Last time:

Thm: If $\varphi: G \to H$ is an injective group homomorphism, then $G \cong \varphi(G)$.

(So G is isomorphic to a subgroup, $\varphi(G)$, of H.)

Ex: We've already seen that labeling the vertices of regular n-gon with $\{1, 2, \dots, n\}$, gives a permutation representation of D_n. (Lecture 18)

This is just an injective homomorphism

$$\varphi : D_n \to S_n,$$

Do you see why?

so D_n is isomorphic to a subgroup of S_n.

More generally...

Thm (Cayley): Every group is isomorphic to a subgroup of a symmetric group.

Proof: Let

$$S_G = \{\text{bijections } G \to G\}$$

be the symmetric group of permutations of G. (If $|G| = n$, then $S_G \cong S_n$.)

For $g \in G$, define the "left multiplication by g" map,

$$\begin{aligned} \lambda_g : G &\to G. \\ x &\mapsto gx. \end{aligned}$$

HW 15: λ_g is a bijection, i.e., $\lambda_g \in S_G$.

So $\lambda_g \in S_G$. (Note: λ_g is not a homomorphism.)

Moreover, for $g, h \in G$,

$$(\lambda_g \circ \lambda_h)(x) = \lambda_g(hx) = ghx = \lambda_{gh}(x),$$

so $\lambda_g \circ \lambda_h = \lambda_{gh}$.

That is,

$$\begin{aligned} \varphi : G &\to S_G \\ g &\mapsto \lambda_g \end{aligned}$$

is a homomorphism!

It is injective because

$$\begin{aligned} \lambda_g = \lambda_h \quad &\Rightarrow \lambda_g(x) = \lambda_h(x) \text{ for all } x \in G \\ &\Rightarrow \lambda_g(e) = \lambda_h(e) \\ &\Rightarrow g = h. \end{aligned}$$

$\blacksquare$

__Remark__: Cayley's theorem isn't practical to use, since S_G is gigantic.

It is of historical importance, since originally groups were __defined__ to be subgroups of symmetric groups.

So Cayley showed that the original notion of a group coincides (up to isomorphism) with our "abstract" definition.

Direct Products

Thm: Let G and H be groups.
Then

$$G \times H = \{(g,h) \mid g \in G \text{ and } h \in H\}$$

is a group under the operation

$$(g_1, h_1) \cdot (g_2, h_2) = (\underbrace{g_1 g_2}_{\text{product in } G},\ \underbrace{h_1 h_2}_{\text{product in } H})$$

Proof: Associativity follows from associativity in G and H.

The identity is (e_G, e_H), where $e_G \in G$ and $e_H \in H$ are the respective identities.

The inverse of (g,h) is (g^{-1}, h^{-1}).

$\blacksquare$

Ex: $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ is a group under coordinate-wise addition:

$$(a, b) + (c, d) = (a+c, b+d).$$

The identity is $(0,0)$ and the inverse of (a, b) is $(-a, -b)$.

Ex: $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (1,0), (0,1), (1,1)\}$

is isomorphic to V_4.

Ex: $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$, since $(1,1)$ is a generator.