

Group Theory: Classification

Semidirect Products

Notation: $G \cong N \rtimes_{\psi} H$ where

$$\psi: H \rightarrow \text{Inn}(N) \triangleq \text{Aut}_{\text{Grp}}(N)$$

$$h \mapsto \left\{ \begin{array}{l} \gamma_h: N \rightarrow N \\ g \mapsto g^h := hgh^{-1} \end{array} \right\}$$

$$h \mapsto h \cdot (\cdot) \cdot h^{-1}$$

Thm (Recognizing semidirect prods)

- $N \trianglelefteq G$, $H \leq G$ (Note: $N, H \trianglelefteq G \Rightarrow G \cong N \times H$)
- $G = NH$ ($g \in G \Rightarrow \exists n, h$ s.t. $g = nh$) (Need ^{one normal} for $HK \leq G$)
- $H \curvearrowright N$ by conjugation

$$\Rightarrow G \cong N \rtimes_{\psi} H$$

$$\psi: H \rightarrow \text{Aut}(N)$$

$$h \mapsto \psi_h$$

Group law on N

Group law on H

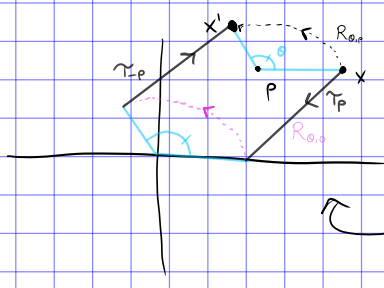
$$\text{Where } (n_1, h_1) \cdot (n_2, h_2) = (n_1 \cdot \psi_{h_1}(n_2), h_1 \cdot h_2)$$

Group law on $N \times H$

$$\text{eg: } (n_1, (h_1 n_2 h_1^{-1}), h_1 h_2)$$

Mnemonic: $N \trianglelefteq G$ necessary for conjugation to be an aut.

Motivating the weird defn:



$$R_{O,P} = \tau_P R_{O,0} \tau_P^{-1} = \tau_P R_{O,0} \tau_P^{-1}$$

Thm: $E(\mathbb{R}^2)$ is generated by

- 1) Rotations about 0
- 2) Reflections through lines (through 0)
- 3) Translations

$$E(\mathbb{R}^2) \cong \mathbb{R}^2 \rtimes O_2(\mathbb{R})$$

Translate

rotate, reflect (linear)

$$\left[\begin{array}{l} \text{Euclidean gp} = \text{isometries} \\ |x-y| = |f(x)-f(y)| \\ \triangleq \text{Aff}(V) = V \rtimes_{\psi} GL(V) \\ f_{\text{lin}} := f_{\text{lin}} \end{array} \right]$$

Enough to just specify a pair $(\vec{v}, M) \in \mathbb{R}^2 \times O_2(\mathbb{R})$

As a set

$$\left[\begin{array}{cc} a & -b \\ b & a \end{array} \right], \left[\begin{array}{cc} c & d \\ d & -c \end{array} \right]$$

But can't be the direct product:

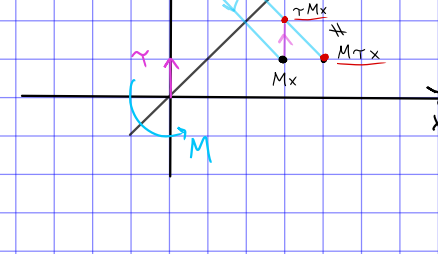
$$G = N \times H \Rightarrow [N, H] = 1$$

$$[n, h] := nhn^{-1}h^{-1} = (nhn^{-1})h^{-1} = h_0 h^{-1} e_H \text{ since } H \trianglelefteq G$$

$$= n(hn^{-1}h^{-1}) = n \cdot n_0 \cdot e_N \text{ since } N \trianglelefteq G$$

$$\Rightarrow [n, h] \in N \cap H = \{1_G\}. \square$$

But $\tau M \neq M \tau$, take $\begin{cases} M = \text{reflect about } y=x \\ \tau = \text{translate by } (1,0) \end{cases}$



or just compute:

$$M[x, y]^T + \tau = [y, x]^T + \tau$$

$$= [y, x+1]^T$$

$$M(\tau + [x, y]^T) = M[x, y+1]^T$$

$$= [y+1, x]^T$$

not equal!

So how do they compose?

$$f(\vec{x}) = A\vec{x} + \vec{v}$$

$$g(\vec{x}) = B\vec{x} + \vec{w}$$

$$(f \circ g)(\vec{x}) = A(B\vec{x} + \vec{v}) + \vec{w}$$

$$= \underbrace{AB}_{\tilde{M}} \vec{x} + \underbrace{A\vec{v} + \vec{w}}_{\tilde{\tau}}$$

$$\Rightarrow (\vec{v}, A) \circ (\vec{w}, B) = (\underbrace{A\vec{v} + \vec{w}}_{\tilde{\tau}}, \underbrace{AB}_{\tilde{M}})$$

Can find a representation:

$$(\vec{v}, A) \rightarrow \begin{bmatrix} A & \vec{v} \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ 1 \end{bmatrix} = \begin{bmatrix} A\vec{x} + \vec{v} \\ 1 \end{bmatrix}$$

$$\text{Check: } \begin{bmatrix} A & \vec{v} \\ 0 & 1 \end{bmatrix} \begin{bmatrix} B & \vec{w} \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} AB & A\vec{v} + \vec{w} \\ 0 & 1 \end{bmatrix} \text{ (works!)} \Rightarrow G \cong \mathbb{R}^2 \rtimes_{\psi} O_2(\mathbb{R})$$

$$\psi: O_2(\mathbb{R}) \rightarrow \text{Aut}(\mathbb{R}^2)$$

$$A \mapsto \psi_A: \mathbb{R}^2 \rightarrow \mathbb{R}^2$$

$$\vec{x} \mapsto A\vec{x}$$

Really $O(\mathbb{R}^2) \rightarrow GL(\mathbb{R}^2)$

the "natural" rep.

$$\text{Where } (\vec{v}, A) \circ (\vec{w}, B) = (\vec{v} + \psi_A(\vec{w}), AB)$$

$$:= (\vec{v} + A\vec{w}, AB)$$

Slogan: Group law on first component "twisted" by a representation ψ , G is a "twisted product" of N and H .

Really:

$$0 \rightarrow N \xrightarrow{i} G \xrightarrow{\pi} H \rightarrow 0 \text{ is a SES in Grp}$$

$$\Rightarrow G \text{ is an extension of } H \text{ by } N \text{ (note } N \cong \ker(\pi) \trianglelefteq G)$$

Thm Split by s: $H \rightarrow G \Rightarrow H \curvearrowright N$, ie N is an H -module.

Pf: Identify $N \cong i(N) \trianglelefteq G$

$$\cdot \text{ Define } \gamma: G \rightarrow \text{Aut}(N) \\ g \mapsto \left\{ \begin{array}{l} \gamma_g: N \rightarrow N \\ x \mapsto g x g^{-1} \end{array} \right\}$$

$$\cdot \text{ Descends to } \text{Aut}(N) \tilde{\gamma}: G \rightarrow \text{Aut}(N)$$

$$g \mapsto \left\{ \begin{array}{l} \gamma_g: N \rightarrow N \\ n \mapsto g n g^{-1} \end{array} \right\}$$

$$(\text{Well-def since } N \trianglelefteq G \Rightarrow g n g^{-1} \in N \forall n \in N)$$

Use splitting to pull back to K

$$\tilde{\gamma}^k: H \rightarrow \text{Aut}(N)$$

$$h \mapsto \left\{ \begin{array}{l} \gamma_{s(h)}: N \rightarrow N \\ n \mapsto s(h) \cdot n \cdot s(h)^{-1} \end{array} \right\}$$

Interesting aside:

Thm There is a correspondence

$$\left\{ \begin{array}{l} \text{SESs} \\ 0 \rightarrow N \rightarrow G \rightarrow H \rightarrow 0 \end{array} \right\} / \sim \cong H^2(H; N)$$

(Group cohomology: $H^n(H; N) = \text{Ext}_{\mathbb{Z}[H]}^n(\mathbb{Z}, N)$)

= Derived functors of $F(\cdot) = H$ -invariants $(\cdot)^H$ on H -mod

Fixed pts of H -action

$$\left\{ \begin{array}{l} \text{Split SESs} \\ 0 \rightarrow N \rightarrow G \xrightarrow{\pi} H \rightarrow 0 \end{array} \right\} / \sim \cong \{ (N, H) \in H\text{-mod} \times \text{Grp} \}$$

$$\cong \{ N \rtimes_{\psi} H \mid \psi: H \rightarrow \text{Aut}(N) \}$$

Back to classifying groups

Ex

$$1) A_n \trianglelefteq S_n \text{ index } 2$$

$$\Rightarrow 1 \rightarrow A_n \rightarrow S_n \rightarrow \mathbb{Z}/2 \rightarrow 1$$

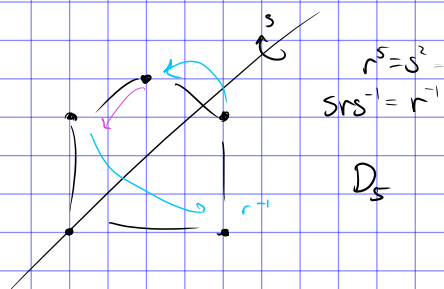
$$\Rightarrow S_n \cong A_n \rtimes \mathbb{Z}_2$$

$$2) D_n = \langle r, s \mid r^n, s^2, srs^{-1} = r^{-1} \rangle$$

$$\langle r \rangle \text{ index } 2$$

$$\Rightarrow 1 \rightarrow \langle r \rangle \rightarrow D_n \rightarrow \langle s \rangle \rightarrow 1$$

$$\Rightarrow D_n \cong \mathbb{Z}/n \rtimes \mathbb{Z}/2$$



Ex

$$\mathbb{Z}/5 \rtimes_{\psi} \mathbb{Z}/3 \cong \mathbb{Z}/5 \times \mathbb{Z}/3 \quad \forall \psi \text{ since}$$

$$\text{Aut } \mathbb{Z}/n \cong (\mathbb{Z}/n)^{\times} = \mathbb{Z}/\phi(n), \quad \phi(3) = 3^1 - 3^0 = 2 \quad \left. \vphantom{\text{Aut } \mathbb{Z}/n} \right\} \phi(p^k) = p^k - p^{k-1}$$

$$\Rightarrow \psi \in \text{Hom}_{\text{Grp}}(\mathbb{Z}/2, \mathbb{Z}/5) = \{0\}$$

$$\text{General fact: } \text{Hom}_{\text{Grp}}(\mathbb{Z}/n, \mathbb{Z}/m) = \{0\} \text{ when } m, n \text{ coprime}$$

$$\text{Why? } f \in \text{Hom} \Rightarrow o(1_n) = n \in \mathbb{Z}/n, \quad o(f(1_n)) \mid o(1_n) \\ \Rightarrow o(f(1_n)) \mid n$$

$$\text{By Lagrange, } o(f(1_n)) \mid |\mathbb{Z}/m| = m$$

$$\Rightarrow o(f(1_n)) \mid \gcd(m, n) = 1 \text{ when coprime.}$$

$$\text{Fact: } \forall \Gamma \in \text{Aut}(H), \quad N \rtimes_{\psi \circ \Gamma} H \cong N \rtimes_{\psi} H$$

$$\text{Fact: } \psi(h) = 1_N \quad \forall h \Rightarrow N \rtimes_{\psi} H \cong N \times H$$

$$\text{Really: } \text{Hom}_{\text{Grp}}(H, \text{Aut}(N)) \in (\text{Aut}(H) \times \text{Aut}(N))\text{-mod} \quad (\text{compose})$$

$$\psi_1, \psi_2 \text{ in the same orbit} \Rightarrow N \rtimes_{\psi_1} H \cong N \rtimes_{\psi_2} H$$

Warning: not conversely! Diff orbits can yield iso groups.

$$\text{Fact: } \text{Aut}((\mathbb{Z}/n)^e) \cong GL_e(\mathbb{Z}/n)$$

$$\text{Hom}_{\text{Grp}}\left(\underbrace{\mathbb{Z}/m}_H, \underbrace{GL_e(\mathbb{Z}/n)}_{\text{Aut}(N)}\right) \cong \{M \in GL_e(\mathbb{Z}/n) \mid M^m = 1\}$$

Conjugation is an Aut on GL_e , so just identify conjugacy classes (eg. by invariant factors)

$$\text{Aut}(\mathbb{Z}/p^e) \cong (\mathbb{Z}/p^e)^{\times} \cong \mathbb{Z}/\phi(p^e)$$

$$\text{Fact: } G = N \rtimes_{\psi} H, \quad \begin{matrix} N \cong \langle \text{Gens}(N) \mid \text{Relns}(N) \rangle \\ H \cong \langle \text{Gens}(H) \mid \text{Relns}(H) \rangle \end{matrix}$$

$$\Rightarrow G = \left\langle \begin{array}{l} \text{Gens}(N) \cup \text{Gens}(H) \\ \text{Relns}(N) \cup \text{Relns}(H) \cup \left\{ \begin{array}{l} h n h^{-1} = \psi_h(n) \quad \forall n \in \text{Gens}(N) \\ \forall h \in \text{Gens}(H) \end{array} \right\} \end{array} \right\rangle$$

$$\text{eg } N = \langle a \mid a^n \rangle$$

$$H = \langle b \mid b^m \rangle$$

$$\Rightarrow N \rtimes_{\psi} H = \langle a, b \mid a^n, b^m, b a b^{-1} = \psi_b(a) \rangle$$

$$\text{Note } N \times H = \langle a, b \mid a^n, b^m, b a b^{-1} = a \rangle \quad N, H \trianglelefteq G \Rightarrow [N, H] = 1$$

Classify all groups of order 18

Soln

$$\cdot 18 = 2 \cdot 3^2$$

$$\cdot n_2 | 3^2 \Rightarrow n_2 \in \{1, 3, 3^2\} \quad \left. \begin{array}{l} n_2 \equiv 1 \pmod{2} \end{array} \right\} \text{All possible "}$$

$$\cdot n_3 | 2 \Rightarrow n_3 \in \{1, 2\} \quad \left. \begin{array}{l} n_3 \equiv 1 \pmod{3} \end{array} \right\} \Rightarrow n_3 = 1$$

$$\cdot n_3 = 1 \Rightarrow \text{Unique normal } \text{Syl}_3(G) \cong S_3 \trianglelefteq G$$

Recognizing semidirect products

$$1) S_3 \trianglelefteq G$$

$$2) G = S_2 S_3 ?$$

$$\hookrightarrow |G| = 2^2 \cdot 3, |S_2| = 2, |S_3| = 3^2$$

$$\hookrightarrow S_2 \cap S_3 = \{1_G\} \text{ since all elts have order dividing } \gcd(2, 3) = 1$$

$$\Rightarrow |S_2 S_3| = \frac{|S_2| \cdot |S_3|}{|S_2 \cap S_3|} = \frac{2 \cdot 3}{1} = |G|$$

$$S_2 S_3 \leq G \Rightarrow \underline{S_2 S_3 = G} \quad \left(\begin{array}{l} \text{subgroup of same size can} \\ \text{only be the entire gp.} \end{array} \right)$$

$$3) S_2 \curvearrowright S_3 ? \quad \text{Sure}$$

$$\psi: S_2 \rightarrow \text{Aut}(G) \quad \begin{array}{l} s \mapsto (g \mapsto sgs^{-1}) \end{array} \quad \begin{array}{l} \text{restricts to} \\ \text{Aut}(S_3) \\ \text{since} \\ gS_3g = S_3 \end{array} \quad \psi|_{S_2}: S_2 \rightarrow \text{Aut}(S_3) \quad \begin{array}{l} s \mapsto (g \mapsto sgs^{-1}) \end{array}$$

$$\Rightarrow G \cong S_3 \rtimes_{\psi} S_2, \quad \psi: S_2 \rightarrow \text{Aut}(S_3)$$

$$\cdot |S_2| = 2 \Rightarrow S_2 \cong \mathbb{Z}/2$$

$$\cdot |S_3| = 3^2, \text{ need to classify gps. of order 9}$$

Thm. Every $|G| = p^2$ is abelian

$$\cdot |G| = p^2 \quad \left\{ \begin{array}{l} G/Z(G) = \mathbb{Z} \times \mathbb{Z}(G) = \langle \times \mathbb{Z}(G) \rangle \\ g \mapsto x^t \mathbb{Z}(G) \rightarrow g = x^t z_1 \rightarrow gh = h g \\ h \mapsto x^m \mathbb{Z}(G) \rightarrow h = x^m z_2 \rightarrow x^t z_1 x^m z_2 \end{array} \right.$$

$$\cdot \text{Consider } \mathbb{Z}(G) \quad \left\{ \begin{array}{l} a) |\mathbb{Z}(G)| = p^2 \Rightarrow \text{Abelian, use classif. of AbGrp.} \\ b) |\mathbb{Z}(G)| = p \Rightarrow |G/\mathbb{Z}(G)| = p \\ \Rightarrow \text{cyclic quotient} \Rightarrow \text{abelian} \end{array} \right.$$

$$c) |\mathbb{Z}(G)| = 1 \Rightarrow \text{Not possible}$$

Thm. p-groups have nontrivial center.

$$\text{Pf: Let } X = \{h \in G \mid o(h) = p\} \leq G, |G| = p^k$$

$$\cdot G \curvearrowright X \quad g \curvearrowright x := gxg^{-1}$$

$$\cdot Gx = \{gxg^{-1} \mid g \in G\} = \bigcup_{g \in G} \{g \curvearrowright x\} = \text{Conj class } G \curvearrowright x$$

$$\cdot G_x = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid g \curvearrowright x = x\} = \text{Centralizer}$$

$$\cdot \text{Orbit-Stabilizer: } \boxed{Gx \cong G/G_x} \quad \text{Mnemonic}$$

$$\Rightarrow |Gx| = [G : G_x]$$

$$\parallel$$

$$|\text{Conj}(x)| = [G : \mathbb{Z}(x)]$$

$$\Rightarrow \mathbb{Z}(x) \leq G \Rightarrow |\mathbb{Z}(x)| = p^e, e \leq k$$

$$\Rightarrow [G : \mathbb{Z}(x)] = p^k / p^e = p^{k-e} := p^n \quad (n \geq 0)$$

$$\cdot |X| \equiv 1 \pmod{p} \quad (\text{claim})$$

$$\text{But } X = \bigsqcup_{\substack{\text{one } x_i \text{ in} \\ \text{each orbit}}} G_{x_i}$$

$$\Rightarrow |X| = \sum_{\substack{\text{one } x_i \text{ in} \\ \text{each orbit}}} |G_{x_i}|$$

$$= \sum_{\substack{\text{one } x_i \text{ in} \\ \text{each orbit}}} |\text{Conj}_G(x_i)|$$

$$= \sum_{\substack{\text{one } x_i \text{ in} \\ \text{each orbit}}} [G : \mathbb{Z}(x_i)]$$

$$= \sum_{\substack{\text{one } x_i \text{ in} \\ \text{each orbit}}} p^{n_i}$$

$$\Rightarrow |X| = \sum_{\substack{\text{one } x_i \text{ in} \\ \text{each orbit}}} p^{n_i} \quad (\text{take mod } p)$$

$$1 \pmod{p} \Rightarrow \text{not all } n_i \geq 1$$

$$\Rightarrow \text{some } n_i = 0$$

$$\Rightarrow [G : \mathbb{Z}(x_i)] = p^0 = 1$$

$$\Rightarrow \mathbb{Z}(x_i) = G \text{ for some } x_i$$

$$\Rightarrow x_i \in \mathbb{Z}(G).$$

$$|G| = |\mathbb{Z}(G)|$$

$$+ \sum_{\substack{\text{one } x_i \\ \text{each class}}} |\text{Conj}(x_i)|$$

$$p$$

$$!!$$

p can't divide both!

$$\therefore S_3 \text{ is abelian, so } S_3 \in \{\mathbb{Z}/3^2, \mathbb{Z}/3 \oplus \mathbb{Z}/3\}$$

$$\left(\begin{array}{l} \langle \mathbb{Z}/3^2 \rangle \\ \langle b, c \mid b^3, c^3, bcb^{-1} = b \rangle \end{array} \right)$$

$$\text{Recall } G \cong S_3 \rtimes_{\psi} \mathbb{Z}/2 = \langle \gamma, \text{Gen}(S_3) \mid \gamma^2, \{ \gamma h \gamma^{-1} = \psi_{\gamma}(h) \forall h \in S^3 \} \rangle$$

$$\text{Case 1: } S_3 \cong \mathbb{Z}/3 \oplus \mathbb{Z}/3 = \langle b, c \rangle \quad \begin{array}{l} b = (1, 0) \\ c = (0, 1) \end{array}$$

$$\cdot \text{Check } \text{Aut}(\mathbb{Z}/3 \oplus \mathbb{Z}/3) \cong (\text{GL}_2(\mathbb{Z}/3), \cdot)$$

$$\cdot \text{Look at } \left\{ \text{Hom}_{\text{Grp}}(\mathbb{Z}/m, \text{Aut}(S_3)) \right\} = \left\{ \text{Hom}_{\mathbb{Z}\text{-mod}} \right\}$$

$$\hookrightarrow \text{Send } [1]_2 \mapsto M \quad M^2 = \text{id}$$

$$\Rightarrow M^2 - I = 0 \Rightarrow \boxed{p(x) := x^2 - 1}$$

$$p(M) = 0.$$

$$\hookrightarrow x^2 - 1 = (x+1)(x-1) \Rightarrow \min_M(x) \in \left\{ \begin{array}{l} x^2 - 1 \\ x + 1 \\ x - 1 \end{array} \right\} := q(x)$$

Pre/post-compose by Auts \Rightarrow only need similarity classes! (JCF)

$$\text{Subcase (a): If } q(x) = x - 1, M \leq I, \quad \psi_{\gamma}(\cdot) = M \cdot \cdot$$

$$\Rightarrow G \cong \langle \gamma, b, c \mid \gamma^2, b^3, c^3, bcb^{-1} = c \rangle$$

$$\left\{ \begin{array}{l} \gamma b \gamma^{-1} = \psi_{\gamma}(b) \\ \gamma c \gamma^{-1} = \psi_{\gamma}(c) \end{array} \right\} \text{ new relations}$$

$$\left\{ \begin{array}{l} \psi_{\gamma}(b) = Mb = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = b \\ \psi_{\gamma}(c) = Mc = c \end{array} \right.$$

$$\Rightarrow G \cong \langle \gamma, b, c \mid \gamma^2, b^3, c^3, bcb^{-1} = c, \gamma b \gamma^{-1} = b, \gamma c \gamma^{-1} = c \rangle$$

$$\text{Conjugation relations } \Rightarrow \langle b, c \rangle \trianglelefteq G, \langle b \rangle, \langle c \rangle \trianglelefteq \langle b, c \rangle$$

$$\text{Recognizing direct products } \Rightarrow G \cong \langle \gamma \rangle \times \langle b \rangle \times \langle c \rangle$$

$$\Rightarrow G \cong \mathbb{Z}/2 \times \mathbb{Z}/3 \times \mathbb{Z}/3$$

$$\text{Subcase (b): } q(x) = x + 1 \Rightarrow M = -I = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$\text{Check } \psi_{\gamma}(b) = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} -1 \\ 0 \end{bmatrix} = -b \mapsto b^{-1} = b^2$$

$$\text{Since } b^3 = e.$$

$$\psi_{\gamma}(c) = -c \mapsto c^{-1} = c^2 \text{ since } c^3 = e$$

$$\Rightarrow G \cong \langle \gamma, b, c \mid \gamma^2, b^3, c^3, bcb^{-1} = c, \gamma b \gamma^{-1} = b^2, \gamma c \gamma^{-1} = c^2 \rangle = \text{Who knows, some group!}$$

$$\text{Subcase (c): } q(x) = x^2 - 1$$

$$\text{Min poly} = \text{char poly} \Rightarrow \text{JCF}(M) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$\psi_{\gamma}(b) = Mb = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = b \mapsto b$$

$$\psi_{\gamma}(c) = Mc = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ -1 \end{bmatrix} = -c \mapsto c^{-1} = c^2$$

Recognizing direct prod

$$\Rightarrow G \cong \langle \gamma, b, c \mid \gamma^2, b^3, c^3, bcb^{-1} = c, \gamma b \gamma^{-1} = b, \gamma c \gamma^{-1} = c^2 \rangle \cong \langle b \rangle \times \langle \gamma, c \mid \gamma c \gamma^{-1} = c^2 \rangle$$

$$\cong \mathbb{Z}/3 \times D_3$$

$$\text{Case 2: } S_3 \cong \mathbb{Z}/3^2 = \langle z \mid z^9 \rangle \quad \phi(3^2) = 3^2 - 3 = 9 - 3 = 6$$

$$\cdot \text{Check } \text{Aut}(G_a(\mathbb{Z}/a)) \cong G_m(\mathbb{Z}/\phi(a)) \cong (\mathbb{Z}/6, \cdot)$$

$$\cdot o([1]_2) = 2 \text{ in } \mathbb{Z}/2 \Rightarrow o(\psi([1]_2)) \mid 2$$

$$\Rightarrow o(\psi([1]_2)) \in \{1, 2\}$$

$$\text{Subcase a: } o(\psi([1]_2)) = 1 \Rightarrow \psi([1]_2) \cong [1]_6$$

$$\Rightarrow [1]_2 \mapsto 1 \in \text{Aut}(\mathbb{Z}/a)$$

\Rightarrow Direct product!

$$G \cong \mathbb{Z}/2 \times \mathbb{Z}/3^2$$

$$\text{Subcase b: } o(\psi([1]_2)) = 2$$

$$\cdot \text{Elts of order 2 in } G_m(\mathbb{Z}/6) = \{[1]_6\}$$

$$\cdot \text{Pulls back to } f: \mathbb{Z}/a \rightarrow \mathbb{Z}/a \in \text{Aut}(\mathbb{Z}/a)$$

$$[1]_a \mapsto [1]_a \quad G_a$$

$$\cdot \text{In mult. notation, } \psi_{\gamma}(z) = z^{-1}$$

$$G \cong \mathbb{Z}/2 \rtimes_{\psi} \mathbb{Z}/3^2$$

$$\Rightarrow G \cong \langle \gamma, z \mid \gamma^2, z^9, \gamma z \gamma^{-1} = z^{-1} \rangle \cong D_9$$

\leadsto 5 groups

$$\left\{ \begin{array}{l} \mathbb{Z}/2 \times \mathbb{Z}/3 \times \mathbb{Z}/3 \\ \mathbb{Z}/2 \times (\mathbb{Z}/3 \times \mathbb{Z}/3) \\ \mathbb{Z}/3 \times D_3 \\ \mathbb{Z}/2 \times (\mathbb{Z}/3^2) \\ D_9 \end{array} \right\} \quad \begin{array}{l} \text{Case 1} \\ \downarrow \\ M^2 = I \leadsto \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \\ \leadsto \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \\ \text{Case 2} \end{array}$$

Classify all abelian groups of order

$$p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$$

$$\hookrightarrow p(n_1) \cdot p(n_2) \cdots p(n_k)$$

$$G \cong \prod_{i=1}^k \mathbb{Z}/p_i^{n_i} \quad p_i \text{ not nec. distinct}$$

Elem divisors:

$$\text{Inv factors: } \prod_{i=1}^n \mathbb{Z}/m_i$$

$$m_1 | m_2 | \cdots | m_n$$

$$\mathbb{Z}_p^n \times \mathbb{Z}_q^n \cong \mathbb{Z}_{pq}^n$$

$$\text{Order } 4225 = 65^2 = 5^2 \cdot 13^2$$

$$p(2) \cdot p(2) = 2 \cdot 2 = 4$$

$$(2, 2) \rightarrow \mathbb{Z}/5^2 \times \mathbb{Z}/13^2 = \mathbb{Z}/4225$$

$$(1+1, 2) \quad \mathbb{Z}/5 \times \mathbb{Z}/5 \times \mathbb{Z}/13^2 = \mathbb{Z}/845 \times \mathbb{Z}/5$$

$$(2, 1+1) \quad \mathbb{Z}/5^2 \times \mathbb{Z}/13 \times \mathbb{Z}/13 = \mathbb{Z}/325 \times \mathbb{Z}/13$$

$$(1+1, 1+1) \quad (\mathbb{Z}/5)^2 \times (\mathbb{Z}/13)^2 = \mathbb{Z}/65 \times \mathbb{Z}/65$$

ED	IF
$5^2, 13^2$	$(5^2 \cdot 13^2)$
$5, 5, 13^2$	$(5)(5 \cdot 13^2)$
$5^2, 13, 13$	$(13)(5^2 \cdot 13)$
$5, 5, 13, 13$	$(5 \cdot 13)(5 \cdot 13)$

$$R/\langle x^2-1 \rangle \rightarrow \frac{R}{\langle x-1 \rangle} \oplus \frac{R}{\langle x+1 \rangle}$$

$$\begin{array}{|c|c|} \hline 5^{n+1} & 5^{n-1} \\ \hline 5 & 13 \\ \hline 13 & \\ \hline \end{array}$$

	$n+1$	$n+1$	$n+2$	$n+3$
2	2^5	2^2	2	2
3	3^{389}	3		
17	17^2	17	17	

Classification gps