

Examples of groupsThe orthogonal group fix $n \geq 1$

$$O_n = \{g \in GL_n(\mathbb{R}) : {}^t g g = 1_n\}.$$

Claim O_n is a gp.

Pf $g_1, g_2 \in O_n$ then ${}^t(g_1 g_2) g_1 g_2 = {}^t g_2 {}^t g_1 g_1 g_2$

$$\begin{aligned} {}^t g_1 g_1 &= 1_n & &= {}^t g_2 g_2 \\ {}^t g_2 g_2 &= 1_n & &= 1_n \end{aligned}$$

• ${}^t 1_n = 1_n \Rightarrow {}^t 1_n 1_n = 1_n \cdot 1_n = 1_n$.

• inverse ${}^t g g = 1_n \Rightarrow \boxed{{}^t g^{-1} g^{-1} = 1_n} \Rightarrow g^{-1} \in O_n$.

Special orthogonal group $SO_n \subseteq O_n$,

$$SO_n = \{g \in O_n : \det(g) = 1\}.$$

Note: If $g \in O_n$, then ${}^t g g = 1 \Rightarrow \det(g)^2 = 1$
 (b/c $\det({}^t g) = \det(g)$)

$$\Rightarrow \det(g) = \pm 1.$$

In other words

$$\det: O_n \rightarrow \{\pm 1\}, \quad \text{gp homom}$$

$\det: O_n \rightarrow \{\pm 1\}$, gp homom

$\cup$
 SO_n is kernel

$$[O_n: SO_n] = |\det(O_n)| = |\{\pm 1\}| = 2$$

check: $\det: O_n \rightarrow \{\pm 1\}$ is surjective

$n=2$ SO_2 : can write very explicitly

Propⁿ: 1) $SO_2 = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R} : a^2 + b^2 = 1 \right\}$
2) SO_2 is abelian

Rmk: If $n > 2$, SO_n is not abelian

Pf: $\cdot g \in SO_n$ means ${}^t g g = I \iff \boxed{g = {}^t g^{-1} \text{ and } \det(g) = 1}$

1)

$$\cdot g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{R})$$

$$g = {}^t \bar{g}^{-1}, \quad \det(g) = ad - bc = 1.$$

$$\bar{g}^{-1} = \frac{1}{\det(g)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \underset{\det(g)=1}{=} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$${}^t \bar{g}^{-1} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix} = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$b^{-1}g = \begin{pmatrix} d & b \\ -b & a \end{pmatrix} = g = \begin{pmatrix} a & b \\ -b & d \end{pmatrix}$$

$$d = a$$

$$c = -b$$

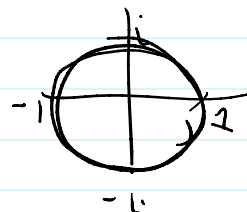
$$\Rightarrow \left(g = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \text{ and } \det(g) = a^2 + b^2 = 1 \right).$$

2) Why is $SO(2)$ abelian

Can verify explicitly w/ matrix $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$.

1) Different proof:

$$\text{Define } S^1 = \{ z \in \mathbb{C} : |z| = 1 \}$$



$$\text{Define: } \varphi: SO(2) \rightarrow S^1$$

$$\text{as } \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mapsto a + ib$$

This lands in S^1 b/c $a^2 + b^2 = 1$ for $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in SO(2)$.

Verify: φ is a gp isomorphism

(S^1 is abelian b/c $S^1 \subseteq \mathbb{C}^\times$, the nonzero complex numbers)

Later in course: $SO(3)$ is the rotations in 3-space

$$SL_2(\mathbb{Z}) = \{g \in SL_2(\mathbb{R}) \cap M_2(\mathbb{Z})\}$$

$$= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z} \text{ and } ad - bc = 1 \right\}.$$

Claim: $SL_2(\mathbb{Z})$ is a gp

Note: If $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, then $g^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} 1 \\ \det(g) \end{pmatrix}^{-1}$
still has integer entries

You should verify: Other conditions

Some subgps: $\left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} : n \in \mathbb{Z} \right\}$

$$\cdot \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

Some elt of $SL_2(\mathbb{Z})$: $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

$$\begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix}$$

Can generalize: $SL_n(\mathbb{Z})$ for $n \geq 2$.

$$SL_n(\mathbb{R}) \cap M_n(\mathbb{Z})$$

Product gps G_1, G_2 gps.

Product gps G_1, G_2 gps.

• The product sp $G = G_1 \times G_2 = \{(g_1, g_2) : g_1 \in G_1, g_2 \in G_2\}$
w/ gp operation

$$(g_1, g_2) \cdot (g'_1, g'_2) = (g_1 g'_1, g_2 g'_2)$$

is componentwise multiplication

Some finite gps

Fix p prime

$$GL_2(\mathbb{Z}/p\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}/p\mathbb{Z} : \underbrace{ad - bc \in (\mathbb{Z}/p\mathbb{Z})^\times} \right\}$$

i.e. $ad - bc \not\equiv 0 \pmod{p}$.

Claim: $GL_2(\mathbb{Z}/p\mathbb{Z})$ is a finite sp w/ order $(p^2-1)(p^2-p)$.

Why is $GL_2(\mathbb{Z}/p\mathbb{Z})$ a sp?

Op operation: Matrix multiplication

$$\underbrace{\begin{pmatrix} a & b \\ c & d \end{pmatrix}}_{a, b, c, d \in \mathbb{Z}/p\mathbb{Z}} \underbrace{\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}}_{a', b', c', d' \in \mathbb{Z}/p\mathbb{Z}} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}$$

$$\underline{aa' + bc' \in \mathbb{Z}/p\mathbb{Z}}$$

Why is this a sp

Why is this a gp

- closed under multiplication

$$\boxed{\det(g_1 g_2) = \det(g_1) \det(g_2)} \quad \text{in } (\mathbb{Z}/p\mathbb{Z})!$$

- $GL_2(\mathbb{Z}/p\mathbb{Z})$ is closed under inverses

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \underbrace{(ad-bc)^{-1}}_{\text{in } (\mathbb{Z}/p\mathbb{Z})^\times} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Should check:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{in } GL_2(\mathbb{Z}/p\mathbb{Z})$$

Some subgps $\det: GL_2(\mathbb{Z}/p\mathbb{Z}) \rightarrow (\mathbb{Z}/p\mathbb{Z})^\times$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto ad-bc$$

$$a, b, c, d \in \mathbb{Z}/p\mathbb{Z}$$

$$\in \mathbb{Z}/p\mathbb{Z}$$

$$\ker(\det) = \{g \in GL_2(\mathbb{Z}/p\mathbb{Z}) : \det(g) \equiv 1 \pmod{p}\}$$

$$=: SL_2(\mathbb{Z}/p\mathbb{Z})$$

Question: What is the size of $SL_2(\mathbb{Z}/p\mathbb{Z})$?

Answer: $\det: GL_2(\mathbb{Z}/p\mathbb{Z}) \rightarrow (\mathbb{Z}/p\mathbb{Z})^\times$

$$\text{is surjective} \Rightarrow \# SL_2(\mathbb{Z}/p\mathbb{Z}) = \# (GL_2(\mathbb{Z}/p\mathbb{Z}))$$

$$\text{is surjective} \Rightarrow \# SL_2(\mathbb{Z}/p\mathbb{Z}) = \frac{\#(GL_2(\mathbb{Z}/p\mathbb{Z}))}{\#((\mathbb{Z}/p\mathbb{Z})^\times)}$$

$$= \frac{(p^2-1)(p^2-p)}{p-1} = (p+1)(p)(p-1)$$

Other subgps of $GL_2(\mathbb{Z}/p\mathbb{Z})$

$$B = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in \mathbb{Z}/p\mathbb{Z} \text{ and } ad \in (\mathbb{Z}/p\mathbb{Z})^\times \right\}$$

$$N = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{Z}/p\mathbb{Z} \right\}$$

is normal

Verify: B, N are subgps of $GL_2(\mathbb{Z}/p\mathbb{Z})$ and $N \subseteq B$ is normal in B .

There is gp homom $\varphi: B \rightarrow (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/p\mathbb{Z})^\times$

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mapsto (a, d)$$

The kernel of this homom is N .