

Last time: defined S_n , sym gp on n -elts

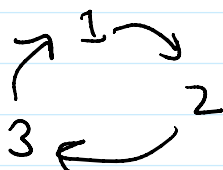
S_n is set of bijective maps

$$\{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$$

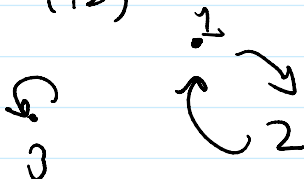
$$|S_n| = n!$$

Play w/ S_3 . $|S_3| = 3! = 3 \cdot 2 \cdot 1 = 6$. Will be non-abelian, the sp.

Denote by x the permutation (123)



Denote by y the perm. (12)



$$x^3 = x \cdot x \cdot x = 1.$$

$$y^2 = 1$$

$$x^{-1} = x^2$$

$$y^{-1} = y$$

Claim:

$$yx \neq xy$$

$$yx: \begin{array}{ccc} & 1 & 2 & 3 \\ x & \downarrow & \downarrow & \downarrow \\ & 2 & 3 & 1 \\ y & \downarrow & \downarrow & \downarrow \\ & 1 & 3 & 2 \end{array}$$

$$xy: \begin{array}{ccc} & 1 & 2 & 3 \\ y & \downarrow & \downarrow & \downarrow \\ & 2 & 1 & 3 \\ x & \downarrow & \downarrow & \downarrow \\ & 3 & 2 & 1 \end{array}$$

$T \in 1 \quad \dots \quad \dots 2 \dots$

In fact, $yx = x^2y$.

Claim The ≤ 6 ^{six} ~~elts~~

$1, x, x^2, y, xy, x^2y$ in S_3 are distinct.

$$\Rightarrow S_3 = \{1, x, x^2, y, xy, x^2y\}.$$

eg. $x^2 \stackrel{?}{=} xy$

If $x^2 = xy$, then $x^{-1}(x^2) = x^{-1}(xy)$

$$\Rightarrow xy = y$$

$$\stackrel{y^{-1}}{\Rightarrow} x = 1 \quad \text{but } x \neq 1.$$

$$\Rightarrow x^2 \neq xy$$

$x^2 \stackrel{?}{=} y$ If $x^2 = y$ then $x(x^2) = xy \stackrel{?}{=} 1$

$$xy = 1$$

$$xy^2 = y$$

$$x = y$$

Ex Let's simplify

$$\underbrace{x^{-2} y x y x^2}_{x^{-2} = x \text{ b/c } x^3 = 1} = x^2.$$

$$= x(y x y) x^2 = x(x^2 y) y x^2 = 1 \cdot y \cdot y x^2 = x^2$$

$$\text{Hence: } yx = x^2y$$

Remark: Using the facts $x^3=1$, $y^2=1$, $yx=x^2y$, can rewrite any word in x, y as one of

$$1, x, x^2, y, xy, x^2y$$

$$1, x, x^2, y, xy, x^2y$$

Subgps: When one gp sits inside another

Examples

- $GL_n(\mathbb{R}) \subseteq GL_n(\mathbb{C})$
- $SL_n(\mathbb{R}) = \{ n \times n \text{ matrices w/ det.} = 1 \}$
is a gp
 $\cap$
 $GL_n(\mathbb{R})$
- $\mathbb{R}^\times$: $\neq 0$ real #'s w/ mult.
 $\cap$
 $\{1, -1\}$ is a subgp
- $S_3 \supseteq \{1, x, x^2\}$

Defⁿ $H \subseteq G$ is a subgp of G if
a gp

Closure: $a, b \in H \Rightarrow a \cdot b \in H$

Identity: $1 \in H$ (1 is the identity of G)

Inverses: If $a \in H$, then $a^{-1} \in H$.

Trivial examples If G is any gp, then $H = \{1\}$ is a subgp.
Also, $H = G$ is a subgp.

Define

Problem: $W \subseteq \mathbb{R}^3$ as $W = \{(x, y, z): x + 2y + 3z = 0\}$.
Prove that W is a subgp of $(\mathbb{R}^3, +)$.

On the other hand, $W' = \{(x, y, z): x + 2y + 3z = 10\}$ is not
a subgp of $(\mathbb{R}^3, +)$

On the other hand, $W = \{(x, y, z) : x + 2y + 3z = 10\}$ is not a subgp of $(\mathbb{R}^3, +)$.

Ans: $\cdot 0 = (0, 0, 0) \in W \Rightarrow W$ has the identity

Inverses If $(x, y, z) \in W$ then $(-x, -y, -z) \in W$.

Closure If $(x, y, z) \in W$ and $(x', y', z') \in W$ then $(x+x', y+y', z+z') \in W$.

Subgps of $(\mathbb{Z}, +)$

- identity of $(\mathbb{Z}, +)$: 0
- gp law: $a, b \mapsto a+b$
- inverses inverse of a : $-a$.

Will do: Classify all subgps H of $(\mathbb{Z}, +)$.

$H \subseteq (\mathbb{Z}, +)$ a subgp means

- $H \subseteq \mathbb{Z}$
- $a, b \in H \Rightarrow a+b \in H$
- $0 \in H$
- If $a \in H$ then $-a$ is in H .

Example $H =$ all multiples of 5.

Propⁿ Suppose $H \subseteq \mathbb{Z}$. Then H is a subgp of $(\mathbb{Z}, +)$

$\Leftrightarrow H = \{0\}$ or $H = \mathbb{Z}a$, all multiples of a , where a is the smallest positive int. in H .

Pf: Clearly $\{0\}$ and $\mathbb{Z}a$ are subgps of $(\mathbb{Z}, +)$.

Conversely, Suppose $H \subseteq \mathbb{Z}$ is a subgp.

Conversely, Suppose $H \subseteq \mathbb{Z}$ is a subgp.

If $H = \{0\}$, then we're done $\checkmark$.

Assume $H \neq \{0\}$. Then $\exists n \in H, n \neq 0$.

B/c H closed under inverses, $-n$ is also in H .

$\Rightarrow H$ contains a positive integer. Let a denote the least pos int in H .

Claim: $H = \mathbb{Z}a$.

Because H is a subgp, and $a \in H$, $\Rightarrow \mathbb{Z}a \subseteq H$.

Need to check! $H \subseteq \mathbb{Z}a$.

Suppose $n \in H$. Write $n = qa + r$ where $q \in \mathbb{Z}$
 $0 \leq r < a$.

Now

$n \in H, qa \in H \Rightarrow -qa \in H \Rightarrow n - qa \in H$.

$0 \leq n - qa = r < a$.

But by assumption, a is smallest pos elt of $H \Rightarrow r = 0$.

$\Rightarrow n = qa \Rightarrow n \in \mathbb{Z}a \checkmark$. $\square$
