Point-Set Topology: Lecture 29

Ryan Maguire

August 23, 2023

In algebraic topology one uses algebraic structures like groups and vector spaces to solve topological problems. This is usually done by *associating* some algebraic object with a given topological space, and showing that homotopy equivalences or homeomorphisms preserve the nature of this algebraic device. We won't be exploring this route, it deserves its own course. Instead we'll dive into *topological algebra*. Here we reverse the idea, attaching a topology to algebraic structures. In particular we'll discuss *topological groups*, perhaps the simplest object of study in topological algebra. There are a few motivating examples for the study of topological groups.

- A *real topological vector space* is a real vector space $(V, +)$ together with a topology τ that makes vector addition $(v, w) \mapsto v + w$ and scalar multiplication $(a, v) \mapsto av$ continuous operations. The additive nature of vector addition yields an Abelian group, meaning every topological vector space has a canonical topological group associated to it.
- A *Banach space* is a normed vector space (usually over $\mathbb{R}$ or $\mathbb{C}$) such that the metric induced by the norm yields a *complete* metric space. Banach spaces are, in particular, topological vector spaces and the addition of vectors forms a topological group.
- A Lie group is a smooth manifold with a group operation that is *smooth*. Lie groups are, in particular, topological groups.

There is no pre-requesite for algebra in this course, so we'll take the time to develop the basics of group theory.

1 Group Theory

There are a few competing views on how best to describe groups. Some say it is the study of symmetry. One may also view groups as combinatorial objects. I'll take the approach of *generalized arithmetic*. The addition of integers and the multiplication of matrices provide two motivating examples of groups. Many of the theorems involving these two arithmetics need only a few common traits. Groups generalize these traits to abstract objects.

Definition 1.1 (**Group**) A group is an ordered pair $(G, *)$ where G is a set and $* : G \times G \to G$ is a function (called a *binary operation*) that is *associative*, has an *identity*, and contains *inverse elements*. That is:

1. For a, b, $c \in G$ it is true that $a * (b * c) = (a * b) * c$ (Associativity)
2. There is an $e \in G$ such that $a * e = e * a = a$ for all $a \in G$ (Identity)
3. For all $a \in G$ there is a $b \in G$ such that $a * b = b * a = e$ (Inverses)

■

Example 1.1 The integers $\mathbb{Z}$ with addition form a group. That is, $(\mathbb{Z}, +)$ is a group. It is perhaps one of the simplest group structures. Addition is associative, zero serves as an identity, and for all $n \in \mathbb{Z}$, $-n$ is an additive inverse. ■

Example 1.2 The real numbers with addition $(\mathbb{R}, +)$ also form a group. Note that we may identify $(\mathbb{Z}, +)$ as a *subgroup* (defined soon) of the real numbers. ■

Example 1.3 The positive real numbers $\mathbb{R}^+$, together with ordinary multiplication, form a group. That is, $(\mathbb{R}^+, \cdot)$ is a group. Multiplication is indeed associative, and 1 serves as the identity. Since we have excluded 0 from the set, for all $x \in \mathbb{R}^+$, $\frac{1}{x}$ is the inverse of x. ■

Example 1.4 Let $GL_n(\mathbb{R})$ be the set of all $n \times n$ matrices of real numbers with non-zero determinant. That is, all matrices $A \in \mathbb{R}^{n \times n}$ such that A^{-1} exists. This set, together with matrix multiplication, forms a group. This is the *general linear group* of order n. Matrix multiplication is associative, and the identity matrix I_n serves as the identity. Since the set consists solely of invertible matrices, inverses exist in $GL_n(\mathbb{R})$. Note that, unlike the previous examples, matrix multiplication is *not* commutative. That is, given $A, B \in GL_n(\mathbb{R})$, it is possible for $AB \neq BA$ to be true. ■

Commutative groups are useful enough to deserve a name.

Definition 1.2 (**Abelian Group**) An Abelian group is a group $(G, *)$ such that for all $a, b \in G$ it is true that $a * b = b * a$. ■

We now take the time to explore the basic properties that all groups have in common. None of these are *deep* theorems, and come straight from the definition.

Theorem 1.1. *If $(G, *)$ is a group, and if $e, e' \in G$ are identities, then $e = e'$*

Proof. Since e and e' are identities we have:

$$e = e * e' = e' \tag{1}$$

and hence $e = e'$. □

Theorem 1.2. *If $(G, *)$ is a group, if $a \in G$, and if b and b' are inverses of a, then $b = b'$.*

Proof. For let $e \in G$ be the unique identity. Then we have:

$$\begin{aligned} b &= b * e && \text{(Identity)} \\ &= b * (a * b') && \text{(Inverse)} \\ &= (b * a) * b' && \text{(Associativity)} \\ &= e * b' && \text{(Inverse)} \\ &= b' && \text{(Identity)} \end{aligned}$$

and hence $b = b'$. □

Because of this, given $a \in G$ we denote by a^{-1} the *unique* inverse of a.

Theorem 1.3. *If $(G, *)$ is a group, and if $a, b \in G$, then $(a * b)^{-1} = b^{-1} * a^{-1}$.*

Proof. Since inverses are unique, we need only prove that $b^{-1} * a^{-1}$ is indeed an inverse of $a * b$. We have:

$$\begin{aligned} (a * b) * (b^{-1} * a^{-1}) &= a * \left((b * b^{-1}) * a^{-1}\right) && \text{(Associativity)} \\ &= a * (e * a^{-1}) && \text{(Inverse)} \\ &= a * a^{-1} && \text{(Identity)} \\ &= e && \text{(Inverse)} \end{aligned}$$

by the uniqueness of inverses, $(a * b)^{-1} = b^{-1} * a^{-1}$. □

Theorem 1.4. *If $(G, *)$ is a group, and if $a \in G$, then $(a^{-1})^{-1} = a$.*

Proof. We have that:

$$\begin{aligned} a &= a * e && \text{(Identity)} \\ &= a * \left(a^{-1} * (a^{-1})^{-1}\right) && \text{(Inverse)} \\ &= (a * a^{-1}) * (a^{-1})^{-1} && \text{(Associativity)} \\ &= e * (a^{-1})^{-1} && \text{(Inverse)} \\ &= (a^{-1})^{-1} && \text{(Identity)} \end{aligned}$$

and hence $a = (a^{-1})^{-1}$. □

Theorem 1.5 (Left-Cancellation Law). *If $(G, *)$ is a group, if $a, b, c \in G$, and if $a * b = a * c$, then $b = c$.*

Proof. Letting $e \in G$ be the unique inverse, if $a * b = a * c$, then we have:

$$\begin{aligned} b &= e * b && \text{(Identity)} \\ &= (a^{-1} * a) * b && \text{(Inverse)} \\ &= a^{-1} * (a * b) && \text{(Associativity)} \\ &= a^{-1} * (a * c) && \text{(Hypothesis)} \\ &= (a^{-1} * a) * c && \text{(Associativity)} \\ &= e * c && \text{(Inverse)} \\ &= c && \text{(Identity)} \end{aligned}$$

so we conclude that $b = c$. □

We can mirror this argument to prove the right-cancellation law.

Theorem 1.6 (**Right-Cancellation Law**)**.** *If $(G, *)$ is a group, if $a, b, c \in G$, and if $b * a = c * a$, then $b = c$.*

Proof. Letting $e \in G$ be the unique inverse, if $b * a = c * a$, then we have:

$$\begin{aligned} b &= b * e && \text{(Identity)} \\ &= b * (a * a^{-1}) && \text{(Inverse)} \\ &= (b * a) * a^{-1} && \text{(Associativity)} \\ &= (c * a) * a^{-1} && \text{(Hypothesis)} \\ &= c * (a * a^{-1}) && \text{(Associativity)} \\ &= c * e && \text{(Inverse)} \\ &= c && \text{(Identity)} \end{aligned}$$

and hence $b = c$. □

Theorem 1.7. *If $(G, *)$ is a group, if $a, b \in G$, and if $a = a * b$, then $b = e$ where $e \in G$ is the unique identity element.*

Proof. We have that:

$$\begin{aligned} a * b &= a && \text{(Hypothesis)} \\ &= a * e && \text{(Identity)} \end{aligned}$$

and hence $a * b = a * e$. By the left-cancellation law, $b = e$. □

Theorem 1.8. *If $(G, *)$ is a group, if $a, b \in G$, and if $a = b * a$, then $b = e$ where $e \in G$ is the unique identity element.*

Proof. We have that:

$$\begin{aligned} b * a &= a && \text{(Hypothesis)} \\ &= e * a && \text{(Identity)} \end{aligned}$$

and hence $b * a = e * a$. By the right-cancellation law, $b = e$. □

Definition 1.3 (**Subgroup**) A subgroup of a group $(G, *)$ is a subset $H \subseteq G$ such that the restriction of $*$ to $H \times H$ yields a group. That is, $(H, *_H)$ is a group. ■

Theorem 1.9. *If $(G, *)$ is a group, if $e \in G$ is the unique identity, and if $H \subseteq G$ is a subgroup, then $e \in H$ and e is the identity of $(H, *_H)$.*

Proof. Since $(H, *_H)$ is a group, there is some identity element $e_H \in H$. But then $e_H *_H e_H = e_H$. But $*_H$ is just the restriction of $*$ to H, so $e_H * e_H = e_H$. By the previous theorem, $e_H = e$, so $e \in H$ and e is the identity of $(H, *_H)$. □

Theorem 1.10. *If $(G, *)$ is a group, if $H \subseteq G$ is a subgroup, and if $a \in H$, then $a^{-1} \in H$.*

Proof. Since $(H, *_H)$ is a group, and since $a \in H$, there is an inverse element a_H^{-1} such that $a * a_H^{-1} = a_H^{-1} * a = e_H$. But by the previous theorem, $e_H = e$, so $a * a_H^{-1} = a_H^{-1} * a = e$. But $(G, *)$ is a group and inverses are unique, so $a_H^{-1} = a^{-1}$. Hence $a^{-1} \in H$. □

Theorem 1.11. *If $(G, *)$ is a group, and if $H \subseteq G$, then H is a subgroup if and only if H is non-empty, for all $a \in H$ it is true that $a^{-1} \in H$, and for all $a, b \in H$ it is true that $a * b \in H$.*

Proof. By the previous two theorems, if $H \subseteq G$ is a subgroup, then it is closed to group multiplication and inversion. It also non-empty since $e \in H$. In the reverse direction, suppose $H \subseteq G$ is non-empty and closed to inversion and multiplication. We need only show that H has an identity element (it has inverses, and the group operation is associative, so the restriction to H is associative as well). Since H is non-empty, there is some $a \in H$. But H is closed to inversion, so $a^{-1} \in H$. But H is also closed under multiplication, meaning $a * a^{-1} \in H$. But $a * a^{-1} = e$, and hence $e \in H$. That is, H is a subgroup. □

For topology and geometry, two of the most important operations that come from groups are *left-translation* and *right-translation*. These are defined as follows.

Definition 1.4 (**Left-Translation of a Group**) Left-translation of a group $(G, *)$ by an element $a \in G$ is the function $L_a : G \to G$ defined by:

$$L_a(x) = a * x \tag{2}$$

That is, each element is translated on the left by a. ■

Right-translation is similarly defined.

Definition 1.5 (**Right-Translation of a Group**) Right-translation of a group $(G, *)$ by an element $a \in G$ is the function $R_a : G \to G$ defined by:

$$R_a(x) = x * a \tag{3}$$

That is, each element is translated on the right by a. ■

Left-translation and right-translation by the same element may yield different functions if $(G, *)$ is not Abelian (commutative). Regardless, translation is always a bijection.

Theorem 1.12. *If $(G, *)$ is a group, if $a \in G$, and if $L_a : G \to G$ is left-translation by a, then L_a is bijective.*

Proof. First, L_a is injective. For let $x, y \in G$ and suppose $L_a(x) = L_a(y)$. By the definition of left-translation this means $a*x = a*y$. By the left-cancellation law, $x = y$, and hence L_a is injective. It is also surjective. For let $y \in G$ and let $x = a^{-1} * y$. Then we have:

$$\begin{aligned} L_a(x) &= a * x && \text{(Definition)} \\ &= a * (a^{-1} * y) && \text{(Substitution)} \\ &= (a * a^{-1}) * y && \text{(Associativity)} \\ &= e * y && \text{(Inverse)} \\ &= y && \text{(Identity)} \end{aligned}$$

and hence $L_a(x) = y$, so L_a is surjective. Since L_a is injective and surjective, it is bijective. □

The same result holds for right-translation. The proof is also a mirror of left-translation.

Theorem 1.13. *If $(G, *)$ is a group, if $a \in G$, and if $R_a : G \to G$ is right-translation by a, then R_a is bijective.*

Proof. Indeed, R_a is injective. For let $x, y \in G$ and suppose $R_a(x) = R_a(y)$. That is, $x * a = y * a$. By the right-cancellation law, $x = y$, and hence R_a is injective. It is also surjective. For let $y \in G$ and let $x = y * a^{-1}$. Then we have:

$$\begin{aligned} R_a(x) &= x * a && \text{(Definition)} \\ &= (y * a^{-1}) * a && \text{(Substitution)} \\ &= y * (a^{-1} * a) && \text{(Associativity)} \\ &= y * e && \text{(Inverse)} \\ &= y && \text{(Identity)} \end{aligned}$$

and hence $R_a(x) = y$, so R_a is surjective. Since R_a is injective and surjective, it is bijective. □

Theorem 1.14. *If $(G, *)$ is a group, if $H \subseteq G$ is a subgroup, and if $a \in H$, then $L_a[H] = H$. That is, left-translation of a subgroup by an element of the subgroup results in the subgroup.*

Proof. For let $x \in H$ and set $y = a^{-1} * x$. Since $a \in H$ and H is a subgroup, we have that $a^{-1} \in H$. Since $x \in H$ and H is a subgroup we also have that $a^{-1} * x \in H$. Hence $y \in H$. But then:

$$L_a(y) = a * (a^{-1} * x) = (a^{-1} * a) * x = e * x = x \tag{4}$$

and therefore $x \in L_a[H]$. That is, $H \subseteq L_a[H]$. In the reverse direction, let $y \in L_a[H]$. Then $y = L_a(x)$ for some $x \in H$. That is, $y = a * x$. But then $x = a^{-1} * y$. But $a^{-1} \in H$ and $y \in H$, and hence $a^{-1} * y \in H$ since H is a subgroup. That is, $x \in H$, and thus $L_a[H] \subseteq H$. We conclude that $H = L_a[H]$. □

Theorem 1.15. *If $(G, *)$ is a group, if $H \subseteq G$ is a subgroup, and if $a \in H$, then $R_a[H] = H$. That is, right-translation of a subgroup by an element of the subgroup results in the subgroup.*

Proof. The proof is a mirrored mimicry of the previous theorem. □

This reverses.

Theorem 1.16. *If $(G, *)$ is a group, if $H \subseteq G$, if H is non-empty, and if for all $a \in H$ it is true that $L_a[H] = H$, then H is a subgroup.*

Proof. First note that $e \in H$, where $e \in G$ is the unique identity. Since H is non-empty there is some $a \in H$. But if $a \in H$, then by hypothesis $L_a[H] = H$, and hence $a \in L_a[H]$. That is, there is some $x \in H$ such that $L_a(x) = a$, and hence $a = a * x$. By the left-cancellation law, $x = e$ and $e \in H$. So H contains the identity. It also contains inverses. Since $e \in H$ and $L_a[H] = H$ we have that $L_a(x) = e$ for some $x \in H$. That is, $a * x = e$. By the uniqueness of inverses, $x = a^{-1}$ so $a^{-1} \in H$. Finally, H is closed under multiplication since $x * y = L_x(y)$ for all $x, y \in H$, and hence $x * y \in H$ since $L_x[H] = H$. So H is a subgroup. □

This cannot be relaxed to just *some* element of H. That is, $L_a[H] = H$ for some $a \in H$ need not imply H is a subgroup. Take, for a simple example, $\mathbb{N}$ with addition $+$. This is a subset of $\mathbb{Z}$ but not a subgroup, it lacks inverses. However $L_0[\mathbb{N}] = \mathbb{N}$ is still true, and $0 \in \mathbb{N}$.

2 Homomorphisms

Continuous functions are the main functions of study in topology. Continuity is solely described by the topologies. For groups we have a set and a binary operation, so not much to play with. The main functions of study for group theory should then be functions that respect or preserve the binary operation in some way. This motivates the definition of *group homomorphisms*.

Definition 2.1 (**Group Homomorphism**) A group homomorphism from a group $(G, *)$ to a group $(G', *')$ is a function $\varphi : G \to G'$ such that for all $a, b \in G$ it is true that $\varphi(a * b) = \varphi(a) *' \varphi(b)$. ■

Example 2.1 Define $\varphi : \mathbb{Z} \to \mathbb{Z}_2$ by $\varphi(n) = n \bmod 2$. If $\mathbb{Z}$ is given integer arithmetic, and if $\mathbb{Z}_2$ is equipped with *modular arithmetic*, then φ is a group homomorphism. φ sends even integers to 0 and odd integers to 1. ■

Group homomorphisms preserve many aspects of the group.

Theorem 2.1. *If $(G, *)$ and $(G', *')$ are groups, if $\varphi : G \to G'$ is a group homomorphism, and if $e \in G$ and $e' \in G'$ are the identities, then $\varphi(e) = e'$.*

Proof. We have:

$$\begin{aligned} \varphi(e) &= \varphi(e * e) && \text{(Identity)} \\ &= \varphi(e) *' \varphi(e) && \text{(Homomorphism)} \end{aligned}$$

and hence $\varphi(e) = \varphi(e) *' \varphi(e)$. By the cancellation law, $\varphi(e) = e'$. □

Theorem 2.2. *If $(G, *)$ and $(G', *')$ are groups, if $\varphi : G \to G'$ is a group homomorphism, and if $a \in G$, then $\varphi(a^{-1}) = \varphi(a)^{-1}$.*

Proof. Since inverses are unique, we need only show that $\varphi(a^{-1})$ is an inverse for $\varphi(a)$. We have:

$$\begin{aligned} \varphi(a) * \varphi(a^{-1}) &= \varphi(a * a^{-1}) && \text{(Homomorphism)} \\ &= \varphi(e) && \text{(Identity)} \\ &= e' && \text{(Previous Theorem)} \end{aligned}$$

and hence $\varphi(a^{-1}) = \varphi(a)^{-1}$. □

Theorem 2.3. *If $(G, *)$ and $(G', *')$ are groups, if $\varphi : G \to G'$ is a group homormorphism, and if $H \subseteq G$ is a subgroup, then $\varphi[H] \subseteq G'$ is a subgroup.*

Proof. Since H is a subgroup, $e \in H$ is true, and hence $e' \in \varphi[H]$ is also true. Hence $\varphi[H]$ is non-empty. If $a' \in \varphi[H]$, then $a' = \varphi(a)$ for some $a \in H$. But H is a subgroup, so $a^{-1} \in H$ and hence $\varphi(a^{-1}) \in \varphi[H]$. But $\varphi(a^{-1}) = \varphi(a)^{-1}$, and hence $a'^{-1} \in \varphi[H]$. Lastly, if $a', b' \in H$, then there are $a, b \in H$ such that $a' = \varphi(a)$ and $b' = \varphi(b)$. But then $a' * b' = \varphi(a) * \varphi(b) = \varphi(a * b)$. Since H is a subgroup, $a * b \in H$ is true, and hence $a' * b' \in \varphi[H]$. Therefore $\varphi[H]$ is a subgroup. □

Mimicing topology, the *pre-image* of a subgroup is also a subgroup.

Theorem 2.4. *If $(G, *)$ and $(G', *')$ and groups, if $\varphi : G \to G'$ is a group homomorphism, and if $H' \subseteq G'$ is a subgroup, then $\varphi^{-1}[H'] \subseteq G$ is a subgroup.*

Proof. Let $H = \varphi^{-1}[H']$. Firstly, the set is non-empty since $e' \in H'$, and hence $e \in H$. Let's prove H is closed to inversions and products. Let $a \in H$. Then $\varphi(a) \in H'$. But H' is a subgroup, so $\varphi(a)^{-1} \in H'$. But $\varphi(a)^{-1} = \varphi(a^{-1})$ and hence $a^{-1} \in H$. That is, H is closed to inversion. Lastly, let $a, b \in H$. Then $\varphi(a) \in H'$ and $\varphi(b) \in H'$. But H' is a subgroup, so $\varphi(a) *' \varphi(b) \in H'$. But $\varphi(a) *' \varphi(b) = \varphi(a * b)$ and hence $a * b \in H$. Thus $H = \varphi^{-1}[H']$ is a subgroup. □

Unlike topology, this does not reverse. That is, homomorphisms can not be described by pre-images.

Example 2.2 Let $(\mathbb{Z}_2, +_2)$ be the group of addition mod 2, and $(\mathbb{Z}_3, +_3)$ be the group of addition mod 3. Define $\varphi : \mathbb{Z}_2 \to \mathbb{Z}_3$ via $\varphi(n) = n$. The only subgroups of $\mathbb{Z}_3$ are $\{ 0 \}$ and $\{ 0, 1, 2 \}$. In both cases the pre-image under φ is a subgroup of $\mathbb{Z}_2$. However, φ is not a homomorphism. Note that $\varphi(1 +_2 1) = \varphi(0) = 0$, but $\varphi(1) +_3 \varphi(1) = 1 +_3 1 = 2$. ■

Just like how *homeomorphisms* tell us when two topological spaces are the same (topologically), *isomorphisms* tell us when two groups are the same (algebraically).

Definition 2.2 (**Group Isomorphism**) A group isomorphism from a group $(G, *)$ to a group $(G', *')$ is a bijective group homomorphism $\varphi : G \to G'$ such that $\varphi^{-1} : G' \to G$ is also a group homomorphism. ■

In topology a bijective continuous function need not have a continuous inverse. Group theorists do not have such worries.

Theorem 2.5. *If $(G, *)$ and $(G', *')$ are groups, and if $\varphi : G \to G'$ is a bijective group homomorphism, then φ^{-1} is a group homomorphism.*

Proof. For let $a', b' \in G'$. Since φ is bijective, there are $a, b \in G$ such that $a' = \varphi(a)$ and $b' = \varphi(b)$. But then, since φ is bijective, we also have $a = \varphi^{-1}(a')$ and $b = \varphi^{-1}(b')$. Hence:

$$\begin{aligned}
\varphi^{-1}(a' *' b') &= \varphi^{-1}\big(\varphi(a) *' \varphi(b)\big) && \text{(Substitution)} \\
&= \varphi^{-1}\big(\varphi(a * b)\big) && \text{(Homomorphism)} \\
&= a * b && \text{(Inverse Function)} \\
&= \varphi^{-1}(a') * \varphi^{-1}(b') && \text{(Substitution)}
\end{aligned}$$

and therefore φ^{-1} is a group homomorphism. □

3 Conjugation and Normal Subgroups

Groups need not be Abelian (commutative). The general linear group of invertible $n \times n$ matrices serves as the counterexample to the claim, and serves as an example of a very useful and important non-Abelian group. *Conjugation* measures, to some extent, how two elements fail to commute.

Definition 3.1 (**Conjugation of a Group**) The conjugation of a group $(G, *)$ by an element $g \in G$ is the function $\text{conj}_g : G \to G$ defined by:

$$\text{conj}_g(a) = g * a * g^{-1} \tag{5}$$

for all $a \in G$. ■

Theorem 3.1. *If $(G, *)$ is an Abelian group, and if $g \in G$, then $conj_g = id_G$.*

Proof. For let $a \in G$. Then:

$$\begin{aligned}
\text{conj}_g(a) &= g * a * g^{-1} && \text{(Definition of conj}_g\text{)} \\
&= g * g^{-1} * a && \text{(Commutativity)} \\
&= e * a && \text{(Inverse)} \\
&= a && \text{(Identity)}
\end{aligned}$$

and hence $\text{conj}_g(a) = a$ for all a, meaning conj_g is the identity function. □

Theorem 3.2. *If $(G, *)$ is a group, if $a \in G$, and if $g \in G$, then:*

$$conj_g(a^{-1}) = conj_g(a)^{-1} \tag{6}$$

Proof. By the uniqueness of inverses, we need only show that $\text{conj}_g(a^{-1})$ is an inverse of $\text{conj}_g(a)$. We have:

$$\begin{aligned}
\text{conj}_g(a^{-1}) * \text{conj}_g(a) &= \left(g * a^{-1} * g^{-1}\right) * \left(g * a * g^{-1}\right) && \text{(Substitution)} \\
&= (g * a^{-1}) * (g^{-1} * g) * (a * g^{-1}) && \text{(Associativity)} \\
&= (g * a^{-1}) * e * (a * g^{-1}) && \text{(Inverse)} \\
&= (g * a^{-1}) * (a * g^{-1}) && \text{(Identity)} \\
&= g * (a^{-1} * a) * g^{-1} && \text{(Associativity)} \\
&= g * e * g^{-1} && \text{(Inverse)} \\
&= g * g^{-1} && \text{(Identity)} \\
&= e && \text{(Inverse)}
\end{aligned}$$

By the uniqueness of inverses, $\text{conj}_g(a^{-1}) = \text{conj}_g(a)^{-1}$. □

Theorem 3.3. *If $(G, *)$ is a group, if $g \in G$, and if $a, b \in G$, then:*

$$conj_g(a * b) = conj_g(a) * conj_g(b) \tag{7}$$

Proof. We have:

$$\begin{aligned}
\text{conj}_g(a * b) &= g * (a * b) * g^{-1} && \text{(Definition of conj}_g\text{)} \\
&= g * (a * e * b) * g^{-1} && \text{(Identity)} \\
&= g * (a * (g^{-1} * g) * b) * g^{-1} && \text{(Inverse)} \\
&= (g * a * g^{-1}) * (g * b * a^{-1}) && \text{(Associativity)} \\
&= \text{conj}_g(a) * \text{conj}_g(b) && \text{(Definition of conj}_g\text{)}
\end{aligned}$$

and so the theorem is proved. □

Theorem 3.4. *If $(G, *)$ is a group, and if $g \in G$, then $conj_g : G \to G$ is a group homomorphism.*

Proof. By the previous theorem $\text{conj}_g(a * b) = \text{conj}_g(a) * \text{conj}_g(b)$ and hence conj_g is a group homomorphism. □

Theorem 3.5. *If $(G, *)$ is a group, if $g \in G$, and if $H \subseteq G$ is a subgroup, then $conj_g[H] \subseteq G$ is a subgroup.*

Proof. Since H is a subgroup and $\text{conj}_g : G \to G$ is a group homomorphism, $\text{conj}_g[H]$ is a subgroup. □

Definition 3.2 (**Normal Subgroup**) A normal subgroup of a group $(G, *)$ is a subgroup $H \subseteq G$ such that for all $g \in G$ it is true that $\text{conj}_g[N] = N$. That is, for all $a \in N$ and for all $g \in G$ we have $g * n * g^{-1} \in N$. ■

Note that it is not required that $g * n * g^{-1} = n$, merely that conjugation of an element in the subgroup yields another element of the subgroup. Normal subgroups are those that are *closed* under conjugation.

4 Cosets and Quotient Groups

Subgroups can be used to decompose a group into disjoint pieces. That is, we take the subgroup and then use left-translation by different elements of the group until every element is covered. This has two uses. First, it gives a nice partitioning of the group and can be used to prove things like *Lagrange's theorem* for finite groups. Secondly, it yields an equivalence relation which can then be used to form quotient sets. Under the right conditions the quotient set can be given a group struct such that the canonical quotient map is a group homomorphism. First, a definition.

Definition 4.1 (**Left-Coset in a Group**) The left-coset of a subset $A \subseteq G$ in a group $(G, *)$ with respect to an element $a \in G$ is the set $L_a[A]$, where L_a is the left-translation function. ■

In most contexts A is actually a subgroup, and we usually label this as $H \subseteq G$. Many textbooks then denote the left-coset of H by a as aH. For topological applications left-translation is a central tool and we usually think of this as a *function*, so we'll stick with $L_a[H]$.

Theorem 4.1. *If $(G, *)$ is a group, if $H \subseteq G$ is a subgroup, and if $a, b \in G$, then either $L_a[H] = L_b[H]$ or $L_a[H] \cap L_b[H] = \emptyset$.*

Proof. For suppose $L_a[H] \cap L_b[H] \neq \emptyset$. That is, there is some $c \in L_a[H] \cap L_b[H]$. Then, by definition of left-translation, there exists $x, y \in H$ such that $c = a * x$ and $c = b * y$. That is, $a * x = b * y$. But then $a = b * y * x^{-1}$. But H is a subgroup, so $y * x^{-1} \in H$, and hence $a \in L_b[H]$. Given $z \in L_a[H]$, we have $z = a * w$ for some $w \in H$, and therefore $z = b * (y * x^{-1} * w)$. But $y * x^{-1} * w \in H$ since H is a subgroup. Thus $z \in L_b[H]$, meaning $L_a[H] \subseteq L_b[H]$. By a similar argument it is true that $L_b[H] \subseteq L_a[H]$ and hence $L_a[H] = L_b[H]$. That is, either $L_a[H]$ and $L_b[H]$ are disjoint or equal. □

Theorem 4.2. *If $(G, *)$ is a group, if $H \subseteq G$ is a subgroup, and if Λ is the set:*

$$\Lambda = \{ L_a[H] \subseteq G \mid a \in G \} \tag{8}$$

then Λ partitions G. That is, $\bigcup \Lambda = G$ and distinct elements of Λ are disjoint.

Proof. By the previous theorem distinct elements of Λ are disjoint. We need only show that $\bigcup \Lambda = G$. Let $a \in G$. Since H is a subgroup, $e \in H$ where $e \in G$ is the unique identity element. But then $a * e = a$, and hence $a \in L_a[H]$. Thus $a \in \bigcup \Lambda$. That is, Λ partitions G. □

Partitions and equivalence relations are really the same thing. If R is an equivalence relation on X, we get a partition by considering the set of all equivalence classes of X. That is, the equivalence classes $[x] \subseteq X$ cover the set, and equivalence classes are either identical or disjoint. Conversely, if we have a partition, we may form an equivalence relation by saying that xRy is true if and only if x and y belong to the same partition set. Because of this, the left-posets of a subgroup give us an equivalence relation on a group, meaning we may form the quotient set, which we denote G/H. It is natural to ask if the quotient set can be endowed with a group operation, much the way we equipped quotients of topological spaces with the quotient topology. Unlike topological spaces, where *any* quotient set can be given the quotient topology, for the quotient of a group to be a group itself the subgroup must be *normal*. If $N \subseteq G$ is a normal subgroup, we may define:

$$L_a[N] \tilde{*} L_b[N] = L_{a*b}[N] \tag{9}$$

Since N is closed under conjugation, this is a well-defined operation. Almost by construction, the quotient map $q : G \to G/N$ defined by $q(a) = [a] = L_a[N]$ is a group homomorphism. That is:

$$q(a * b) = L_{a*b}[N] = L_a[N] \tilde{*} L_b[N] = q(a) \tilde{*} q(b) \tag{10}$$

so q is a group homomorphism.