What are all the groups?

Def. A **homomorphism** from a group $(G, \circ_G)$ to a group $(H, \circ_H)$ is a map $\phi : G \to H$ which respects the group operations, in the sense that

$$\phi(g_1 \circ_G g_2) = \phi(g_1) \circ_H \phi(g_2), \quad \forall\, g_1, g_2 \in G.$$

i.e.,

$$\begin{array}{ccc} G \times G & \xrightarrow{\circ_G} & G \\ \downarrow{\scriptstyle \phi \times \phi} & \circlearrowright & \downarrow{\scriptstyle \phi} \\ H \times H & \xrightarrow{\circ_H} & H \end{array}$$

An **isomorphism** is a bijective homomorphism. If an isomorphism $\phi : G \to H$ exists, we say that G is **isomorphic** to H.

Thm. Isomorphism is an equivalence rel'n btwn groups.

Ex.

① $R(n) = \{\exp(2\pi i k/n) \mid 0 \le k \le n-1\} \subset \mathbb{C}^*$ is isomorphic to $\mathbb{Z}_n$.

Let $\xi_n = \exp(2\pi i/n)$. Define $\phi : \mathbb{Z}_n \to R(n)$, $k \mapsto \xi_n^k$.

\xi

Notice that ϕ is surjective. Because $\mathbb{Z}_n$ & $R(n)$ are finite of the same order, ϕ is bijective.

Homom. property:

$$\phi(k+m) = \xi_n^{k+m} = \xi_n^k \cdot \xi_n^m = \phi(k) \cdot \phi(m). \checkmark$$

② Every subgroup $n\mathbb{Z}$ of $\mathbb{Z}$ is isomorphic to $\mathbb{Z}$.

$$\phi: \mathbb{Z} \longrightarrow n\mathbb{Z}$$
$$k \longmapsto nk.$$

Check: This is an isomorphism.

③ Because isomorphisms are bijections, groups with distinct orders are never isomorphic.

e.g., $\mathbb{Z}_n \not\cong \mathbb{Z}_m$ if $n \neq m$.

④ Converse is false: non-isomorphic groups can have equal order.

e.g., $D_3 = \langle r, s \mid r^3 = s^2 = (rs)^2 = 1 \rangle \not\cong \mathbb{Z}_6$.

$\not\exists\ \phi: \mathbb{Z}_6 \to D_3$ is an isomorphism.

Pick $m, n \in \mathbb{Z}_6$ s.t. $\phi(m) = r$ & $\phi(n) = s$.

Then

$$rs = \phi(m)\phi(n) = \phi(m+n)$$
$$= \phi(n+m) = \phi(n)\phi(m) = sr.$$

Contradiction! $rs \neq sr$.

⑤ Find all six isomorphisms between $U(8) = \{1, 3, 5, 7\}$ & $U(12) = \{1, 5, 7, 11\}$.

$U(8)$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

$U(12)$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

$1 \mapsto 1$, $3 \mapsto 5$, $5 \mapsto 7$, $7 \mapsto 11$

Thm. Let $\phi: G \to H$ be an isomorphism of groups. Then:

1. $\phi^{-1}: H \to G$ is an isomorphism;
2. $|G| = |H|$;
3. if G is abelian, then H is abelian;
4. if G is cyclic, then H is cyclic;
5. if G has a subgroup of order n, then H has a subgroup of order n.

Idea: If $K \leq G$ has order n, then $\phi(K) \leq H$ has order n.

Thm. A cyclic group G is isomorphic to

- $\mathbb{Z}_n$, if $|G| = n < \infty$;
- $\mathbb{Z}$, if $|G| = \infty$.

(Proof.) Let $a \in G$ be a generator of G, so that

$$G = \{a^k \mid k \in \mathbb{Z}\}.$$

We define $\phi: \mathbb{Z}_{|G|} \to G$, $k \mapsto a^k$

where $\mathbb{Z}_{|G|} = \mathbb{Z}$ if $|G| = \infty$. Then ϕ is a homom., since

$$\phi(m+k) = a^{m+k} = a^m a^k = \phi(m)\phi(k),$$

$\forall\, m, k \in \mathbb{Z}_{|G|}$. Notice that ϕ is surjective: every elt. of G has the form $\phi(k) = a^k$.

If $|G| = n < \infty$, we're finished.

If $|G| = \infty$. Pick $m, k \in \mathbb{Z}$ s.t. $\phi(m) = \phi(k)$.

i.e., $a^m = a^k$. Then $e = a^{m-k}$. (WLOG, $k \leq m$.)

If $m \neq k$, this means a has finite order, a contradiction. So $m = k$. So ϕ is injective. ∎

Cor. Up to isomorphism, the only group of prime order p is $\mathbb{Z}_p$.

Representability

Thm. (Cayley's Theorem)
Every group is isomorphic to a permutation group.

(Proof.) Let G be a group and consider the set $X = G$. We will construct a subgroup

$$\overline{G} \leq S_X$$

and an isomorphism $\phi : G \to \overline{G}$.

Given $g \in G$, define $\lambda_g : X \to X$
$a \mapsto ga$.

Claim. λ_g is a bijection.

- Injectivity: $\lambda_g(a) = \lambda_g(b) \Rightarrow ga = gb \to a = b$ ✓
- Surjectivity: given $a \in X$, $\lambda_g(g^{-1}a) = a$ ✓

So $\lambda_g \in S_X$. Define $\overline{G} := \{\lambda_g \mid g \in G\}$.

NTS: $\overline{G} \leq S_X$.

- $\overline{G} \neq \emptyset$, since $\lambda_e \in \overline{G}$, for instance.
- Given $\lambda_g, \lambda_h \in \overline{G}$, notice that $(\lambda_g)^{-1} = \lambda_{g^{-1}}$, since $(\lambda_{g^{-1}} \circ \lambda_g)(a) = \lambda_{g^{-1}}(ga) = a$.

So $(\lambda_g)^{-1} \circ \lambda_h = \lambda_{g^{-1}} \circ \lambda_h = \lambda_{g^{-1}h} \in \overline{G}$.

Check: $\Phi: G \longrightarrow \overline{G}$ is an isomorphism
$g \longmapsto \lambda_g$ of groups. ∎