Groups and Rings

Labix

May 15, 2025

Abstract

These notes will survey one of the most basic constructions in the entirely of algebra. Algebra had came to be from the study of symmetry, and symmetric will the definitions of a group will be. Broadly speaking abstract algebra is the study of algebraic structures.

The first 5 chapters are dedicated to group theory , which is what happens when a set can be endowed with a binary operation that achieves some level of symmetry through inverses and identities. In particular, Lagrange's theorem and results from normal subgroups such as the first isomorphism theorem form the technical foundation of group theory, while group actions can be widely seen from all areas of mathematics.

The remaining chapters introduces the notion of rings, which is a set with two operations instead of one, again satisfying some level of symmetry with inverses and identities. Rings form an even larger class of objects than groups, in which we classify them according to what additional properties they and the ideals of the ring has. Two important types of rings include polynomials and fields, which are themselves closely related and we will lay the foundations here and will be extensively studied and field and Galois theory.

Famous mathematicians who contributed to this area in mathematics include Joseph Louis Lagrange, Niels Henrik Abel and Évariste Galois and, Emmy Noether, Augustin Louis Cauchy, Arthur Cayley many more.

References
- Abstract Algebra by David S. Dummit and Richard M. Foote

Contents

1   Introduction to Groups

We begin our venture to abstract algebra with group theory. Group theorists are interested in a particular algebraic structure called a group. While they are not the simplest algebraic structure (semi groups are arguably simpler in definition), they serve as the foundation of most other algebraic structures. For example, rings, fields, vector spaces and modules can all be thought of as a group with additional structure. While semi groups and monoids are groups losing some of its constraints.

1.1   Basic Concepts of Groups

We begin not by the definition of a group, but by that of a binary operation. It will serve as a central notion differentiating an ordinary set and a group.

> **Definition 1.1.1** (Binary Operation)   A binary operation $*$ on a set G is a function
> $$* : G \times G \to G$$

Notice that the definition of a binary operation depends on both the underlying set and the definition on how the operation works on each element. To define a binary operation, one must show how any two elements of a set are combined. The new element must more over lie within the set.

> **Definition 1.1.2** (Groups)   A group is an ordered pair $(G, *)$ where G is a set and $* : G \times G \to G$ is a binary operation on G satisfying the following axioms.
> - Associativity: $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$
> - Identity element: There exists an element $e \in G$, called an identity of G, such that for all $a \in G$ we have $a * e = e * a = a$
> - Inverse element: For each $a \in G$ there is an element a^{-1} of G, called an inverse of a, such that $a * a^{-1} = a^{-1} * a = e$.

We say that the above 3 defining properties the group axioms. It does feel out of place to call them axioms because they are not universal truths. To check that a set emits a group structure, we must also check that the operation defined on the set is a binary operation. This means that we actually have four axioms to check, with the fourth one being called the closure property, closure meaning that the operation on two elements lands in the same set.

We often call the binary operation the group operation of $(G, *)$ to distinguish other algebraic structures on $(G, *)$ if it exists. Later on we often shorthand the notion of $(G, *)$ to just G, either when notation is clear or implicit.

> **Definition 1.1.3** (Abelian Groups)   A group $(G, *)$ is abelian if $a * b = b * a$ for all $a, b \in G$. More generally, two elements g, h in a general group $(H, *)$ is said to commute if $g * h = h * g$.

Simply put, it is a group where its elements are commutative with each other. Most groups that one naturally think of maybe abelian, due to the readers previously being accustomed to it. However groups that are non-abelian are also central in the study of algebraic structures. Some important examples of non-abelian groups would be the dihedral group and the symmetric group.

> **Lemma 1.1.4**   Let $(G, *)$ be a group. Then the following are true regarding the identity and inverses within G.
> - The identity of G is unique
> - For each $a \in G$, a^{-1} is unique
> - $(a^{-1})^{-1} = a$ for all $a \in G$
> - $(a * b)^{-1} = (b^{-1}) * (a^{-1})$
>
> **Proof**   Let G be a group.
>
> - Let e, f be identities of G. Let $a \in G$. Since e is the identity, $ef = e$. Since f is the identity, $ef = f$. Thus $e = ef = f$.

- Suppose that $b, c \in G$ are inverses of a. Since groups are associative, $(ba)c = b(ac)$. From the left, $(ba)c = ec = c$. From the right, $b(ac) = be = b$. Thus $b = (ba)c = b(ac) = c$.

- Suppose that $a^{-1} = b$. Since the inverse of a is b, we have $ab = e$. But since $ab = e$, the inverse of b is a.

- Suppose that the inverse of a is c and the inverse of b is d. Then $(ab)(dc) = a(bd)c = ac = e$. Thus the inverse of ab is $dc = b^{-1}a^{-1}$.

■

Do be aware that since in general a group is not abelian, the inverse law above is rather important as taking the inverse also inverse the order of multiplication. It may be best to say here that we typically denote the identity as 1. In the theory of abelian groups, the group operation will usually be denoted additively with $+$ so that the identity 0 would make sense. However for non-abelian groups, 1 being the identity is more common, together with the symbol of multiplication like $\cdot$ or $\times$. In these notes we will not distinguish between the two notions and we will predominantly use 1 as the identity. Most of the time the identity should be understood through context, at least for the first few chapters on groups.

It is also customary to write 1_G for the identity element of G and 1_H for the identity element of H and etc when we would like to distinguish between the identity of different groups.

> **Definition 1.1.5** (Order of an Element)   For a group G and an element $x \in G$ define the order of x to be the smallest integer n such that $x^n = 1$, and denote this integer by
> $$|x| = \min\{n \in \mathbb{N} \mid x^n = 1\}$$
> If no positive power of x is the identity, the order of x is defined to be infinity and x is said to be of infinite order.

Aside from the order of an element, we also have the order of the entire group, which is an easier definition.

> **Definition 1.1.6** (Order of a Group)   Let G be a group. The order of G is the number of elements that G has, denoted by $|G|$. We say that G is a finite group if $|G|$ is a finite number. Otherwise G is an infinite group.

Both finite groups and infinite groups form an important class of groups, both of which studied extensively in different areas of abstract algebra.

Be wary that a group does not necessarily have to contain an element of the same order of the group. However it is true that for any element $g \in G$ in a group, $|g| \leq |G|$. It is an easy consequence of Lagrange's theorem which we will see later.

> **Lemma 1.1.7**   Let G be a group. Let $k \in \mathbb{N}$. Then $a^k = 1$ if and only if $|a|$ divides k.
>
> **Proof**   If $k = n|a|$ for some $n \in \mathbb{N}$ then we have
> $$a^k = a^{|a|n} = (a^{|a|})^n = 1$$
> Conversely if $a^k = 1$, then since $|a|$ is by definition the smallest number such that the $a^{|a|} = 1$, we can apply division algorithm to obtain $k = |a|q + r$ for some $q \in \mathbb{N}$ and $0 \leq r < n$. Now $a^k = a^{|a|q+r}$ implies that $1 = a^r$, which contradicts the minimality of $|a|$. Thus we conclude. ■

The following theorem gives a formula for calculating the order of the power of a given element. It is exceptionally useful given that we know of the element's order.

Lemma 1.1.8 Let G be a group and $g \in G$ an element of finite order n. Then

$$\left| g^k \right| = \frac{n}{\gcd(k, n)} = \frac{\text{lcm}(k, n)}{k}$$

for any $k \in \mathbb{N}$

Proof The equality between the two expressions is trivial since $\gcd(m, n) \times \text{lcm}(m, n) = m \times n$. Now let $b = \frac{n}{\gcd(k,n)}$ and $c = \frac{k}{\gcd(k,n)}$. Then we must have $\gcd(b, c) = 1$. Now

$$\begin{aligned}
(g^k)^b &= g^{kb} \\
&= g^{\gcd(k,n)cb} \\
&= g^{nc} \\
&= (g^n)^c \\
&= 1
\end{aligned}$$

Thus we must have $\left| g^k \right|$ divides $\frac{n}{\gcd(k,n)}$. Now we know that $g^{k\left| g^k \right|} = (g^k)^{\left| g^k \right|} = 1$. Thus we must have n divides $k\left| g^k \right|$, meaning $\gcd(k, n)b$ divides $\gcd(k, n)c\left| g^k \right|$ and b divides $c\left| g^k \right|$. We know that $\gcd(b, c) = 1$ thus b divides $\left| g^k \right|$. From the fact that $b = \frac{n}{\gcd(k,n)}$ we have $\left| g^k \right|$ divides b as well and thus $b = \left| g^k \right|$ and

$$\left| g^k \right| = \frac{n}{\gcd(k, n)}$$

∎

In general finding the order of the product of elements is a hard problem. In the case that two elements commute, the order of their product is somehow determined by their individual orders, which makes it easier to deduce.

Lemma 1.1.9 Let G be a group. Let $a, b \in G$ be elements that commute with each other. Then $|ab|$ divides $\text{lcm}(|a|, |b|)$.

Proof Let $l = \text{lcm}(|a|, |b|)$. Since a and b commutes, we have that

$$(ab)^l = a^l b^l = 1$$

and so $|ab|$ divides l.

∎

We will see in the section of cyclic groups that we can impose a stronger condition so that the above result is an equality.

1.2 Subgroups

The idea of a subgroup is that some (not all) elements in a group can also form a group in and of itself. Most of the structure of a group carries on to its subgroup, while the converse may not necessarily be true.

Definition 1.2.1 (Subgroups) If $(G, *)$ is a group and H is a subset of G such that $(H, *)$ is a group $(H, *)$. Then H is called a subgroup of G and is denoted $H \leq G$.

Subgroups are still part of the larger group. This means that if H is a subgroup of G, then certain properties of H are inherited from G. For example, the uniqueness of the identity element ensures that H and G share the same identity element.

Lemma 1.2.2 Let G be a group and $H \leq G$. Then $1_H = 1_G$.

Proof If $1_H \neq 1_G$ then there will be two identities in H.

∎

To check that a subset of a group is a subgroup, it is not necessary to go through the four axioms of a group as it is rather tedious. Instead, we may turn to an easier criterion which involves less work.

> **Theorem 1.2.3** (Criterion for a Subgroup)   Let $(G, *)$ be a group. A subset H of G is a subgroup if and only if the following are true.
> - If $a, b \in H$ then $a * b \in H$
> - If $a \in H$ then $a^{-1} \in H$

Proof   We first prove the forward implication. Suppose that H is a subgroup. Then by definition of a group the above are all true.
Suppose that H is satisfies the above two conditions. We show that it implies the four definitions of a group. Since $a, b \in H$ implies $ab \in H$, closure is satisfied. Since $H \subseteq G$, and G is associative, H is also associative. If $a \in H$ then $a^{-1} \in H$ thus inverse exists. Finally since H is closed, $aa^{-1} = 1 \in H$ thus identity is in H. Thus H is a group. ∎

We thern have subgroups that exists within every group. They are called trivial since we usually do not want to deal with them.

> **Lemma 1.2.4** (Trivial Subgroups)   Let G be a group. Then G and $\{1\}$ are subgroups of G.

Proof   Both can easily be seen to satisfy the subgroup criterion. ∎

The final proposition gives a new way of generating a subgroup given two subgroups. In particular, their overlapping part is also a subgroup in itself.

> **Proposition 1.2.5**   Let G be a group and H, K subgroups of G. Then $H \cap K$ is a subgroup of G.

Proof   Suppose that H, K are subgroups of G. We show that $H \cap K$ with the subgroup criterion. We have that

- $1 \in H$ and $1 \in K$ thus $1 \in H \cap K$

- Suppose that $a, b \in H \cap K$. Then since $ab \in H$ and $ab \in K$ we have $ab \in H \cap K$

- Suppose that $a \in H \cap K$ since H and K are subgroups respectively, $a^{-1} \in H$ and $a^{-1} \in K$ thus $a^{-1} \in H \cap K$.

The subgroup criterion is satisfied thus $H \cap K$ is a subgroup of G. ∎

1.3   Generators of a Group

Cyclic groups appear in a lot of diverse areas of mathematics such as topology and number theory. It structure is simple enough to be employed in different areas while the notions it encapsulates is broad.

> **Definition 1.3.1** (Cyclic Subgroups)   Let G be a group. Define
>
> $$\langle g \rangle = \{ g^k | k \in \mathbb{Z} \}$$
>
> to be the cyclic subgroup generated by g. In this case, g is the generator of $\langle g \rangle$.
> A group G is called cyclic if there exists some $g \in G$ such that $G = \langle g \rangle$.

Cyclic subgroups arise in the simplest context in any group. The following proposition demonstrates that every group contains a cyclic subgroup.

> **Proposition 1.3.2**   Let G be a group and $g \in G$. Then $\langle g \rangle$ is a subgroup of G.

Proof   We prove that it satifies the subgroup criterion.
- $g^0 = 1$ thus $1 \in \langle g \rangle$

- g^{-1} is in $\langle G \rangle$ is trivial
- Let $a, b \in \langle g \rangle$. Then $a = g^n$ and $b = g^m$ for some $n, m \in \mathbb{Z}$ thus $ab = g^{n+m} \in \langle g \rangle$.

The subgroup criterion is satisfied thus we are done. ∎

In particular, the cyclic subgroup of a group G can be constructed simply by taking any one element in G and consider all the powers (positive and negative) of the element.

it is easy to see that cyclic groups commute through their power.

Lemma 1.3.3   Cyclic groups are abelian.

Proof   Let $\langle g \rangle$ be a cyclic group. Then for any $g^m, g^n \in \langle g \rangle$, we have that

$$g^m \cdot g^n = g^{m+n} = g^{n+m} = g^n \cdot g^m$$

and so we conclude. ∎

The following result would seem quite trivial at first sight. It makes sense to think that a subgroup of a cyclic group would be cyclic. The proof however does not look trivial at all. It is one of the first proofs that uses some notion in number theory, showing some linkage between the two subjects.

Proposition 1.3.4   Let $G = \langle g \rangle$ be a cyclic group. Then any subgroup H of G is also cyclic.

Proof   Let $H \leq G = \langle g \rangle$. Every element in H is of the form g^n for some $n \in \mathbb{Z}$. Take the smallest positive k such that $g^k \in H$. Consider another element $g^n \in H$. By the division algorithm, $n = qk + r$ for some $r \in \{0, \ldots, k-1\}$. Thus we have

$$g^n = g^{kq+r} \iff g^r = (g^k)^{-q}(g^n)$$

Now since $g^k \in H$, $(g^k)^{-1} \in H$ and $(g^k)^q \in H$ thus $(g^k)^q \in H$ and $(g^k)^q(g^n) \in H$ by inverse and closure of a group. Thus $g^r \in H$. However this is a contradiction since k is the least power of g such that $g^k \in H$ but g^r with $r < k$ is now in H. Thus we must have $r = 0$ and $g^n = (g^k)^q$. This applies for every $g^n \in H$ thus $H = \langle g^k \rangle$. ∎

One can also show that in the case of a cyclic group, the order of the group is equal to the order of the generator. However the converse is not always true. That is, the order of the group and the order of one particular element being the same does not imply that the group is cyclic.

Proposition 1.3.5   Suppose that $G = \langle g \rangle$. Then $|G| = |g|$.

Proof   Suppose that $|g| = n$ Note that $g^{n+k} = g^k$ for any $k \in \{0, \ldots, n-1\}$. Thus $\{g^n | n \in \mathbb{Z}\}$ has n distinct elements. Thus $|G| = n$.
If $|g| = \infty$ then $g^n \neq 1$ for all n not equal to 0. Thus $\{g^n | n \in \mathbb{Z}\}$ are all distinct and $|G| = \infty$. ∎

Using cyclic subgroups, we can impose a stronger condition so that the order of the product of two elements can be given an explicit formula.

Proposition 1.3.6   Let G be a group and $a, b \in G$ such that a, b commutes. If furthermore $\langle a \rangle \cap \langle b \rangle = \{1\}$, then
$$|ab| = \mathrm{lcm}(|a|, |b|)$$

Proof   Let $n = |ab|$. Since a and b commute, we have that

$$1 = (ab)^n = a^n b^n$$

so that $a^n = b^{-n}$. Thus $a^n \in \langle b \rangle$. But $a^n \in \langle a \rangle \cap \langle b \rangle = \{1\}$ implies that $a^n = 1$. Similarly, we have that $b^n = 1$. This means that we have $|a|, |b|$ divides n. and thus $\mathrm{lcm}(|a|, |b|)$. We know from

groups and rings that $|ab|$ divides $\text{lcm}(|a|, |b|)$ and so we conclude. ■

1.4   Homomorphisms and Isomorphisms

Homomorphisms and isomorphisms are important concepts not only in terms of the ability to classify groups with similar structure, but is also useful in the creation of new groups, such as subgroups and quotient groups. One common idea throughout all of mathematics is to not only study the object itself, but to also study functions in and out of the object. In the case of groups, a meaningful function would be one that preserve the study of a group. This leads to the definition of a group homomorphism.

Definition 1.4.1 (Group Homomorphisms)   Let $(G, *)$ and $(H, \circ)$ be groups. A map $\phi : G \to H$ such that
$$\phi(x * y) = \phi(x) \circ \phi(y)$$
for all $x, y \in G$ is called a homomorphism.

As a result of preserving group structures, group homomorphisms are way more rigid compared to a regular function. In particular, all of the following are true regarding an arbitrary group homomorphism.

Proposition 1.4.2   Let $\phi : G_1 \to G_2$ be a group homomorphism. Then the following are true regarding ϕ.
- $\phi(1) = 1$
- $\phi(g^{-1}) = \phi(g)^{-1}$ for all $g \in G_1$
- $\phi(g^n) = \phi(g)^n$ for all $n \in \mathbb{N}$ and all $g \in G_1$

Proof   Let $\phi : G \to H$ be a homomorphism.

- We have that
$$\phi(1) = \phi(1 \cdot 1)$$
$$\phi(1) = \phi(1) \cdot \phi(1)$$
$$\phi(1)\phi(1)^{-1} = \phi(1)\phi(1)\phi(1)^{-1}$$
$$1 = \phi(1)$$

- We have that
$$\phi(g)\phi(g^{-1}) = \phi(gg^{-1}) = \phi(1) = 1$$
and
$$\phi(g)\phi(g)^{-1} = 1$$
Also since the inverse is unique, we have that $\phi(g^{-1}) = \phi(g)^{-1}$

- We have that $\phi(g) \cdots \phi(g) = \phi(g \cdots g)$ by applying the definition of homomorphism $n - 1$ times

And so we conclude. ■

Structures that can be seen carrying over would be power, inverses, subgroups and identities. But these are only some of the capabilities of a homomorphism.

Definition 1.4.3 (Kernel)   Let $\phi : G \to H$ be a homomorphism. Define the kernel of ϕ to be
$$\ker(\phi) = \{g \in G \,|\, \ker(g) = 1_H\}$$

This notion is exactly parallel to that of linear algebra. They are both the kernel in the sense that they are the element that maps to the identity. In fact, as readers will see in module theory, the entire theory of linear algebra is simply a special case of module theory.

Proposition 1.4.4   Let $\phi : G \to H$ be a homomorphism. Then $\ker(\phi)$ is a subgroup of G.

Proof   We prove closure, identity and inverse as stated by the subgroup criterion.

- $\phi(1_G) = 1_H$, thus we have $1_G \in \ker(\phi)$
- If $a, b \in \ker(\phi)$, then $\phi(a) = 1$ and $\phi(b) = 1$ and

$$\phi(ab) = \phi(a)\phi(b) = 1$$

  thus $ab \in \ker(\phi)$.

- If $a \in \ker(\phi)$ then
$$1 = \phi(1) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1}) = \phi(a^{-1})$$

  By the subgroup criterion $\ker(\phi) \leq G$.

∎

When a map of sets have an inverse, we say that the two sets are bijective. When a group homomorphisms has an inverse, we have the corresponding notion called isomorphic.

Definition 1.4.5 (Group Isomorphisms)   Let G, H be groups. A map $\phi : G \to H$ is said to be an isomorphism if ϕ is a bijective homomorphism. In this case we say that $G \cong H$ and that G and H are isomorphic groups.

Isomorphisms are stricter in the sense that the structure between the two groups it reflects has a higher compatibility than that of homomorphism.

Proposition 1.4.6 (Properties of Isomorphism)   Let G, H be groups. If a map $\phi : G \to H$ is isomorphic, then
- ϕ^{-1} is an isomorphism
- $|G| = |H|$
- $\ker(\phi) = \{1\}$
- G is abelian if and only if H is abelian
- G is cyclic if and only if H is cyclic
- $|x| = |\phi(x)|$
- G has a subgroup of order k if and only if H has a subgroup of order k.

Proof   Suppose that ϕ is a bijection of G and H.

- Since ϕ is bijective, ϕ^{-1} is also bijective thus it is well defined. But we also need to prove that ϕ^{-1} is a homomorphism. Let $h_1, h_2 \in H$. Then there exists unique $g_1, g_2 \in G$ such that $\phi(g_1) = h_1$ and $\phi(g_2) = h_2$. Then

$$\phi^{-1}(h_1 h_2) = \phi^{-1}(\phi(g_1)\phi(g_2)) = \phi^{-1}(\phi(g_1 g_2)) = g_1 g_2 = \phi^{-1}(h_1)\phi^{-1}(h_2)$$

  thus we are done.

- Since ϕ is bijective, $|G| = |H|$

- Since ϕ is bijective and $1 \in \ker(\phi)$, we must have $\ker(\phi) = \{1\}$

- Suppose that G is abelian. $\phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a)$. Thus H is abelian. Since ϕ is bijective it has a bijective inverse. Thus the backwards implication is proved.

- Suppose that $x \in G$ has order n. $1_H = \phi(1_G) = \phi(x^n) = \phi(x)^n$

- If $|x| = n$ then $\phi(x)^n = \phi(x^n) = \phi(1) = 1$ thus we know that $|\phi(x)|\big| n$. However for any $k < n$, $\phi(x)^k = \phi(x^k) \neq 1$ since ϕ is an isomorphism and $\ker(\phi) = \{1\}$. Thus we must have $|\phi(x)^n| = 1$.

- Suppose that G has a subgroup of order k, then $\phi(G)$ is a subgroup as well and every element

preserves its order, we have that $\phi(G) \leq H$ is order k. For the reverse statement, just take ϕ^{-1} to be the isomorphism.

And so we conclude. ∎

Isomorphisms capture more sturcture than homomorphism such as orders, commutativity, subgroups of particular orders and whether the group is cyclic. Most of the classification results require groups to be identified up to isomorphism.

To provide more examples of group, we can construct the automorphism group from a group.

Definition 1.4.7 (The Automorphism Group)   Let G be a group. An automorphism of G is a group homomorphism $\phi : G \to G$. Define the automorphism group G to be

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

Lemma 1.4.8   Let G be a group. Then the automorphism group $\operatorname{Aut}(G)$ is indeed a group.

Proof   Composing bijective maps also gives bijective maps and so composition is a binary operation. This operation is associative since composition of functions is associative. The identity map id_G of G is the identity of the automorphism group since for any automorphism $\phi : G \to G$, we have that

$$\phi \circ \operatorname{id}_G = \phi = \operatorname{id}_G \circ \phi$$

Finally, each automorphism is a bijection and so is invertible. The inverse of an automorphism is again an automorphism and so we conclude. ∎

We will see it reappear later on when inner automorphisms is defined. For now, treat it as another example for you to work on as a group.

1.5   The Cyclic Groups

The collection of all cyclic groups is one of the many classes of groups that serves as the equivalent of primes in the collection of all groups. These groups are called finite simple groups.

Definition 1.5.1 (The Cyclic Group C_n)   Let $n \in \mathbb{N}$. The cyclic group of order n is defined to be the group
$$C_n = \{1, g, g^2, \ldots, g^{n-1}\} = \langle g \rangle$$
where multiplication is defined by $g^m \cdot g^k = g^{m+k}$. It may also be denoted as Z_n

This class of groups form an infinite family since two cyclic groups are isomorphic if and only if they have the same order. However, there may be more than 1 generators for the group, all of which are demonstrated in the following theorem.

Theorem 1.5.2   Let $n \in \mathbb{N}$ and $0 \leq k \leq n - 1$ be an integer. Then g^k is a generator of C_n if and only if $\gcd(k, n) = 1$.

Proof   Suppose that g^k is a generator of C_n. Then $g = g^{ak}$ for some $a \in \mathbb{Z}$. Since $g^n = 1$, there exists $b \in \mathbb{Z}$ such that $g^{ak-bn} = g$ and $0 \leq ak - bn \leq n - 1$. Then $ak - bn = 1$ has a solution if and only if $\gcd(k, n) = 1$ thus we are done.
Now suppose that $\gcd(k, n) = 1$. Then $\left|g^k\right| = \frac{n}{\gcd(k,n)=n}$ thus we are done. ∎

2 Cosets and Quotient Groups

2.1 Cosets

Definition 2.1.1 (Cosets) Let H be a subgroup of G. Let $g \in G$.
- $gH = \{gh | h \in H\}$ the left cosets of H generated by H
- $Hg = \{hg | h \in H\}$ the right cosets of H generated by H

Proposition 2.1.2 Let H be a subgroup of G and let $g_1, g_2 \in G$. Then the following are equivalent.
- $g_1 H = g_2 H$
- $g_2 \in g_1 H$
- $g_1^{-1} g_2 \in H$

Proof Let $H \leq G$.

- (1) $\implies$ (2) Suppose that $g_1 H = g_2 H$. Let $g_1 h \in g_1 H$. Then there exists k such that $g_1 h = g_2 k$. Then $g_2 = g_1 h k^{-1}$ and since H is a subgroup, $h k^{-1} \in H$ and thus $g_2 \in g_1 H$

- (1) $\implies$ (3) Similar to the above argument but we rewrite the expression as $g_1^{-1} g_2 = h k^{-1}$ thus $g_1^{-1} g_2 \in H$

- (3) $\implies$ (1) Let $g_2 h \in g_2 H$. By (3) there exists $k \in H$ such that $g_1^{-1} g_2 = k$. We then have

$$g_1^{-1} g_2 = k$$
$$g_1^{-1} g_2 h = kh$$
$$g_2 h = g_1 kh$$
$$g_2 h \in g_1 H$$

Since $kh \in H$. Thus $g_2 H \subseteq g_1 H$. Mirror the argument for $g_2^{-1} g_1 \in H$ and we have that $g_1 H \subseteq g_2 H$ and we are done

∎

Proposition 2.1.3 Let H be a subgroup of G. Let $g_1, g_2 \in G$. Then $g_1 H = g_2 H$ if and only if $Hg_1 = Hg_2$.

Proof Let $g_1 H = g_2 H$. Let $hg_1 \in Hg_1$. Since we know that $g_1 g_2^{-1} \in H$, then $hg_1 g_2^{-1} \in H$. Let $hg_1 g_2^{-1} = k \in H$. Then $hg_1 = kg_2 \in Hg_2$ thus we have that $Hg_1 \subseteq Hg_2$. The argument is similar for $Hg_2 \subseteq Hg_1$ thus we have that $Hg_1 = Hg_2$. For the reverse, the argument is also similar. ∎

Proposition 2.1.4 Let H be a subgroup of G. Then the left (right) cosets of G partition G.

Proof We first show that if $g_1 H \neq g_2 H$, then $g_1 H \cap g_2 H = \emptyset$. Suppose that $k \in g_1 H \cap g_2 H$, then by the above we have $g_1 H = kH = g_2 H$ thus a contradiction. Thus we must have $g_1 H \cap g_2 H = \emptyset$. Now we must have that

$$\bigcup_{g \in G} gH = G$$

since every gH must at least have $g \in gH$. Thus we are done. ∎

Proposition 2.1.5 Let H be a subgroup of G. Then the number of distinct left cosets is equal to the number of distinct right cosets.

Proof Since all the distinct left cosets partition G and $g_1 H = g_2 H$ if and only if $Hg_1 = Hg_2$, we must have the same number of distinct right cosets as well in order to partition G. ∎

Proposition 2.1.6   Let H be a subgroup of a finite group G. Then for any $g \in G$, $|gH| = |H|$.

Proof   Let $g \in G$. We prove that the map $\phi : H \to gH$ defined by $\phi(h) = gh$ is a bijection. For injectivity, $gh_1 = gh_2$ implies $h_1 = h_2$ by applying g^{-1} on both sides. Let $k \in gH$, then there exists $h \in H$ such that $k = gh \in gH$. This proves surjectivity and we are done.   ∎

Definition 2.1.7 (Number of Distinct Cosets)   Let H be a subgroup of G. Define $[G : H]$ to be the number of distinct left cosets of H in G.

The set of all left (right) cosets is also important for the construction of quotient groups as well as one of the major players in group actions.

Definition 2.1.8 (Set of Cosets)   Let G be a group and H a subgroup. Define

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

the set of cosets of H in G.

2.2   Lagrange's Theorem

Lagrange's theorem is a powerful theorem that has many applications. Some indirect results include the class equation and orbit stabilizer theorem as we will later see.

Theorem 2.2.1 (Lagrange's Theorem)   Let G be a finite group and H a subgroup of G. Then

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

Proof   We know that distinct left cosets partition G and every left coset has $|H|$ elements thus $|G| = [G : H]|H|$.   ∎

An immediate result is that orders of subgroups must divide the order of the group. Notice that this does not imply the converse: given any number n that divides the order of G, it does not necessarily mean that there exists a subgroup of G with order n. As always, it is good to think of counterexamples. A prototypical one would be A_4 (see chapter 5 for definition) that does not have subgroups of order 6. This is the smallest example.

Another immediate result of Lagrange's theorem is the following.

Corollary 2.2.2   Let G be a finite group and $g \in G$. Then the order of g divides the order of G.

Proof   For every $g \in G$, $\langle g \rangle \leq G$ thus by Lagrange's Theorem $|g| = |\langle g \rangle| \, \big| \, |G|$ ∎

Corollary 2.2.3   Let G be a group of prime order p. Then G is cyclic.

Proof   For any $1 \neq g \in G$, $\langle g \rangle$ is a subgroup of G. By Lagrange's theorem, it must divide the order of G, which is p. Since p is a prime, we must have $\langle g \rangle = G$.   ∎

2.3   Normal Subgroups

Given we have defined the set of cosets $\frac{G}{H}$ for a group G and a subgroup H, it is normal to ask in what situations will $\frac{G}{H}$ be a group in its own right. The answer to this is completely characterized by the notion of normal subgroups.

> **Definition 2.3.1** (Normal Subgroups)   Let N be a subgroup of G. N is called a normal subgroup of G if $gN = Ng$ for all $g \in G$. We write $N \trianglelefteq G$ in this case.

> **Definition 2.3.2** (Conjugates)   Let H be a subgroup of G. The set
> $$gHg^{-1} = \{ghg^{-1} | h \in H\}$$
> is called the conjugate of H.

It does not need deep results to see that conjugations and normal subgroups are related notions.

> **Theorem 2.3.3** (Normality Test)   Let N be a subgroup of G. The following are equivalent.
> - N is normal in G
> - $gNg^{-1} \subseteq N$ for all $g \in G$
> - $gNg^{-1} = N$ for all $g \in G$

Proof   Let $N \trianglelefteq G$.

- (1) $\implies$ (2) Let N be normal. Let $gng^{-1} \in gNg^{-1}$. Since N is normal there exists $k \in N$ such that $gn = kg$. Then $gng^{-1} = kgg^{-1} = k \in N$.

- (2) $\implies$ (1) Let $gNg^{-1} \subseteq N$. Then for all $n \in N$ there exists $k \in N$ such that $gng^{-1} = k$. Then $gn = kg$ for all n thus $gN = Ng$ and we are done.

- (2) $\implies$ (3) We only need to show that $N \subseteq gNg^{-1}$. Let $n \in N$. Then $ng \in Ng$. Since N is normal, there exists $k \in N$ such that $gk = ng$ and $k = g^{-1}ng$. But then $n = gkg^{-1}$ thus $n \in gNg$ and we are done.

- (3) $\implies$ (2) is trivial.

■

While the second item above is simply for ease of proving things, the important thing to take away here is that as long as conjugating results in the same group, that group would be normal.

> **Theorem 2.3.4**   Let H be a subgroup of a group G. Write $g_1 H \cdot g_2 H = \{ab | a \in g_1 H, b \in g_2 H\}$. Then
> $$g_1 H \cdot g_2 H = (g_1 g_2)H$$
> for all $g_1, g_2 \in G$ if and only if $H \trianglelefteq G$.

Proof   Suppose first that $g_1 H \cdot g_2 H = (g_1 g_2)H$. Let $g \in G$. We want to show that $gHg^{-1} \subseteq H$. Notice that $gH \cdot g^{-1}H = H$. For any $h \in H$, we have $gh \in gH$ and $g^{-1} \in g^{-1}H$ so that $ghg^{-1} \in G$.

Now suppose that N is normal. Let $g_1 h_1 \in g_1 H$ and $g_2 h_2 \in g_2 H$. Then we have

$$g_1 h_1 g_2 h_2 = g_1 g_2 h_3 h_2 \in (g_1 g_2)H$$

since N is normal and $h_1 g_2 = g_2 h_3$. Thus $g_1 H \cdot g_2 H \subseteq (g_1 g_2)H$. Now suppose that $g_1 g_2 h \in (g_1 g_2)H$. Then in particular this element lies in $g_1 H \cdot g_2 H$ because $g_1 g_2 h = g_1 \cdot 1 \cdot g_2 \cdot h$. And so we conclude. ■

This theorem shows that if N is a normal subgroup, then the above operation is a binary operation on G/N. The rest of the conditions to check that G/N forms a group is fairly straight forward.

> **Proposition 2.3.5**   Let G be a group and N a normal subgroup of G. Then G/N together with the binary operation $\cdot : G/N \times G/N \to G/N$ defined by
> $$(gN) \cdot (hN) = (gh)N$$

is a group.

Proof We check the group axioms:

- Associativity: Let gN, hN and kN be in G/N. Then by two applications of the above theorem, we have that $((gN) \cdot (hN)) \cdot (kN) = (ghN) \cdot (kN) = (gh)kN$ By associativity of G, we conclude.

- Identity: Let $gN \in G/N$. Then it is clear that $(gN) \cdot (N) = (g \cdot 1)N = gN$ so that N is the identity in G/N.

- Inverse: Let $gN \in G/N$. Then we can see that $(gN) \cdot (g^{-1}N) = (gg^{-1})N = N$ so that each element in G/N has an inverse.

All the group axioms are satisfied and so we conclude. $\blacksquare$

Definition 2.3.6 (Quotient Group) Let G be a group and N a normal subgroup of G. Define the quotient group of G with N to be the group G/N.

Normal subgroups are also closely related to kernels. This is because for any group G and normal subgroup N, there is a canonical projection map $p : G \to G/N$.

Proposition 2.3.7 A subgroup N of the group G is normal if and only if it is the kernel of some homomorphism.

Proof Suppose that N is a normal subgroup of G. Then consider the homomorphism $\phi : G \to G/N$ defined by $\phi(g) = gN$. Then

$$\begin{aligned}
\ker(\phi) &= \{g \in G | \phi(g) = N\} \\
&= \{g \in G | gN = N\} \\
&= \{g \in G | g \in N\} \\
&= N
\end{aligned}$$

Thus we are done.

Let N be the kernel of the homomorphism $\phi : G \to H$. Then $\ker(\phi) = \{g \in G | \phi(g) = 1\} = N$. By the normality test, showing that $gng^{-1} \in N$ is sufficient for $n \in N$ and $g \in G$. We have that

$$\phi(gng^{-1}) = \phi(g)\phi(n)\phi(g^{-1}) = \phi(g)\phi(g)^{-1} = 1$$

thus $gng^{-1} \in \ker(\phi) = N$ thus we are done. $\blacksquare$

Undoubtedly aside from the construction of the quotient group, the above proposition is the main result of this section. It is equivalent to say that a normal subgroup is exactly the kernel of some homomorphism.

2.4 Normalizers

Sometimes, not every element in a group allows a subgroup H to normalize. Therefore can obtain a subset of G that contains all the elements that allows H to be normal.

Definition 2.4.1 (Normalizers) Let G be a group. Let $S \subseteq G$. Then the normalizer is defined to be

$$N_G(S) = \{g \in G \mid gS = Sg\} = \{g \in G \mid gSg^{-1} = S\}$$

Proposition 2.4.2 Let G be a group and $S \subseteq G$. Then $S \subseteq N_G(S) \le G$.

Proof   Let $g, h \in N_G(S)$. Then $h^{-1} \in N_G(S)$ since $h^{-1}S = Sh^{-1}$ if and only if $hS = Sh$ thus $h^{-1} \in N_G(S)$. Now we want $gh^{-1} \in N_G(S)$. We have

$$gh^{-1}S = g(Sh^{-1}) = (gS)h^{-1} = Sgh^{-1}$$

and so we have that $N_G(S) \leq G$. For the remaining part, if $s \in S$, then $sS = S = Ss$ and so $S \subseteq N_G(S)$. ∎

Proposition 2.4.3   Let G be a group and H a subgroup of G. Then we have $H \trianglelefteq N_G(H)$.

Proof   We know that $H \subseteq N_G(H)$. Since H and $N_G(H)$ are both subgroups of G, we must have $H \leq N_G(H)$. By definition of $N_G(H)$, if $g \in N_G(H)$ then $gHg^{-1} = H$ and so we conclude. ∎

Proposition 2.4.4   Let G be a group and $N \subseteq G$. Then $N \trianglelefteq G$ if and only if $N_G(N) = G$.

Proof   Let $N \trianglelefteq G$. Trivially we already have $N_G(N) \leq G$. Let $g \in G$. Then since N is normal, we have $gN = Ng$ thus $g \in N_G(N)$ and we are done.
Let $N_G(N) = G$. Then for all $g \in G$, $gN = Ng$ thus N is normal. ∎

As motivated from above, $N_G(S)$ is just all the elements in G so that S is allowed to be normal. Then obviously if $N_G(S)$ is the entirety of G then S would be allowed to be normal.

2.5   The Isomorphism Theorems for Groups

Theorem 2.5.1 (The First Isomorphism Theorem)   Let $\phi : G \to H$ be a homomorphism. Then the following are true regarding the kernel and the image of the homomorphism.
- $\ker(\phi) \trianglelefteq G$
- $\operatorname{im}(\phi) \leq H$

Moreover we have that
$$\frac{G}{\ker(\phi)} \cong \phi(G)$$

Proof   Proposition 2.3.7 shows that $\ker(\phi)$ is a normal subgroup of G.

Let $\phi(g), \phi(h) \in \operatorname{im}(\phi)$. Then $\phi(g) \cdot \phi(h) = \phi(gh) \in \operatorname{im}(\phi)$ so that closure is satisfied. Now clearly $\phi(g)^{-1} \in \operatorname{im}(\phi)$ since $\phi(g^{-1}) = \phi(g)$ and so we conclude.

We construct an isomorphism f between cosets of G of $\ker(phi)$ and elements of $\phi(G)$. Write N for $\ker(\phi)$ Let $gN \in G/\ker(\phi)$. Define f by $f(gN) = \phi(g)$. I claim that this is the isomorphism we need.
We first show that this map is well defined. The point here is to show that any representative is fine. In particular, if $gH = hN$ are two representations of $thesamecoset$ and g, h is distinct, then we want $f(gN) = f(hN)$. Well $gN = hN$ if and only if $gh^{-1} \in N$. This means that $gh^{-1} \in \ker(\phi)$ and $\phi(gh)^{-1} = 1$. This means that $\phi(g)\phi(h)^{-1} = 1$ and $\phi(g) = \phi(h)$. This means that the map is well defined.
We now show that it is a homomorphism. Let gN and hN be cosets. Then

$$f((gN)(hN)) = f((gh)N) = \phi(gh) = \phi(g)\phi(h) = f(gN)f(hN)$$

thus we are done. Finally we show that it is an isomorphism. Firstly let $f(gN) = f(hN)$. Then

$$f(gN) = f(hN)$$
$$\phi(g) = \phi(h)$$
$$\phi(g)\phi(h)^{-1} = 1$$
$$\phi(gh^{-1}) = 1$$

This means that $gh^{-1} \in \ker(\phi)$ thus $gN = hN$. Now let $\phi(g) \in \phi(G)$. Then quite obviously $f(gN) = \phi(g)$ thus it is surjective and bijective and we are done. ∎

The first isomorphism theorem is one of the first substantial and fundamental result in group theory. The theorem itself may not seem surprising, but it has a wide application across different areas of Mathematics that make use of group theory. In particular, the following two isomorphism theorems are in part due to the first isomorphism theorem.

Theorem 2.5.2 (The Second Isomorphism Theorem)   Let G be a group, let $A \leq G$ and $B \trianglelefteq G$. Then the following are true.
- AB is a subgroup of G
- $B \trianglelefteq AB$ and $A \cap B \trianglelefteq A$

Moreover, we have that
$$\frac{A}{A \cap B} \cong \frac{AB}{B}$$

Proof   We first prove that AB is a subgroup of G. By theorem 3.2.1, AB is a subgroup if and only if $AB = BA$. We have that
$$AB = \bigcup_{a \in A} aB = \bigcup_{a \in A} Ba = BA$$

and thus $AB \leq G$.

To show that $B \trianglelefteq AB$, we show that $abb'(ab)^{-1} \in B$ for any $b' \in B$ and $ab \in AB$. But this is trivial since $ab \in G$ and we know that since $B \trianglelefteq G$, $abb'(ab)^{-1} \in B$ thus we are done.

For $A \cap B \trianglelefteq A$, we want $kak^{-1} \in A$ for $k \in A \cap B$ and $a \in A$. But since $k \in A \cap B$ implies $k \in A$ and A is a subgroup, $kak^{-1} \in A$ thus we are done.

Define $\phi : A \rightarrow \frac{AB}{B}$ by $\phi(a) = aB$. Then ϕ is a homomorphism. Indeed $\phi(a_1 a_2) = a_1 a_2 B$ and $\phi(a_1)\phi(a_2) = a_1 B \cdot a_2 B = a_1 a_2 B$. Also, we have that $a \in \ker(\phi)$ if and only if $a \in B$. This shows that $\ker(\phi) = A \cap B$. Finally, given $aB \in \frac{AB}{B}$, it is clear that $\phi(a) = aB$ such that ϕ is surjective. By the first isomorphism theorem, we have that
$$\frac{A}{A \cap B} = \frac{A}{\ker(\phi)} \cong \phi(A) = \frac{AB}{B}$$

and so we conclude. ∎

Theorem 2.5.3 (The Third Isomorphism Theorem)   Let G be a group and H, K normal subgroups of G with H a subgroup of K. Then $K/H \trianglelefteq G/H$ and
$$\frac{G/H}{K/H} \cong \frac{G}{K}$$

Proof   Let $kH \in K/H$. Let $gH \in G/H$ I want to show that $(gH)(kH)(gH)^{-1} \in \frac{K}{H}$. But
$$(gH)(kH)(gH)^{-1} = gkg^{-1}H = k'H \in \frac{K}{H}$$

for some $k' = gkg^{-1}$. This is true since K/H is normal.

Define $\phi : \frac{G}{H} \rightarrow \frac{G}{K}$ by $\phi(gH) = gK$. This is a group homomorphism since
$$\phi(g_1 g_2 H) = g_1 g_2 K = g_1 K \cdot g_2 K = \phi(g_1 H)\phi(g_2 H)$$

Moreover, notice that $gH \in \ker(\phi)$ if and only if $g \in K$. This means that $gH \in \ker(\phi)$ if and only if $gH \in K/H$. Thus $\ker(\phi) = K/H$. Finally, given $gK \in G/K$, it is clear that $\phi(gH) = gK$ so that

ϕ is surjective. By the first isomorphism theorem, we have that

$$\frac{G/H}{K/H} = \frac{G/H}{\ker(\phi)} \cong \phi(G/H) = \frac{G}{K}$$

and so we conclude.   ■

3 Permutation and Symmetries

Évariste Galois first defined a group to something similar to symmetric groups. Indeed they encompass a high amount of symmetrical information, which is the at the heart of group theory. They arise in most situations and surprisin GLy, we will see that every group embeds into a symmetric group of some order, finite or infinite (we will not see infinite symmetric groups here, but the result is still true) as an immediate application of the notion of group actions.

3.1 The Symmetric Groups

We begin with the definition of a symmetric group. Notice that we will only define the finite case here, but there is also a version in which the symmetric group is infinite.

> **Definition 3.1.1** (The Symmetric Group) Let X be a finite set. Denote
>
> $$\text{Sym}(X) = \{f : X \to X \mid f \text{ is bijective}\}$$
>
> the set of all bijections from X to itself. The symmetric group of X is defined to be X together with the usual composition of functions. Elements of $\text{Sym}(X)$ are called permutations.

Note that the symmetric group is indeed a group by the following reasons.

- The composition of functions are associative.
- The identity element: id_X which is the identity function on X has the property that $f \circ \text{id}_X = \text{id}_X = \text{id}_X \circ f$ for any $f \in \text{Sym}(X)$.
- For each $f \in \text{Sym}(X)$, f is bijective and so it has an inverse $f^{-1} : X \to X$ which is also bijective and thus lies in $\text{Sym}(X)$.

We can represent each element in the symmetric group in the following way.

> **Definition 3.1.2** (Matrix Notation) Let X be a finite set. Each $f : X \to X$ in $\text{Sym}(X)$ is represented by a $2 \times |X|$ matrix as follows: Label the elements of X as $1, \ldots, n$ for $n = |X|$. Then we write $f : X \to X$ as
>
> $$\begin{pmatrix} 1 & 2 & \cdots & n \\ \phi(1) & \phi(2) & \cdots & \phi(n) \end{pmatrix}$$

It is easy to see that the order of the symmetric group is just how many rearrangements of the elements of X.

> **Lemma 3.1.3** Let X be a finite set with $|X| = n$. Then the order of $\text{Sym}(X)$ is $n!$.
>
> **Proof** Using the matrix form, we see that $\phi(1), \ldots \phi(n)$ is a permutation of $1, \ldots, n$. In particular, if $\phi(1)$ has n possibilities, then $\phi(2)$ has $n-1$ options etc. Then there will be $n!$ different permutations. ∎

> **Proposition 3.1.4** Let X be a finite set of cardinality n. Then $\text{Sym}(X)$ is non-abelian if and only if $n \geq 3$.
>
> **Proof** Suppose that $n \geq 3$. By fixing $n-3$ elements to map to themselves in $\text{Sym}(X)$, we see that $S_3 \leq S_n$. It remains to show that S_3 is non-abelian. Write $X = \{1, 2, 3\}$. Let $f : X \to X$ be defined by $f(1) = 2$, $f(2) = 1$ and $f(3) = 3$. Let $g : X \to X$ be defined by $g(1) = 3$, $g(2) = 2$ and $g(3) = 1$. Then it is clear that $f(g(3)) = f(1) = 2$ and $g(f(3)) = g(3) = 1$ so that f and g does not commute.
>
> For $n = 1$ and 2, it is clear by inspection that S_1 and S_2 must be abelian. ∎

> **Proposition 3.1.5** Let X and Y be finite sets. If $|X| = |Y|$ then $\text{Sym}(X) \cong \text{Sym}(Y)$.

Since $\text{Sym}(X)$ is invariant under the number of elements of X, we denote S_n once and for all for $\text{Sym}(\{1, \ldots, n\})$.

3.2 Cycle Notation

Notice that matrix presentation is unique since each element $f \in \text{Sym}(X)$ is uniquely defined by where it sends each element to. While this presentation makes it clear the images of each element in X, it is often rather cumbersome to write. Therefore we have an alternate and more compact notation.

> **Definition 3.2.1** (Cycle Notation) Let X be a finite set. Let $a_1, \ldots, a_r \in X$ be distinct. Then denote $\begin{pmatrix} a_1 & \ldots & a_r \end{pmatrix}$ the permutation in $\text{Sym}(X)$ where
> - $f(a_i) = a_{i+1}$ for $\leq i \leq r$
> - $f(a_r) = a_1$
> - $f(b) = b$ for $b \notin \{a_1, \ldots, a_r\}$
>
> If $f \in \text{Sym}(X)$ is equal to $\begin{pmatrix} a_1 & \ldots & a_r \end{pmatrix}$ for some distinct elements in $a_1, \ldots, a_r$ then we say that f is a cycle in $\text{Sym}(X)$.

We also have the notion of disjoint cycles.

> **Definition 3.2.2** (Disjoint Cycles) Let X be a finite set. Two cycles $\begin{pmatrix} a_1 & \ldots & a_r \end{pmatrix}$ and $\begin{pmatrix} b_1 & \ldots & b_s \end{pmatrix}$ in $\text{Sym}(X)$ are said to be disjoint if $\{a_1, \ldots, a_r\} \cap \{b_1, \ldots, b_s\} = \emptyset$.

Since a cycle fixes any element not within the cycle, disjoint cycles should commutes.

> **Proposition 3.2.3** Let X be a finite set. Then disjoint cycles in $\text{Sym}(X)$ commute.
>
> **Proof** Suppose that $f = (a_1, \ldots, a_r)$ and $g = (b_1, \ldots, b_s)$ are disjoint cycles in $\text{Sym}(X)$. Let $x \in X$. If $x \in \{b_1, \ldots, b_s\}$, then $g(x) \in \{b_1, \ldots, b_s\}$ so that $g(x) \notin \{a_1, \ldots, a_r\}$ and $f(g(x)) = g(x)$. On the other hand, we have $f(x) = x$ which implies $g(f(x)) = g(x)$.
>
> If $x \notin \{b_1, \ldots, b_s\}$, then the same argument gives $f(g(x)) = f(x) = g(f(x))$ and so we conclude. ∎

Compared to matrix presentations, the cycle notation is far from being unique. In particular, we can represent the same element in $\text{Sym}(X)$ by either swapping the order of the individual cycles or by changing the starting element of each cycle by another element in the same cycle. We prove that the cycle notation is unique up the following sense.

> **Theorem 3.2.4** Let X be a finite set. Then every element in $\text{Sym}(X)$ can be written as a product of disjoint cycles. Moreover, this product is unique in the following sense: If $f \in \text{Sym}(X)$ has the form $f = f_1 \cdots f_p = g_1 \cdots g_q$ where each f_i are disjoint cycles of length > 1 from each other for $1 \leq i \leq p$ and similarly for g_i, then $p = q$ and $\{f_1, \ldots, f_p\} = \{g_1, \ldots, g_q\}$.
>
> **Proof** If id_X is the identity element then we can write it as $()$ the empty cycle. Now assume that $\text{id}_X \neq f \in \text{Sym}(X)$. Let $Y = \{x \in X \mid f(x) \neq x\}$. Let $a_1 \in Y$. Since $\text{Sym}(X)$ has finite order, f has finite order, say n. Let
> $$m_1 = \min\{m \in \mathbb{N} \mid (f^m)(a_1) = a_1\}$$
> Then for $2 \leq i \leq m_1$, define $a_i = f(a_{i-1})$. If $Y = \{a_1, \ldots, a_{m_1}\}$ then f is now a cycle and we are done. So suppose that $Y \setminus \{a_1, \ldots, a_{m_1}\}$ is non-empty with the element $a_{m_1+1} \in Y \setminus \{a_1, \ldots, a_{m_1}\}$. Set
> $$m_2 = \{m \in \mathbb{N} \mid (f^m)(a_{m_1+1}) = a_{m_1+1}\}$$
> Then for $m_1 + 2 \leq i \leq m_2$, define $a_i \in X$ by $a_i = f(a_{i-1})$. Since f is injective, the sets $\{a_1, \ldots, a_{m_1}\}$ and $\{a_{m_1+1}, \ldots, a_{m_2}\}$ have empty intersection. If $Y = \{a_1, \ldots, a_{m_2}\}$ then f is a product of two

disjoint cycles and we are done.

If not, this process can be repeated. It also terminates in finite steps since $\text{Sym}(X)$ is finite. When it terminates, we will have obtained a product of disjoint cycles representing f. Uniqueness follows because if $f = f_1 \cdots f_m$ we have seen by construction that each f_i completely determines f. ∎

Cycle notations make multplication of elements in S_n easier. Suppose that we want to find the following product

$$\tau \cdot \psi = \begin{pmatrix} 2 & 4 & 7 & 8 \end{pmatrix} \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 5 & 6 \end{pmatrix} \cdot \begin{pmatrix} 1 & 3 & 7 \end{pmatrix} \begin{pmatrix} 2 & 5 & 6 & 9 \end{pmatrix} \begin{pmatrix} 4 & 10 \end{pmatrix}$$

We start with any element, say 1. Then observe that ψ maps 1 to 3. We then see that 3 maps to 1 in τ so 1 maps to itself and we can omit the trivial cycles. Now for 2, we see that 2 maps to 5 in ψ and 5 maps to 6 in τ. So we can write down $\begin{pmatrix} 2 & 6 & \cdots \end{pmatrix}$. Now instead of choosing another element to begin. We follow up on 6 to see that 6 maps to 9. This means we can continue to chain and write $\begin{pmatrix} 2 & 6 & 9 & \cdots \end{pmatrix}$. Once you reach the end, you begin a new cycle with another element not in previous cycles.

3.3   The Permutation Groups

Definition 3.3.1 (Permutation Groups)   Let X be a set. A permutation group is a subgroup of $\text{Sym}(X)$.

In particular, $\text{Sym}(X)$ is also a permutation group.

Definition 3.3.2 (Support)   Let X be a set. Let $g \in \text{Sym}(X)$. Define the support of g to be

$$\text{supp}(g) = \{x \in X | g(x) \neq x\}$$

Let G be a permutation group on X. Define the support of G to be

$$\text{supp}(G) = \{x \in X | g(x) \neq x \text{ for some } g \in G\}$$

Lemma 3.3.3   Let G be a permutation group on a finite set X. Let $g \in G$. Then

$$\text{supp}(\langle g \rangle) = \text{supp}(g)$$

Proof   Let $x \in \text{supp}(g)$. Then $g(x) \neq x$ so that $x \in \text{supp}(\langle g \rangle)$. Now suppose that $x \in \text{supp}(\langle g \rangle)$. Then there exists some $g^n \in \langle g \rangle$ such that $g^n(x) \neq x$. But then $g(x) \neq x$. Otherwise if $g(x) = x$ then $g^n(x) = x$, a contradiction. Thus $x \in \text{supp}(g)$ and so we conclude. ∎

Lemma 3.3.4   Let G be a permutation group on a finite set X and $H \leq G$. Then $\text{supp}(H) \subseteq \text{supp}(G)$.

Proof   Let $x \in \text{supp}(H)$. Then there exists some $h \in H$ such that $h(x) \neq x$. Then in particular $h \in G$ so that $x \in \text{supp}(G)$. ∎

Proposition 3.3.5   Let G, H be permutation groups on a finite set X. If $\text{supp}(G) \cap \text{supp}(H) = \emptyset$ then $G \cap H = \{1\}$.

Proof   We show the contrapositive. Suppose that $G \cap H$ has a non-trivial element, say g. Then since $\langle g \rangle \leq G, H$, we have that $\text{supp}(\langle g \rangle) \subseteq \text{supp}(G), \text{supp}(H)$ so that

$$\text{supp}(g) = \text{supp}(\langle g \rangle) \subseteq \text{supp}(G) \cap \text{supp}(H)$$

But $\text{supp}(g)$ cannot be empty because if it is, then g fixes all $x \in X$ so that g is the identity, a contradiction. Thus $\text{supp}(G) \cap \text{supp}(H)$ is non-empty. ∎

3.4   Cycle Types

Definition 3.4.1 (Cycle Types)   Let $\phi \in S_n$. We say that ϕ has cycle type $2^{r_2}3^{r_3}\cdots$ if it has exactly r_k k cycles for $k \geq 2$.
A transposition is a cycle of type 2.

Notice that the following proposition means that we will have a third notation for elements of S_n.

Proposition 3.4.2   Let τ be a cycle of type k in S_n. Then the following are true.
- τ has order k
- τ can be decomposed into a product of $k-1$ transpositions

Proof

- Let τ be a cycle of order k. Notice that multiplying n times of the same element means that we are taking the ith element in τ to the $i+n$ modulo k element in the cycle. If $n = k$ then every element goes to itself, which means that τ^k is just the permutation that maps every element to iself, which is the identity of the permutation group.

- For a cycle $(x_1, \ldots, x_k)$. Notice that the product

$$\begin{pmatrix} x_{k-1} & x_k \end{pmatrix} \cdots \begin{pmatrix} x_2 & x_3 \end{pmatrix} \begin{pmatrix} x_1 & x_2 \end{pmatrix}$$

  returns the original cycle.

Thus we are done.   ∎

Proposition 3.4.3   Let X be a finite set. Let $f \in \text{Sym}(X)$ be such that $f = f_1 \cdots f_k$ is a product of k-cycles. Then
$$|f| = \text{lcm}(|f_1|, \ldots, |f_k|)$$

Proof   We proceed by induction. We have done the case $n = 1$ above. Now suppose that for all $1 \geq m < k$, we have $|f_1 \cdots f_m| = \text{lcm}(n_1, \ldots, n_m)$. Let $g = f_1 \cdots f_{k-1}$. Write $f_i = \begin{pmatrix} a_{i,1} & \cdots & a_{i,t_i} \end{pmatrix}$. Then
$$\text{supp}(g) = \{a_{i,j} \mid 1 \, leqi < k, 1 \leq j \leq t_i\}$$
and $\text{supp}(f_k) = \{a_{k,1}, \ldots, a_{k,t}\}$ so that by lemma 3.4.4, we have $\langle g \rangle \cap \langle f_k \rangle = \{1\}$. By proposition 1.3.6 and since disjoint cycles commute, we have that

$$|f| = \text{lcm}(|g|, |f_k|) = \text{lcm}(|f_1|, \ldots, |f_k|)$$

and so we conclude.   ∎

Proposition 3.4.4   Let $f, g \in S_n$ be permutations such that $f = (a_1, \ldots, a_r)$, then

$$gfg^{-1} = \begin{pmatrix} g(a_1) & \cdots & g(a_r) \end{pmatrix}$$

Proof   For $1 \leq i \leq r$, let $b_i = g(a_i)$. For $1 \leq i \leq r-1$, we have that

$$\begin{aligned}(gfg^{-1})(b_i) &= g(f(a_i)) \\ &= g(a_{i+1}) \\ &= b_{i+1}\end{aligned}$$

Similarly, we have that $(gfg^{-1})(b_r) = a_1$. For $b \in X \setminus \{b_1, \ldots, b_r\}$, suppose that $c \in X$ is such that $g(c) = b$. Then we have that $(gfg^{-1})(b) = g(f(c)) = g(c) = b$ and so we conclude.   ∎

Proposition 3.4.5   Two permutations in S_n are conjugate if and only if they have the same cycle types.

> **Proof**   If f and g are conjugate in S_n, then by the above theorem they have the same cycle type.
>
> $\blacksquare$

3.5   The Alternating Groups

Based on the number of transpositions an element can be decomposed to, we classify them into odd and even permutations. This motivates the definition of the alternating group.

> **Definition 3.5.1** (Odd/Even Permutations)   A permutation $\phi \in S_n$ is said to be even if it has an even number of transpositions, and odd if it has an odd number of transpositions.

> **Definition 3.5.2** (The Alternating Group A_n)   Let $n \in \mathbb{N}$. The alternating group A_n is defined to be
> $$A_n = \{\phi \in S_n | \phi \text{ is even}\}$$

> **Theorem 3.5.3**   The alternating group is the kernel of the homomorphism $f : S_n \to \{-1, 1\}$. $\{-1, 1\}$ is defined by ordinary multiplication and f is given by
> $$f(\phi) = \begin{cases} 1 & \text{if } \phi \text{ is even} \\ -1 & \text{if } \phi \text{ is odd} \end{cases}$$

> **Lemma 3.5.4**   Let $n \in \mathbb{N}$. Then
> $$\frac{S_n}{\{-1, 1\}} \cong A_n$$
> and thus $|A_n| = \frac{n!}{2}$.

4   Group Actions

Group actions are in a sense more fundamental then the notion of groups. One of the pioneers of group theory, Galois first used techniques in group actions to manipulate roots of a polynomial by permutations. Galois eventually gave an argument without the use of group theory or field theory why the roots of some quintic polynomials can not be expressed in radicals or the standard operations on $\mathbb{R}$.

4.1   Group Actions

Within group theory, there are also interesting applications of group actions by considering groups acting on particular sets such as the set of conjugacy classes and the set of cosets.

> **Definition 4.1.1** (Groups Actions)   Let G be a group and X a set. An action of G on X is a map $\cdot : G \times X \to X$ such that the following properties are satisfied.
> - Associativity: $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$
> - Identity: $1 \cdot x = x$

Depending on how one looks at action of the group on the set (element wise, or group wise), we obtain two viewpoints of the same idea.

> **Proposition 4.1.2**   Let G be a group acting on a set X. Let $\phi : G \to \mathrm{Sym}(X)$ be defined by $\phi(g)(x) = g \cdot x$. We have that
> - For each $g \in G$, $\phi(g) : X \to X$ is a permutation of X
> - The mapping $\phi : G \to \mathrm{Sym}(X)$ is a homomorphism
>
> **Proof**
>
> - To show that $\phi(g)$ is a permutation, we simply need to show that it is a bijection on itself. $\phi(g)$ is a bijection if and only if it has an inverse. For all $x \in X$, we have that
>
> $$(\phi(g^{-1}) \circ \phi(g))(x) = \phi(g^{-1})(\phi(g)(x))$$
> $$= \phi(g^{-1} g)(x)$$
> $$= \phi(1)(x)$$
> $$= x$$
>
> Thus we have that $\phi(g^{-1}) = \phi(g)^{-1}$.
> - We have that
>
> $$\phi(g_1 g_2)(x) = (g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x) = \phi(g_1)(g_2 \cdot x) = (\phi(g_1) \circ \phi(g_2))(x)$$
>
> so that $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$
>
> And so we conclude.   ■

In particular, the theorem also shows that G is isomorphic to a subgroup of $\mathrm{Sym}(X)$ provided that ϕ is injective. This is the content of Cayley's theorem.

> **Theorem 4.1.3** (Cayley's Theorem)   Every group G is isomorphic to a subgroup of $\mathrm{Sym}(G)$.
>
> **Proof**   Consider the map $\phi_g : G \to G$ defined by $\phi_g(x) = gx$ for any $g \in G$. $\phi_{g^{-1}}$ is an inverse of ϕ_g and thus ϕ_g is bijective and thus $\phi_g \in \mathrm{Sym}(G)$ by definition.
> Consider the function $T : G \to \mathrm{Sym}(G)$ defined by $T(g) = \phi_g$. We have that
>
> $$(\phi_g \circ \phi_h)(x) = \phi_g(\phi_h(x))$$
> $$= \phi_g(hx)$$
> $$= ghx$$
> $$= \phi_{gh}(x)$$

and thus T is a homomorphism.

Now we show that T is injective. Suppose that $T(g) = \mathrm{id}_G$. This means that $gx = x$ for all $x \in G$. But by definition of a group this means that $g = 1$ and thus $\ker(T) = 1$. Thus G is isomorphic to the image of T, which is a subgroup of $\mathrm{Sym}(G)$. $\blacksquare$

Using the fact that ϕ gives a homomorphism from G to the symmetric group $\mathrm{Sym}(X)$ of the acting set X, we can define the kernel of a group action, which are precisely elements of g that fix the set X.

> **Definition 4.1.4** (Kernel)   Let G be a group acting on X. Define the kernel of the action to be the kernel of $\phi : G \to \mathrm{Sym}(X)$, which is
>
> $$\ker(G, X, \cdot) = \{g \in G \mid g \cdot x = x \text{ for all } x \in X\}$$
>
> An action is faithful if $\ker(G, X, \cdot) = \{1\}$

This idea of a kernel is also employed in the proof of Cayley's theorem above. We can also improve on the result of Cayley's theorem using the kernel of an action. Moreover, notice that the kernel of a group action is a normal subgroup of G just because the definition of it is just a special case of the kernel of a general group homomorphism.

> **Proposition 4.1.5**   Let X be a finite set of cardinality n and let G be a group acting on X. If G acts on X faithfully then G is isomorphic to a subgroup of S_n.
>
> **Proof**   Write $\phi : G \to \mathrm{Sym}(X)$ to be the isomorphism given in theorem 4.1.2. By the first isomorphism theorem, we have that
>
> $$G \cong \frac{G}{\ker(G, X, \cdot)} \cong \mathrm{im}(\phi) \leq \mathrm{Sym}(X)$$
>
> where the last inequality follows because $\mathrm{im}(\phi)$ is a permutation group on X. $\blacksquare$

This is a stronger result then Cayley's theorem because for example, the group G could act on a set X with strictly lower cardinality than G so that the above proposition gives a stronger result.

4.2   Orbits and Stabilizers

Orbits and stabilizers form the core of group actions. Lagrange's theorem applies to orbits and stabilizers to mimic a very similar result to Lagrange's theorem itself. Similar to how Lagrange's theorem is fundamental in group theory, the orbit-stabilizer theorem is fundamental in the theory of group actions.

> **Definition 4.2.1** (Orbits)   Let G be a group acting on the nonempty set X. Define the orbit of G containing x to be the set
> $$\mathrm{Orb}_G(x) = \{g \cdot x \mid g \in G\}$$
> for any $x \in X$.

Different $x \in X$ could give the same orbit. Indeed if $g \cdot x = y$ then $g^{-1} \cdot y = x$. In fact, this gives an equivalence relation on X defining the orbits of G on X. For $x, y \in X$, suppose that $x \sim y$ if there exists $g \in G$ such that $g \cdot x = y$. It is easy to check that $\sim$ defines an equivalence relation on X and its equivalence classes are in fact the orbits.

> **Definition 4.2.2** (Stabilizer)   Let G be a group that acts on X. Let $x \in X$. Define the stabilizer of x to be
> $$\mathrm{Stab}_G(x) = \{g \in G \mid g \cdot x = x\}$$

The stabilizer cam be seem as a generalization of normalizers. Indeed one can consider the group action of G on the set $\{xHx^{-1} \mid x \in G\}$ for H a subgroup of G. This action is given by $g \cdot xHx^{-1} = gxHx^{-1}g^{-1}$.

Then notice that the set of all $g \in G$ that stabilizes H is precisely

$$N_G(H) = \text{Stab}_G(H)$$

We will also see important types of stabilizers when considering particular applications of group actions to some sets.

Proposition 4.2.3 Let G be a group acting on X. Then the following are true.
  • $\text{Stab}_G(x) \leq G$
  • $\bigcap_{x \in X} \text{Stab}_G(x) = \ker(G, X, \cdot)$

Proof Suppose that $\cdot : G \times X \to X$ is a group action.

  • Let $g, h \in \text{Stab}_x$. Then $h^{-1} \in \text{Stab}_G(x)$ since $h^{-1} \cdot x = h^{-1} \cdot (h \cdot x) = (h^{-1}h) \cdot x = x$. Then

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

Thus $gh^{-1} \in \text{Stab}_x$ and the subgroup criterion is satisfied.

  • We show inclusion of the sets. Let $g \in \bigcap_{x \in X} \text{Stab}_G(x)$. Then for any $x \in X$, $g \cdot x = x$ and thus $g \in \ker(G, X)$. Let $g \in \ker(G, X)$, then for any $x \in X$, $g \cdot x = x$ which means that $g \in \text{Stab}_G(x)$ for all $x \in X$. Thus $g \in \bigcap_{x \in X} \text{Stab}_G(x)$.

This gives the desired result. ■

Now come the major result of the theory of group actions. As mentioned before it stands in a similar stance as Lagrange's theorem in the theory of group actions. Most other major results such as the class equation and Cauchy's theorem also stems on the orbit-stabilizer theorem.

Theorem 4.2.4 (Orbit Stabilizer Theorem) Let G be a finite group acting on X. If $x \in X$, then

$$|\text{Orb}_G(x)| = [G : \text{Stab}_G(x)] \quad \text{and} \quad |G| = |\text{Orb}_G(x)||\text{Stab}_G(x)|$$

Proof The goal is to define a bijection between cosets of $\text{Stab}_G(x)$ and elements in $\text{Orb}_G(x)$. Define $f : \text{Orb}_G(x) \to G/G_x$ by $f(g) = g\text{Stab}_G(x)$. This map is clearly well defined.
Injectivity:
Let $g\text{Stab}_G(x) = h\text{Stab}_G(x)$. Then $g^{-1}h \in \text{Stab}_G(x)$ which means that $(g^{-1}h) \cdot x = x$. Then applying the action of g on both sides, we have

$$h \cdot x = g \cdot x$$

which proves that $g = h$.
Surjectivity:
For any $g\text{Stab}_G(x)$, just choose $g \in G$. Then clearly $f(g) = g\text{Stab}_G(x)$.
Thus $|\text{Orb}_G(x)| = [G : \text{Stab}_G(x)]$. ■

The following corollary is an important consequence of the Orbit Stabilizer theorem.

Corollary 4.2.5 Let G be a finite group acting on a set X. Then the following are true regarding the orbits of the action.
  • Either $\text{Orb}_G(x) = \text{Orb}_G(y)$ or $\text{Orb}_G(x) \cap \text{Orb}_G(y) = \emptyset$
  • The set of all orbits form a partition of X

Proof Define a relation where for $x, y \in X$, we say that $x \sim y$ if and only if $g \cdot x = y$ for some $g \in G$. It is clear that this is an equivalence relation and thus the corollary follows. ■

4.3   The Action of Conjugation

Conjugation marks one of the most important group actions that one should consider, with the other two being rather trivial: the action of left multiplication and the action of G on the set of cosets of H in G. In particular, Cauchy's theorem is a major application of such a group action.

> **Definition 4.3.1** (Conjugation)   Let G be a group. Define conjugation to be an action of G on G where $\cdot : G \times G \to G$ is defined by $g \cdot x = gxg^{-1}$. Define the conjugacy classes of a group to be the orbits of conjugation:
> $$\mathrm{Cl}(x) = \{gxg^{-1} \mid g \in G\} = \mathrm{Orb}_G(x)$$
> Two elements are said to be conjugate to each other if they lie in the same conjugacy classes.

It is easy to see that the action of conjugation is indeed a group action. Aside from the conjugacy classes of a group, we also have the notion of centralizers.

> **Definition 4.3.2** (Centralizer and Center)   Let G be a group. Define the centralizer of a group to be the stabilizer of conjugation:
> $$C_G(x) = \{g \in G \mid gx = xg\} = \mathrm{Stab}_G(x)$$
> Define the center of a group to be the kernel of conjugation:
> $$Z(G) = \{g \in G \mid gxg^{-1} = x \text{ for all } x \in X\} = \ker(G, G, \cdot)$$

Since $Z(G)$ consists of all elements of G that commute with other elements, $Z(G) = G$ naturally implies that G is abelian.

Note that conjugacy classes and centralizers and centers can be defined independent of the notion of group action. Indeed they can be defined by the set of conditions. However, by defining these notions through the use of group actions show that group actions are indeed a rather general theory and applies to all kinds of subgroups one can imagine.

> **Lemma 4.3.3**   Let G be a group. Then $Z(G) \trianglelefteq G$ and $C_G(x) \leq G$.
>
> **Proof** $Z(G)$ is the kernel by definition and so it is a normal subgroup of G. $C_G(x)$ is a special case of the stabilizer and so it is a subgroup of G. ∎

The following proposition is a non-trivial result of what one can do with the center of a group.

> **Proposition 4.3.4**   Let G be a group. If $\frac{G}{Z(G)}$ is cyclic, then G is abelian.
>
> **Proof**   Suppose that $\langle xZ(G) \rangle = G/Z(G)$. Let $g \in G$. Then $gZ(G) = x^a Z(G)$ for some $a \in \mathbb{N}$. This means that $x^{-a}g \in Z(G)$. This means that there is some $z \in Z(G)$ such that $x^{-a}g = z$ which implies that $g = x^a z$. Now suppose that we go through the same process with $h \in G$ to obtain $h = x^b z'$. Then we have
> $$\begin{aligned} gh &= x^a z x^b z' \\ &= x^{a+b} z z' &(z \in Z(G)) \\ &= x^{b+a} z' z \\ &= x^b z' x^a z \\ &= hg \end{aligned}$$
> Thus we are done. ∎

Proposition 4.3.5   Let p be a prime and let $n \in \mathbb{N}$. Let G be a finite group with $|G| = p^n$. Then $|Z(G)| > 1$.

Proof   Consider the action of G on itself by conjugation. Then corollary 4.2.5 shows that the order of $\mathrm{Cl}(x)$ is a power of p. A rewrite of definition shows that $Z(G) = \{x \in G | \, |\mathrm{Cl}(x)| = 1\}$. Suppose that $|Z(G)| = 1$. Then corollary 4.2.5 again implies that $p^n = |G| = 1 + p^{a_1} + \cdots + p^{a_m}$ since all the conjugacy classes partition G. However this is a contradiction since the left hand side is divisible by p while the right hand side is not. ∎

Corollary 4.3.6   Let p be a prime and $n \in \mathbb{N}$. Let G be a finite group with $|G| = p^n$. Then the following are true.
- If $n = 2$, then $|G|$ is abelian.
- If $n = 3$, then either G is abelian or $|Z(G)| = p$

Proof   Suppose that $|G| = p^2$. By Lagrange's theorem, $|Z(G)|$ is either p or p^2. If $|Z(G)| = p$, then $\frac{G}{Z(G)}$ has order p a prime. This means that $\frac{G}{Z(G)}$ is cyclic. By proposition 4.3.4, G is abelian. If $|Z(G)| = p^2$, then $|Z(G)| = G$ thus G is again abelian.

Now suppose that $|G| = p^3$. By Lagrange's theorem, $|Z(G)|$ is either p, p^2 or p^3. If it is p^2, then $\frac{G}{Z(G)}$ has order p and thus is cyclic. By proposition 4.3.4, G is abelian. If $|Z(G)| = p^3$, then $|Z(G)| = G$ and thus G is again abelian. Finally, the case $|Z(G)| = p$ is left. ∎

We end the section with two important consequence of the Orbit Stabilizer theorem applied to the action of conjugacy.

Theorem 4.3.7 (Cauchy's Theorem)   Let G be a finite group. Let p be a prime divisor of $|G|$. Then G contains an element of order p. Moreover, the number of elements of order p is congruent to -1 modulo p.

Proof   Define $X = \{(x_1, \ldots, x_p) | x_i \in G \text{ and } x_1 \cdots x_p = 1\}$. Notice that

$$\begin{aligned}
(x_1, \ldots, x_p) \in X &\implies x_1 \cdots x_p = 1 \\
&\implies x_2 \cdots x_p x_1 = 1 \\
&\implies (x_2, \ldots, x_p, x_1) \in X
\end{aligned}$$

Repeatedly applying the above proves that

$$(x_i, \ldots, x_p, x_1, \ldots, x_{i-1}) \in X$$

for all $i \leq p$. Now let $C = \langle (1, \ldots, p) \rangle \leq S_p$ be the subgroup of the symmetric group S_p generated by the p-cycle $(1, \ldots, p)$. Define an action $\cdot : C \times X \to X$ by

$$(\sigma, (x_1, \ldots, x_p)) = (x_{\sigma(1)}, \ldots, x_{\sigma(x_p)})$$

for $\sigma \in C$. This is indeed a group action: Associativity and Identity is easy to check in conjunction with the above fact that $(x_i, \ldots, x_p, x_1, \ldots, x_{i-1}) \in X$ for $(x_1, \ldots, x_p) \in X$.

By corollary 4.2.5, the orbits of this action partition X. There are now three types of orbits.
- Type 1: Orbits of size 1.
  Notice that $f = (1, \ldots, p) \in \mathrm{Stab}_C((1, \ldots, 1))$. Since $C = \langle f \rangle$ has prime order and $\mathrm{Stab}_C(1, \ldots, 1) \leq C$, we conclude that $\mathrm{Stab}_C((1, \ldots, 1)) = C$ which implies that $|\mathrm{Orb}_C((1, \ldots, 1))| = 1$ by the orbit stabilizer theorem. A similar argument shows that the p-tuple $(x, \ldots, x)$ has also orbit size 1.

  In fact, every orbit of size 1 must be one of the above two cases. Suppose that S is an orbit of size 1. Let $(x_1, \ldots, x_p) \in X$. Then the orbit stabilizer theorem implies that

$\text{Stab}_C((x_1, \ldots, x_p)) = C$. Since $f = (1, \ldots, p) \in C$, we have

$$(x_1, \ldots, x_p) = f \cdot (x_1, \ldots, x_p) \qquad (f \in \text{Stab}_C((x_1, \ldots, x_p)))$$
$$= (x_2, \ldots, x_p, x_1)$$

which means that $x_1 = \cdots = x_p$. This means that $x_1^p = 1$. Since p is a prime this means that $|x_1| = 1$ or p. In which either way it falls into one of the two above cases.

- Type 2: Orbits of size p.
  Any orbit of size greater than 1 must have orbit size p. Indeed if $T_1, \ldots, T_n$ are all the distinct orbits of size greater than 1, the fact that $|C| = p$ together with the orbit stabilizer theorem implies that each T_i must have order p.

Now we show that $|X| = |G|^{p-1}$. Define a map $\phi : X \to G^{p-1}$ by $\phi((x_1, \ldots, x_p)) = (x_1, \ldots, x_{p-1})$. Injectivity is clear since x_p is uniquely determined: $x_p = (x_1 \cdots x_{p-1})^{-1}$. Surjectivity is also clear since for $(x_1, \ldots, x_{p-1}) \in G^{p-1}$, we can just choose $x_p = (x_1 \cdots x_{p-1})^{-1}$. Thus $|X| = |G^{p-1}| = |G|^{p-1}$.

Now let $\mathcal{P} = \{x \in G \mid |x| = p\}$. Then since the orbits partition X, we have

$$|G|^{p-1} = |X| = |\text{Orb}_G((x_1, \ldots, x_p))| + \sum_{x \in \mathcal{P}} |\text{Orb}_G((x, \ldots, x))| + \sum_{i=1}^{n} |T_i| = 1 + |\mathcal{P}| + np$$

Since $p \mid\mid G|$, we deduce that $|\mathcal{P}| \equiv -1 \pmod{p}$. In particular, G must contain an element of order p. ∎

Cauchy's theorem is a useful tool on analysing the the elements of a group.

Theorem 4.3.8 (The Class Equation) Let G be a finite group and let $g_1, g_2, \ldots, g_r$ be representatives of the distinct conjugacy classes of G not contained in $Z(G)$. Then

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(g_i)] = |Z(G)| + \sum_{i=1}^{r} |\text{Orb}_G(x_i)|$$

Proof Suppose that G acts on itself by conjugation. We know that the orbits partition the group G since it is a quotient of an equivalence relation. However, for any $g \in Z(G)$, $gxg^{-1} = x$ for any $x \in X$. Thus every element in $Z(G)$ is itself an orbit. Combining these facts, we have that

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)| = |Z(G)| + \sum_{i=1}^{r} |\text{Cl}(g_i)|$$

∎

4.4   Free Actions and Fixed Points

Definition 4.4.1 (Fixed Points) Let G be a group acting on X. Let $g \in G$. We say that $x \in X$ is a fixed point of g if $g \cdot x = x$. The set of all fixed points of $g \in G$ is

$$\text{Fix}_X(g) = \{x \in X \mid g \cdot x = x\}$$

We say that $g \in G$ is fixed point free if $\text{Fix}_X(g) = \emptyset$.

Lemma 4.4.2 (The Not Burnside Lemma)   Let G be a finite group acting on a finite set X. Then

$$|\{\mathrm{Orb}_G(x) \mid x \in X\}| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}_X(g)|$$

Proof   Define the set
$$A = \{(g, x) \in G \times X \mid g \cdot x = x\}$$
It is clear that $|A| = \sum_{g \in G} |\mathrm{Fix}_X(g)| = \sum_{x \in X} |\mathrm{Stab}_G(x)|$. Let $\mathrm{Orb}_G(x_1), \dots, \mathrm{Orb}_G(x_r)$ denote all the distinct orbits in X. We have seen that

$$X = \coprod_{i=1}^{r} \mathrm{Orb}_G(x_i)$$

Also if $x \in \mathrm{Orb}_G(x_i)$, then $\mathrm{Stab}_G(x) = \mathrm{Stab}_G(x_i)$ by the orbit stabilizer theorem. Thus we have

$$\begin{aligned}
\sum_{g \in G} |\mathrm{Fix}_X(g)| &= \sum_{x \in X} |\mathrm{Stab}_G(x)| \\
&= \sum_{x \in X} |\mathrm{Stab}_G(x)| \\
&= \sum_{i=1}^{r} |\mathrm{Stab}_G(x)| \cdot |\mathrm{Orb}_G(x_i)| \\
&= \sum_{i=1}^{r} |G| \\
&= r|G|
\end{aligned}$$

and so we conclude. $\blacksquare$

Corollary 4.4.3   Let G be a finite group acting on a finite set X with $|X| > 1$. Suppose that G has precisely one orbit. Then G contains fixed point free element.

Proof   Suppose for a contradiction that G contains no fixed point free elements. Then $|\mathrm{Fix}_X(g)| \geq 1$ for all $g \in G$. Then since $\mathrm{Fix}_X(1_G) = |X|$, the above lemma implies that

$$|G| = \sum_{g \in G} |\mathrm{Fix}_X(g)| = |X| + \sum_{g \in G \setminus \{1\}} |\mathrm{Fix}_X(g)| \geq |X| + |G| - 1$$

which is a contradiction since $|X| \geq 1$. Thus we conclude. $\blacksquare$

Notice that it is important that G is a finite group in this corollary, otherwise it would not hold.

Definition 4.4.4 (Free Actions)   Let G be a group acting on X. We say that G is a free action on X if $g \in G$ is such that there exists some $x \in X$ such that $g \cdot x = x$, then $g = 1$.

Lemma 4.4.5   Let G be a group acting on X. Then G is a free action on X if and only if $\mathrm{Fix}_X(g) = \emptyset$ for all $g \neq 1$.

Proof   Suppose that G is a free action. Then for all $g \neq 1$, $g \cdot x \neq x$ for all x. Thus $\mathrm{Fix}_X(g) = \emptyset$. Now suppose that the converse is true. Then $g \cdot x \neq x$ for all $x \in X$ and all $g \neq 1$. Thus G is a free action on G. $\blacksquare$

4.5   Transitive Actions

Definition 4.5.1 (Transitive Actions)   Let G be a group acting on a set X. We say that G is a transitive action on X if for all $x, y \in X$, there exists $g \in G$ such that $g \cdot x = y$.

Lemma 4.5.2   Let G be a group acting transitively on a set X. Then $\mathrm{Orb}_G(x) = X$.

Proof   Immediate from definitions.   ■

4.6   Equivariant Functions

Definition 4.6.1 (Equivariant Functions)   Let G be a group and let G act on two sets X and Y. Let $f : X \to Y$ be a function. We say that f is G-equivariant if

$$f(g \cdot x) = g \cdot f(x)$$

for all $x \in X$ and $g \in G$.

5   Products of Groups

Groups are defined as a set with additional constraints. Since sets have the Cartesian product, it is natural to also consider group structures on the Cartesian product. There are, however, three different notions of products of groups.

5.1   External Direct Products

We first have the external product. It is the most direct and natural way to construct multiplication between two groups.

> **Definition 5.1.1** (External Product)   Let $(G, *)$ and $(H, \circ)$ be groups. Define a group operation of G and H called the external (direct) product $G \times H$ with the operation
>
> $$(g_1, h_1) \times (g_2, h_2) = (g_1 * g_2, h_1 \circ h_2)$$
>
> for $g_1, g_2 \in G$ and $h_1, h_2 \in H$.

It is easy to see that the group operation indeed defines a group structure on $G \times H$. Indeed we can check the group operations element wise. Moreover, from set theory we know that the order of $G \times H$ is equal to $|G| \times |H|$. There is nothing mysterious about external direct products.

> **Theorem 5.1.2**   Let $(g, h) \in G \times H$. If g and h has finite order r and s respectivelty, then
>
> $$|(g, h)| = \operatorname{lcm}(r, s)$$
>
> **Proof**   Trivially we have that $|(g, h)| | \operatorname{lcm}(r, s)$. Suppose that $|(g, h)| < \operatorname{lcm}(r, s)$. Then by definition of the lcm, either $r | |(g, h)|$ or $s | |(g, h)|$ but not both. But then maximally we only have one of the elements in (g, h) be the identity. Thus we must have $|(g, h)| = \operatorname{lcm}(r, s)$. ∎

> **Proposition 5.1.3**   Let $G_1, \ldots, G_n$ be groups and G their exrternal product. Then
>
> $$G/G_i \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n$$
>
> **Proof**   Let $g = (g_1, \ldots, g_n) \in G$. Take the function $f(gG_i) = (g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_n)$ to be the isomorphism. Indeed the function is well defined. For any $g \in G$, gG_i is unique up to the ith element. It is a homomorphism since $f((gG_i)(hG_i)) = f(ghG_i)$ is easy to check.
> To show injectivity, let $f(gG_i) = f(hG_i)$. Then
>
> $$f(gG_i) = f(hG_i)$$
> $$(g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_n) = (h_1, \ldots, h_{i-1}, h_{i+1}, \ldots, h_n)$$
>
> Note that the ith element does not matter since two $g_i \in G_i$ gives the same coset. Thus $gG_i = hG_i$ and we are done. Surjectivity is trivial since for any given $(g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_n)$, take $g = (g_1, \ldots, g_{i-1}, 1, g_{i+1}, \ldots, g_n)$ and $f(gG_i) = (g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_n)$ and we are done.
> Thus the two groups are isomorphic. ∎

> **Proposition 5.1.4**   Let $m, n \in \mathbb{N}$. Then
>
> $$C_m \times C_n \cong C_{mn}$$
>
> if and only if $\gcd(m, n) = 1$.
>
> **Proof**   Let $C_m \times C_n \cong C_{mn}$. Let g, h be the generator of C_m, C_n respectively. Then (g, h) is the generator of $C_{m,n}$ since isomorphisms map generators to generators. We have proved that $|\gcd(g, h)| = \operatorname{lcm}(m, n) = \frac{mn}{\gcd(m,n)}$. But $|C_n \times C_m| = mn$ thus $mn = \frac{mn}{\gcd(m,n)}$ and $\gcd(m, n) = 1$.
> Now let $\gcd(m, n) = 1$. Define a function $\phi : C_m \times C_n \to C_{m \times n}$ where $\phi(g^a, h^b) = g^a h^b$. I will

show that it is an isomorphism. Firstly ϕ is a homomorphism since

$$\phi((g^{a_1}, h^{b_1})()) =$$

∎

5.2   Internal Direct Products

While the external product is concerned of the product between two groups, the internal direct product is interested in how two subgroups of a group could be "multiplied" to form the group itself. Essentially, we are trying to decompose a group into its internal direct product.

Definition 5.2.1 (Internal Direct Product)   Let G be a group and $H, K \leq G$. Define

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

If $G = HK \cong H \times K$ we say that HK is the internel direct product of G.

Notice that the set HK is not necessarily a group by its own right. Even if it is, it could happen that HK is a subgroup of G. In particular, we have a necessary and sufficient criterion for HK to be a subgroup of G.

Theorem 5.2.2   Let G be a group. Let $H, K \leq G$. HK is a subgroup if and only if $HK = KH$.

Proof   First suppose that HK is a subgroup. Since $K \subseteq HK$ and $H \subseteq HK$, we have that $KH \subseteq HK$. by closure. To show the reverse. Let $hk \in HK$. Then there exists some $a \in HK$ such that $a^{-1} = hk$ since HK is a group. Then $a \in HK$ implies that $a = h'k'$ for some $h'k' \in HK$. Then

$$hk = a^{-1} = k'^{-1}h'^{-1} \in KH$$

thus we are done.
Now suppose that $HK = KH$. Let $h_1 k_1 \in HK$ and $h_2 k_2 \in HK$. We show that it satisfies the subgroup criterion.

- $1 \in HK$ is trivial

- For closure, Note that $k_1 h_2 = h'k'$ since $KH = HK$. Then

$$h_1 k_1 h_2 k_2 = h_1 h'k'k_2 = HK$$

  The last part is true since H, K are subgroups.

- Let $hk \in HK$. Then $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$

Thus we are done.   ∎

Applying the theory of group actions gives us to important propositions to proceed in finding the criteria for $HK \cong G$.

Proposition 5.2.3   Let G be a finite group. Let H, K be subgroups of G. Then

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

Proof   Consider K acting on G/H be left multiplication defined by $k \cdot gH = (kg)H$. We have that

$$KH = \coprod_{i=1}^{s} k_i H$$

for each $k_i H$ and $k_j H$ disjoint if $i \neq j$. Thus $|KH| = \sum_{i=1}^{s} |k_i H| = \sum_{i=1}^{s} |H| = s|H|$. On the other hand, notice that $gH \in \text{Orb}_K(H)$ if and only if $gH = kH$ for some $k \in K$. Thus

$$\mathrm{Orb}_K(H) = \{kH \mid k \in K\} = \{k_1 H, \dots, k_s H\} \text{ and } |\mathrm{Orb}_K(H)| = s = \frac{|KH|}{|H|}.$$

Now if $k \in K$, then $k \in \mathrm{Stab}_K(H)$ if and only if $kH = H$ which is true if and only if $k \in H$. Thus $\mathrm{Stab}_K(H) = H \cap K$. By the orbit stabilizer theorem, we have that

$$|K| = |\mathrm{Orb}_K(H)| \cdot |\mathrm{Stab}_K(H)|$$

implies that $|K| = \frac{|KH|}{|H|}|H \cap K|$ and so we conclude. ∎

Proposition 5.2.4   Let G be a finite group. Let $H, K \leq G$ be subgroups of G. Then

$$[G : H \cap K] \leq [G : H][G : K]$$

Proof   Let $X_1 = G/H$ and $X_2 = G/K$ be the set of left cosets of H and K respectively. It is clear that G acts on X_1 and X_2 so that G acts on $X_1 \times X_2$. Let $x = (H, K) \in X_1 \times X_2$. For $g \in G$, we have that

$$g \in \mathrm{Stab}_G(x) \iff gH = H \ \text{ and } \ gK = K$$

But this is true if and only if $g \in H$ and $g \in K$. Thus $\mathrm{Stab}_G(x) = H \cap K$. By the orbit stabilizer theorem, we have that

$$[G : H \cap K] = |\mathrm{Orb}_G(x)| \leq |X| = [G : H][G : K]$$

and so we conclude. ∎

Proposition 5.2.5   Let G be a finite group. Let H and K be subgroups of G such that $\gcd([G : H], [G : K]) = 1$. Then $G = HK$.

Proof   Notice that since the gcd is 1, we have that

$$\mathrm{lcm}([G : H], [G : K]) = \frac{|G|^2}{|H||K|}$$

Also we have that $[G : H \cap K] = [G : H][H : H \cap K]$ and $[G : H \cap K] = [G : K][K : H \cap K]$ which means that $[G : H \cap K]$ is a common multiple of $[G : H]$ and $[G : K]$ so that

$$\mathrm{lcm}([G : H], [G : K]) \leq [G : H \cap K]$$

Then we have that

$$\frac{|G|^2}{|H||K|} \leq [G : H \cap K] = \frac{|G|}{|H \cap K|}$$

which shows that

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

We also have trivially that $|HK| \leq |G|$. Thus we conclude. ∎

The following theorem gives a sufficient criterion for HK to be the internal direct product so that the external and internal direct product coincide.

Theorem 5.2.6   Suppose that G is a group with normal subgroups H, K such that $H \cap K = \{1\}$ and $G = HK$, then the following are true.
- All $h \in H$ and all $k \in K$ commute
- $G \cong H \times K$

Proof

- Let $h \in H$ and $k \in K$. Consider the element $g = hkh^{-1}k^{-1}$. Since both H and K are normal,

we have $hkh^{-1}, k \in K$ and $khk^{-1}, h \in H$ so that $g \in H \cap K = \{1\}$. Thus $hkh^{-1}k^{-1} = 1$.

- Define $\varphi : H \times K \to G$ by $\varphi(h, k) = hk$. Then we have

$$
\begin{aligned}
\varphi((h_1, k_1)(h_2, k_2)) &= \varphi(h_1 h_2, k_1 k_2) \\
&= h_1 h_2 k_1 k_2 \\
&= h_1 k_1 h_2 k_2 \\
&= \varphi(h_1, k_1)\varphi(h_2, k_2)
\end{aligned}
$$

so that φ is a homomorphism. Notice that φ is surjective because $G = HK$. Suppose that $\varphi(h, k) = 1$. Then $hk = 1$ implies $h = k^{-1} \in H \cap K = \{1\}$. Thus $h = k = 1$ so that φ is an isomorphism and we conclude.

$\blacksquare$

5.3   Semidirect Product

We would like to generalize the direct product of two finite groups.

Proposition 5.3.1   Let H, K be groups and let ϕ be a homomorphism from K into $\mathrm{Aut}(H)$. Let G be the set of all ordered pairs (h, k) where $h \in H$ and $k \in K$. Then the operation

$$
(h_1, k_1)(h_2, k_2) = (h_1 \cdot \phi_{k_1}(h_2), k_1 k_2)
$$

allows G to be a group.

Proof   Clearly closure is satisfied. We check associativity since it is asymetrical. We have that

$$
\begin{aligned}
((h_1, k_1)(h_2, k_2))(h_3, k_3) &= (h_1 \cdot \phi_{k_1}(h_2), k_1 k_2)\,(h_3, k_3) \\
&= (h_1 \cdot \phi_{k_1}(h_2) \cdot (\phi_{k_1 k_2}(h_3)), k_1 k_2 k_3) \\
&= (h_1 \cdot \phi_{k_1}(h_2) \cdot (\phi_{k_1} \circ \phi_{k_2})(h_3), k_1 k_2 k_3) \\
&= (h_1 \cdot \phi_{k_1}(h_2 \cdot \phi_{k_2}(h_3)), k_1 k_2 k_3) \\
&= (h_1, k_1)(h_2 \cdot \phi_{k_2}(h_3), k_2 k_3) \\
&= (h_1, k_1)((h_2, k_2)(h_3, k_3))
\end{aligned}
$$

The identity in this group will be $(1_H, 1_K)$. Indeed we have that $(h, k)(1_H, 1_K) = (h \cdot \phi_k(1_H), k) = (h, k)$ and $(1_H, 1_K)(h, k) = (\phi_{1_K}(h), k) = (h, k)$. The inverse of (h, k) is $(\phi_{k^{-1}}(h^{-1}), k^{-1})$ $\blacksquare$

Definition 5.3.2 (Semidirect Product)   Let H, K be groups such that there exists a homomorphism $\phi : K \to \mathrm{Aut}(H)$. Define the semidirect product of H and K to be

$$
H \rtimes_\phi K
$$

equipped with the operation above.

Some authors define semidirect products alternatively as $H \ltimes_\psi K$ for $\psi : H \to \mathrm{Aut}(K)$. It is easy to see that the two definitions are equivalent by establishing an isomorphism

$$
H \rtimes_\phi K \cong K \ltimes_\phi H
$$

by swapping the order of the cartesian pair.

Theorem 5.3.3   Let $G = H \rtimes_\phi K$ be a semidirect product. Then $|G| = |H||K|$ and

$$
H \cong \{(h, 1) \mid h \in H\} \le G \quad \text{and} \quad K \cong \{(1, k) \mid k \in K\} \le G
$$

Proof   Clearly $H \cong \{(h,1)|h \in H\}$. Notice that $(h_1,1)(h_2,1) = (h_1 \cdot (\phi(1))(h_2),1) = (h_1 h_2,1)$ since $\phi(1)$ is the identity automorphism. This means that the multiplication structure of H is preserved. Since H itself is a group, this makes the set a subgroup of G.

Similarly, notice that $(1,k_1)(1,k_2) = (\phi(k_1)(1),k_1 k_2) = (1,k_1 k_2)$. The results then follow. ∎

Lemma 5.3.4 Let $G = H \rtimes_\phi K$ be a semidirect product. Then the following are true.
- $H \trianglelefteq G$
- $H \cap K = 1$

Proof

- Let $(h,k) \in G$. Let $(h_0,1) \in H$. Then
$$(h,k)(h_0,1)(\phi_{k^{-1}}(h^{-1}),k^{-1}) = (h,k)(h_0 \cdot (\phi_{k^{-1}}(h^{-1})),k^{-1})$$

  Notice that the second term multiplies to 1 which means that the entire product lies in H. Thus we have proven $(h,k)H(h,k)^{-1} \subseteq H$

- From the above identification we clearly see that they are disjoint except from the identity.

∎

These are the fundamental results that we want the semidirect product to have when we construct it.

Proposition 5.3.5 Let H,K be groups and $\phi : K \to \operatorname{Aut}(H)$ be a group homomorphism. Then the following are equivalent characterizations of when the semidirect product is equivalent to the direct product:
- The identity map between $H \rtimes_\phi K \cong H \times K$ is a group isomorphism
- ϕ is the trivial homomorphism from K to $\operatorname{Aut}(H)$
- $K \trianglelefteq_\phi H \rtimes K$

The above proposition gives a necessary and sufficient condition for the semi direct product to be isomorphic to the external direct product. The following theorem gives a sufficient criterion for the semi direct product to be isomorphic to the internal direct product.

Theorem 5.3.6 Let G be a group with subgroups H,K such that $H \trianglelefteq G$ and $H \cap K = 1$. Let $\phi : K \to \operatorname{Aut}(H)$ be the homomorphism defined by $\phi(k)(h) = khk^{-1}$. Then $HK \cong H \rtimes_\phi K$.

Proof   Firstly note that if $h_1 k_1 = h_2 k_2$ in the product HK, then $h_2^{-1} h_1 = k_2 k_1^{-1}$ and together with $H \cap K = 1$, this implies that $h_2^{-1} h_1 = 1$ and $k_2 k_1^{-1}$ and $h_1 = h_2$ and $k_1 = k_2$.

Define a map $\psi : HK \to H \rtimes_\phi K$ by $\psi(hk) = (h,k)$. It is well defined because every element in HK can be written uniquely as an element h times an element in K by the above. It is a group homomorphism because we have
$$\begin{aligned}
\psi(h_1 k_1 h_2 k_2) &= \psi(h_1 k_1 h_2 k_1^{-1} k_1 k_2) \\
&= \psi(h_1 h_3 k_1 k_2) &&(H \text{ is normal, } h_3 = k_1 h_2 k_1^{-1}) \\
&= (h_1 h_3, k_1 k_2) \\
&= (h_1 \phi(h_2)(k_1), k_1 k_2) \\
&= (h_1, h_2)(k_1, k_2) \\
&= \psi(h_1, k_1)\psi(h_2, k_2)
\end{aligned}$$

It remains to show that this is a bijection. But $|HK| = \frac{|H||K|}{|H \cap K|} = |H||K|$ by assumption and

$|H \rtimes_\phi K| = |H||K|$. Also it is clear that ϕ is surjective. Thus ψ is a bijection and we are done. ■

As a direct result, if in addition to the above conditions, we have $G = HK$ then $G \cong H \rtimes_\phi K$.

6   Introduction to Rings

6.1   Basic Concept of Rings

Definition 6.1.1 (Rings)   A ring consists of an abelian group $(R, +)$ together with a binary operation $\cdot : R \times R \to R$ such that the following are true.
- Associativity: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in R$
- Unitality: There exists an element $1 \in R$ such that $a \cdot 1 = 1 \cdot a = a$ for all $a \in R$.
- Left distributivity: $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ for all $a, b, c \in R$
- Right distributivity: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ for all $a, b, c \in R$

Lemma 6.1.2   Let $(R, +, \cdot)$ be a ring.
- $0 \cdot a = a \cdot 0 = 0$ for all $a \in R$
- $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$ for all $a, b \in R$
- $(-a) \cdot (-b) = a \cdot b$ for all $a, b \in R$
- $-a = (-1) \cdot a$

Proof   Trivial.   ■

As with subgroups and groups, we have subrings of a ring.

Definition 6.1.3 (Subring)   Let R be a ring. Let $S \subseteq R$ be a subset. We say that S is a subring of R if S is a ring in its own right.

Proposition 6.1.4 (Subring Criterion)   Let R be a ring and S a subset of R. Then S is a subring of R if and only if
- $a, b \in S \implies ab \in S$
- $a, b \in S \implies a - b \in S$
- $1 \in S$

Proof   Suppose that R is a ring and S is a subring. Then the subgroup criterion is already satisfied. If $a, b \in S$ then $ab \in S$ since S is a ring. Identity also exists since it is a ring.
Now suppose that S is a subset that satisfies the three criterion. By the subgroup criterion S is an abelian subgroup. Associativity and distributivity is automatically satisfied. The closure property is also satisfied by the first item. The identity is also satisfied by the third item thus we are done.
■

Proposition 6.1.5   Let R be a ring and I, J subrings of R. Then $I \cap J$ is also a subring of R.

Proof   We show it using the subring criterion. The subgroup criterion is met since I, J are subgroups. If $a, b \in I \cap J$ then $ab \in I$ and $ab \in J$ by closure of rings thus $ab \in I \cap J$. Since I, J are subrings, $1 \in I$ and $1 \in J$ thus we are done.   ■

Similar to the order of a group, we have the characteristic of a ring.

Definition 6.1.6 (Characteristic)   Let R be a ring. If there exists a positive integer n such that $nx = 0$ for $x \in R$, then the smallest of such integer is called the characteristic of R. If there is no such integer then it has characteristic 0.

Definition 6.1.7 (Commutative Rings)   Let R be a ring. We say that R is commutative if $ab = ba$ for all $a, b \in R$.

6.2   The Cancellation Law

We first proof some equivalent characterizations of the cancellation law.

Proposition 6.2.1 (Cancellation Law)   The following are equivalent in a ring R.
- If $ab = 0$ in R then $a = 0$ or $b = 0$
- If $ab = ac$ and $a \neq 0$ then $b = c$
- If $ba = ca$ and $a \neq 0$ then $b = c$

Proof   Let R be a ring.

- (1) $\implies$ (2) We have that $ab = ac$ implies $ab - ac = 0$ by additive inverse and $a(b - c) = 0$ by distributivity and we are done. (1) $\implies$ (3) is similar.

- (2) $\implies$ (1) Rewriting $ab = ac$ as $a(b - c) = 0$ gives the result. (3) $\implies$ (1) is similar.

And so we conclude.   ∎

If a domain satisfies the above cancellation law, we give it a fancy name.

Definition 6.2.2 (Domain)   A ring that is not equal to the 0 ring is a domain if the above condition is satisfied.

Note that we necessarily need $0 \neq 1$ for this to work or else the cancellation law will fail automatically. Now we give another fancy name when we flavour our domain with commutativity.

Definition 6.2.3 (Integral Domain)   A commutative domain is called an integral domain.

6.3   Division in a Ring

Definition 6.3.1 (Units of a Ring)   Let R be a ring. An element $a \in R$ is a unit in R if there is some $b \in R$ such that $ab = ba = 1$. The set of units in R is denoted $R^{\times}$.

Lemma 6.3.2   Let R be a ring. Let $a \in R$ be a unit. Then there exists a unique $b \in R$ such that $ab = ba = 1$.

Proof   Suppose that $b, c \in R$ are two elements satisfying $ab = ba = 1$ and $ac = ca = 1$. Then we have that
$$c1 \cdot c = (ba)c = b(ac) = b \cdot 1 = b$$
so we conclude.   ∎

Proposition 6.3.3   Let $(R+, \cdot)$ be a ring. Then $(R^{\times}, \cdot)$ is a group.

Proof   By the unitality axiom of rings, 1_R is the identity element of the group. By definition of units, every element of $R^{\times}$ has an inverse. Associativity follows from the associativity axiom of rings.   ∎

Definition 6.3.4 (Division Rings)   A ring R is a division ring if every non-zero element of R is a unit in R.

In particular, division ring as the name suggests, allows division in the ring. This is because since every element in R is a unit, for any $a, b \in R$, we have that $a = a(b^{-1}b) = (ab^{-1})(b)$. It looks u GLy but if we let $k = ab^{-1}$, then we are in fact expressing $a = kb$ for any $a, b \in R$. Unfortunately we do not have the notion of size in a general division ring so it is not particularly useful that we can do this.

Proposition 6.3.5   Every division ring is a domain.

Proof   Let R be a division ring and $a, b \in R$ such that $ab = 0$. Then $a^{-1}ab = a^{-1}0$ thus $b = 0$ and we are done.   ∎

> **Definition 6.3.6** (Fields)   Let F be a ring. We say that F is a field if F is a commutative division ring.

Fields are studied extensively in field theory, where its unique properties as a field is discussed. In groups and rings, we perform treatment on fields by considering its properties as a ring, rather than a field.

> **Proposition 6.3.7**   Let $(R, +, \cdot)$ be a ring. Then R is a field if and only if $(R, +)$ and $(R \setminus \{0\}, \cdot)$ are abelian groups and the distributive law $a(b + c) = ab + ac$ holds.
>
> **Proof**   Let R be a field. Then $(R, +)$ is already an abelian group. Since every field is a division ring, every element except 0 is a unit and thus $(R, \cdot)$ is a group. Since a field is also commutative, $(R, \cdot)$ is abelian. Since every field is a ring, the distributive law already holds and we are done. Suppose that the three criteria is satisfied. Then R is a division ring since every nonzero element has an inverse in the group $(R, \cdot)$. It is also commutative since $(R, \cdot)$ is abelian thus we are done. ∎

I give the distributive law here although it seems redundant. Sometimes we want to check that a set with two binary operations is a field. In this case, we will need the distributive law to link the two binary operations in to action.

> **Proposition 6.3.8**   Every field is an integral domain.
>
> **Proof**   Let R be a field. Since R is a division ring, it is a domain. Since R is also commutative, we thus have that R is an integral domain. ∎

> **Proposition 6.3.9**   Every finite integral domain is a field.
>
> **Proof**   Let $\{0, a_1, \ldots, a_n\}$ be elements of a finite integral domain. We simply show that every element has a mupltiplicative inverse. Fix $1 \leq i \leq n$. Notice that the n products $a_i a_j$ for $1 \leq j \leq n$ are all distinct and nonzero. This means that $a_i a_1, \ldots, a_i a_n$ is a permutation of $a_1, \ldots, a_n$. Since one of $a_1, \ldots, a_n$ is the multiplicative identity, we must have that for some j, $a_i a_j = 1$ thus we are done. ∎

The following diagram shows roughly the relationship between different types of rings.
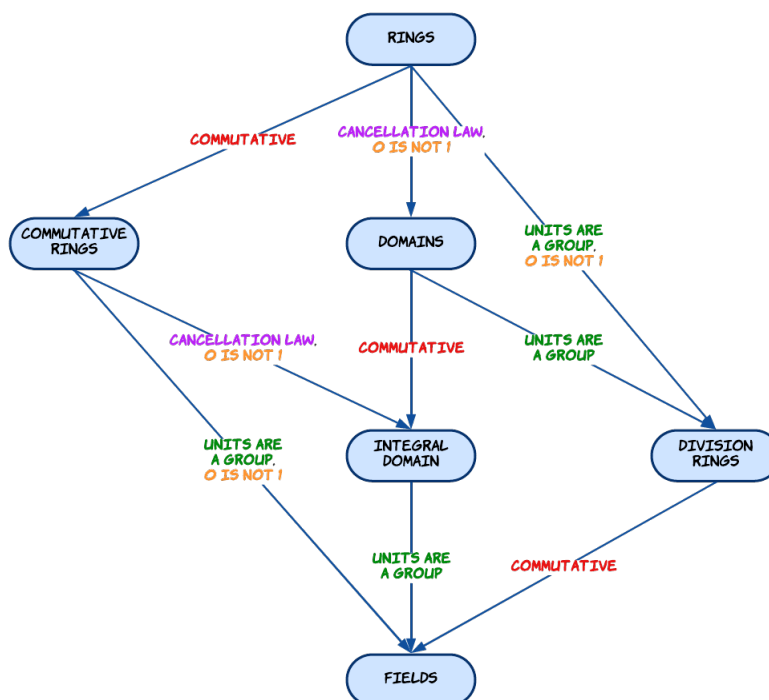
There is a subtle sense of symmetry here. The conditions on the arrow is the condition for the ring in the tail to be a ring in the arrow head. For instance, if a domain R satisfies the property that elements in R are commutative, then R is an integral domain. On the other hand, every integral domain will necessarily be a domain.

6.4   Products of Rings

> **Definition 6.4.1** (Direct Product of Rings)   Let $\{R_i \mid i \in I\}$ be a collection of rings. Define the direct product of the collection of rings to be the set
>
> $$\prod_{i \in I} R_i = \{(r_i)_{i \in I} \mid r_i \in R_i\}$$
>
> together with pointwise addition and multiplication.

6.5   Elements of a Ring

> **Definition 6.5.1** (Zero Divisors)   Let R be a ring. Let $0 \neq a \in R$. We say that a is a zero divisor if there exists $0 \neq b \in R$ such that $ab = 0$.

> **Lemma 6.5.2**   Let R be a ring. Then R is a domain if and only if R has no zero divisors.

> **Proof**   Suppose that R is a domain. Then if $a, b \neq 0$, we must have $ab \neq 0$ by the cancellation law. Hence R has no zero divisors. Conversely, if R has no zero divisors, then $ab = 0$ and $a \neq 0$ implies that $b = 0$. Hence the cancellation law is satisfied.   ∎

> **Definition 6.5.3** (Nilpotents)   Let R be a ring. An element $x \in R$ is said to be nilpotent if $x^n = 0$ for some $n \in \mathbb{N}$.

> **Lemma 6.5.4**   Let R be a ring. Let $x \in R$. If x is nilpotent, then x is a zero divisor.

Proof   Suppose that $n \in \mathbb{N}$ is smallest for which $x^n = 0$. Then $x \cdot x^{n-1} = 0$ but x and x^{n-1} is non-zero. Hence x is a zero divisor. ∎

Definition 6.5.5 (Idempotents)   Let R be a ring. An element $x \in R$ is said to be idempotent if $x^2 = x$.

7   Ideals and their Properties

7.1   Basic Definition of Ideals

Definition 7.1.1 (Left, Right and Two-Sided Ideals)   Let $(R, +, \cdot)$ be a ring. Let $I \subseteq R$.
- I is a left ideal of R if $(I, +)$ is a subgroup of $(R, +)$ and $r \cdot i \in I$ for all $r \in R$ and $i \in I$
- I is a right ideal of R if $(I, +)$ is a subgroup of $(R, +)$ and $i \cdot r \in I$ for all $r \in R$ and $i \in I$
- I is a two-sided ideal of R is I is both a left ideal and a right ideal

Lemma 7.1.2   Let R be a commutative ring. Let $I \subseteq R$ be a subset. Then I is a left ideal of R if and only if I is a right ideal of R.

Lemma 7.1.3   Let R be a ring. Let I be an ideal of R. Then $I = R$ if and only if I contains a unit of R.

Proof   Let $I = R$. Then trivially $1 \in I$. Now let $u \in I$ be a unit. Let $x \in R$, I want to show that $x \in I$ thus completing the proof that $R \subseteq I$. Now $x = x(u^{-1}u) = (xu^{-1})u$. Since $xu^{-1} \in R$ and $u \in I$, their multiplication will also be in I, thus $x \in I$. ∎

This lemma is also very useful if you consider the fact that the multiplicative identity is also a unit.

Definition 7.1.4 (Maximal Ideals)   Let R be a ring. Let I be a left ideal of R. We say that I is a maximal ideal of R if the following are true.
- $I \neq R$.
- No proper ideal of R contains I.

Becareful that maximal ideals are not necessarily unique. A typical example would be the fact that (2) and (3) are principle ideals that are both maximal in $\mathbb{Z}$.

Proposition 7.1.5   Let R be a non-zero ring. Then R has a maximal left ideal.

Proof   Let $\mathcal{P}$ be the set of all proper left ideals of R ordered by inclusion. Since R is non-zero, the ideal (0) is proper and so belongs to $\mathcal{P}$. Thus $\mathcal{P} \neq \emptyset$. Let $\mathcal{C}$ be a chain in $\mathcal{P}$. Define

$$Z = \bigcup_{X \in \mathcal{C}} X$$

If $\mathcal{C}$ is empty then $Z = \{0\}$. We show that Z is a left ideal. Clearly $0 \in Z$. If $a \in Z$ and $r \in R$, then $a \in X$ for some $X \in \mathcal{C}$ so that $ra \in X \subseteq Z$. Now suppose that $a, b \in Z$. Then $a \in X$ and $b \in Y$ for some $X, Y \in \mathcal{C}$. Since $\mathcal{C}$ is a chain, without loss of generality assume that $X \subseteq Y$. Then $a \in Y$ so that $a + b \in Y \subseteq Z$. Thus Z is a left ideal.

Since all $X \in \mathcal{C}$ are proper ideals with $1 \notin X$, then $1 \notin Z$. Then Z is proper and $Z \in \mathcal{P}$. Z is then an upper bound of $\mathcal{C}$. By Zorn's lemma, $\mathcal{P}$ has a maximal element. Then the maximal element is a maximal left ideal of R. ∎

Proposition 7.1.6   Let R be a ring. Let I be an ideal of R. Then I is a maximal left ideal if and only if R/I is a division ring.

Proof   Suppose that I is a maximal ideal. Let $x \notin R$. We show that $x + I$ has an inverse. We know that $I + (x)$ is an ideal containing I. Since I is maximal, we must have $I + (x) = R$. This means that $1 \in I + (x)$ which means there exists $m \in I$ and $r \in R$ such that $1 = m + rx$. Now

consider $r + M$. We have that

$$(x + I)(r + I) = xr + I$$
$$= (1 - m) + I$$
$$= 1 + I$$

Now suppose that R/I is a field. Let J be an ideal such that $I \subseteq J \subseteq R$ and $I \neq J$. Now let $x \in J \setminus I$. Then $I + x$ has a multiplicative inverse in R/I since $I + x \neq I$, the additive identity. Let the inverse be $I + y$. Then

$$I + 1 = (I + x)(I + y) = I + xy$$

Trivially $xy \in (x)$, thus $1 \in I + (x) \subseteq J$. But if the identity is in the ideal, the ideal is equal to the ring thus we are done. ∎

Corollary 7.1.7 Let R be a commutative ring with identity and M an ideal of R. Then M is maximal if and only if R/M is a field.

Proof Immediate from the above. ∎

Definition 7.1.8 (Prime Ideals) Let R be a ring. Let $P \subseteq R$ be a proper ideal of R. We say that P is a prime ideal of R if $ab \in P$ implies that $a \in P$ or $b \in P$.

Proposition 7.1.9 Let R be a commutative ring with identity not equal to 0. Then P is a prime ideal in R if and only if R/P is an integral domain.

Proof Suppose that P is a prime ideal. Then let $(a + P)(b + P) = P$. Since we also have that $(a + P)(b + P) = ab + P$. This means that $ab \in P$ thus either $a \in P$ or $b \in P$ which in turns leads to either $a + P = P$ or $b + P = P$ and thus the cancellation law applies.
Now suppose that R/P is an integral domain. Let $ab \in P$. Since R/P is an integral domain, we have that

$$(a + P)(b + P) = ab + P = P$$

means that either $a + P = P$ or $b + P = P$ which means that either $a \in P$ or $b \in P$ and we are done. ∎

Corollary 7.1.10 Let R be a commutative ring. Let I be an ideal of R. If I is a maximal ideal, then I is a prime ideal.

Proof If M is maximal then R/I being a field implies that R/I is an integral domain thus I is prime. ∎

7.2 Ideals and Generating Sets

Definition 7.2.1 (Elements Generating an Ideal) Let R be a ring. Let I be an indexing set. Let $S = \{a_i \mid i \in I\} \subseteq R$ be a set of elements of R. Define

$$(S) = (a_i \mid i \in I) = \left\{ \sum_{k=1}^{n} r_k a_k \mid r_k \in R \right\}$$

Lemma 7.2.2 Let R be a ring. Let I be an indexing set. Let $\{a_i \mid i \in I\} \subseteq R$ be a set of elements of R. Then $(a_i \mid i \in I)$ is a left ideal of R.

Proof Let $s_1, s_2 \in (r_i \mid i \in I)$. We can write $s_1 = \sum_{k=1}^{n_1} r_k a_k$ and $s_2 = \sum_{j=1}^{n_2} r_j a_j$. Then every term in $s_1 + s_2$ is the product of $r \in R$ and $a \in \{a_i \mid i \in I\}$. Hence the additivity rule is satisfied.

For $a = \sum_{k=1}^{n} r_k a_k \in (a_i \mid i \in I)$, we can use distibutivity to see that

$$r \cdot a = r \cdot \sum_{k=1}^{n} r_k a_k \in (a_i \mid i \in I) = \sum_{k=1}^{n} (r \cdot r_k) \cdot a_k \in (a_i \mid i \in I)$$

for any $r \in R$. Hence we conclude. ■

Definition 7.2.3 (Generators of an Ideal)   Let R be a ring. Let I be a left ideal of R. Let $S \subseteq R$ be a subset. We say that S are generators of I if

$$I = (S)$$

Definition 7.2.4 (Principal Ideals)   Let R be a ring. Let I be a left ideal of R. We say that I is a principal ideal if
$$I = (a)$$
is generated by a sin GLe element $a \in R$.

7.3   Operations on Ideals

Definition 7.3.1 (Sums and Intersections of Ideals)   Let R be a ring. Let I, J be left ideals of R.
- Define the sum of I and J by

$$I + J = \{i + j \mid i \in I, j \in J\}$$

- Define the intersection of I and J by

$$I \cap J = \{r \in R \mid r \in I, r \in J\}$$

Proposition 7.3.2   Let R be a ring. Let I, J be left ideals of R. Then $I + J$ and $I \cap J$ are both left ideals of R.

Proof   Let R be a ring and I, J its ideals.
- We first show that $I + J$ is an ideal. Let $i_1 + j_1, i_2 + j_2 \in I + J$. Then since R is an abelian group an I, J are subgroups of R,

$$i_1 + j_1 + i_2 + j_2 = (i_1 + i_2) + (j_1 + j_2) \in I + J$$

thus closure is satisfied. Associativity is satisfied since it inherits from R. We also have $0 \in I, J$ thus $0 \in I + J$. The inverse of $i + j \in I + J$ is $-i - j \in I + J$ since $-i \in I$ and $-j \in J$. Thus $I + J$ is a subgroup of R.
Now let $r \in R$ and $i + j \in I + J$. Then $r(i + j) = ri + rj$ by distributivity. Since I, J are ideals, there exists $s \in I$ such that $s = ri$ and $t \in J$ such that $t = rj$. Then $r(i+j) = ri+rj = s + t \in I + J$ thus we are done.
- $I \cap J$ are already subgroups of R. Let $k \in I \cap J$. Let $r \in R$. Then $rk \in r(I \cap J)$. Then there exists $i \in I$ and $j \in J$ such that $i = rk = j$. Then $i = j \in I \cap J$ thus we are done.

■

The following definition is only useful when the ring is commutative.

Definition 7.3.3 (Product of Ideals)   Let R be a ring. Let I, J be two-sided ideals of R. Define

the product of I and J to be

$$IJ = (ij \mid i \in I, j \in J) = \left\{ \sum_{k=1}^{n} a_k b_k \mid a_k \in I, b_k \in J \right\}$$

Lemma 7.3.4 Let R be a ring. Let I_1, I_2 be two-sided ideals of R. Then the following are true.
- $I_1 I_2$ is an ideal of R.
- $I_1 I_2 \subseteq I_1, I_2$.

Lemma 7.3.5 Let R be a commutative ring. Let I_1, I_2, I_3 be ideals of R. Then the following are true.
- Product is Commutative: $I_1 I_2 = I_2 I_1$.
- Product is Associative: $(I_1 I_2) I_3 = I_1 (I_2 I_3)$.
- Distributivity: $I_1 (I_2 + I_3) = I_1 I_2 + I_1 I_3$.

8 The Isomorphism Theorem for Rings

8.1 Ring Homomorphisms

Definition 8.1.1 (Ring Homomorphism)   Let R, S be rings. A ring homomorphism is a map $\phi : R \to S$ such that the following are true:
- $\phi(a + b) = \phi(a) + \phi(b)$ for all $a, b \in R$
- $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in R$
- $f(1_R) = 1_S$

A bijective ring homomorphism is called a ring isomomorphism.

Lemma 8.1.2   Let R, S be rings. Let $\phi : R \to S$ be a ring homomorphism. Then the following are true.
- $\phi(0_R) = 0_S$.
- $\phi(-a) = -\phi(a)$.
- $\phi|_{R^\times} : R^\times \to S^\times$ is a group homomorphism. Moreover, $\phi(a^{-1}) = \phi(a)^{-1}$.

Proof   We have that
$$\phi(0_R) = \phi(0_R + 0_R) = \phi(0_R) + \phi(0_R)$$
Since all elements of S has an additive inverse, we conclude that $\phi(0_R) = 0_S$ by applying the inverse on both sides.

We have that
$$0_S = \phi(0_R) = \phi(a + (-a)) = \phi(a) + \phi(-a)$$
Hence $\phi(-a) = -\phi(a)$.

We first show ϕ sends units to units. Let $r \in R^\times$. Then we have
$$1_S = \phi(1_R) = \phi(r \cdot r^{-1}) = \phi(r)\phi(r^{-1})$$
Since multiplicative inverses are unique, we conclude that $\phi(r^{-1}) = \phi(r)^{-1}$. It follows that $\phi|_{R^\times}$ is a group homomorphism by the fact that $\phi(ab) = \phi(a)\phi(b)$. ∎

Lemma 8.1.3   Let R, S be rings. Let $\varphi : R \to S$ be a ring homomorphism. Then the following are true.
- If I is an ideal of R, then $\varphi(I)$ is an ideal of S if and only if φ is surjective.
- If J is an ideal of S, then $\varphi^{-1}(J)$ is an ideal of R.

Proof   Suppose that I is an ideal of R. Let $a, b \in \varphi(I)$. Then there exists $x, y \in I$ such that $\varphi(x) = a$ and $\varphi(y) = b$. Since I is an ideal, we have $x + y \in I$ and so $a + b = \varphi(x) + \varphi(y) = \varphi(x + y) \in \varphi(I)$. Now suppose that $s \in S$. Since φ is surjective, there exists $r \in R$ such that $\varphi(r) = s$. Then we have $sa = \varphi(r)\varphi(x) = \varphi(rx) \in \varphi(I)$ since I is an ideal. Hence we are done.

Conversely, if φ sends ideals to ideals, then $\varphi(R)$ is an ideal containing 1_S. Hence $\varphi(R) = S$ and so φ is surjective.

Now suppose that J is an ideal of S. Let $x, y \in \varphi^{-1}(J)$. Since J is an ideal of S, we have $\varphi(x) + \varphi(y) = \varphi(x + y) \in J$. Hence $x + y \in \varphi^{-1}(J)$. Now let $r \in R$. Then we have $\varphi(r)\varphi(x) = \varphi(rx) \in J$ since J is an ideal. Hence $rx \in \varphi^{-1}(J)$ and so φ^J is an ideal. ∎

Lemma 8.1.4   Let R, S be rings. Let $\varphi : R \to S$ be a ring homomorphism. Let m be a maximal ideal of S. If φ is surjective, then $\varphi^{-1}(m)$ is a maximal ideal of R.

Proof   It is clear that $\varphi^{-1}(m)$ is an ideal. If it is not maximal, then there exists a proper ideal I such that $\varphi^{-1}(m) \subset I \subset R$. Then we have $m \subseteq \varphi(I) \subseteq \varphi(R) = S$. Since m is maximal, either $\varphi(I) = \varphi(R)$ or $\varphi(I) = m$. If it is the former, then   ∎

Lemma 8.1.5   Let R, S be commutative rings. Let $\varphi : R \to S$ be a ring homomorphism. Let P be a prime ideal of S. Then $\varphi^{-1}(P)$ is a prime ideal of R.

Proof

                                                                                                        ∎

8.2   Kernels and the Quotient Ring

Definition 8.2.1 (Kernel)   Let R, S be rings. Let $\phi : R \to S$ be a ring homomorphism. Define the kernel of ϕ to be
$$\ker(\phi) = \{r \in R \mid \phi(r) = 0\}$$

Proposition 8.2.2   Let R, S be a ring. Let $\phi : R \to S$ be a ring homomorphism. Then $\ker(\phi)$ is an ideal of R.

Proposition 8.2.3   Let I be an ideal of a ring R. Then the cosets of I in R,
$$R/I = \{r + I \mid r \in R\}$$
is a ring with addition defined the same as quotient groups
$$(r + I) + (s + I) = (r + s) + I$$
and multiplication defined as
$$(r + I)(s + I) = \{ab \in R \mid a \in r + I, b \in s + I\} = rs + I$$

Proof   Since $(I, +)$ is a subgroup of $(R, +)$, we know that R/I is already an abelian group. We simply show that multplication is well defined. Suppose that $x_1 + I = x_2 + I$ and $y_1 + I = y_2 + I$. Then
$$\begin{aligned}
(x_1 + I)(y_1 + I) &= x_1 y_1 + I \\
&= (x_1 y_1 - x_1 y_2 + x_1 y_2 - x_2 y_2 + x_2 y_2) + I \\
&= (x_1(y_1 - y_2) + (x_1 - x_2)y_2 + x_2 y_2) + I \\
&= x_2 y_2 + I
\end{aligned}$$
since $y_1 - y_2 \in I$ and $x_1 - x_2 \in I$. This shows that taking different represetatives of the cosets of an ideal does not matter for multiplication.
Now we show that $1 + I$ is the muplicative identity of R/I. Let $x + I \in R/I$. We have that $(1 + I)(x + I) = x + I$ thus we are done. Associativity and distributivity follows from the fact that R has these properties.   ∎

Definition 8.2.4 (Quotient Rings)   Let R be a ring. Let I be an ideal of R. Define the quotient ring of R by I to be the abelian group
$$\frac{R}{I} = \{r + I \mid r \in R\}$$
together with multiplication defined by
$$(r + I) \cdot (s + I) = rs + I$$

Proposition 8.2.5   Let R be a ring. Let $I \subseteq R$ be a subset. Then I is an ideal of R if and only if it is the kernel of some ring homomorphism.

8.3   Isomophism Theorem for Rings

The isomorphism theorem for rings is a direct result that extends the group isomorphism theorems. Their proofs are mostly the same except that we also have to check that multiplication is preserved so that the isomorphisms inherited from groups is indeed a ring isomorphism.

Theorem 8.3.1 (The First Isomorphism Theorem for Rings)   If $\phi : R \to S$ is a homomorphism of rings, then the following are true.
- $\ker(\phi)$ is an ideal of R
- $\operatorname{im}(\phi) \leq S$ is a subring of S

Moreover, we have an isomorphism

$$\frac{R}{\ker(\phi)} \cong \phi(R)$$

in rings.

Proof   A group isomorphism $R/\ker(\phi) \cong \phi(R)$ can be established from the first isomorphism theorem for groups. Moreover we know that $\ker(\phi)$ is a normal subgroup. To show that $\ker(\phi)$ is an ideal, notice that for $r \in R$ and $k \in \ker \phi$, $\phi(rk) = \phi(r)\phi(k) = 0$ thus $rk \in \ker(\phi)$. To show that $R/\ker(\phi) \cong \phi(R)$ is a ring isomorphism, suppose that π is the induced group isomorphism. Notice that

$$\begin{aligned}
\pi((r_1 + \ker(\phi))(r_2 + \ker(\phi))) &= \pi(r_1 r_2 + \ker(\phi)) \\
&= \phi(r_1 r_2) \\
&= \phi(r_1)\phi(r_2) \\
&= \pi(r_1 + \ker(\phi))\pi(r_2 + \ker(\phi))
\end{aligned}$$

and so we conclude.   ∎

Theorem 8.3.2 (The Second Isomorphism Theorem for Rings)   Let $A \leq R$ and B an ideal of R. Then the following are true.
- $A + B = \{a + b \mid a \in A, b \in B\}$ is a subring of R
- $A \cap B$ is an ideal of A

Moreover, we have an isomorphism

$$\frac{A + B}{B} \cong \frac{A}{A \cap B}$$

in rings.

Theorem 8.3.3 (The Third Isomorphism Theorem for Rings)   Let I, J be ideals of R with $I \subset J$. Then J/I is an ideal of R/I and $(R/I)/(J/I) \cong R/J$

Theorem 8.3.4 (The Correspondence Theorem)   Let R be a ring. Let I be a left ideal of R. Then there is an inclusion preserving one-to-one bijection

$$\left\{\begin{matrix} \text{Subrings of } R \\ \text{containing } I \end{matrix}\right\} \quad \overset{1:1}{\longleftrightarrow} \quad \{\text{Subrings of } R/I\}$$

induced by the surjective ring homomorphism $\varphi : R \to R/I$. Moreover, there is an inclusion preserving one-to-one bijection

$$\left\{\begin{matrix} \text{Ideals of } R \\ \text{containing } I \end{matrix}\right\} \quad \overset{1:1}{\longleftrightarrow} \quad \{\text{Ideals of } R/I\}$$

given by the map $A \mapsto A/I$ for A an ideal of R containing I.

8.4   Chinese Remainder Theorem

In this section we develop the necessary notions in order to illustrate the Chinese Remainder Theorem.

Definition 8.4.1 (Coprime Ideals)   Let R be a ring. Let I, J be left ideals of R. We say that I and J are coprime if
$$I + J = R$$

Notice that in $\mathbb{Z}$, the prime ideals are exactly the ideals (p) where p is a prime. We also have a nice inclusion of ideals whenever $p \mid a$ which is $(a) \subseteq (p)$, which we will prove later. This means that in general, the smaller the number a is, the larger the ideal (a) is and indeed, the smaller the number is in $\mathbb{Z}$, the more numbers it can possibly divide. Now recall that if a and b are coprime in $\mathbb{Z}$, then their gcd will be 1. Indeed we will develop the notion of gcd for ideals as well, which is to say that if $d = \gcd(a, b)$ in the usual sense, then $(a) \subseteq (d)$ and $(b) \subseteq (d)$. Then if a and b are coprime, their ideals are both subsets of (1), which is exactly R. This leads to why we say that two ideals are coprime.

Proposition 8.4.2   Let R be a commutative ring. Let $I_1, \ldots, I_k$ be pairwise coprime ideals of R. Then we have
$$\prod_{i=1}^{k} I_i = \bigcap_{i=1}^{k} I_i$$

Proof   We first consider the case $k = 2$. Suppose that I and J are coprime ideals. Notice that we have $IJ \subseteq I, J$ hence $IJ \subseteq I \cap J$. On the other hand, we have

$$\begin{aligned}
I \cap J &= (I + J)(I \cap J) & (I, J \text{ are coprime}) \\
&= I(I \cap J) + J(I \cap J) \\
&\subseteq IJ + JI \\
&= IJ
\end{aligned}$$

Hence we are done.

We then induct on $k \geq 3$. For the base case, suppose that I_1, I_2, I_3 are pairwise coprime. I claim that $I_1 \cap I_2$ and I_3 are coprime. Since I and K are coprime, we can write $1 = i + k_1$ for $i \in I$ and $k_1 \in K$. Similarly, we can write $1 = j + k_2$ for $j \in J$ and $k_2 \in K$. Then $1 = (i + k_1)(j + k_2) = ij + ik_1 + jk_2 + k_1k_2$. The last three elements lie in K and the first element lie in $I \cap J$. Hence $I \cap J$ and K are coprime. Now assuming that the result is true for some $n \in \mathbb{N}$. Then we have

$$\bigcap_{i=1}^{n+1} I_i = I_1 \cap \bigcap_{i=2}^{n+1} I_i = I_1 \cap \prod_{i=2}^{n+1} = I_1 \cdot \prod_{i=2}^{n+1} I_i$$

since I_1 and $\prod_{i=2}^{n+1}$ are coprime by another set of induction.   ■

Theorem 8.4.3 (Chinese Remainder Theorem)   Let $I_1, \ldots, I_n$ be ideals of a ring R. Then the ring homomorphism
$$\phi : R \to \frac{R}{I_1} \times \cdots \times \frac{R}{I_n}$$
defined by $\phi(x) = (x + I_1, \ldots, x + I_n)$ has kernel
$$I = \bigcap_{k=1}^{n} I_k$$

Moreover, if each I_j and I_k are pairwise coprime, then there is an isomorphism
$$\frac{R}{I} \cong \frac{R}{I_1} \times \cdots \times \frac{R}{I_n}$$
given by ϕ.

Proof   Since ϕ is a collection of projections on to each factor, ϕ is a ring homomorphism. It is clear that I is the kernel of the homomorphism. Indeed given $x \in I$, then x lies in each and every I_k for $1 \le k \le n$. Thus $\phi(x) = (x + I_1, \ldots, x + I_n) = 0$. Conversely, if $(x + I_1, \ldots, x + I_n)$ is such that applying ϕ gives 0, then $x \in I_1, \ldots, I_n$ so that $x \in I$.

When the ideals are pairwise corpime, consider the elements $e_k = (0, \ldots, 0, x + I_k, 0, \ldots, 0)$ for $1 \le k \le n$ (these are called full system of orthogonal central idempotents). Notice that they satisfy the equation $1 = e_1 + \cdots + e_n$ and $e_k^2 = e_k$ for $1 \le k \le n$ for $i \ne j$, we have $e_i e_j = 0$. Now since I_i and I_j are coprime, we have that $R = I_i + I_j$ so that $1 = a_j + z_j$ for $a_j \in I_i$ (note the subscript) and $z_j \in I_j$. Define $x_i = z_1 \cdots z_{i-1} \cdot z_{i+1} \cdots z_n$ for each $1 \le i \le n$. Write the projection homomorphism as $\psi : R \to R/I_j$. If $i \ne j$, then $\phi_j(x_i) = 0$ because x_i contains the element z_j that lies in I_j. Also, we have that

$$\psi_i(z_j) = \psi_i(1 - a_j) = \psi_i(1) - \psi_i(a_j) = \psi_i(1) = 1$$

in R/I_i since $a_j \in I_i$. Thus we have that

$$\psi_i(x_i) = \psi_i(z_1) \cdots \psi_i(z_n) = 1$$

All this means that $x_i \in R$ is such that $\psi(x_i) = (0, \ldots, 0, 1 + I_i, 0, \ldots, 0)$ for $1 \le i \le n$. Now to prove surjectivity, let $(r_1, \ldots, r_n)$ be an element in the product. Then we have that

$$(r_1, \ldots, r_n) = \sum_{j=1}^{n} \psi(r_i) e_i = \sum_{j=1}^{n} \psi(r_i x_i)$$

and so $r_1 x_1 + \cdots + r_n x_n \in R$ is our desired element. And so we are done.   ■

This is a more generalized version of the Chinese Remainder Theorem in number theory. Indeed, to recover the one in number theory, take $R = \mathbb{Z}$ and $I_k = (n_k)$ for some $n_k \in \mathbb{Z}$ so that I_k is the principal ideal on n_k. Moreover, by choosing each n_k to be pairwise coprime, we obtain the isomorphism which proves that the congruence relation can be solved.

Notice that the proof is instructive. Indeed we can simply follow the steps of the proof to find a solution. Namely, given $(r_1, \ldots, r_n)$ in the product, we can find $r \in R$ such that $\phi(r) = (r_1, \ldots, r_n)$. The steps are as follows.

1. Fix $1 \le i \le n$. Using $R = I_i + I_j$, find $a_j \in I_i$ and $z_j \in I_j$ such that $1 = a_j + z_j$ for each j. This can be done for example by Bezout's lemma in $R = \mathbb{Z}$.

2. Define $x_i = z_1 \cdots z_{i-1} \cdot z_{i+1} \cdots z_n$ for $1 \le k \le n$.

3. Do the same for each $1 \le i \le n$. The solution is then $r = r_1 x_1 + \cdots + r_n x_n$.

Corollary 8.4.4   Let R be a commutative ring. Let $I_1, \ldots, I_k$ be pairwise coprime ideals of R. Then we have a ring isomorphism

$$\frac{R}{\prod_{i=1}^{k} I_i} = \frac{R}{\bigcap_{i=1}^{k} I_i} \cong \prod_{i=1}^{k} \frac{R}{I_i}$$

Proof   Follows from the Chinese Remainder Theorem and the fact that $\prod_{i=1}^{k} I_i = \bigcap_{i=1}^{k} I_i$.   ■

9   Integral Domains

9.1   Field of Fractions

Definition 9.1.1 (Fractional Equivalence)   Let R be an integral domain. Let

$$S = \{(a, b) \mid a, b \in R \text{ and } b \neq 0\}$$

Define a relation on S by $(a, b) \sim (c, d)$ if $ad = bc$.

Lemma 9.1.2   The relation $\sim$ between elements of S is an equivalence relation.

Proof   Since R is an integral domain, symmetry is satisfied. Clearly it is reflexive since $ab = ba$. For transitivity, suppose that $ad = bc$ and $cf = de$. Then $adcf = bcde$ and by cancellation law, $af = be$.   ∎

Proposition 9.1.3   The set of equivalence classes of S of an integral domain R, under the equivalence relation $\sim$, together with the operations of addition and multiplication defined by

$$(a, b) + (c, d) = (ad + bc, bd)$$

and

$$(a, b) \cdot (c, d) = (ac, bd)$$

is a field, called the field of fractions, denoted $\text{Frac}(R)$.

Proof   Note that R is a field if and only if $(R, +)$ and $(R \setminus \{0\}, \cdot)$ are commutative groups and the distributive law holds.

- Let $(a, b), (c, d) \in S$. Then $ad + bc, bd \in R$ since R is closed thus $(ad + bc, bd) \in S$. Let (e, f) also be in S. Then

$$
\begin{aligned}
((a, b) + (c, d)) + (e, f) &= (ad + bc, bd) + (e, f) \\
&= ((ad + bc)f + (bd)e, bdf) \\
&= (adf + bcf + bde, bdf)
\end{aligned}
$$

  and

$$
\begin{aligned}
(a, b) + ((c, d) + (e, f)) &= (a, b) + (cf + de, df) \\
&= (a(df) + b(cf + de), b(df)) \\
&= (adf + bcf + bde, bdf)
\end{aligned}
$$

  Thus associativity is satisfied. I claim that $(0, 1)$ is an identity. We have $(a, b) + (0, 1)(a \cdot 1 + b \cdot 0, b \cdot 1) = (a, b)$. If $(a, b) \in S$ then $(-a, b) \sim (a, -b)$ is an inverse. We have

$$(a, b) + (-a, b) = (ab - ab, b^2) = (0, b^2) \sim (0, 1)$$

  Finally we have

$$
\begin{aligned}
(a, b) + (c, d) &= (ad + bc, bd) \\
&= (da + cb, db) && (R \text{ is an Integral Domain}) \\
&= (cb + da, db) \qquad = (c, d) + (a, b) && (R \text{ is an abelian group})
\end{aligned}
$$

  Thus we have shown that $(S, +)$ is an abelian group.

- We now show that $(S, \cdot)$ is an abelian group. Let $(a, b), (c, d), (e, f) \in S$. Then $(a, b) \cdot (c, d) = (ac, bd) \in S$ sincve $ac, bd \in R$ by closure of rings. Thus the closure property is satisfied. Associativity is inherited from R since elements in S are pairs of R. I claim that the identity is $(1, 1) \sim (k, k)$ for any $k \in R$. We have

$$(a, b) \cdot (1, 1) = (a \cdot 1, b \cdot 1) = (a, b)$$

If $(a, b) \in S$ then its inverse is (b, a). We have

$$(a, b) \cdot (b, a) = (ab, ba) = (ab, ab) = (1, 1)$$

thus $(S, \cdot)$ is a group. Now to show abelian, we have

$$(a, b) \cdot (c, d) = (ac, bd) = (ca, db) = (c, d) \cdot (a, b)$$

since R is an integral domain. Thus we have shown that $(S, \cdot)$ is an abelian group.

- Finally we show distributivity. Let $(a, b), (c, d), (e, f) \in S$. Then

$$(a, b) \cdot ((c, d) + (e, f)) = (a, b) \cdot (cf + de, df)$$
$$= (acf + ade, bdf)$$

and

$$(a, b) \cdot (c, d) + (a, b) \cdot (e, f) = (ac, bd) + (ae, bf)$$
$$= (acbf + bdae, bdbf)$$
$$= (acf + ade, bdf) \qquad \text{(equivalence relation)}$$

Thus we are done.

∎

In particular, the field of fractions of $\mathbb{Z}$ is precisely $\mathbb{Q}$.

Lemma 9.1.4   For any integral domain R, R is a subring of $\text{Frac}(R)$.

Proof   Define a function $\phi : R \to Q(R)$ by $\phi(r) = \frac{r}{1}$. Then ϕ_R is the identity homorphism thus $\phi(R) = R$. Then $\phi(R)$ is trivially a subring of $Q(R)$ and we are done. ∎

9.2 Divisibility

Division is a property that only commutative rings enjoy.

Definition 9.2.1 (Division)   Let R be a commutative ring and let $a, b \in R$ with $b \neq 0$. a is said to be a multiple of b if there exists an element $x \in R$ with $a = bx$. In this case b is said to divide a or be a divisor of a, written $b \mid a$.

Proposition 9.2.2   Let R be a commutative ring. Let $x, y \in R$ and $y \neq 0$. Then the following are equivalent.
- $x \mid y$
- $y \in (x)$
- $(y) \subseteq (x)$

Proof   Let R be a commutative ring. Let $x, y \in R$ and $y \neq 0$.

- (1) $\implies$ (2) Suppose that $y = kx = xk$ for some $k \in R$. Then $y \in (x) = \{ax \mid a \in R\}$ by definition.

- (2) $\implies$ (3) Suppose that $y \in (x)$. Then there exists $k \in R$ such that $y = kx = xk$. To show that $(y) \subseteq (x)$, let $ry \in (y)$. Then $ry = rkx$ and $rk \in R$ thus $ry \in (x)$ thus we are done.

- (3) $\implies$ (1) Suppose that $(y) \subseteq (x)$. Then there exists $k \in R$ such that $y = kx$. Then we are done.

∎

Definition 9.2.3 (Greatest Common Divisor)   Let R be a commutative ring and let $a, b \in R$. A greatest common divisor of a and b is a non-zero element $d \in R$ such that
- $d \mid a$ and $d \mid b$
- If $c \mid a$ and $c \mid b$ then $c \mid d$

It is denoted $\gcd(a, b)$.

Definition 9.2.4 (Least Common Multiple)   Let R be a commutative ring and let $a, b \in R$. A least common multiple of a and b is a non-zero element $l \in R$ such that
- $a \mid l$ and $b \mid l$
- If $a \mid m$ and $b \mid m$ then $l \mid m$

It is denoted $\operatorname{lcm}(a, b)$.

Unfortunately, these numbers do not always exists for any a, b in a general ring. The existence of such a number depends on the ideal generated by the two given elements.

Proposition 9.2.5   Let R be a commutative ring. Let $x, y \in R$ such that they are nonzero. If the ideal generated by a and b, namely (a, b) is a principal ideal (d), then d is the gcd of a and b.

Proof   Suppose that $(a, b) = (d)$ for some $d \in R$. Then $a \in (d)$ and $b \in (d)$ already implies that $d \mid a$ and $d \mid b$. Suppose that $c \mid a$ and $c \mid b$. This means that $a \in (c)$ and $b \in (c)$. Since $d \in (a, b)$ there exists $r, s \in R$ such that $ra + sb = d$. This means that $d \in (c)$ thus $c \mid d$. ∎

Definition 9.2.6 (Associates)   Let R be a commutative ring. Let $x, y \in R$. We say that x and y are associates if $x \mid y$ and $y \mid x$. We denote it as $x \sim y$.

Proposition 9.2.7   Let R be a integral domain. Let $x, y \in R$. Then the following are equivalent.
- $x \sim y$
- $(x) = (y)$
- There exists a unit $u \in R$ such that $x = qy$.

Proof

- (1) $\implies$ (2): Suppose that $x \sim y$ then $x \mid y$ and $y \mid x$ which means that $(x) \subseteq (y)$ and $(y) \subseteq (x)$.

- (2) $\implies$ (3): Suppose that $(x) = (y)$. Then since $x \in (y)$, there exists $s \in R$ such that $x = sy$ and likewise $y = tx$. Then $x = stx$ and since R is an integral domain, $st = 1$ which means that s, t are units.

- (3) $\implies$ (1): Suppose that $x = qy$ for some unit q. Then clearly $y \mid x$. Since q is a unit, $q^{-1}x = y$ and thus $x \mid y$ which means that x and y are associates.

∎

9.3   Primes and Irreducibles

Primes and irreducibles are two similar concepts, their difference is only made clear in Euclidean domains that are not principles ideal domains, both of which we will see later.

Definition 9.3.1 (Irreducibles)   Let D be an integral domain. A nonzero element $p \in D$ that is not a unit is said to be irreducible if $p = ab$ implies a or b is a unit.

Definition 9.3.2 (Primes)   Let D be an integral domain. A nonzero element $p \in D$ that is not a unit is said to be a prime if $p \mid ab$ implies $p \mid a$ or $p \mid b$.

Lemma 9.3.3   Let D be an integral domain. Let p be a non-unit. Then p is prime if and only if (p) is a prime ideal.

Proof   Suppose that p is prime. Suppose that $rp \in (p)$. Then $p \in P$ and we are done. Now suppose that (p) is a prime ideal. Suppose that $p \mid ab$. Then $pd = ab$ for some $d \in D$ thus $ab \in (p)$. WLOG take $a \in (p)$ by definition of prime ideal. Then we are done since $a \in (p)$ implies $p \mid a$. ∎

Proposition 9.3.4   Let D be an integral domain and $p \in D$. If p is a prime then p is irreducible.

Proof   Let p be a prime in D. Suppose that $p = ab$. Then trivially $p \mid ab$ thus $p \mid a$ or $p \mid b$. WLOG take $p \mid a$. Trivially $a \mid p$ since $a \mid ab$. This means that a and p are associates. Thus $p = aq$ for some unit q. Then since $aq = ab$ and integral domains have cancellation law, we must have $q = b$ which means that b is a unit. Thus p is irreducible. ∎

9.4   Unique Factorization Domains

Definition 9.4.1 (Unique Factorization Domains)   An integral domain D is a unique factorization domain if the following are true
- Let $a \in D$ such that $a \neq 0$ and a is not a unit. Then a can be written as the product of irreducible elements in D.
- Let $a = p_1 \cdots p_r = q_1 \cdots q_s$, where p_i and q_j are irreducible. Then $r = s$ and there is a permutation such that $p_i = q_{\pi(i)}$ for $i \in \{1, \ldots, r\}$.

Notice that in general integral domains, primes are not the same as irreducibles. But they have the nice property that they coincide in UFDs, which is why they are put in the chapter on UFDs here. Below gives a full converse to the relation between prime and irreducibles we gave above under the umbrealla that is UFDs.

Proposition 9.4.2   Let D be a UFD and $p \in D$. Then p is a prime if and only if p is irreducible.

Proof   We have already shown the forward implication. Now let p be irreducible. We show that (p) is prime. Let $ab \in (p)$. Then there exists $d \in D$ such that $pd = ab$. We can factorize ab and pd respectively into a product of irreducibles elements in D. But since they are equal, by uniqness of fatorization, p is exactly an associate of one of the irreducibles in the factorization of ab. If p is in the factorization of a then $p \mid a$ and we are done. Otherwise it is in b and we are also done. ∎

Notice that in the above proof, the fact that every prime is irreducible does not use the properties of UFD. This means that this is true in general integral domains.

9.5   Principal Ideal Domains

Definition 9.5.1 (Principal Ideal Domains)   A principal ideal domain is an integral domain in which every ideal is principal, meaning every ideal is of the form
$$(a) = \{ra : r \in R\}$$

Proposition 9.5.2   Let R be a PID and $x, y \in R$. Then $\gcd(x, y)$ and $\mathrm{lcm}(x, y)$ exists and there exists $r, s \in R$ such that
$$\gcd(x, y) = rx + sy$$

Proof   Let $x, y \in R$. Then $(x) + (y)$ is an ideal of R, thus it must be prciniple, say $(d) = (x) + (y)$. Similarly, $(x) \cap (y)$ is also an ideal, say $(l) = (x) \cap (y)$.
We prove that d and l are the gcd and lcm respectively. Trivially, $(x) \subseteq (d)$ and $(y) \subseteq (d)$ implies $d \mid x$ and $d \mid y$. Also for any z such that z divides x and y, $(x) \subseteq (z)$ and $(y) \subseteq (z)$ thus $(d) \subseteq (z)$. The proof is similar for (l).

Since $(d) = (x) + (y)$, there exists $r, s \in (x), (y)$ respectively such that $d = rx + sy$ and we are done. ∎

Proposition 9.5.3 Let R be a PID and (p) a nonzero ideal in R. Then the following are equivalent.
- (p) is maximal
- p is irreducible
- p is prime ((p) is prime)

We have seen that every maximal ideal is a prime ideal. We have seen that if (p) is a prime ideal then p is prime. We have also seen that every prime is irreducible. We show separately that if p is irreducible then p is a prime, and also if p is prime then (p) is maximal.

For the first part, suppose that p is irreducible. Suppose that $p \mid ab$ for $a, b \in R$. By the above proposition, $d = \gcd(p, a)$ exists. Then for some $t \in R$, $p = dt$. Since p is irreducible, either d or t is a unit. We consider both cases. If t is a unit, then p and d are associates and thus $p \mid d$. Since $d \mid a$, we have that $p \mid a$ and we are done. Now if d is a unit, then $d = ra + sp$ for some $r, s \in R$. Multplying both sides with b gives $db = rab + spb$. Since $p \mid ab$ and $p \mid spb$, we have that $p \mid db$. Then $pu = db$ for some unit $u \in R$. Since d is a unit, we have that $d^{-1}pu = b$, which means that $p \mid b$ and we are done.

Now we show that if p is a prime then (p) is maximal. We know that (p) is a prime ideal. Suppose that $(p) \subseteq (q) \subseteq R$ for some ideal q of R. Since $p \in (q)$, $p = tq$ for some $t \in R$. Since $p \in (p)$, we have that $tq \in (p)$. Now (p) is prime implies that either $t \in (p)$ or $q \in (p)$. If $q \in (p)$ then $(q) \subseteq (p)$ and thus $(q) = (p)$ and we are done. If $t \in (p)$, then $t = rp$ for some $r \in R$, which means that $p = rpq$. Then $rq = 1$ by cancallation law in integral domains. This means that $1 \in (q)$ thus $(q) = R$ and we are done.

Proposition 9.5.4 Every PID is a UFD.

Proof Suppose that D is a principal ideal domain. Suppose for a contradiction that x, a non-unit cannot be factorized into a product of irreducibles. Clearly x is not irreducible else a contradiction. Then there exists x_1, y_1 non unit such that $x = x_1 y_1$. Since x is assumed to be not a product of irreducibles, WLOG take x_1 to be not irreducible. Then we can repeat the process to get non units $x_2 y_2$ such that $x_1 = x_2 y_2$. Notice that $(x) \subset (x_1)$ is a proper containment of ideals if $x_1 \mid x$. Then we have a chain of ideals

$$(x) \subset (x_1) \subset (x_2) \subset \ldots$$

I claim that

$$I = \bigcup_{k=0}^{\infty} (x_k)$$

is an ideal. Indeed if $r, s \in I$, then $r \in (x_m)$ and $s \in (x_n)$ for some $m, n \in \mathbb{N}$. WLOG rtake $m \leq n$. Then $(x_m) \subseteq (x_n)$ implies $r, s \in (x_n)$ thus $r + s \in (x_n) \subseteq I$. Also if $t \in R$, then $tr \in (x_m) \subseteq I$ thus I is indeed an ideal.

Since R is a PID, there exists some $d \in I$ such that $I = (d)$. This also means that $d \in (x_m)$ for some $m \in \mathbb{N}$. Then this means that $I = (d) \subseteq (x_m)$. This proves that the chain eventually stops and this is a contradiction since we assumed that the chain of ideals are properly contained.

This menas that x can indeed be factorized into a product of irreducibles. ∎

Notice that the key in the proof is that the union of the countably finite principal ideals is again a principal ideals which allows the infinte chain of ideals to stop.

9.6 Euclidean Domains

Technically, division algorithms can exist in general domains so long that it has the notion of division. But without a measurement of size to guarantee division is taking larger numbers into smaller numbers, we cannot promise that division algorithms will halt eventually. Therefore we restrict the notion of division algorithm only to integral domains that has a notion of size.

Definition 9.6.1 (Euclidean Valuation)   Let R be an integral domain. A function $f : R \setminus \{0\} \to \mathbb{N} \cup \{0\}$ is said to be a Euclidean Valuation of R if
- $f(ab) \geq f(b)$ for all $a, b \in R \setminus \{0\}$
- For all $a, b \in R$ with $b \neq 0$, there exists q, r such that

$$a = qb + r$$

with $r = 0$ or $f(r) < f(b)$

In the above definition the second item is simply the division algorithm, with size of a number decided by the function f. Thus the Euclidean domain is simply an integral domain that possess a division algorithm.

Definition 9.6.2 (Euclidean Domain)   An integral domain R is said to be a Euclidean Domain that admits a Euclidean Valuation.

Theorem 9.6.3   Let R be a Euclidean Domain. Let a, b be nonzero elements of R. Let $d = r_n$ be the last nonzero remainder in the Euclidean Algorithm for a and b. Then d is the greatest common divisor of a and b and (d) is generated by a and b. In particular, there exists $x, y \in R$ such that $d = ax + by$.

Proposition 9.6.4   Every Euclidean Domain is a PID.

In general, we have that

$$\text{Fields} \subset \text{Euclidean Domains} \subset \text{PID} \subset \text{UFD} \subset \text{Integral Domains}$$

in which all containments are strict.

10   The Ring of Polynomials

10.1   Polynomials over Commutative Rings

In this section we formulate the basic theory of generating polynomials from a ring.

Definition 10.1.1 (Indeterminates)   Let R be a ring. A symbol x is called an indeterminate over R if
$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = 0$$
where $a_i \in R$, implies that $a_i = 0$ for each i.

Definition 10.1.2 (Polynomial over a Ring)   Any expression of the form
$$f(x) = \sum_{k=0}^{n} a_k x^k$$
where x is an indeterminate and $a_0, \ldots, a_n \in R$ and $a_n \neq 0$ is called a polynomial over R. We define the the degree of f in this case to be n.

Definition 10.1.3 (Ring of Polynomials)   Let R a ring. Define $R[x]$ to be the set of all polynomials over R.

Proposition 10.1.4   Let R be a commutative ring with identity. Then $R[x]$ is a commutative ring with identity.

Proof   Since $R \leq R[x]$ by considering all the constant polynomials, the identity of R is also the identity of $R[x]$. Let $f, g \in R[x]$. Then the coefficient of x^n in $f(x)g(x)$ is
$$c_n = \sum_{k=0}^{n} a_k b_{n-k}$$
Since $a_k b_{n-k} = b_{n-k} a_k$, we have that $f(x)g(x) = g(x)f(x)$. ∎

Definition 10.1.5 (The Evaluation Map)   Let R be a ring and let a be an element in the center $Z(R)$ of R. Define the evaluation map $\phi_a : R[x] \to R$ by the formula
$$\phi_a \left(\sum_{k=0}^{n} c_k x^k \right) = \sum_{k=0}^{n} c_k a^k$$

Proposition 10.1.6   Let R be a ring and let a be an element in the center $Z(R)$ of R. Then the evaluation homomorphism $\phi_a : R[x] \to R$ is a surjective ring homomorphism.

Proof   Let $f, g \in R[x]$ be given as $f(x) = \sum_{k=0}^{n} c_k x^k$ and $g(x) = \sum_{i=0}^{m} b_i x^i$. Then we have

$$
\begin{aligned}
\phi_a(f+g) &= \phi_a\left(\sum_{k=0}^{n} c_k x^k + \sum_{i=0}^{m} b_i x^i\right) \\
&= \phi_a\left(\sum_{k=0}^{\max\{m,n\}} (c_k + b_k) x^k\right) \\
&= \sum_{k=0}^{\max\{m,n\}} (c_k + b_k) a^k \\
&= \sum_{k=0}^{n} c_k a^k + \sum_{i=0}^{m} b_i a^i \\
&= \phi_a(f) + \phi_a(g)
\end{aligned}
$$

Moreover, we have that

$$
\begin{aligned}
\phi_a(fg) &= \phi_a\left(\sum_{k=0}^{n} c_k x^k \sum_{i=0}^{m} b_i x^i\right) \\
&= \phi_a\left(\sum_{k=0}^{m+n} \left(\sum_{i=0}^{k} c_i b_{k-i}\right) x^k\right) \\
&= \sum_{k=0}^{m+n} \left(\sum_{i=0}^{k} c_i b_{k-i}\right) a^k \\
&= \sum_{k=0}^{n} c_k a^k \sum_{i=0}^{m} b_i a^i \qquad\qquad (a \in Z(R)) \\
&= \phi_a(f) \phi_a(g)
\end{aligned}
$$

Thus ϕ_a is a ring homomorphism. To show that ϕ_a is surjective, let $b \in R$. Then clearly $\phi_a(x - a + b) = b$. ∎

10.2   The Roots of a Polynomial

Definition 10.2.1 (The Roots of a Polynomial)   Let R be a commutative ring. Let $f \in R[x]$. We say that $a \in R$ is a root of f if $\phi_a(f) = 0$. In this case we write $f(a) = 0$.

Definition 10.2.2 (Degree of a Polynomial)   Let R be a commutative ring. Let $f \in R[x]$ be written as $f = \sum_{k=0}^{n} a_k x^k$ so that $a_n \neq 0$. Then define the degree of f to be

$$
\deg(f) = n
$$

Theorem 10.2.3 (Monic Linear Division Algorithm)   Let R be a commutative ring. Let $f \in R[x]$. Let $x - a \in R[x]$ be a polynomial. Then there exists $q \in R[x]$ and $r \in R$ such that

$$
f(x) = (x - a)q(x) + r
$$

Proof   If $f(x) = 0$ then just take $q(x) = 0$ and $r = 0$. So assume that $f(x) \neq 0$. We induct on $\deg(f)$. If $\deg(f) = 1$, then $f(x) = cx + d$ for some $c \neq 0$. Set $q(x) = c$ and $r = ca + d$. Then we have

$$
q(x)(x - a) + r = c(x - a) + ca + d = cx + d = f(x)
$$

so we are done. Now assume that the result is true for all polynomials whose degree is less than n. Let f be a degree n polynomial, given by $f = \sum_{k=0}^{n} a_k x^k$. Let

$$g(x) = f(x) - a_n x^{n-1}(x-a) = (a_{n-1} + a_n a)x^{n-1} + \sum_{k=0}^{n-2} a_k x^k$$

Notice that $\deg(g) \leq n - 1$ and we can apply the inductive hypothesis to obtain $q' \in R[x]$ and $r \in R$ such that $g(x) = q'(x)(x-a) + r$. Now we have that

$$
\begin{aligned}
f(x) &= g(x) + a_n x^{n-1}(x-a) \\
&= q'(x)(x-a) + r + a_n x^{n-1}(x-a) \\
&= \left(q'(x) + a_n x^{n-1}\right)(x-a) + r
\end{aligned}
$$

We are done as we set $q(x) = q'(x) + a_n x^{n-1}$. ∎

Theorem 10.2.4 (Factor Theorem)   Let R be a commutative ring. Let $f \in R[x]$. Then $a \in R$ is a root of f if and only if $x - a$ divides f.

Proof   Let $a \in R$ be a root of f. By the monic linear division algorithm, $f(x) = q(x)(x-a) + r$ for some $q \in R[x]$ and $r \in R$. Then

$$0 = \phi_a(f) = \phi_a(q(x)(x-a) + r) = \phi_a(q(x))\phi_a(x-a) + \phi_a(r) = 0 + r$$

since $\phi_a(x-a) = a - a = 0$. Hence $r = 0$ and we have $f(x) = q(x)(x-a)$. Hence f is divisible by $x - a$.

Now suppose that $x - a$ divides f. Then there exists $q \in R[x]$ such that $f(x) = q(x)(x-a)$. Then it is clear that
$$\phi_a(f) = \phi_a(q)\phi_a(x-a) = 0$$
and so we conclude. ∎

10.3   Polynomials over Integral Domains

Proposition 10.3.1   Let R be a commutative ring. Then R is an integral domain if and only if $R[x]$ is an integral domain.

Proof   Commutativity is clear since for $f, g \in R[x]$, coefficients of the product fg inherits commutativity from R thus $fg = gf$. Now we show that cancellation law exists in $R[X]$. Let $f, g \in R[x]$ such that $fg = 0$. Suppose for a contradiction that $f \neq 0$ and $g \neq 0$. This means that $\deg(f) = n$ and $\deg(g) = m$ for some $n, m \neq 0$. Consider the coefficient of x^{n+m} in fg, which is $a_n b_m$. Since $fg = 0$, $a_n b_m = 0$ and by cancellation law in R either $a_n = 0$ or $b_m = 0$. This contradicts the fact that $\deg(f) = n$ and $\deg(g) = m$ thus we are done.

Now suppose that $R[x]$ is an integral domain. Then R is a subring of $R[x]$ so that R is also an integral domain. ∎

Proposition 10.3.2   Let R be an integral domain. Let $f \in R[x]$. Then f has at most $\deg(f)$ roots in R.

Proposition 10.3.3   Let R be an integral domain. Then

$$\{r \in R \mid r \text{ is a unit}\} = \{f \in R[x] \mid f \text{ is a unit}\}$$

Proof   It is clear that $\subseteq$ is trivial. Now let $f \in R[x]$ such that f is a unit. Suppose that $fg = 1$ for some $g \in R[x]$. Write $f = \sum_{k=0}^{n} a_k x^k$ and $g = \sum_{i=0}^{m} b_i x^i$ for $a_n \neq 0$. comparing top coefficients with fg and 1 shows that $a_n b_m = 0$. Since R is an integral domain, we conclude that $b_m = 0$. We induct decreasin GLy on the coefficients of g. Suppose we showed that $b_n = \cdots = b_{k+1} = 0$ for some $k \geq 0$. Then the coefficient of x^{k+n} in fg is given by

$$a_{k+n-m} b_m + \cdots + a_{n-1} b_{k+1} + a_n b_k$$

Comparing coefficients with the polynomial 1 shows that the above expression is 0. Since $b_n = \cdots = b_{k+1} = 0$, we are left with $a_n b_k = 0$. Since $a_n \neq 0$, we have that $b_k = 0$. Thus $b_n = \cdots = b_1 = 0$ by induction. We are left with the fact that g is a constant, say $g(x) = b$. But now $a_0 \cdot b = 1$ implies that b is a unit, hence the constant $g \in R$ is a unit. ∎

Proposition 10.3.4   Let R be an integral domain. Then if $f \neq 0$ and $g \neq 0$ in $R[x]$, then

$$\deg(fg) = \deg(f) + \deg(g)$$

Proposition 10.3.5   Let R be a commutative ring. Let I be an ideal of R. Then the following are true.
- $I[x]$ is an ideal of R
- There is an isomorphism $\frac{R[x]}{I[x]} \cong \frac{R}{I}[x]$ given by the map $\left(f = \sum_{k=0}^{n} a_k x^k + I[x]\right) \mapsto \left(\sum_{k=0}^{n} (a_k + I) x^k\right)$
- If I is a prime ideal of R, then $I[x]$ is a prime ideal of $R[x]$.

Proposition 10.3.6   Let R be a commutative ring. Then R is a UFD if and only if $R[x]$ is an UFD.

10.4   Irreducibility over UFDs and Integral Domains

The primary goal of this chapter is to compute results relating to finding out irreducible polynomials in integral domains, rather than investigating the structure of polynomial rings.

Definition 10.4.1 (Primitive)   Let R be an integral domain. Let $f \in R[x]$ be non-zero and is given by $f = \sum_{k=0}^{n} a_k x^k$ for $a_n \neq 0$. We say that f is primitive if $\gcd(a_0, a_1, \ldots, a_n) = 1$.

Proposition 10.4.2   Let R be a UFD. Let $f, g \in R[x]$ be primitive. Then fg is also primitive.

Theorem 10.4.3 (Generalized Gauss's Lemma)   Let R be a UFD. Let $f \in R[x]$ be primitive. Then f is irreducible if and only if f is irreducible in $\text{Frac}(R)[x]$.

Proposition 10.4.4 (Eisentein's Criterion)   Let R be an integral domain. Let $f \in R[x]$ be primitive. Suppose that P is a prime ideal of R such that the following are true.
- $a_n \notin P$.
- $a_0, \ldots, a_{n-1} \in P$.
- $a_0 \notin P^2$.

Then f is irreducible in $R[x]$.

10.5   Irreducibility over a Field

Theorem 10.5.1 (Polynomial Division Algorithm over Fields)   Let F be a field. Let $f, g \in F[x]$ such that $f \neq 0$. Then there exists unique $q, r \in F[x]$ such that
- $g = qf + r$
- Either $r = 0$ or $\deg(r) < \deg(g)$

> **Lemma 10.5.2**   Let F be a field. Then $F[x]$ is an Euclidean domain with valuation given by
>
> $$\deg : F[x] \to \mathbb{N}$$
>
> that sends f to $\deg(f)$.

A number of results follows from this. For instance,

- $F[x]$ is a PID, a UFD and an integral domain.
- $f \in F[x]$ is irreducible if and only if (f) is maximal if and only if f is prime.
- Every $f \in F[x]$ has at most $\deg(f)$ roots.
- The gcd and hcf of two elements exists, Bezout's lemma is also applicable.
- Factor theorem and Remainder theorem both hold.

> **Proposition 10.5.3**   Let F be a field. Let $f \in F[x]$. If $\deg(f) = 1$ so that f is linear, then f irreducible.

> **Proposition 10.5.4**   Let F be a field. Let $f \in F[x]$ such that $2 \leq \deg(f) \leq 3$. Then f is irreducible if and only if f has no roots in F.

10.6   Irreducibility over $\mathbb{Z}$

> **Theorem 10.6.1** (Rational Root Test)   Let $f(x) = \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[x]$. If $r/s \in \mathbb{Q}$ for $\gcd(r, s) = 1$ is a root then r divides a_0 and s divides a_n.

Finally, recall that $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ is a field. We can descend the polynomial to the prime field and check irreducibility there. This is typically easier for small primes since there are less total roots to check in that case.

> **Theorem 10.6.2**   Let $f(x) = \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[x]$. Suppose that p is a prime such that p does not divide a_n. Write $\overline{a_k} \equiv a_k \pmod{p}$ for $0 \leq k \leq n$ and
>
> $$\overline{f} = \sum_{k=0}^{n} \overline{a_k} x^k \in \mathbb{F}_p[x]$$
>
> If $\overline{f}$ is irreducible in $\mathbb{F}_p[x]$ then f is irreducible in $\mathbb{Z}[x]$.

11   Field Theory

11.1   Properties of a Field

Definition 11.1.1 (Fields)   A field is a commutative division ring, denoted $(F, +, \times)$. In particular, it satisfies the following
- $(F, +)$ is an abelian group with identity 0
- $(F \setminus \{0\}, \times)$ is an abelian group with identity 1
- (Distributivity) $a(b + c) = ab + ac$ for $a, b, c \in F$

Definition 11.1.2 (Subfields)   A subfield is a subset E of a field F such that the subset is a field. It is denoted $E < F$

Proposition 11.1.3   A commutative ring is a field if and only if its only ideals are the trivial ideal and the ring itself.

Proof   Let F be a field. Suppose that I is a non trivial ideal of F. Then there exists $i \in I$. Since I is an ideal, then $i^{-1}I \subseteq I$ thus $i^{-1}i = 1 \in I$. But 1 in I implies that $I = F$ thus we are done. Suppose that the non trivial ideal of a commutative ring R is only R itself. We want to show that every element except 0 is a unit. Let $r \in R \setminus \{0\}$. Then the principal ideal (r) is nonzero and thus $(r) = R$. Then there exists $b \in R$ such that $rb = br = 1$. Thus b is an inverse of r. ∎

Proposition 11.1.4 (Characteristic)   Let F be a field. Then either $\text{char}(F) = 0$ or $\text{char}(F) = p$ a prime number.

Proof   Suppose that $\text{char}(F) = a \cdot b \neq 0$. Then $(a \cdot b) \cdot 1 = 0$ implies that $a = 0$ or $b = 0$ since F is an integral domain. Either way this implies $\text{char}(F) = 0$ which is a contradiction. ∎

As usual in understanding different structures in algebra, it is important to study the homomorphisms betweens the structure.

Definition 11.1.5 (Field Homomorphisms)   Let F, K be fields. A field homomorphism from F to K is a ring homomorphism $\phi : F \to K$.

The structure of fields are very rich and thus they are very rigid.

Lemma 11.1.6   Let F, K be fields and $\phi : F \to K$ a field homomorphism. Then ϕ is injective.

Proof   Suppose that $a \in \ker(\phi)$. Then we have $\phi(a)\phi(a^{-1}) = \phi(aa^{-1}) = 1$ and $\phi(a)\phi(a^{-1}) = 0$. Thus there is a contradiction. ∎

In particular, a field homomorphism $\varphi : F \to K$ means that F embeds into K since F is now isomorphic to $\varphi(F)$ which is a subfield of K. Instead of writing $\varphi(F)$ a subfield of K we will write $F \subset K$ instead. This embedding however depends on φ and so the embedding is unclear, we will use $\varphi(F) \subset K$ for F being isomorphic to a subfield of K.

11.2   New Fields from Old

Definition 11.2.1 (Prime Subfields)   Let F be a field. Define the prime subfield of F to be the subfield whose set is given by
$$F_0 = \{n \cdot 1 \mid n \in \mathbb{Z}\}$$

Proposition 11.2.2   Let F be a field. The prime subfield of F is equal to
$$F_0 = \bigcap_{K < F} K$$

Proof   The fact that it is a field itself is trivial. Write E for the prime subfield. Let $L = \bigcap_{K < F} K$. Then $L < E$ is trivial. Now $1 \in L$ since L is a subfield of F. Since E is the smallest subfield containing 1, $E < L$ and we are done. ∎

Proposition 11.2.3   The prime subfield of a field F is isomorphic to either $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$

Definition 11.2.4 (Composite Field)   Let $E, F < K$. Then the composite field FE is defined to be the smallest subfield of K that contains both E and F.

Proposition 11.2.5   Let $E, F < K$. Then

$$FE = \bigcap_{\substack{U \text{ a field} \\ E, F < U < K}} U$$

12   The Ring of Matrices

12.1   Matrices and its Ring Structure

Definition 12.1.1 (Matrix)   Let R be a ring. Let $m, n \in \mathbb{N} \setminus \{0\}$. An $m \times n$ matrix A is a rectangular array of m rows and n columns of elements of R, denoted by

$$
A = \begin{pmatrix}
a_{11} & a_{12} & \cdots & a_{1n} \\
a_{21} & a_{22} & \cdots & a_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
a_{m1} & a_{m2} & \cdots & a_{mn}
\end{pmatrix}
$$

For $i = 1, \ldots, m$ and $j = 1, \ldots, n$, define

$$
r_i = \begin{pmatrix} a_{i1} & a_{i2} & \cdots & a_{in} \end{pmatrix} \quad \text{and} \quad c_j = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix}
$$

Then r_i is called the ith row of A and c_j is called the jth row of A. The element of A at the intersection of the ith row and jth column is called the (i, j)th entry of A. The set of all $m \times n$ matrices over R is denoted by $M_{m \times n}(R)$. We sometimes denote A as $(a_{i,j})_{m \times n}$

Definition 12.1.2 (Matrix Addition)   Let R be a ring. Let $m, n \in \mathbb{N} \setminus \{0\}$. Define matrix addition to be the binary operation $+ : M_{m \times n}(R) \times M_{m \times n}(R) \to M_{m \times n}(R)$ given by

$$
(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij})
$$

Definition 12.1.3 (Scalar Multiplication)   Let R be a ring. Let $m, n \in \mathbb{N} \setminus \{0\}$. Define scalar multiplication to be the function $\cdot : \mathbb{R} \times M_{m \times n}(\mathbb{R}) \to M_{m \times n}(\mathbb{R})$ given by

$$
\lambda \cdot (a_{ij}) = (\lambda a_{ij})
$$

Proposition 12.1.4   Let $A, B \in M_{m \times n}(\mathbb{R})$ and $\lambda, \mu \in \mathbb{R}$. Then
- $(\lambda \mu) A = \lambda(\mu A)$
- $\lambda(A + B) = \lambda A + \lambda B$
- $(\lambda + \mu) A = \lambda A + \mu A$

Definition 12.1.5 (Matrix Multiplication)   Let R be a ring. Let $n \in \mathbb{N} \setminus \{0\}$. Define matrix multiplication to be the binary operation $\cdot : \mathbb{R} \times M_{n \times n}(\mathbb{R}) \to M_{n \times n}(\mathbb{R})$ given by

$$
(a_{ij}) \cdot (b_{ij}) = (c_{ij})
$$

where

$$
c_{i,j} = \sum_{k=1}^{p} a_{ik} b_{kj}
$$

Proposition 12.1.6   Let R be a ring. Let $n \in \mathbb{N}$. Then $(M_n(R), +, \cdot)$ is a ring.

Definition 12.1.7 (Invertible Matrices)   Let R be a ring. Let $n \in \mathbb{N} \setminus \{0\}$. Let $A \in M_n(R)$. We say that A is invertible if A has a multiplicative inverse.

Definition 12.1.8 (Upper Triangular Matrices)   A matrix is called upper triangular if all of its entries below the main diagonal are zero.

Definition 12.1.9 (Diagonal Matrices)   A square matrix is said to be a diagonal matrix if $d_{ij} = 0$ whenever $i \neq j$

Definition 12.1.10 (Transpose)   Let $A = (a_{ij})_{m \times n}$. The transpose of A is the $n \times m$ matrix denoted by A^T obtained by interchanging the row and columns of A, that is, $A^T = (a_{ji})_{n \times m}$

12.2   Row Operations

Definition 12.2.1 (Recombine Matrix)   Let $\mathbb{F}$ be a field. Let $n \in \mathbb{N} \setminus \{0\}$. Let $a \in \mathbb{F} \setminus \{0\}$. Define the $n \times n$ recombine matrix to be

$$
R_{i,j,a} = \begin{pmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & & a & & & \\ & & & \ddots & & & & \\ & & & & 1 & & & \\ & & & & & \ddots & & \\ & & & & & & 1 \end{pmatrix}
$$

where the diagonals are all 1 and other elements that are not shown is 0.

Multiplying a matrix $A \in M_n(\mathbb{F})$ with the recombine matrix $R_{i,j,a}$ has the effect of adding $a \cdot r_j$ to r_i, where $r_1, \ldots, r_n$ are the rows of A.

Definition 12.2.2 (Scale Matrix)   Let $\mathbb{F}$ be a field. Let $n \in \mathbb{N} \setminus \{0\}$. Let $a \in \mathbb{F} \setminus \{0\}$. Define the $n \times n$ scale matrix to be

$$
R_i(a) = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & a & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}
$$

where the diagonals are all 1 except for the i, ith element and other elements that are not shown is 0.

Multiplying a matrix $A \in M_n(\mathbb{F})$ with the scale matrix $R_i(a)$ has the effect of multiplying the ith row r_i of A by the scalar $a \in \mathbb{F} \setminus \{0\}$.

Definition 12.2.3 (Transposition Matrix)   Let $\mathbb{F}$ be a field. Let $n \in \mathbb{N} \setminus \{0\}$. Define the $n \times n$ transposition matrix to be

$$
R_{i,j} = \begin{pmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 0 & & & 1 & & \\ & & & 1 & & & & \\ & & & & \ddots & & & \\ & & & & & 1 & & \\ & & 1 & & & 0 & & \\ & & & & & & \ddots & \\ & & & & & & & 1 \end{pmatrix}
$$

where the diagonals are all 1 except for the i, ith and j, jth element and other elements that are

> not shown is 0.

Multiplying a matrix $A \in M_n(\mathbb{F})$ with the transposition matrix $R_i(a)$ has the effect of interchanging the ith row r_i of A with the jth row r_j of A.

Proposition 12.2.4 Let $\mathbb{F}$ be a field. Let $a \in \mathbb{F} \setminus \{0\}$ be non-zero. Then the following are true.
- The multiplicative inverse of $R_{i,j,a}$ is given by $R_{i,j,-a}$
- The multiplicative inverse of $R_i(a)$ is given by $R_i(a^{-1})$ The multiplicative inverse of $R_{i,j}$ is given by $R_{j,i}$

Definition 12.2.5 (Upper Echelon Form)   A matrix satisfying the below properties is said to be in upper echelon form.
- All zero rows are below all non-zero rows.
- The first non-zero entry of a row is to the right of the first non-zero entry of the row above.
- The first non-zero entry of every row is 1

Definition 12.2.6 (Row-reduced Form)   We say that a matrix in upper echelon form is in row-reduced form if above and below every first non-zero entry of a row, all entries are 0.

Definition 12.2.7 (Reduction Procedure)   Let $\mathbb{F}$ be a field. Let $m, n \in \mathbb{N} \setminus \{0\}$. Let $A = (a_{ij}) \in M_{m \times n}(\mathbb{F})$. Define the reduction procedure on A as follows. Start with $i = j = 1$.
1. If a_{ij} and all entries below are 0, move on pivot to the right to $a_{i,j+1}$ and repeat step 1, or terminate if $j = n$
2. If $a_{ij} = 0$ but $(a_k j) \neq 0$ for some $k > i$, apply $R_{i,j}$
3. If $a_{ij} \neq 1$, apply $R_{a_{i,j}^{-1}}$
4. If for any $k \neq i$, $a_{kj} \neq 0$, apply $R_{k,i,-a_{kj}}$
5. If $i = m$ or $j = n$ then terminate, else move pivot to $i+1, j+1$ and go back to step 1.

12.3   Determinants

Let $n \in \mathbb{N} \setminus \{0\}$. Recall that S_n is the group of all bijections of the set $\{1, \dots, n\}$ together with functional composition.

Definition 12.3.1 (Determinants)   The determinant of a $n \times n$ matrix $A = (a_{ij})$ is the scalar quantity
$$\det(A) = \sum_{\phi \in S_n} \text{sign}(\phi) a_{1\phi(1)} a_{2\phi(2)} \dots a_{n\phi(n)}$$

Lemma 12.3.2   Let $n \in \mathbb{N} \setminus \{0\}$. Then $\det(I_n) = 1$.

Proof
$$\begin{aligned}
\det(I_n) &= \sum_{\phi \in S_n} \text{sign}(\phi) a_{1\phi(1)} a_{2\phi(2)} \dots a_{n\phi(n)} \\
&= a_{11} a_{22} \dots a_{nn} \\
&= 1
\end{aligned}$$
∎

Proposition 12.3.3   If A has two equal rows then $\det(A) = 0$

Proposition 12.3.4   Applying elementary row operations does the following to the determinant of a matrix.
- $\det(R_{i,j,a} A) = \det(A)$

- $\det(R_i(a)A) = a \det(A)$
- $\det(R_{i,j}) = -\det(A)$

Proposition 12.3.5 If $A = (a_{ij})_{n \times n}$ is upper triangular, then

$$\det(A) = a_{11}a_{22}\ldots a_{nn}$$

Proposition 12.3.6 Let $A = (a_{ij})_{n \times n}$, $B = (b_{ij})_{n \times n}$. Then
- $\det(A^T) = \det(A)$
- $\det(AB) = \det(A)\det(B)$

12.4   Formula for the Inverse of an Invertible Matrix

Definition 12.4.1 (The Adjoint of a Matrix)   Let $\mathbb{F}$ be a field. Let $n \in \mathbb{N} \setminus \{0\}$. Let $A \in M_n(\mathbb{F})$. Define the adjoint of A to be

$$\text{adj}(A) = (A_{ij})^T$$

where A_{ij} is given by the formula

$$A_{ij} = (-1)^{i+j} \begin{vmatrix} a_{1,1} & \cdots & a_{1,j-1} & a_{1,j+1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{i-1,1} & \cdots & a_{i-1,j-1} & a_{i-1,j+1} & \cdots & a_{i-1,n} \\ a_{i+1,1} & \cdots & a_{i+1,j-1} & a_{i+1,j+1} & \cdots & a_{i+1,n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,j-1} & a_{m,j+1} & \cdots & a_{m,n} \end{vmatrix}$$

Proposition 12.4.2   Let $\mathbb{F}$ be a field. Let $n \in \mathbb{N} \setminus \{0\}$. Let $A \in M_n(\mathbb{F})$. Then we have

$$A \cdot \text{adj}(A) = \det(A) \cdot I_n = \text{adj}(A) \cdot A$$

Theorem 12.4.3   Let $\mathbb{F}$ be a field. Let $n \in \mathbb{N} \setminus \{0\}$. Let $A \in M_n(\mathbb{F})$. Then A is invertible if and only if $\det(A) \neq 0$. In this case,

$$A^{-1} = \frac{1}{\det(A)} \text{adj}(A)$$

Proposition 12.4.4   Let $\mathbb{F}$ be a field. Let $n \in \mathbb{N} \setminus \{0\}$. Let $A, B \in M_n(\mathbb{F})$. If A and B are invertible, then the following are also true.
- AB is invertible and $(AB)^{-1} = B^{-1}A^{-1}$
- A^k is invertible for $k \in \mathbb{N}$ and $(A^k)^{-1} = (A^{-1})^k$
- A^{-1} is invertible and $(A^{-1})^{-1} = A$
- A^T is invertible and $(A^T)^{-1} = (A^{-1})^T$

12.5   Direct Sum or Matrices

Definition 12.5.1 (Direct Sum)   Let $\mathbb{F}$ be a field. Let $n, m \in \mathbb{N} \setminus \{0\}$. Let $\in M_n(\mathbb{F})$ in $B \in M_m(\mathbb{F})$. Define the direct sum of A and B to be

$$A \oplus B = \begin{pmatrix} A & 0_{n \times m} \\ 0_{m \times n} & B \end{pmatrix}$$

Lemma 12.5.2   Let $\mathbb{F}$ be a field. Let $n, m \in \mathbb{N} \setminus \{0\}$. Let $\in M_n(\mathbb{F})$ in $B \in M_m(\mathbb{F})$. Then for any $k \in \mathbb{N} \setminus \{0\}$, we have that

$$(A \oplus B)^n = A^n \oplus B^n$$

12.6   The General Linear Group and its Subgroups

Definition 12.6.1 (The General Linear Group)   Let k be a field. Define the general linear group of $n \times n$ matrices over k to be

$$GL(n,k) = (M_n(k))^\times = \{M \in M_n(k) \mid M \text{ is invertible in } M_n(k)\}$$

Definition 12.6.2 (The Orthogonal Group)   Let k be a field. Let $n \in \mathbb{N} \setminus \{0\}$. Define the orthogonal group to be
$$O(n,k) = \{M \in GL(n,k) \mid M^T M = I_n\}$$

Definition 12.6.3 (The Special Linear Group)   Let k be a field. Let $n \in \mathbb{N} \setminus \{0\}$. Define the special linear group to be
$$SL(n,k) = \{M \in GL(n,k) \mid \det(M) = \pm 1\}$$

Definition 12.6.4 (The Special Orthogonal Group)   Let k be a field. Let $n \in \mathbb{N} \setminus \{0\}$. Define the special orthogonal group to be

$$SO(n,k) = \{M \in GL(n,k) \mid \det(M) = 1\}$$

Lemma 12.6.5   Let k be a field. Let $n \in \mathbb{N} \setminus \{0\}$. Then

$$SO(n,k) = O(n,k) \cap SL(n,k)$$