Finite Group Theory Notes

Ari Boyarsky[*]

August 10, 2021

1 Basic Group Theory

Definition 1 (Groups)**.** A **group**, G, is a set with an addition-like or multiplication-like operation that satisfies the following axioms,

1. Associativity: If $a, b, c \in G$ then $a + (b + c) = a + b + c$ or equivalently for multiplicative groups we have $a(bc) = abc$.
2. Identity: G must contain an identity element denoted 0 (for additive groups) or 1 (for multiplicative groups) such that for $a \in G$ we have $a + 0 = a$ or $a \cdot 1 = a$ respectively. Sometimes the identity element is also denoted by e or I.
3. Inverses: The group must be closed under inverses of the operation. That is for all multiplicative group elements $a \in G$ there is a $a^{-1} \in G$ such that $aa^{-1} = 1$. For additive groups we have $(-a) \in G$ such that $a + (-a) = 0$.

Definition 2 (Abelian Group)**.** Suppose that G is a group in which the group operation, $\circ$, satisfied commutativity. That is, for $a, b \in G$

$$a \circ b = b \circ a$$

Then we say that this group is an **Abelian Group.**

Remark 3. The main idea of group theory is the study of symmetry. Indeed the axioms in definition 1 are exactly the axioms we need to describe the symmetries of any mathematical object. For example, we can describe the symmetries of a pentagon (or equivalently a circle with 5 points) by the **cyclic group of order 5** denoted by $\mathbb{Z}\backslash 5\mathbb{Z}$which consists of the set rotations of a pentagon. We can represent this group with the set $\{0, 1, 2, 3, 4\}$ whose operation is addition modulo 5. There are two main goals of group theory:

1. Classify all the possible groups up to isomorphism. That is, what are all the groups that have the same structure. Isomorphisms are structure preserving bisections that are natural for this problem.
2. What are the representations of these groups, that is, what are the symmetries that these groups describe and symmetries of what object. This is the study of *representation theory* where we can either let the group act on a set and get a *permutation representation* or on a vector space and get a *linear representation.*

Definition 4 (Group Isomorphisms)**.** We say that a group isomorphism is a bijective function between groups, $f : G \to H$, that preserves group structure. That is,

1. f is bijective.
2. f is a homomorphism. For $a, b \in G$ we have $f(ab) = f(a)f(b)$ (preserving the group operation)
   (a) $a, a^{-1} \in G$ we have $f(a^{-1}) = f(a)^{-1}$ (preserving group inverses)

[*] Based on a first year graduate course taught online by Richard Borcherds and the group theory chapters of "*A Course in Algebra*" by E.B. Vinberg.

(b) If $I \in G$ is the identity then $f(I) \in H$ is the identity.

A natural question to ask is if Definition 1 does actually capture all the axioms of symmetry. It turns out that indeed it does exactly. This result is known as Cayley's Theorem.

1.1 Group Actions and Cayley's Theorem

Definition 5. A **action** of a group G on a set X is a homomorphism,

$$f : G \times X \to X$$

such that for $f(g) \in Sym(X)$ and $g \in G$ we have $f(gh) = f(g)f(s)$ and $1s = s$. Where $Sym(X)$ is the **symmetric or permutation group** of X.

Remark 6. We can also see that G acts on itself. Take $S = G$ then,

$$g(s) = \underbrace{gs}_{\text{group product}}$$

This tells us that G is a **subgroup** of S. Thus, this gives a weaker form of Cayley's theorem which is that every group is the subgroup of some group of permutations of some set. To get the full version of Cayley's theorem we need to show that in fact this group contains ALL the permutations of that set (since permutations are essentially symmetries).

Definition 7. A **subgroup** G of another group H is a subset of H with the same group operation, that contains the identity element, and is closed under the group operation.

Definition 8. There are two important types of actions of $g \in G$ on X to consider,

1. The **left action** which we will write as,
$$l(g)x = gx$$
2. The **right action** which we will write as,
$$r(g)x = xg$$
satisfying $x1 = x$ and $(xg)h = x(gh)$.

If $l(g)x = r(g)x$ then we say that x, g commute and that G is **commutative** or equivalently **Abelian**.

Proposition 9. *Suppose G acts on $S = G$ on left. Then, $g(sh) = (gs)h$.*

Proof. The proof follows from the associative law. □

Remark 10. Suppose G is the symmetries of a triangle which has 6 symmetries (identity, swapping corners, 2 rotations 2/3s of the way). If we label the corner $\{1, 2, 3\}$ we can write these elements in the notation $(12) \implies 1 \to 2$. So, G consists of,

$$(e), (12), (23), (13), (123), (132)$$

We can make a Cayley table,

	e	12	23	13	123	132
e	e					
12			23			
23		123				
13						
123						
132						

Which shows that this group is not Abelian. That is the left action and right action on itself are not equal. The idea of left actions on acting on the symmetric group of itself is enough to prove Cayley's theorem below.

Remark 11. This suggests that a group can act itself on the left and right. In fact there are 8 ways a group can act on itself. There are 4 left actions and 4 right actions.

	Left Action $l(g) = gx$	Right Action $r(g) = xg$
Trivial	x	x
Left/Right Translation	gx	xg
Left/Right Shift Actions	xg^{-1}	$g^{-1}x$
Left/Right Adjoints	gxg^{-1}	$g^{-1}xg$

Theorem 12 (Cayley's Theorem). *Every group G is isomorphic to a subgroup of the symmetric group acting on G.*

Proof. Define the action $\phi : G \to Sym(G)$. If the kernel of ϕ is trivial then ϕ is injective. Suppose $g \in Ker(\phi)$ then $ge = g = e$ thus the kernel is trivial. Then we know that by the first Isomorphism theorem for groups (since ϕ is a homomorphism) that the image ϕ (or $Sym(G)$) is isomorphic to $G/ker(\phi)$ but since $ker(\phi)$ is trivial we have that ϕ is an isomorphism. □

Remark 13. This remark tell us that every group can be thought of as describing the symmetries of some object trivially given by the symmetric group of the original group.

1.2 Group Homomorphisms

We have previously used the term "homomorphism" in our definitions of group actions and isomorphisms. Let us now describe these maps in more detail.

Definition 14 (Group Homomorphism)**.** Suppose $(G, \cdot)$ and $(H, \circ)$ are groups. Then a group homomorphism is a map $f : G \to H$ such that,

$$f(g \cdot h) = f(g) \circ f(h)$$

for all $g, h \in G$.

Proposition 15. *Let $1_G \in G$ be the identity in G and $1_H \in H$ be the identity in H. Then if f is a homorphism between G and H we have that,*

$$f(1_G) = 1_H$$

Proof. Take any $g \in G$ that is not the identity such that $f(g) = h$. Consider,

$$h = f(g) = f(g1_G) = f(g)f(1_G) = hf(1_G)$$

Now since H is a group note that $h^{-1} \in H$ so consider,

$$h^{-1}h = h^{-1}hf(1_G) \implies 1_H = f(1_G)$$

□

Proposition 16. *Let G, H be groups and f be a homomorphism between them. Take $g \in G$ such that $f(g) = h \in H$. Then,*

$$f(g^{-1}) = h^{-1}$$

Proof. Consider that from the previous proposition if 1_H is the identity in H and 1_G is the identity in G then,

$$1_H = f(1_G) = f(g^{-1}g) = f(g)f(g^{-1}) = hf(g^{-1})$$

But then, $f(g^{-1}) = h^{-1}$ by definition of the inverse as the element h^{-1} that satisfies $hh^{-1} = 1_H$. □

Definition 17 (Automorphism)**.** We say that an isomorphism onto itself, i.e. $f : G \to G$ is an **automorphism**. Thus, it is a symmetry of itself. We can also define the **automorphism group** as the group consisting of all automorphism of some object X. This is also a **symmetry group** and its subgroups are sometimes referred to as **transformation groups.**

Definition 18. The **kernel** of a group homomorphism $f : G \to H$ is the set,

$$ker(f) = \{x \in G : f(x) = 1_H\}$$

Remark 19. The kernel is a way to measure if a homomorphism is one-to-one (injective). Suppose we have a homomorphism f that is not one-to-one then we may have $x_1, x_2, \ldots$ such that $f(x_1) = f(x_2) = y \in H$. So,

$$f(x_1) = y, f(x_2) = y$$
$$\implies f(x_1)f(x_1^{-1}) = yf(x_1^{-1}), f(x_2)f(x_1^{-1}) = yf(x_1^{-1})$$

Since homomorphism map inverses to inverse $f(x_1^{-1}) = y^{-1}$ and so,

$$f(x_1)f(x_1^{-1}) = 1_H, f(x_2)f(x_1^{-1}) = 1_H$$
$$\implies f(\underbrace{x_1x_1^{-1}}_{=1_G}) = 1_H, f(\underbrace{x_2x_1^{-1}}_{\neq 1_G}) = 1_H$$

Thus, we have several elements $x_2x_1^{-1}, x_1x_2^{-1}, \ldots$ that map to the identity in H. Thus these elements make up the Kernel of the homomorphism. Notice, that the kernel will always contain at least one element, in this case the identity in G. If the kernel only contains this element we say that it is **trivial.** However, if f is not one-to-one we immediately know that where f fails to be one-to-one will yield to a kernel with more than 1 element. If the kernel is indeed trivial (contains only one element, i.e. 1_G) then f is one-to-one (because if it were not we could use that element and the inverse property of groups to get another element of the kernel).

Proposition 20. *Suppose $f : G \to H$ is a homomorphism. Then $ker(f)$ is a subgroup of G.*

Proof. The proof is trivial. First, note that indeed $ker(f) \subset G$ simply by the definition that each element of the kernel is in G. Next, consider that 1_G is always in $ker(f)$ and so it has an identity. Suppose $g \in Ker(f)$ then, $f(g) = 1_H$. But then $f(g^{-1}) = 1_H^{-1} = 1_H$ by properties of group homomorphisms and identities. Finally, take $g, h \in ker(f)$ consider $f(gh) = f(g)f(h) = 1_H 1_H = 1_H$ and so $gh \in ker(f)$. Thus, the $ker(f) \subset G$ is a group and closed under the group operation and thus a subgroup of G. □

Example 21. Consider $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = e^x$. Note that this has the property,

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

So this is a homomorphism from the group of reals with addition to the non-zero real numbers under multiplication. This is not onto. But, it is isomorphic from $\mathbb{R}, + \to \mathbb{R}_{++}, \cdot$.

Example 22. Consider $\det AB = \det A \det B$. So this is a homomorphism from $GL_n(\mathbb{R})$ ($n \times n$ invertible linear maps) to $\mathbb{R}$. The kernel of this map is $SL_n(\mathbb{R})$ which is the special linear group or the group of $n \times n$ matrices with determinant equal to 1, thus we know that this map is not injective.

Example 23. Consider the circle group, S^1, given by points (x, y) such that $x^2 + y^2 = 1$. The group operation is given by $s_1s_2 = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1)$. In polar coordinates, this is equivalent to $s_1s_2 = (\cos\theta_1 \cos\theta_2 - \sin\theta_1 \sin\theta_2 = \cos(\theta_1 + \theta_2), \sin(\theta_1 + \theta_2))$ where $s_1 = (x_1, y_1) = (\cos\theta_1, \sin\theta_1)$ and the same for s_2. Then there is a map,

$$f : \mathbb{R} \to S^1 \text{given by} \theta \mapsto (\cos\theta, \sin\theta)$$

And by our group operation $f(\theta_1 + \theta_2) = f(\theta_1)f(\theta_2)$. The kernel is every $\theta \in \mathbb{R}$ such that $\cos\theta = 1$ and $\sin\theta = 0$ which is any integer multiple of 2π.

1.3 Cyclic Groups and Lagrange's Theorem

We can define the integer powers of an element of a group, $g \in G$, as,

$$g^k = \begin{cases} gg\cdots g & k > 0 \\ 1 & k = 0 \\ g^{-1}g^{-1}\cdots g^{-1} & k < 0 \end{cases}$$

Notice that like the exponential map, integer powers also define a homomorphism because,

$$g^{k+l} = g^k g^l$$

And $g^0 = 1$. Thus, the powers of an element $g \in G$ form a subgroup, **the cyclic group generated by** g. If all the powers of g are different then this subgroup (and thus the encompassing group) are infinite. If they are not, then we have for some k, l that,

$$g^k = g^l \implies g^{k-l} = 1$$

Definition 24. The **order of an element** denoted $ord(g)$ is the least $n \in \mathbb{N}$ such that $g^n = 1$. If no natrual n exists then $ord(g) = \infty$.

This definition makes sense because after the lowest such n the powers of g begin to repeat. This is made clear in the next proposition.

Proposition 25. *Suppose* $ord(g) = n$ *then,*

1. $g^m = 1 \iff n|m$
2. $g^k = g^l \iff k \equiv l (\mod n)$

Proof. For 1 write for remainder r,

$$m = qn + r$$

Then,

$$1 = g^m = (g^n)^q g^r = 1g^r = g^r$$

So $r = 0$. For 2 notice that,

$$g^{k-l} = 1 = g^n$$

Which by part 1 implies that,

$$n|k - l$$

But then $k - l = qn$ so $k \equiv l (\mod n)$ □

Definition 26. A group G is called **cyclic** if there is an element $g \in G$ called a **generator** such that $\langle g \rangle = G$.

1.3.1 Cosets

To prove Lagrange's theorem we must add some additional structure. Suppose G acts on a set S. Pick $s \in S$ and look at $H = \{g \in G : gs = s\}$. This is clearly a subgroup of G because $ggs = g(gs) = gs = s$, $1s = s$, and $s = g^{-1}gs = g^{-1}s$. Note that this is essentially a subgroup of "fixed points".

Pick some $s \in S$ for some H as defined above. Then $t_1 = g_1 s, t_2 = g_2 s$ and notice that $g_2^{-1} g_1 s = g_2^{-1} s = s$ so that $g_2^{-1} g_1 \in H$ but also that $g_1 \in g_2 H$. $g_2 H$ is an object called the **left coset of** H. For some $t \in S$ we can have the map,

$$\begin{aligned} t &\to \{g \in G : gs = t\} \\ gs &\longleftarrow gH \end{aligned}$$

This implies that the left cosets are just elements of a set acted on by G. Notice that this is "left" but we could just as easily have right cosets if G acts on the set from the right. More generally we can do this for any subgroup H of G,

Definition 27 (Congruence Modulo)**.** We say that $g_1, g_2 \in G$ are **congruent modulo** H if,

$$g_2^{-1} g_1 \in H$$

That is, $g_1 = g_2 h$ for some $h \in H$. We can denote this using the notation.

$$g_1 \equiv g_2 \pmod{H}$$

Indeed **congruence modulo** H defines an equivalence relation.

The classes of this equivalence relation are given by left cosets.

Definition 28 (Cosets)**.** For some subgroup H of G the **left coset** is given by,

$$gH = \{gh : h \in H\}$$

Since in general we do not know that the group is Abelian we also define the **right coset** by,

$$Hg = \{hg : h \in H\}$$

Similarly we call the (left) **stabilizer**,

$$G_h = \{g \in G : gh = h\}$$

Definition 29 (Orbit)**.** Let G be the transformation group of some set X. We say that $x, y \in X$ are equivalent with respect to G or $x \overset{G}{\sim} y$ if there exists a $g \in G$ such that $y = gx$. The different equivalence classes of x are called its **orbit**. That is, the orbit of x under G is,

$$Gx = \{gx : g \in G\}$$

Remark 30. Given a group G and the subgroup $H = \{g \in G : gs = s\}$ for some $s \in S$ is it possible to reconstruct S? Yes! S is given by the set of left cosets of H. First, notice that cosets do not overlap. Suppose $g_1 H$ and $g_2 H$ do overlap then,

$$g_1 h_1 = g_2 h_2 \implies g_1 = g_2 h_2 h_1^{-1} = g_2 h_3 \implies g_1 H = g_2 \underbrace{h_3 H}_{H}$$

Because for all $h' \in H$ we have $h's = s$ and so $h_3 h' s = h_3 s = s$. That is a group action on itself yields itself, $g \in G, s \in S = G \implies g(s) = gs \in S = G$. So if two cosets have any single element in common then they must be the same. Thus, G is the disjoint union of cosets, gH. Also G acts on the cosets by $g(g_1 H) = g g_1 H$ which is a group action. If G is finite then G is made up of a finite union of cosets $g_1 H, \ldots, g_n H$.

Proposition 31. *Suppose G is a group and H is a subgroup then any cosets gH will have the same size as the order as H.*

Proof. Notice that $gH = \{gh : h \in H\}$ thus there will be exactly the same number of elements as H. Now we just need to make sure there are no duplicate elements. Suppose $gh_1 = gh_2$. Then since $g^{-1} \in G$ we have $h_1 = g^{-1} g h_2 = h_2$. So there cannot be any duplicates. □

Remark 32. Note that while H is a group, the cosets gH need not be groups. *Borcherds notes* that that this result uses the fact that all group elements have inverses (i.e. they are bijections). If we had omitted the need for inverses in our group we would get an object called a **semi-group**. We still can define cosets for semi-groups but we cannot say that each coset has the same size.

1.3.2 Lagrange's Theorem

We are now ready for Lagrange's theorem.

Theorem 33 (Lagrange's Theorem)**.** *The order of a subgroup H of a finite group G divides the order of G. That is, $|H|$ divides $|G|$ with zero remainder.*

Proof. Suppose $|G| = n$ and $|H| = k$. Notice that G is the disjoint union of the cosets of H. Suppose there are $q = |G : H|$ (sometimes called the **index of subgroup** H) such cosets. Then $n = qk$ which implies that $|H|$ divides $|G|$ or $k|n$. □

Corollary 34. *Given an element, $g \in G$, its order, $ord(g)$ also divides the order of G.*

Proof. Note that for $g \in G$ we have that $\langle g \rangle = \left\{1, g^2, \ldots, g^{n-1}\right\} \subset G$. Furthermore since $g^k g^l = g^{k+l} \in \langle g \rangle$ either because $k + l < n$ or because $n|k - l$ and indeed $\left(g^k\right)^{-1} = g^{-k}$. Thus, the cyclic subgroup is indeed a subgroup of G and so it's order must divide the order of G by Lagrange's theorem. □

Corollary 35. $|G| = |H| \times$ *number of cosets* $= |H|\,|G/H|$.

Remark 36. This is very useful in finding the order of some unknown group $|G|$ because it means we can try to just find a subgroup whose order we know and work out how many cosets there are by identifying the cosets with some geometric object that the group acts on. For example, imagine trying to find the order of an icosahedran. This is a platonic solid with 20 triangular faces. So we know the triangular group of order 3 is a subset and there are exactly 20 cosets and thus we have that the order of the icosahedral group is 60.

Remark 37. We can use this tool to classify all groups of order p for some prime p. The order of an element divides the order of G so if $|G| = p$ then the order of any element must be either 1 or p. If $ord(g) = p$ then that means that $G = \left\{1.g, g^2, \ldots\right\}$ and is thus a cyclic group denoted by $\mathbb{Z}/p\mathbb{Z}$. That is, $G \cong \mathbb{Z}/p\mathbb{Z}$.

Corollary 38. *If $|G| = n$ then $g^{|G|} = 1$ for every $g \in G$.*

Proof. Let $ord(g) = m$ we know that $m|n$. Thus, $g^n = 1$. □

Example 39 (Fermat's Little Theorem)**.** $x^p \equiv x \pmod p$ for some prime p. Define the cyclic multiplicative group $G = (\mathbb{Z}/p\mathbb{Z})^*$. All the nonzero elements have an inverse. So $ax + bp = 1$ by Euler's theorem. Also $|G| = p - 1$. Then for all $x \in G$ we have $x^{p-1} \equiv 1 \mod p$. This is useful because take for example $z^{10} - z$ this will be divisible by 11 for all integers z by this theorem.

A generalization is due to Euler. If x is coprime to $m > 0$ then $x^{\varphi(m)} \equiv 1 \pmod m$. Note that $(\mathbb{Z}/m\mathbb{Z})^*$ forms a group so $x^{|G|} \equiv 1 \pmod m$ if $x \in G$ or that x is coprime to m. $|G| = \varphi(m)$ by definition which is called Euler's function, which is a function on the natural numbers. An example of this might be,

$$(\mathbb{Z}/12\mathbb{Z})^* = \{1, 5, 7, 11\}$$

Which are the coprimes of 12. Well, $\varphi(12) = 4$ so this says each of these elements are congruent to 1 under modulo 12.

1.3.3 Burnside's Lemma

Suppose we have a group G that acts on a set S we may be curious to know how many orbits there are. Recall, that two elements of S are in the same orbit if there is some $g \in G$ that can map between them. Thus, we are essentially asking the question how many ways are there to arrange S up to symmetry. The answer to this question is given by Burnside's lemma. First, we prove the following theorem that will be helpful in proving Burnside's lemma.

Theorem 40 (Orbit-Stabilizer Theorem)**.** *There is a one-to-one correspondence between an orbit Gx and the set of cosets G/G_x that maps $y = gx \in Gx$ to gG_x.*

Proof. Take $g_1, g_2 \in G$ then if,

$$\begin{aligned} g_2 \in g_1 G_x &\iff g_1 \equiv g_2 \pmod{G_x} \\ &\iff g_1^{-1} g_2 \in G_x \iff g_1^{-1} g_2 x = x \iff g_2 x = g_1 x \end{aligned}$$

Thus, if we take some $g_1, g_2 \in G$ that are in the same coset of G_x they must map to the same point in the orbit Gx. □

Remark 41. This implies that there is a correspondence between the number of cosets of a stabilizer and the number of elements in an orbit.

Corollary 42. $|G| = |Gx|\,|G_x|$.

Proof. Lagrange's theorem gives us that since G_x is a subgroup,

$$|G| = |G : G_x|\,|G_x|$$

But, notice that the index $|G : G_x|$ is equal to the number of cosets of G_x which by the orbit-stabilizer theorem is equal to the size of the orbit $|Gx|$. Thus, $|G| = |Gx|\,|G|$. □

Remark 43. If G acts on a set then the size of G must be equal to the size of the set times a subgroup fixing one element. For example, suppose $|G| = 12$ and $|Gs| = 6$ that means that every other time an element of G acts on s it produces an element we have already seen. But that exactly means that there must be 2 $g, g' \in G$ such that $g's = gs = s$ so $|G_s| = 2$. If $|Gs| = 12$ that would mean there was only one $g \in G$ that $gs = g$ – the identity element.

Theorem 44 (Burnside's Lemma)**.** *The number of orbits of a finite set S acted on by a finite group G is the average number of fixed points. That is,*

$$\textit{Number of orbits of } S := |S/G| = \frac{1}{|G|} \sum_{g \in G} |S^g|$$

where $S^g = \{gs = s : s \in S\}$.

Proof. We want to look at the number of pairs (g, s) where $gs = s$ for $g \in G$ and $s \in S$. We can count this by summing over the elements g so the number of pairs is given by,

$$\sum_{g \in G} |S^g|$$

Furthermore, we can also sum over all elements S so that the number of pairs is given by,

$$\sum_{s \in S} |G_s|$$

where $G_s = \{g \in G : gs = s\}$ which forms a subgroup of G called the **stabilizer** of s. Furthermore, by the orbit-stabilizer theorem,

$$|G_s| = \frac{|G|}{|Gs|}$$

Then,

$$\sum_{s \in S} |G_s| = \sum_{Gs \in \underbrace{GS}_{\text{Set of all Orbits}}} |Gs| \frac{|G|}{|Gs|} = |G| \cdot \underbrace{|S/G|}_{\text{Number of Orbits}}$$

But then,

$$\begin{aligned} \sum_{g \in G} |S^g| &= |G|\,|S/G| \\ \implies |S/G| &= \frac{1}{|G|} \sum_{g \in G} |S^g| \end{aligned}$$

Finishing the result. □

1.4 Normal and Quotient Groups

Suppose $H \subset G$ and H is a subgroup. Can we form a **quotient group** G/H? The idea is that this forces all the elements of H to be trivial. For example, take the cyclic group $\mathbb{Z}/n\mathbb{Z}$we force all multiples of n to be trivial!

In general, we can get an exact sequence,

$$I \to H \to G \to G/H \to I$$

So what we do is define the set G/H as the set of left cosets of H. But is this a group with a sensible group structure? To make it so we define the quotient group operation for $g_1, g_2 \in G$ as,

$$(g_1H)(g_2H) = g_1g_2H$$

Is this well defined? Suppose $g_3 = g_1H$ then,

$$g_3g_2H = g_1g_2H?$$

$$\implies g_1hg_2H = g_1g_2H \iff g_1\left(g_2g_2^{-1}\right)hg_2H = g_1g_2\left(g_2^{-1}hg_2\right)H = g_1g_2H$$

Notice that this will hold if and only if $g_2^{-1}hg_2 \in H$! If this is always in H then we have a well defined multiplication on cosets and so we can define a **quotient group** and we call H a **normal subgroup**.

Definition 45. Given a group G and a normal subgroup H. The **quotient group** G/H (if it exists) is the set of all left cosets of H (i.e. $G/H = \{gH : g \in G\}$) with operation $(g_1H)(g_2H) = g_1g_2H$.

Remark 46. The quotient group is not a subgroup of the original group. It is a group of the left cosets of the group.

Example 47. Take the group $\mathbb{Z}^+$ and a subgroup $5\mathbb{Z}^+$. Then we can partition $\mathbb{Z}$ by $\{0+5\mathbb{Z}, 1+5\mathbb{Z}, 2+5\mathbb{Z}, 3+5\mathbb{Z}, 4+5\mathbb{Z}\}$ because $\{1,2,3,4\}$ are all the remainders of the integers when diving by 5. Furthermore, $5\mathbb{Z}^+$ is a normal subgroup because for some $g \in \mathbb{Z}^+$ we have $g(5\mathbb{Z})g^{-1} = g + 5\mathbb{Z} - g = 5\mathbb{Z}$satisfying property 2 below. Thus we can form the quotient group (what we have before called a cyclic group over the integers modulo 5) $\mathbb{Z}/5\mathbb{Z} = \{5\mathbb{Z}, 1+5\mathbb{Z}, 2+5\mathbb{Z}, 3+5\mathbb{Z}, 4+5\mathbb{Z}\}$ note that all the elements $h \in 5\mathbb{Z}$ are mapped to the identity in this group and that we have essentially divided the group $\mathbb{Z}$into 5 left cosets (equivalence classes) hence the term quotient group.

Proposition 48 (Normal Subgroup Conditions)**.** *The following are equivalent,*

1. *H is the kernel of some map $G \to X$.*
2. *$gHg^{-1} = H$ for all $g \in G$.*
3. *$gH = Hg$ for all $g \in G$.*
4. *Left cosets are the same as right cosets.*
5. *Quotient group G/H exists defined as above, i.e the cosets form a group.*

Definition 49. If H satisfies any of the conditions in Proposition 48 then we say that it is a **normal subgroup** we sometimes denote this as $H \lhd G$.

Proof. 2 implies 3: $gHg^{-1} = H \iff gH\left(g^{-1}g\right) = gH = Hg$. 3 implies 4 by definition of left costs as gH and right cosets as Hg. 4 implies 5 because if the right/left cosets are the same we have $gH = Hg \implies gHg^{-1} = H$. Then, take two cosets g_1H and g_2H and note that,

$$(g_1H)(g_2H) = g_1\left(g_2g_2^{-1}\right)Hg_2H = \underbrace{g_1g_2}_{\in G}\underbrace{\left(g_2^{-1}Hg_2\right)}_{=H \text{ by } 4}H$$

$$= g_1g_2H = g_3H$$

Hence the group operation is closed. If $g_1 = I \in G$ then we have $g_1 H = IH \in G/H$ and $(IH)(g_2 H) = Ig_2 H = g_2 H$ hence the identity element is in the group. Furthermore, $g_2^{-1} \in G$ and so $g_2^{-1} H \in G/H$ thus we have,

$$\left(g_2^{-1} H\right)(g_2 H) = g_2^{-1} g_2 H = H$$

Hence, G/H has inverses and thus satisfies the group axioms. Finally, we show 5 implies 2. If G/H exists and is a group we want to show that $g^{-1}Hg = H$ to do this first we show that $g^{-1}Hg \subset H$ to see this note take $g_1 H$ and $g_2 H$ and pick an element from each say $g_1 h_1$ and $g_2 h_2$ we know by assumption that G/H is a group that $(g_1 h_1)(g_2 h_2) \in g_1 g_2 H$ then,

$$\begin{aligned}
(g_1 h_1)(g_2 h_2) &= g_1 g_2 h_3 \\
\iff g_1^{-1}(g_1 h_1)(g_2 h_2) &= g_1^{-1} g_1 g_2 h_3 \\
\iff h_1 g_2 h_2 &= g_2 h_3 \\
\iff g_2^{-1} h_1 g_2 h_2 &= h_3 \\
\iff g_2^{-1} h_1 g_2 h_2 h_2^{-1} &= \underbrace{h_3 h_2^{-1}}_{\in H} \\
\implies g_2^{-1} h_1 g_2 &\in H
\end{aligned}$$

Now we need to show that $g^{-1}Hg \supset H$. Take some $h \in H$ then,

$$\begin{aligned}
h = g^{-1} g h &= \left(g^{-1} h_1\right)(g h_2) \\
\iff \underbrace{h h_2^{-1}}_{\in H} &= g^{-1} h_1 g \\
\implies h h_2^{-1} &\in gHg^{-1}
\end{aligned}$$

Which finishes the proof because 2 → 3 → 4 → 5 → 2. □

Proposition 50. *If G is Abelian then all subgroups are normal.*

Proof. Commutative implies $gH = Hg \iff gHg^{-1} = H$. □

Example 51. Consider S_3 the symmetric group of 3 elements (consider permutations of $\{0, 1, 2\}$ and note that $|S_3| = 6$). First, I, S_3 are both normal subgroups of S_3. Consider $H = \{1, (123), (132)\}$ note that $|G : H| = 2$. Also note that we can map left to write cosets by $gH \mapsto (gH)^{-1} = H^{-1}g^{-1}$. This map is one-to-one so we know that there is the same number of cosets. Then, all subgroups of index 2 must be normal! This is because there are only two cosets one with everything in H and one with everything not in H but then this is exactly the same for the right coset so the left and right cosets are the same! Which gives us the following fact.

Fact 52. *Subgroups of index 2 are always normal.*

Example 53. $\{1, (12)\} \subset G$ with order 2 and index 3. This is not normal because left and right cosets are not the same!

Definition 54 (Conjugate action on Subgroup)**.** Let G be a group with $g \in G$ and subgroup H then the **conjugate action** is $g(H) = gHg^{-1}$.

Definition 55. We say that two subgroups H_1 and H_2 of a group G are **conjugate** if for some $g \in G$ we have $gH_1g^{-1} = H_2$ with exact equality. We may also say that two elements $g_1, g_2 \in G$ are conjugate if there is a $g_3 \in G$ such that $g_3 g_1 g_3^{-1} = g_2$.

Remark 56. The operation of taking ghg^{-1} is called **conjugation** and it essentially measures how normal a group is (since if H is normal we have $ghg^{-1} = h$). Furthermore, conjugation defines an equivalence relation and we can divide a group into conjugacy classes of elements.

Remark 57. Conjugation is a symmetry of the group. So it will persevere structure such that if one subgroup is not normal then its conjugates are also not normal. A normal subgroup will always be invariant under conjugation by any element. This is because these groups obey $gH = Hg$ for all $g \in G$ so,

$$g(H) = gHg^{-1} = gg^{-1}H = H$$

Remark 58. Suppose G has a normal subgroup H then,

$$I \to H \to G \to G/H \to I$$

and H and G/H will usually be smaller than G but will maintain many of the same properties. This does not determine G of course (because of non-split sequences) but it can give us a lot of information.

Definition 59 (Simple Group)**.** Suppose that G is a group. Then it has *normal* subgroups $\{I\}, G$. If these are the only normal subgroups of G then we say G is a **simple group.**

2 Group Products

2.1 Direct Products

Consider a group of order 4. By Lagrange's theorem we know that it has subgroups of order 1,2,4. If there is some element of order 4 say $g \in G$ with,

$$\langle g \rangle = \left\{1, g, g^2, g^3\right\} \cong \mathbb{Z}/4\mathbb{Z}$$

Thus, we can classify this group as cyclic. Instead, let us assume that all elements $x \in G$ have the property that $g^2 = 1$. Then, take $x, y \in G$ and note that,

$$\begin{aligned} 1 &= y^2x^2 = (yx)^2 = yxyx \\ \implies x^{-1} &= x = yxy \implies x^{-1}y^{-1} = yx \\ \implies & xy = yx \end{aligned}$$

Hence, we see that this group is commutative. So now we will attempt to classify all groups with $x^p = 1$ for some prime p (for example $p = 2$ as above). Then, G with the operation $+$ is a vector space over some field F_P with p elements. Note that since we are considering a group operation of addition we switch our notation so that,

$$x^p = 1 \iff px = 0$$

Now note that $G \cong F_p^n$ because each dimension of a vector space is simply isomorphic to the field that it is over. Thus, $|G| = p^n$. We call such groups **elementary Abelian groups**.

Going back to $p = 2$ and G with order 4 we have exactly two possible groups of order 4 to consider. We can have the one dimensional group that is isomorphic ot the cyclic group with $p = 4$ or we could have a 2 dimensional group in which each dimension is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ (since its order is computed as $p^n = 2^2 = 4$). So,

$$\mathbb{Z}/4\mathbb{Z}, \qquad \underbrace{\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z}}_{\text{This is the Klein 4 Group - symmetries of a rectangle}}$$

Definition 60 (Direct Sum)**.** The **direct sum** of (additive) groups $G_1 \oplus \cdots \oplus G_k$ consists of all sequences $(g_1, \ldots, g_k)$ with $g_i \in G$ where the group operation is applied component-wise.

Example 61. $\mathbb{Z}^3 = \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$.

Remark 62. Typically direct sums are used to describe additive groups and *direct products* are used to describe the multiplicative groups. However, the definitions are compatible modulo notation and how we define $g = (g_1, \ldots, g_k)$ (i.e. as $g = g_1 \cdots g_k$).

Definition 63 (Product Group)**.** Suppose we have two groups G and H then we can define a **product group**, $G \times H$, where we simply take take the product of their sets and define the group operation as,

$$(g_1 \times h_1)(g_2 \times h_2) = g_1 g_2 \times h_1 h_2 = (g_1 g_2, h_1 h_2)$$

Or if $G = G_1 \times \cdots \times G_k$ we write the operation for $gh \in G$ as,

$$gh = (g_1 \cdots g_k)(h_1 \cdots h_k) = (g_1 h_1, \ldots, g_k h_k)$$

Equivalently, if a group G decomposes into a **direct product** of subgroups $G_1, \ldots, G_k$ if:

1. every element $g \in G$ can be written as $g = g_1 \cdots g_k$,$g_i \in G_i$.
2. $g_i g_j = g_j g_i$

An equivalent definition can also be given using normal subgroups.

Definition 64 (Direct Product Group)**.** We say a group G is isomorphic to a direct product of M and N if there exists subgroups H and K of G such that,

1. $H \cong M$ and $K \cong N$.
2. H and K are normal groups.
3. $H \cap K = \{I\}$.
4. $G = HK := \{hk : h \in H, k \in K\}$.

Remark 65. Take $h \in H$ and $k \in K$ if $hk = kh$ then $k^{-1}hk = h$ and $hkh^{-1} = k$ hence both groups must be normal which is why we can rewrite the definition in terms of these groups. We will see why this is useful later when we discuss semi-direct products.

Example 66. Take $\mathbb{Z}^+$ and $G^\times = \{1, -1, i, -i\}$. Then the direct product is $\mathbb{Z}^+ \times G^\times = \{(a, b) : a \in \mathbb{Z}^+, b \in G^\times\}$ with group operation $xy = (x_1 + y_1, x_2 \times y_2)$. For example $(5, 2)(2, i) = (7, 2i)$.

Proposition 67. *Suppose G has subgroups A, B and A, B commute and every element of G is of the unique form $ab, a \in A, b \in B$ then,*

$$G \cong A \times B$$

Proof. There is a homomorphism from $A \times B$ defined by $f : a, b \to ab$ and if this happens uniquely then it is also a bijection. □

Proposition 68. *A group G decomposes into a direct product of subgroups say $G_1 \times G_2$if and only if,*

1. *G_1 and G_2 are normal.*
2. *$G_1 \cap G_2 = \{I\}$*
3. *For all $g \in G$ we have $g = g_1 g_2$ for $g_1 \in G_1$and $g_2 \in G_2$.*

Proof. TODO □

Example 69. Examples of product groups:

1. $\mathbb{R}^* \cong \{1, -1\} \times \mathbb{R}_{++}$ (positive reals).
2. $\mathbb{C}^* = S^1 \times \mathbb{R}_{++}$ circle group and positive reals, i.e. polar decomposition).
3. $(\mathbb{Z}/(mn)\mathbb{Z})^* \cong (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$ where mn is coprime. Recall, the $*$ signifies that we use multiplication as the operation instead of addition and only take the coprime elements. Recall, two elements are coprime if their only integer divisor is 1 (i.e. 3 and 5).
4. $\mathbb{Q}^* = (\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots) \times \mathbb{Z}/2\mathbb{Z}$because every rational number $q = \pm 2^{n_1} 3^{n_3} \cdots$
5. Let G be the group of all roots of unity of complex numbers, that is all $z \in \mathbb{C}$ such that $z^2 = 1$ (this group looks like a circle which you would not expect to split). $G = R_2 \oplus R_3 \oplus R_7 \oplus \cdots$ this are roots of order $2^n, 3^n$ and so on.

2.2 Semi-direct Products

2.2.1 Automorphisms

Recall that automorphisms are isomorphisms of a group onto itself.

Example 70. The map $X \to \left(X^T\right)^{-1}$ is an automorphism of $GL(n)$.

Definition 71 (Automorphism Group)**.** The automorphisms of a group G form a group themselves. We denote the **automorphism group** as $Aut(G)$. To define this group note that the map $a(g) : x \mapsto gxg^{-1}$ for $g \in G$ and $x \in G$ is an automorphism. To see this note that,

$$a(g)(xy) = gxyg^{-1} = \left(gxg^{-1}\right)\left(gyg^{-1}\right) = \left(a(g)x\right)\left(a(g)y\right)$$

So it is homomorphic and indeed defines an isomorphism. This particular automorphism is called the **inner automorphism defined by** g.

Then the map $f : g \mapsto a(g)$ is a homomorphism from G to $Aut(G)$. We find that the **center**,

$$Z = \ker f = \{h \in G : gh = hg \text{ for all } g \in G\}$$

Furthermore, the image of f is the **group of inner automorphisms defined by** g denoted by $Inn(G)$. Such that,

$$Inn(G) \cong G/Z$$

Suppose we have subgroups A and B such that $G = AB := \{ab : a \in A, b \in B\}$ uniquely as defined by the right action of A on B. The right action is defined as for any $a \in A, b \in B$ we have $(b)a = b^a$ which preserves products of b because $(b_1b_2)a = (b_1b_2)^a = b_1^a b_2^a$ and $((b)a_1)a_2 = (b^{a_1})a_2 = b^{a_1a_2}$thus this a homomorphisms from A to $Sym(B)$.

2.2.2 Semi-direct Products

Problem 72. Now suppose we have groups A and B and right action of A on B. Can we construct a group G from these so that A is a normal subgroup, B and is subgroup and the action is given by conjugation?

Solution 73. Naturally we can define $G = A \times B$ and define the operation $(a_1b_1)(a_2b_2) \mapsto (a_1a_2)(b_1^{a_2}b_2)$. Then all we need to do is show associativity. Take $a_1b_1, a_2b_2, a_3b_3 \in G$ and consider,

$$\begin{aligned} (a_1b_1)(a_2b_2) &= a_1a_2b_1^{a_2}b_2 \\ (a_1a_2b_1^{a_2}b_2)(a_3b_3) &= a_1a_2a_3\left(b_1^{a_2}b_2\right)^{a_3}b_3 \\ &= a_1a_2a_3b_1^{a_2a_3}b_2^{a_3}b_3 \\ \iff a_1b_1\left((a_2b_2)(a_3b_3)\right) &= a_1b_1\left(a_2a_3b_2^{q_3}b_3\right) \\ &= a_1a_2a_3b_1^{a_2a_3}b_2^{a_3}b_3 \end{aligned}$$

Which shows associativity. Showing identity and inverse is simple. This group is called the semi-direct product of A and B defined formally below.

Definition 74 (Semi-direct Product)**.** A group G decomposes into a **semi-direct product** of subgroups M and N if G has subgroups A and B such that,

1. $A \cong N$ and $B \cong M$.
2. A is a normal subgroup of G, i.e. $A \lhd G$.
3. $A \cap B = \{I\}$.
4. $G = AB := \{ab : a \in A, b \in B\}$.

and we write $G = A \ltimes B$ (or $G = B \rtimes A$). The conjugate action $a \mapsto b^{-1}ab$ in $A \ltimes B$ is the same as the right action of B on A. We can also form a semi-direct product with a left action by $B \rtimes A$ where now B is the normal subgroup (the line should be opposite of the normal subgroup).

Proposition 75. *If $G = A \ltimes B$ is finite. Then, $|G| = |A|\,|B|$.*

Proof. This is immediate from property 3 and we know there are no nontrivial duplicates by property 2. □

Example 76. $S_3 \cong \mathbb{Z}/2\mathbb{Z} \ltimes \mathbb{Z}/3\mathbb{Z}$=$\{\{1\},\{12\}\} \times \{\{1\},(132),\{123\}\}$.

Remark 77. Groups of order 6 can be classified using semi-direct products.

1. If G has order 6 then it has an element of order 3 and this subgroup must be normal because all subgroups of index 2 must be normal.

2. It also must have an element of order 2.

So G is a semi-direct product of A and B where $|A| = 3$ and $|B| = 2$. What is the action of B on A? How can a group of order 2 act on a group of order 3. The solution is to look at automorphisms of the subgroup of order 3. All the automorphisms must also map into groups of order 3 so there are exactly two automorphisms,

$$g \mapsto g, g \mapsto g^{-1}$$

So either B acts trivially on A and so we get a direct product $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} = \mathbb{Z}/6\mathbb{Z}$or it acts non-trivially and $\langle g \rangle = \mathbb{Z}/3\mathbb{Z}$ and $g^b = g^{-1}$.

Example 78. $ax + b$ forms a group of transformations on $\mathbb{R}$ of the form $\begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$ with $x \mapsto ax + b$. This has a normal subgroup of all translations $x \mapsto x + b$ and a subgroup $x \mapsto ab$. These operations do not commute.

2.3 Group Extensions

Definition 79 (Short Split and Non-split Extensions)**.** Consider a sequence of maps between groups,

$$I \to A \underbrace{\to}_{f} B \underbrace{\to}_{g} C \to I$$

where I is some group identity. If this sequence is **exact** we say that B is an extension of C by A.

We say that this sequence is **exact at** B if these maps are homomorphisms of groups and the image of f is exactly the kernel of g,

$$\text{im}(A) = \ker g \implies C \cong B/\text{im}(f)$$

We say that this sequence is **split** if there is a homomorphism $h : C \to B$ such that $g \circ h$ is the identity map on C(i.e. $B = Z \times W$). Furthermore, if the groups are Abelian then,

$$B \cong A \oplus C$$

Definition 80 (Extension)**.** We say that G is isomorphic to an **extension** of M by N if there exists a subgroup H of G such that,

1. $H \cong M$.

2. H is a normal subgroup of G.

3. $G/H \cong N$.

We might sometimes denote this with the diagram,

$$I \to H \to G \to N \to I$$

Example 81. In our Abelian group of order 4 example we have two possibilities for what B might be. We could have non-split sequence:

$$I \to \mathbb{Z}/2\mathbb{Z} \to Z/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to I$$

Or we could have a split sequence:

$$I \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to I$$

Example 82 (Groups of Order 8)**.** Consider classifying a group G of order 8. We know it's subgroups are of order $1, 2, 4, 8$. We know that if it is of order 2 we can simply classify G as $\mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z} + \mathbb{Z}/2\mathbb{Z}$.So what if the subgroup H is of order 4? Well $|G : H| = 2$ so H must be normal and $H = \left\{1, g, g^2, g^3\right\}$. We can also use *extensions*,

$$I \to \mathbb{Z}/4\mathbb{Z} \to G \to \mathbb{Z}/2\mathbb{Z} \to I$$

Which is saying that the subgroup $H \cong \mathbb{Z}/4\mathbb{Z}$ and that $G/H \cong \mathbb{Z}/2\mathbb{Z}$. This is an extension problem because we have an exact sequence,

$$I \to A \to G \to B \to 1$$

We know A and B and we want to figure out G. In fact, we say that G is an **extension of** B **by** A**.** We know that B normalizes A so we have six option,

$$b^{-1}ab = a \text{ or } b^{-1}ab = a^{-1}$$

with

$$b^2 = 1\text{or } b^2 = a \text{ or} b^2 = a^2$$

The most interesting of the options are $b^2 = a^2$ with $b^{-1}ab = a^{-1}$ because this implies that $b^4 = a^4 = 1$. This turns out to be the quaternion group of order 8 or Q_8. So,

$$A = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, B = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

And,

$$G = \left\{ \pm a, \pm b, \pm c, \pm \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}$$

Which gives Hamilton's ring of quaternions $a^2 = b^2 = c^2 = abc = -1$.

2.3.1 Review of Direct Products, Semi-direct Products, and Extensions

When we look at the definition of direct products, semi-direct products, and extensions using normal subgroups it is clear that direct products are a special case of semi-direct products which are a special case of extensions.

Remark 83. There are several different things to notice about the relationship of these objects.

1. If $G = HK$, $H \lhd G$, and $H \cap K = \{I\}$ then $K \cong G/H$ via the natural projection.

2. Direct products are also the least general. Notice that as we have seen before if $H \lhd G, K \lhd G$ and $H \cap K = \{I\}$ then clearly $hk = kh$ for all $h \in H, k \in K$.

3. However, semidirect products are more general (and thus more complicated) because the second subgroup need not be normal and so the above argument is false.

   (a) An example we considered was S_3 where we use the the normal subrgroup $\mathbb{Z}/3\mathbb{Z}$ and the non-normal subgroup $\mathbb{Z}/2\mathbb{Z}$.

4. In a semi-direct product $G = K \ltimes H$ because H is normal we have $kHk^{-1} = H$. This means that K induces an homomorphism, $K \to Aut(H)$ defined by $k \mapsto \underbrace{\left\{h \mapsto khk^{-1}\right\}}_{Aut(H)}$. If the map is trivial, that is $k \mapsto k$ then we simply have a direct product. There may also be many ways to construct a semi-direct product while there is only one way to construct a direct product.

   (a) A semi-direct product of Abelian groups may not be Abelian.

   (b) A semi-direct of exponent n groups may also not be of exponent n.

5. Extension groups are even more general. In fact, every finite group is a *sequence of extensions* of simple groups. This is the idea behind the analogy of simple groups as building blocks. The sequence itself may not be unique but the simple groups that appear are (Jordan-Holder Theorem).

6. Not every extension is a semi-direct product. Take $\mathbb{Z}/4\mathbb{Z}$ which can be an extension of $\mathbb{Z}_2$ by $\mathbb{Z}_2$.

3 Important Examples of Groups

3.1 Tranformation Groups

3.2 Cyclic Groups

3.3 Dihedral Groups

3.4 Qauternion Group

Definition 84. The quaternion group or Q_8 is a non-abelian group of order 8 given by the set $\{1, i, j, k, -1, -i, -j, -k\}$ under quaternion multiplication defined by the multiplication table,

$\times$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

To make sense of the definition note that the quaternions are written in terms of four basis elements,

$$i = (i, -i)^T, j = (1, -1), k = (i, i), 1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

We can define a ring $\mathbb{H}$ with $a, b, c, d \in \mathbb{R}$,

$$a + bi + cj + dk$$

Notice that the basis elements are anticommutative,

$$ij = -ji, jk = -kj, ki = -ik$$

We can multiply these much how we multiply complex numbers so that for $z \in \mathbb{H}$ with conjugate $\bar{z} = a - bi - cj - dk$ we have,

$$z\bar{z} = a^2 + b^2 + c^2 + d^2 \geq 0$$

Also,

$$(\bar{z_1 z_2}) = \bar{z}_1\bar{z}_2$$

We can also define a norm $||z|| = z\bar{z}$. Then let us take,

$$||z|| = 1 \iff a^2 + b^2 + c^2 + d^2 = 1$$

which forms a 3-sphere which is the group S_3. Much like how for $z \in \mathbb{C}$ we have $|z| = 1$ forms a circle or S_1. **Note that the only spheres that are groups are S_0, S_1, S_3!** Of course, S_0 and S_1 are commutative but S_3 is not.

Take $v \in \mathbb{R}^3 = \{bi + cj + dk\}$ where we have set $a = 0$. Then take $g \in S_3 \subset \mathbb{H}$ then $gvg^{-1} \in \mathbb{R}^3$ which is a rotation in $\mathbb{R}^3$. Notice, that this is super useful because normally we would use 3×3 matrices to represent rotations in 3d but we can do the same with quaternions which are easier to compute!

Remark 85. However, S_3 is not the group of rotations of 3d space instead we have a homomorphism into the rotations of $\mathbb{R}^3$ that is,

$$\phi : S_3 \to SO(3)$$

This map has a nontrivial kernel which is the group of order two consisting of $\{+1, -1\}$. So we can write a sequence,

$$I \to \{1, -1\} \to S_3 \to SO(3) \to I$$

This is called a **double cover** (in this case of the special orthogonal group) which is a group extension of index two. Essentially thsi is a 2 to 1 mapping. Sometimes S_3 is called the **spin group** by physicists because electrons and other fermions have half interval spin.

3.5 General Linear Groups

4 Appendix

4.1 Algebraic Structures

4.1.1 Equivalence Relations

Definition 86 (Equivalence Classes)**.** Suppose R is some equivalence relation on a set M. Recall this means that R is reflexive, symmetric, and transitive. For all $a \in M$ $R(a) = \left\{ b \in M : a \overset{R}{\sim} b \right\}$ so that if $R(a) \cap R(b) \neq \varnothing \implies R(a) = R(b)$. Thus, we can partition M by subsets $R(a)$ called **equivalence classes under** R.

Definition 87 (Quotient Set and Map)**.** The set of equivalence classes under R is called the **quotient set of** M **by** R and is denotes M/R. The map,

$$M \to M/R, \quad a \mapsto R(a)$$

is called the **quotient map.**

Example 88. Consider a group M with $x, y \in M$ and operation $(x, y) \mapsto x * y$. We say that an equivalence relation **agrees** with $*$ if,

$$\left\{ a \overset{R}{\sim} a', b \overset{R}{\sim} b' \right\} \implies a * b \overset{R}{\sim} a' * b'$$

Then we can identify M/R by $R(a) * R(b) = R(a * b)$, i.e. a homomorphism.

4.1.2 Rings, Fields, and Algebras

Definition 89 (Ring)**.** A **ring** is a set R with two operations $+$ and $\cdot$ such that,

1. $(K, +)$ is an abelian group (say the *additive group of R).*
2. A distributive property holds for any $a, b, c \in R$:

$$a \cdot (b + c) = a \cdot b + b \cdot c$$

Proposition 90. *Suppose R is a ring. Then,*

1. *For any $a \in R$ and additive identity $0 \in R$ we have,*

$$0a = a0 = 0$$

2. *For any $a, b \in R$ we have,*

$$a\,(-b) = (-a)\,b = -ab$$

3. *For any $a, b, c \in R$ we have,*

$$a(b - c) = ab - ac \text{ and } (a - b)\,c = ac - bc$$

Proof. For one suppose that $a0 = b$ then,

$$\begin{aligned} b + b &= a0 + a0 = a\,(0 + 0) = a0 = 0 \\ \implies b &= 0 \end{aligned}$$

Let $0a = b$ then,

$$\begin{aligned} b + b &= (0 + 0)\,a = 0a = 0 \\ \implies b &= 0 \end{aligned}$$

For two,

$$\begin{aligned} & ab + a(-b) = a\left(b + (-b)\right) = a0 = 0 \\ \implies & a\left(-b\right) = -ab \end{aligned}$$

For three,

$$a\left(b + (-c)\right) = ab + a\left(-c\right) = ab - ac$$

by property two. □

Definition 91. We say that R is a **commutative ring** if the multiplication operator commutes so that, $ab = bc$. Furthermore, we say that R is an **associative ring** if the multiplication operator is associative so that, $(ab)c = a(bc)$.

Definition 92 (Field (Group Definition))**.** A **field** is a set F with two abelian groups. First, it is an additive abelian group, $(F, +)$, with additive identity 0. Second, it is a multiplicative abelian group of the nonzero elements, $(F/\left\{0\right\}, \cdot)$. F also satisfies distributivity of the multiplicative and additive operations so that,

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$

Remark 93. Notice that a field is a multiplicative group only over the non-zero elements because 0 does not have a multiplicative inverse. We can also write an equivalent definition of fields in terms of rings (see below).

Definition 94 (Field (Ring Definition))**.** A **field**, F, is a commutative associative ring where $0 \neq 1$ (the additive identity does not equal the multiplicative identity) and all nonzero elements are invertible.

Definition 95 (Vector Space)**.** A **vector space** over a field F is a set V with operations of addition and multiplication by elements of F that satisfies for $a, b \in V$ and $\lambda, \mu \in F$,

1. V is an abelian group with respect to the addition operation.
2. $\lambda\left(a + b\right) = \lambda a + \lambda b$
3. $\left(\lambda + \mu\right) a = \lambda a + \mu a$
4. $\left(\lambda\mu\right) a = \lambda\left(\mu a\right)$
5. $1a = a$

Example 96. If K is a subfield of F. Then F is a vector space over K. For example, $\mathbb{C}$ is a vector space over $\mathbb{R}$.

Proposition 97. *A vector space V over a field F with a basis of n vectors is isomorphic to the space F^n.*

Proof. Suppose $\{e_1, \ldots, e_n\}$ is a basis of V. Then define a map $\varphi : V \to K^n$ defined by,

$$a \mapsto a_1 e_1 + \cdots + a_n e_n$$

where $a_i \in K$, $e_i \in V$. This is clearly isomorphic by the distributive and associative properties of multiplication of an element of K with an element of V. □

Example 98. Consider that $\mathbb{C} \cong \mathbb{R}^2$.

Definition 99 (Algebra)**.** An **algebra**, A, is a set over a field F with the operations of addition and multiplication that satisfy the following properties,

1. A is a vector space over F by addition and multiplication .
2. A is a ring with respect to addition and multiplication.
3. $\left(\lambda a\right) b = \lambda\left(ab\right) = a\left(\lambda b\right)$ for all $\lambda \in F$ and $a, b \in A$.

Remark 100. Notice that an algebra need not be commutative in it's multiplicative operation. For example the matrix algebra over $\mathbb{R}$ of $n \times n$ matrices forms an algebra that does not commute in multiplication nor does every element have a multiplicative inverse (matrices of determinant zero).

Example 101 (Algebra of Quaternians)**.** The algebra of quaternions sometimes denoted as $\mathbb{H}$ is given by the basis $\{1, i, j, k\}$. This is also an example of a noncommutative field.

4.2 Isomorphism Theorems

Theorem 102 (First Isomorphism Theorem for Groups)**.** *Suppose G and H are groups and there is a homomorphism $f : G \to H$ then,*

1. *The kernel of f is a normal subgroup of G.*
2. *The image of f is a subgroup of H.*
3. *The image of f is isomorphic to the quotient group $G/\ker f$ or,*

$$Im(f) \cong G/\ker f \iff \varphi : Im(f) \xrightarrow{\sim} G/\ker f$$

Proof. First note that,

$$\begin{aligned} f(g_1) = f(g_2) &\iff f(g_1^{-1}g_2) = I \iff g_1^{-1}g_2 \in \ker f \\ &\implies g_1 \equiv g_2 \pmod{\ker f} \end{aligned}$$

Then for any $a \in g\ker f$ we have that $f(a) = h$ with $h = f(g) \in Im(f)$ because $f(a) = f(g)f(\ker f) = f(g)$ because all $v \in \ker f$ map to the identity. Thus $\varphi : Im(f) \to G/\ker f$ is well defined and bijective. So we just need to show that it is also a homomorphism. Take $g_1, g_2 \in G$ with $f(g_1) = h_1$ and $f(g_2) = h_2$. Then,

$$f(g_1g_2) = h_1h_2$$

And,

$$\varphi(h_1h_2) = g_1g_2\ker f = (g_1\ker f)(g_2\ker f) = \varphi(g_1)\varphi(g_2)$$

Thus, φ is an isomorphism. □

Theorem 103 (Second Isomorphism Theorem for Groups)**.** *Let G be a group and let S be a subgroup of G and N be a normal subgroup of G. Then,*

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