# Subgroups, isomorphisms, Cayley's theorem.

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

$f$ is <u>injective</u> $\iff$ for all $y \in Y$, $f^{-1}(y)$ has <u>at most</u> one element
$f$ is <u>surjective</u> $\iff$ for all $y \in Y$, $f^{-1}(y)$ has <u>at least</u> one element.
$f$ is <u>bijective</u> $\iff$ for all $y \in Y$, $f^{-1}(y)$ has <u>exactly</u> 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 $\{x \in X \mid f(x) = y\} = \{g(y)\}$.

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 $id_X: X \to X$, $id_X(x) = x$. So $f: X \to Y$ is bijective iff there is a function $g: Y \to X$ such that $g \circ f = id_X$ and $f \circ g = id_Y$.

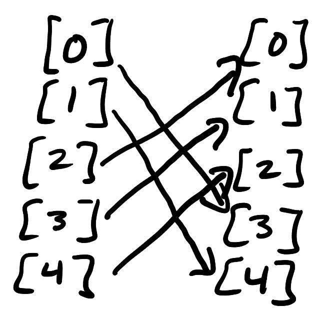
Let $G$ be a group, and fix $a \in G$. Left and right multiplication by $a$ define functions:

$$L_a: G \to G \qquad L_a(g) = ag$$
$$R_a: G \to G \qquad R_a(g) = ga$$

<u>Example</u>: $G = (\mathbb{Z}_5, +)$ $[3] \in \mathbb{Z}_5$

$$L_{[3]}([b]) = [3] + [b] = [b+3]$$

so



<u>Proposition</u> 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 $L_e = \mathrm{id}_G = R_e$.

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

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

<u>Proposition</u> 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.

<u>Proof</u> $L_a \circ L_{a^{-1}} = L_{aa^{-1}} = L_e = \mathrm{id}_G$
$L_{a^{-1}} \circ L_a = L_{a^{-1}a} = L_e = \mathrm{id}_G$ , similar for $R_a$.

Some easy and useful consequences of this:

<u>Corollary</u> Let $G$ be a group, $a, b \in G$. The equation $ax = b$ has a unique solution $x \in G$, as does the equation $xa = b$.

<u>Proof</u> 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. $\boxtimes$

In fact, the unique solution to $ax = b$ is $x = a^{-1}b$, unique solution to $xa = b$ is $x = ba^{-1}$!

<u>Corollary</u> Suppose $a, x, y \in G$ satisfy $ax = ay$. Then $x = y$.
Similarly, if $xa = ya$ then $x = y$.

<u>Proof</u> Suppose $ax = ay$. Then $L_a(x) = L_a(y)$. Since $L_a$ is injective, we conclude $x = y$. If $xa = ya$, $R_a(x) = R_a(y)$, so $x = y$ since $R_a$ is injective. $\boxtimes$

Let $X$ be a set. Define $\mathrm{Sym}(X) = \{ f : X \to X \mid f \text{ is bijective} \}$
$\mathrm{Sym}(X)$ is a group where the group operation is composition of functions. The identity is $\mathrm{id}_X$, and the inverse is the inverse function.

Now let $G$ be a group. Then we have constructed a function

$$\begin{aligned} G &\longrightarrow \mathrm{Sym}(G) \\ g &\longmapsto L_g \end{aligned}$$

This function is <u>injective</u> 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 $f \in \mathrm{Sym}(G)$ are not of the form $L_a$ for $a \in G$.]

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

<u>Definition</u> Let $G$ be a group. A subset $H \subseteq G$ is called a <u>subgroup</u> if the operation makes $H$ into a group in its own right.
We write $H \leq G$ when $H$ is a subgroup.

<u>Ex</u> 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 $\{e\} \subset G$ is a subgroup, called the trivial subgroup.

<u>Proposition</u> Let $G$ be a group, $H \subseteq G$ 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).

<u>Proof</u> 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 $h^{-1} \in H$ by ②, so $hh^{-1} = e \in H$ by ① thus $H$ contains identity.
- inverses by ②.

Let $G$ be a group, and consider $H = \{L_g \mid g \in G\} \subseteq \mathrm{Sym}(G)$. Then $H$ is a subgroup:

① $L_g, L_h \in H \Rightarrow L_g \circ L_h = L_{gh} \in H$ ✓

② $L_g \in H \Rightarrow L_{g^{-1}} = L_g^{-1} \in H$. ✓

<u>Definition</u>: Let $G$ and $H$ be groups, and let $\varphi : G \to H$ be a function. $\varphi$ is called an <u>isomorphism</u> if $\varphi$ is bijective and for all $g_1, g_2 \in G$, we have $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$.

<u>Example</u> $G$ a group. $H = \{L_g \mid g \in G\} \leq \mathrm{Sym}(G)$. Define $\varphi : G \to H$ 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,

$$\varphi(g_1 g_2) = L_{g_1 g_2} = L_{g_1} \circ L_{g_2} = \varphi(g_1)\varphi(g_2)$$

So $\varphi$ is an isomorphism.

This proves <u>Cayley's theorem</u>: Every group $G$ is isomorphic to a subgroup of a symmetric group.

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

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

<u>Proposition</u> If $\varphi : G \to H$ is an isomorphism of groups, then $\varphi(e_G) = e_H$, and for all $g \in G$, $\varphi(g)^{-1} = \varphi(g^{-1})$

$$\underbrace{e_G}_{\text{identity of } G} \qquad \underbrace{e_H}_{\text{identity of } H}$$

<u>Proof</u> $e_H \varphi(e_G) = \varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G)$

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, $\varphi(g^{-1}) = \varphi(g)^{-1}$!

<u>Example</u>: Recall complex numbers $a+bi$ $i^2=-1$

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

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

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