Subgroups, isomorphisms, Cayley's theorem.

Injective, Surjective, Bijective functions: X, Y, sets,
f: X \to Y a function. For y \in Y, the set of preimages of y is \( f^{-1}(y) = \{ x \in X | f(x) = y \} \), a subset of X.

- \( f \) is injective \iff \( \forall y \in Y, f^{-1}(y) \) has at most one element.
- \( f \) is surjective \iff \( \forall y \in Y, f^{-1}(y) \) has at least one element.
- \( f \) is bijective \iff \( \forall y \in Y, f^{-1}(y) \) has exactly one element.

\( f: X \to Y \) is bijective iff there is an inverse function \( g: Y \to X \), meaning that \( g(f(x)) = x \) for all \( x \in X \) and \( f(g(y)) = y \) for all \( y \in Y \). In this case \( \{ x \in X | f(x) = y \} = \{ g(y) \} \).

Given functions \( f: X \to Y \) and \( g: Y \to Z \), define \( g \circ f: X \to Z \) by \( (g \circ f)(x) = g(f(x)) \). For any set \( X \), there is an identity function \( \text{id}_X: X \to X \), \( \text{id}_X(x) = x \). So \( f: X \to Y \) is bijective iff there is a function \( g: Y \to X \) such that \( g \circ f = \text{id}_X \) and \( f \circ g = \text{id}_Y \).

Let \( G \) be a group, and fix \( a \in G \). Left and right multiplication by a definite functions:

\[
L_a: G \to G \quad L_a(g) = ag
\]
\[
R_a: G \to G \quad R_a(g) = ga
\]

Example: \( G = (\mathbb{Z}_5, +) \), \([3] \in \mathbb{Z}_5\)

\[
\]

\[
R_{[3]}([6]) = [6] + [3] = [9] = [4]
\]
Proposition let $G$ be a group, $a, b \in G$. Then $L_a \circ L_b = L_{ab}$ and $R_a \circ R_b = R_{ba}$. Also, if $e \in G$ denotes the identity, then $L_e = \text{id}_G = R_e$.

Proof $L_a \circ L_b (x) = L_a (L_b (x)) = L_a (bx) = a (bx) = (ab) x = L_{ab} (x)$. $R_a \circ R_b (x) = R_a (R_b (x)) = R_a (xb) = xb a = x (ba) = R_{ba} (x)$.

$L_e (x) = ex = x$ and $R_e (x) = xe = x$.

Proposition let $G$ be a group, $a \in G$. Then $L_a$ and $R_a$ are bijective, with inverses $L_a^{-1}$ and $R_a^{-1}$, respectively.

Proof $L_a \circ L_a^{-1} = L_{aa^{-1}} = L_e = \text{id}_G$, similar for $R_a$.

Some easy and useful consequences of this:

Corollary let $G$ be a group, $a, b \in G$. The equation $ax = b$ has a unique solution $x \in G$, as does the equation $xa = b$.

Proof The equation $ax = b$ is equivalent to $L_a (x) = b$. Since $L_a$ is bijective, there is a unique $x$ with this property. Similarly, $xa = b$ means $R_a (x) = b$, and as $R_a$ is bijective there is a unique solution. \( \blacksquare \)

In fact, the unique solution to $ax = b$ is $x = a^{-1}b$, unique solution to $xa = b$ is $x = ba^{-1}$.\( \blacksquare \)
Corollary  Suppose \( a, x, y \in G \) satisfy \( ax = ay \). Then \( x = y \).

Similarly, if \( xa = ya \) then \( x = y \).

**Proof**  Suppose \( ax = ay \). Then \( L_a(x) = L_a(y) \). Since \( L_a \) is injective, we conclude \( x = y \). If \( xa = ya \), then \( Ra(x) = Ra(y) \), so \( x = y \) since \( Ra \) is injective. \( \Box \)

Let \( X \) be a set. Define \( \text{Sym}(X) = \{ f : X \to X \mid f \text{ is bijective} \} \).

\( \text{Sym}(X) \) is a group where the group operation is composition of functions. The identity is \( \text{id}_X \), and the inverse is the inverse function.

Now let \( G \) be a group. Then we have constructed a function

\[
G \to \text{Sym}(G)
\]

\[
g \mapsto L_g
\]

This function is injective in its own right. Why?

If \( L_a = L_b \) as functions, then \( L_a(e) = L_b(e) \) so \( ae = be \) so \( a = b \).

[However, most functions \( f \in \text{Sym}(G) \) are not of the form \( L_a \) for \( a \in G \).]

The subset \( \{ L_g \mid g \in G \} \subseteq \text{Sym}(G) \) has an important property:

**Definition**  Let \( G \) be a group. A subset \( H \subseteq G \) is called a **subgroup** if the operation makes \( H \) into a group in its own right.

We write \( H \leq G \) when \( H \) is a subgroup.

**Ex.**  1. Group \( (\mathbb{Z}, +) \). \( 2\mathbb{Z} = \{ 2k \mid k \in \mathbb{Z} \} \subset \mathbb{Z} \) is a subgroup.

\( \mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C} \)

2. \( G \) a group. Then \( \emptyset \subset G \) is a subgroup, called the **trivial subgroup**.
Proposition: let $G$ be a group, $H \leq G$ a nonempty subset. $H$ is a subgroup iff the following conditions hold:

1. for all $h_1, h_2 \in H$, $h_1 h_2 \in H$ (H is closed under the operation)
2. for all $h \in H$, $h^{-1} \in H$ (H is closed under taking inverse).

Proof: Conditions are clearly necessary. To see they suffice,

- Note that 1 says that the operation on $G$ actually gives an operation on $H$. We verify the axioms:
  - Associativity follows from associativity of $G$.
  - Take any $h \in H$, then $h \cdot e \in H$ by 2, so $h \cdot e = e \in H$ by 0.

Thus, $H$ contains identity.

- Inverses by 2.

Let $G$ be a group, and consider $H = \{ L_g \mid g \in G \} \subseteq \text{Sym}(G)$.

Then $H$ is a subgroup:

1. $L_{g_1}, L_{g_2} \in H \Rightarrow L_{g_1} \circ L_{g_2} = L_{g_1 \cdot g_2} \in H$ \checkmark
2. $L_g \in H \Rightarrow L_g = L_{g^{-1}} \in H$. \checkmark

Definition: let $G$ and $H$ be groups, and let $\varphi : G \rightarrow H$ be a function.

$\varphi$ is called an isomorphism if $\varphi$ is bijective and for all $g_1, g_2 \in G$, we have $\varphi(g_1 g_2) = \varphi(g_1) \varphi(g_2)$.

Example: $G$ a group. $H = \{ L_g \mid g \in G \} \subseteq \text{Sym}(G)$.

Define $\varphi : G \rightarrow H$ by $\varphi(g) = L_g$.

Said before that $\varphi$ is injective. It is surjective (onto $H$) because of the way $H$ is defined. So $\varphi$ is bijective. Furthermore,$$
\varphi(g_1 g_2) = L_{g_1} \circ L_{g_2} = L_{g_1 \cdot g_2} = \varphi(g_1) \varphi(g_2)
$$

So $\varphi$ is an isomorphism.
This proves Cayley's theorem: Every group $G$ is isomorphic to a subgroup of a symmetric group.

(Groups of the form $\text{Sym}(X)$ are known as symmetric groups or permutation groups.)

In fact, $G$ is isomorphic to a subgroup of $\text{Sym}(G)$.

**Proposition** If $\varphi: G \rightarrow H$ is an isomorphism of groups, then $\varphi(e_G) = e_H$, and for all $g \in G$, $\varphi(g)\varphi(g^{-1})$ are identity.

**Proof** $e_H \varphi(e_G) = \varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G) \varphi(e_G)$

cancel $\varphi(e_G) \Rightarrow e_H = \varphi(e_G)$.

Take $g \in G$ then $e_H = \varphi(e_G) = \varphi(gg^{-1}) = \varphi(g) \varphi(g^{-1})$

by uniqueness of inverses, $\varphi(g^{-1}) = \varphi(g)^{-1}$.

**Example:** Recall complex numbers $a+bi$, $i^2 = -1$

$$e^{i\theta} = \cos \theta + i \sin \theta, \quad e^{x+yi} = e^x e^{yi}, \quad e^{2\pi i} = 1.$$

Fix $n \in \mathbb{N}$. Consider $C_n = \{e^{2\pi ik/n} \mid k \in \mathbb{Z}\}$

I claim $C_n$ is a group, where the operation is multiplication of complex numbers. Furthermore, the function $\varphi: \mathbb{Z}/n \rightarrow C_n$ $\varphi([k]) = e^{2\pi ik/n}$ is an isomorphism.