for any $x \in I$ it must be true that $x = a \cdot r$ for some $r \in R$ to call I a principal ideal.

✓ **Proposition 60.** In a ring R with identity, the ideal (S) generated by a subset S is the set of all **finite** sums of elements of the form $x \cdot s \cdot y$ where $s \in S$ and $x, y \in R$. That is,

$$(S) = \{x_1 \cdot s_1 \cdot y_1 + \cdots + x_n \cdot s_n \cdot y_n \mid s_i \in S\ ,\ \ x_i, y_i \in R\ ,\ \ n \in \mathbb{N}\}$$

Moreover, if R is commutative, then (S) is the set of all **finite** linear combinations of elements of S with coefficients in R.

Proof. Construct the subset $I = \{x_1 \cdot s_1 \cdot y_1 + \cdots + x_n \cdot s_n \cdot y_n \mid s_i \in S\ ,\ \ x_i, y_i \in R\ ,\ \ n \in \mathbb{N}\}$. We hence need to show that I is the smallest ideal containing subset S. To begin with, let's ensure first that I is a subgroup of $(R,+)$. Take $z_1, z_2 \in I$, hence $z_1 = \sum_{i\in J} x_i \cdot s_i \cdot y_i$ and $z_2 = \sum_{j\in K} x_j \cdot s_j \cdot y_j$ for finite index sets J and K. We have that inverse of z_2 which is $-z_2 = -\sum_{j\in K} x_j \cdot s_j \cdot y_j = \sum_{j\in K}(-x_j) \cdot s_j \cdot y_j \in I$. Therefore $z_1 \cdot (-z_2) = \sum_{i\in J, j\in K} x_i \cdot s_i \cdot y_i \cdot (-x_j) \cdot s_j \cdot y_j \in I$ as each term $x_i \cdot s_i \cdot y_i \cdot (-x_j) \in R$, therefore $x_i \cdot s_i \cdot y_i \cdot (-x_j) \cdot s_j \cdot y_j \in I$ and hence $z_1 \cdot (-z_2) \in I$. By Proposition 6, we have that I is a subgroup.
We now show that I is an Ideal. Take any $z \in I$. By the definition of I, $z = \sum_{i\in J} x_i \cdot s_i \cdot y_i$ for some finite index set J. Now, for any $w \in R$, due to distributive & associative property, we have $w \cdot z = \sum_{i\in J}(w \cdot x_i) \cdot s_i \cdot y_i \in I$ because $w \cdot x_i \in R$. Similarly, $z \cdot w \in I$. Hence I is an ideal.
Finally, to show that I is generated by S, that is, I is the smallest ideal to contain S. Assume I' to be another ideal which contains S such that $S \subseteq I' \subseteq I'$. Now for any $z \in I$, we have that $z = \sum_{j\in J} x_j \cdot s_j \cdot y_j$. But for any $s \in S \subseteq I'$, we have that $x \cdot s \in I' \implies x \cdot s \cdot y \in I'$ for all $x, y \in R$. Now since I' is an ideal so it is a subgroup of $(R,+)$, hence $\sum_{j\in J} x_j \cdot s_j \cdot y_j \in I'$. Which means that $z \in I'$ for all $z \in I$. That is, $I \subseteq I'$. Hence $I = I'$ and I is the smallest ideal which contains S.

If R is commutative, then $x \cdot s \cdot y = (x \cdot y) \cdot s$ and hence I becomes the subset of R which contains all the finite linear combinations of elements of S with coefficients in R. ■

[3] *From this section onward, all rings are rings with identity & all homomorphisms of rings are homomorphisms of rings with identity.*

✓ **Proposition 61.** In a commutative ring R with identity, the principal ideal generated by $a \in R$ is the set $(a) = R \cdot a$ of all multiples of a.

Proof. Trivially follows from Proposition 55 and distributive property. ■

Union of Ideals is generally *not* an Ideal, with some particular exceptions.

✓ **Proposition 62.** The union of a non-empty directed family of ideals of a ring R with identity is an ideal of R. In particular, the union of a non-empty chain of ideals of a ring R is an ideal of R.

Proof. TRIVIAL. Simply use Definition 17 to good use. ■

Remark. ⋆ This Proposition implies that we can use *Zorn's Lemma*. That is, since we have a poset where every subset has an upper bound, courtesy of directed family (Definition 17), then we are allowed to ascertain that in the directed family of ideals there is a non-trivial ***Maximal Ideal***.

⋆ **Definition 58.** (**Maximal Ideal**) A maximal ideal of a Ring R is a non-trivial ideal $M \neq R$ such that there is **no** ideal I such that $M \subsetneq I \subsetneq R$.

✓ **Proposition 63.** In a ring R with identity, every proper ideal is contained in a maximal ideal.

Proof. Consider the set $\mathcal{S}$ of all proper ideals $(I_j)_{j\in J}$ which is *partially-ordered* by inclusion ($\subseteq$) relation. $\mathcal{S}$ is hence a poset. Now we are not sure whether taking the union $\bigcup_{j\in J} I_j$ would be proper or not (however, it would be an ideal, Proposition 55). So let's work this out first.
Note that all I_j's are proper, hence $I_j \neq R$ for all j. Also note that if $1_R \in I_j$ for all j, then $I_j = R$ as I_j would necessarily have to contain all elements of R. Therefore, if I_j is proper, then $1_R \notin I_j$ for all j. So, $1_R \notin \bigcup_{j\in J} I_j$ and hence $\bigcup_{j\in J} I_j$ is also proper.
Now, we simply use *Zorn's Lemma* in the poset $\mathcal{S}$ since every non-empty chain (Definition 16) in $\mathcal{S}$ has upper bound as it's union. Therefore we get that $\mathcal{S}$ contains a maximal ring M which is the maximal ideal. ■

⋆ **Definition 59.** (**Sum of Ideals**) The sum of ideals $(J_i)_{i\in I}$ of a ring R is

$$\sum_{i\in I} J_i = \left\{ \sum_{i\in I} x_i \mid x_i \in J_i \text{ and } x_i = 0 \text{ for almost all } i \in I \right\}.$$

✓ **Proposition 64.** Every sum of ideals of a ring R is an ideal of R.

Proof. Consider $z \in \sum_{i\in I} J_i$ where $(J_i)_{i\in I}$ is a collection of ideals. Clearly, $z = \sum_{i\in I} x_i$ where $x_i \in J_i$. Hence for any $w \in R$ we have $w \cdot z = \sum_{i\in I} w \cdot x_i$ where we used distributive property. Now since $x_i \in J_i$ and J_i is ideal so $w \cdot x_i \in J_i$ for any $w \in R$ for all $i \in I$. Therefore $\sum_{i\in I} w \cdot x_i \in \sum_{i\in I} J_i$. Similar steps will prove the $z \cdot w$ case. Hence any sum of ideals is an ideal in R. ■

2.2 Homomorphisms

It turns out that the homomorphisms of rings introduced earlier also preserve subrings and to some extent ideals.

SUBGRINGS & IDEALS

✓ **Proposition 65.** Let $\varphi : R \to S$ be a homomorphism of rings. If A is a subring of R and B is a subring of S, then

- $\varphi(A) = \{\varphi(x) \in S \mid x \in A\}$ is a subring of S.
- $\varphi^{-1}(B) = \{x \in R \mid \varphi(x) \in B\}$ is a subring of R.

Moreover, if A is an ideal of R, B is an ideal of S and φ is **surjective**, then :

- $\varphi(A)$ is an ideal of S.
- $\varphi^{-1}(B)$ is an ideal of R.

Proof. Simple (but long) verification of the respective definitions. ■

⋆ **Definition 60.** (**Image & Kernel of Homomorphisms**) Let $\varphi : R \to S$ be a homomorphism of rings, then:

- The image/range of φ is
$$\text{Im } \varphi = \{\varphi(x) \mid x \in R\}$$
- The kernel of φ is
$$\text{Ker } \varphi = \{x \in R \mid \varphi(x) = 0_S\}$$

Remark. Note that Im $\varphi = \varphi(R)$ and Ker $\varphi = \varphi^{-1}(0_S)$.

✓ **Proposition 66.** Let $\varphi : R \to S$ be a homomorphism of rings.

- The image subset Im φ is a **subring** of S.
- The kernel subset Ker φ is an **ideal** of R.
- $\varphi(x) = \varphi(y)$ **if and only if** $x - y \in$ Ker φ.

Proof. Since R is a subring of R, hence by Proposition 58 Im $\varphi = \varphi(R)$ is a subring of S. Take any $r \in R$ and some $k \in$ Ker $\varphi \subseteq R$. By definition, $\varphi(k) = 0_S$. Since $\varphi(r \cdot k) = \varphi(r) \cdot \varphi(k) = 0_S$ (Proposition 45), therefore $r \cdot k \in$ Ker $\varphi \ \forall \ r \in R$ and any $k \in$ Ker φ. Hence Ker φ is an ideal of R.
Take any two $x, y \in R$. If $\varphi(x) = \varphi(y) \implies \varphi(x - y) = 0_S$, hence $x - y \in$ Ker φ. Conversely, if $x - y \in$ Ker φ, then by definition, $\varphi(x - y) = \varphi(x) - \varphi(y) = 0_S \implies \varphi(x) = \varphi(y)$. ■

QUOTIENT RINGS

✓ **Proposition 67.** Let I be an Ideal of a ring R. The cosets of I in the abelian group $(R, +)$ constitute a ring R/I with the following operations and properties:

- $(x + I) + (y + I) = (x + y) + I$ for all $x, y \in R$.
- $(x + I) \cdot (y + I) = x \cdot y + I$ for all $x, y \in R$.
- The map $\varphi : x \longrightarrow x + I$ is a surjective ring homomorphism such that Ker $\varphi = I$.

Proof. Note that R/I is a subgroup of $(R, +)$ and since $(R, +)$ is abelian, then any subgroup of it is normal (Definition 24). Therefore, R/I is an abelian group. Now, any coset of I in $(R, +)$ is $x + I$ for any $x \in R$. Take any two $x + I$ and $y + I$ in R/I. Due to distributive property and I being an Ideal, we have $(x + i) \cdot (y + j) = x \cdot y + x \cdot j + i \cdot y + i \cdot j \in x \cdot y + I$ for any $i, j \in I$. Therefore R/I is a ring. Finally, Ker $\varphi = \{x \in R \mid \varphi(x) = 0\}$. Note that $y + I = 0$ in R/I is such that $(x + I) + (y + I) = (y + I) + (x + I) = x + I$. Now since $(x + I) + (y + I) = (x + y) + I = x + I \implies y = 0_R$ so that $y + I = 0_R + I = I$. Hence Ker $\varphi = I$. ■

★ **Definition 61.** (**Quotient Ring**) Let I be an ideal of a ring R. The ring of all cosets of I in $(R,+)$ is the quotient ring R/I of R by I.

★ **Definition 62.** (**Canonical Projection**) The surjective homomorphism $x \longrightarrow x + I$ is the canonical projection of R onto R/I.

Remark. Integers modulo n, $\mathbb{Z}_n$, is hence the quotient ring $\mathbb{Z}/n\mathbb{Z}$.

✓ **Proposition 68.** Let I be an Ideal of a ring R. Every subring of R/I is the quotient S/I of a unique subring S of R that contains I. Moreover, every ideal of R/I is the quotient J/I of a unique ideal J of R that contains I.

Proof. Take A to be a subring of R/I. By definition, $A \leq (R/I,+)$. By Proposition 25, there is a unique subgroup S of $(R,+)$ such that $A = S/I$ and $I \subseteq S$. Since S is a subgroup of $(R,+)$, is closed under multiplication and $1_R \in S$, hence S is a subring of R and then S/I is the quotient of subring S. Finally, since any ideal X of the quotient ring R/I is a subgroup of $(R/I,+)$, hence we can use Proposition 25 to prove the existence of a unique subgroup J of $(R,+)$ such that $X = J/I$ and $I \subseteq J$. Since X is ideal therefore J/I is also ideal. Therefore $(j+I)\cdot(r+I) = j\cdot r + I \in J/I \implies j\cdot r \in J$ for all $r \in R$. Similarly for $(r+I)\cdot(j+I)$. Hence J is a unique ideal of R. ■

2.3 Domains & Fields

These are the two major types of rings.

★ **Definition 63.** (**Integral Domain**) An Integral Domain is a *commutative ring* $R \neq 0_R$ with identity in which,

$$x, y \neq 0_R \text{ implies } x \cdot y \neq 0_R$$

Remark. Note:

- The condition can contra-positively be written as:

$$x \cdot y = 0_R \implies x = 0_R \text{ or } y = 0_R.$$

- One can otherwise say that a *ring* R *is an integral domain if* $R \setminus \{0_R\}$ *is a commutative monoid under multiplication.*
- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are domains.
- If one defines *zero divisors* of a commutative ring R to be a non-zero element $x \neq 0_R$ such that $x \cdot y = 0_R$ for some $y \neq 0_R \in R$, then *integral domain can be defined as the commutative ring which contains no zero divisors.*
- Integral domain is sometimes referred to just as domain.

★ **Definition 64.** (**Field**) A Field is a *commutative ring* $F \neq 0$ such that $F \setminus \{0_F\}$ is a group under multiplication.

Remark. Note:

- Clearly, $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are also fields.
- This definition reflects that any commutative ring is a field if and only if every non zero element has a multiplicative inverse.

✓ **Proposition 69.** The ring $\mathbb{Z}_n$ is a domain if and only if n is prime.

Proof. *Thank You.* ■

PROPERTIES

✓ **Proposition 70.** In an integral domain D,

$$x \cdot y = x \cdot z \implies y = z \text{ when } x \neq 0_D.$$

Proof. Take elements $x \in D$ which is not 0_D and two $y, z \in D$ such that $x \cdot y = x \cdot z \implies x \cdot (y - z) = 0$. Furthermore, by first remark in Integral Domain's definition, either $x = 0_D$ or $y - z = 0_D$. Since $x \neq 0_D$, therefore $y - z = 0_D \implies y - z + z = 0_D + z \implies y = z$. ■

Add More Results after the clearance.

PRIME IDEALS

★ **Definition 65.** (**Prime Ideals**) Consider a commutative Ring R with identity. A prime ideal $\mathfrak{p}$ of R is

- $\mathfrak{p}$ is a Proper Ideal of R.
- For two