Exam 2 next Friday

- Know how to do computations in D_n, S_n (also A_n, Q_8)
- Understand cosets (right vs. left, $aH = bH \iff a^{-1}b \in H$, etc.)
- Lagrange's theorem and its corollaries.

Homomorphisms

Def: Let G and H be groups. A **homomorphism** is a function $\varphi : G \to H$ such that for all $g_1, g_2 \in G$,

$$\varphi(g_1 g_2) = \varphi(g_1)\,\varphi(g_2)$$

product in G product in H

If a homomorphism $\varphi : G \to H$ is also a bijection, then φ is an **isomorphism** and we write $G \cong H$. ("G is isomorphic to H")

$\mathbb{R}\setminus\{0\}$ under multiplication

Ex:

$$\begin{aligned} \det : GL_n(\mathbb{R}) &\to \mathbb{R}^\times \\ A &\mapsto \det(A) \end{aligned}$$

is a homomorphism, since

$$\det(AB) = \det(A)\det(B).$$

It is not an isomorphism (not injective) if $n \geq 2$.

Ex: $\varphi : \mathbb{Z} \to D_n$, $k \mapsto r^k$ is a homomorphism,

since

$$\varphi(k+l) = r^{k+l} = r^k \cdot r^l = \varphi(k)\varphi(l).$$

It is not an isomorphism (not surjective and not injective).

Ex: $\varphi : \mathbb{R} \to (\mathbb{R}_{>0}, \cdot)$, $x \mapsto e^x$

is an isomorphism, since

$$\varphi(x+y) = e^{x+y} = e^x \cdot e^y = \varphi(x)\varphi(y)$$

and φ is a bijection with inverse function $x \mapsto \ln(x)$.

So $\mathbb{R} \cong \mathbb{R}_{>0}$

group under +

group under $\cdot$

Previously (Lecture 12) we proved that if $G = \langle a \rangle$ is a cyclic group, then either

- $|a| = \infty$ and

$$\begin{aligned} \varphi : \mathbb{Z} &\to G \\ k &\mapsto a^k \end{aligned}$$

is an isomorphism

OR

- $|a| = n$ and

$$\begin{aligned} \varphi : \mathbb{Z}_n &\to G \\ k &\mapsto a^k \end{aligned}$$

is an isomorphism.

Ex: $U(9) = \langle 2 \rangle \cong \mathbb{Z}_6$

<u>Remark</u>: It's not too hard to prove the following: For groups G, H, K,

① $id_G : G \to G$ is an isomorphism

Bijection ✓

$id_G(g_1 g_2) = g_1 g_2 = id_G(g_1) \cdot id_G(g_2)$ ✓

② If $\varphi : G \to H$ is an isomorphism, then $\varphi^{-1} : H \to G$ is an isomorphism.

Bijection ✓

Given $h_1, h_2 \in H$, $h_1 = \varphi(g_1)$ and $h_2 = \varphi(g_2)$ for some $g_1, g_2 \in G$.

Then $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) = h_1 h_2$,

so

$\varphi^{-1}(h_1 h_2) = g_1 g_2 = \varphi^{-1}(h_1)\, \varphi^{-1}(h_2)$ ✓

③ If $\varphi : G \to H$ and $\psi : H \to K$ are isomorphisms, then $\psi \circ \varphi : G \to K$ is an isomorphism.

Bijection ✓

For $g_1, g_2 \in G$, $\psi(\varphi(g_1 g_2)) = \psi(\varphi(g_1) \cdot \varphi(g_2)) = \psi(\varphi(g_1)) \cdot \psi(\varphi(g_2))$. ✓

Thus,

1. $G \cong G$
2. $G \cong H \Rightarrow H \cong G$
3. $G \cong H$ and $H \cong K \Rightarrow G \cong K$

That is, $\cong$ is an equivalence relation on groups!

It tells us when two groups are "the same up to relabelling."

We call the equivalence classes of $\cong$ <u>isomorphism classes</u>.

<u>Ambitions project</u>: Describe all groups "up to isomorphism" – that is, describe all isomorphism classes.

<u>Ex</u>: Here are some groups of order 1:

- $\{0\}$ under $+$
- $\{1\}$ under $\cdot$
- $\left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right\}$ under matrix multiplication

$\vdots$

These groups are <u>not equal</u>, because the sets are different.

But they have the <u>same group structure</u>: They each are $\{e\}$, where

$$e \cdot e = e.$$

We say:

$$\boxed{\text{Up to isomorphism, there is only one group of order 1, the \underline{trivial group}.}}$$

Ex: By Corollary 2 to Lagrange's theorem, any group of prime order p is cyclic.

So if $|G| = p$, then $G \cong \mathbb{Z}_p$ (since every cyclic group of order p is isomorphic to $\mathbb{Z}_p$).

Thus:

$$\boxed{\text{Up to isomorphism, there is only one group of order } p \text{ for any prime } p, \text{ namely } \mathbb{Z}_p.}$$

Ex: I claim that

> Up to isomorphism, there are 2 groups of order 4, namely $\mathbb{Z}_4$ and the <u>Klein 4-group</u> V_4.

We have $V_4 = \{e, a, b, c\}$, where

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Some groups isomorphic to V_8:

- $U(8)$
- $U(12)$
- $\{e, r^2, s, sr^2\} \leq D_4$
- $\{e, r^2, sr, sr^3\} \leq D_4$
- $\{id, (12)(34), (13)(24), (14)(23)\} \leq S_4$

Suppose G is a group of order 4.
Then either

<u>Case 1</u>: There is some $g \in G$ with $|g| = 4$.
Then $G = \langle g \rangle$ is cyclic, so $G \cong \mathbb{Z}_4$.

<u>Case 2</u>: There is no $g \in G$ with $|g| = 4$.
Then $|g| = 2$ for all non-identity elements $g \in G$ by Lagrange.

If $x, y \in G$ are distinct non-identity elements, then xy must be the other non-identity element, since

$$xy = e \Rightarrow y = x^{-1} = x \; \times$$
$$xy = x \Rightarrow y = e \; \times$$
$$xy = y \Rightarrow x = e \; \times$$

So $G \cong V_4$.

We must also show $\mathbb{Z}_4 \ncong V_4$.

Suppose $\varphi : \mathbb{Z}_4 \to V_4$ is a homomorphism.

If $\varphi(1) = e$, then

$$\varphi(2) = \varphi(1+1) = \varphi(1)\cdot\varphi(1) = e\cdot e = e,$$

so $\varphi(1) = \varphi(2)$ and φ is not injective.

If $\varphi(1) = x$, where $x = a, b,$ or c, then

$$\varphi(3) = \varphi(1+1+1) = \varphi(1)\cdot\varphi(1)\cdot\varphi(1) = x^3 = x,$$

so $\varphi(1) = \varphi(3)$ and φ is not injective.

Thus, in all cases, φ is not a bijection, so there is no isomorphism between $\mathbb{Z}_4$ and V_4.