Lecture 1. Groups (chapter 2)

- Definition and Examples
- Subgroups
- Homomorphism
- Quotient Groups.

1. Groups

Def: A "Law of composition" (or "binary operation") $*$ on a set S is a rule for asigning each ordered pair (a, b) $(a \in S, b \in S)$ an element c of S.

$$* : S \times S \to S$$
$$(a, b) \mapsto a * b.$$

Ex: $(\mathbb{Z}^+, +)$. $\quad \mathbb{Z}^+ \times \mathbb{Z}^+ \to \mathbb{Z}^+$
$$(a, b) \mapsto a+b.$$

Nonex: $(\mathbb{Z}^+, -)$

Def: (Associativity) A binary operation $(S, *)$ is associative if $(a*b)*c = a*(b*c)$

Ex: $(\mathbb{Z}, +)$

Nonex: $(\mathbb{Z}, -)$.

Def: A group $(G, *)$ is a set with binary operation satisfying the following properties. (write $ab = a*b$).

- Associativity $(ab)c = a(bc)$
- Identity element $1 \in G$, $1 \cdot a = a$ and $a \cdot 1 = a$.
- Inverse: $\forall a \in G$, $\exists b \in G$ such that $a \cdot b = b \cdot a = 1$.

Ex: Permutation group. symmetric group of n-elements.

$$S_n = \{ x : \{1, \cdots n\} \to \{1 \cdots n\} \}.$$

Ex: General linear group.

$GL(n, \mathbb{R}) = \{ n \times n \text{ invertible matrices } A \}$.

$GL(n, \mathbb{C})$

- Subgroup.

Def: A subset S of a group G is a subgroup if.

- closure: $a \cdot b \in S$. $a, b \in S$

- Identity $1 \in S$
- Inverse: if $a \in S$, then $a^{-1} \in S$

Ex: $\{x \in S_n \mid x(n) = n\} \overset{1:1}{\longleftrightarrow} S_{n-1} \subset S_n$

Ex: $\{x \in GL(n) \mid \det x = 1\} \subset GL(n)$

(special linear group) $= SL(n)$

Non ex: $\mathbb{Z}^+ \subset \mathbb{Z}$

Normal subgroup

Def: A subgroup H of G is normal if

$\forall g \in G, h \in H. \quad ghg^{-1} \in H$

Ex: $SL(n) \subset GL(n)$ Non Ex: $S_{n-1} \subset S_n$.

Homomorphism:

Def: A homomorphism $\varphi: G \to G'$ is a map from G to G'.

s.t. $\forall a, b \in G$. $\varphi(ab) = \varphi(a) \cdot \varphi(b)$

Ex: $GL(n, \mathbb{R}) \longrightarrow \mathbb{R}^\times = \mathbb{R} \setminus \{0\}$

$A \longmapsto \det A$.

Ex: $(\mathbb{C}, +) \longrightarrow (\mathbb{C}^\times, \times)$

$a \longmapsto \exp(2\pi\sqrt{-1}\, a)$

Thm: $\ker \varphi = \varphi^{-1}(1)$ is normal subgroup.

Def: An isomorphism is a bijective group homomorphism.

Equivalence relation:

$\sim$ is certain subset of $S \times S$. such that.

(write $a \sim b$ if $(a,b) \in \sim$)

- Transitive
- symmetric
- reflexive.

Partition: S = union of disjoint subsets

Equivalence relation $\Leftrightarrow$ Partition.

$C_a = \{ b \in S \mid a \sim b \}$ then $C_a = C_b$ or $C_a \cap C_b = \phi$.

$$S = \bigsqcup_{a \in S} C_a.$$

$$\bar{S} = \{ C_a \mid a \in S \}$$

Surjective map: $\pi : S \to \bar{S}$

Ex: $S = GL(n)$. $a \sim b$ if $\det a = \det b$.

Ex: $H \subset G$ subgroup

$a \sim b$ if $a = bh$ for some $h \in H$.

Coset: A left coset $aH = \{ ah \mid h \in H \}$.

G/H = set of cosets.

Lagrange's Thm: $|G| = |H| \cdot |G/H|$.
(2.8.9)

Quotient group.

Def and Thm: If $N \subset G$ is a normal subgroup, then G/N has a natural structure of group. such that $G \to G/N$ is a group homomorphism.

Pf: Define $aN \cdot bN = (ab)N$.

(Need to check this well-defined).

If $aN = a'N$, $bN = b'N$, then

$abN = a'b'N$.

$a' = ah_1$, $b' = bh_2$

$$a'b' = ah_1bh_2 = ab\underbrace{(b^{-1}h_1b)}_{\in H}\underbrace{h_2}$$

(First isomorphism Thm)

If $\varphi: G \to G'$ is surjective homo with kernel N. then $\exists!$ isomorphism $\bar{\varphi}: G/N \to G'$, s.t.

$$\begin{tikzcd} G \arrow[rr, "\varphi"] \arrow[dr, "\pi"'] & & G' \\ & G/N \arrow[ur, "\bar{\varphi}"'] & \end{tikzcd}$$

Ex:

$$\mathbb{R} \to U(1) = \{ z \in \mathbb{C}^\times \mid |z| = 1 \}.$$
$$x \mapsto \exp(2\pi\sqrt{-1}\,x)$$

$$\mathbb{R}/\mathbb{Z} \cong S^1 \text{ (circle)}.$$

Ex: Cyclic groups $\mathbb{Z}$. $\mathbb{Z}/n\mathbb{Z} = C_n$.

Product group:

Defn: If G and G' are two groups, there is a natural group structure on its product $G \times G'$, defined by
$$(a, a') \cdot (b, b') = (ab, a'b')$$

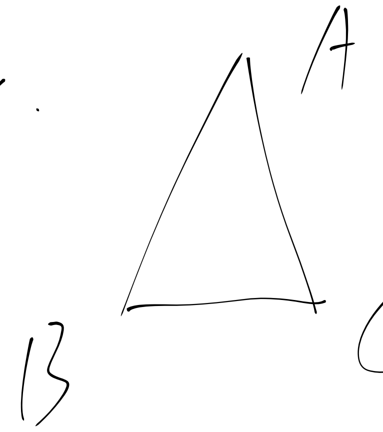
Ex: $C_2 \times C_3 \cong C_6$.

Prop (2.11.4) Let $H, K \subset G$ be subgroups.

$$f: H \times K \to G$$
$$(h, k) \mapsto hk.$$

is an group isomorphism if and only if $H \cap K = \{1\}$, $HK = G$, H, K are normal subgroups of G. and $hk = kh$ for $(h, k) \in H \times K$.

Symmetry

Ex. 

Symmetry of equilateral triangle $\cong S_3$.

$\{1\}$, rotation by $120°$, rotation by $240°$.

reflections fixing A, or B, or C.

Ex. Symmetry of n elements $\cong S_n$.

Ex. Symmetry of vector space $\mathbb{R}^n \cong GL(n)$.

Group operations (actions)

Defn: An operation of a group G on a set S is a map $G \times S \to S$ satisfying
$(g, s) \mapsto g \cdot s$.

a) $1 \cdot s = s$

b) $g_1(g_2 \cdot s) = (g_1 g_2) \cdot s$.

Ex: $G = S_n$. $S = \{1, 2 \cdots n\}$.

$g \cdot k = g(k)$.

Left multiplication: $g \in G$, induces a <u>bijection</u>:

$$m_g : S \to S.$$
$$s \mapsto g \cdot s.$$

Why m_g is a bijection

$$(m_{g^{-1}} \circ m_g) = m_{g^{-1}g} = m_1 = id.$$

Another interpretation of Group operation.

Let $\text{Bijection}(S) = \{f : S \to S \mid f \text{ is a bijection}\}$.

With the natural group structure by composition.

Then a group operation G on S is equivalent to a morphism: $G \to \text{Bijection}(S)$.

$$g \mapsto m_g.$$

More group actions.

$G \to S_n$. as a subgroup of S_n

Ex: G on G itself.

① Left multiplication $g \cdot s = g \cdot s$

(Cayley's Thm) $|G| = n$. then

② right multiplication $g \cdot s = s \cdot g^{-1}$

③ conjugation. $g \cdot s = g s g^{-1}$.

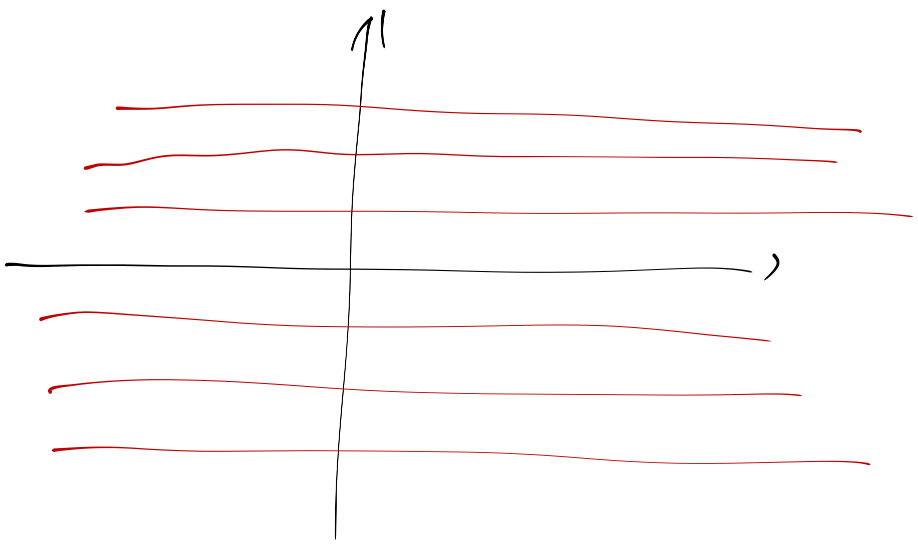
Orbits. $G \circlearrowright S$ (G operates on S).

Defn: $s_1 \sim s_2$ if $g \cdot s_1 = s_2$ for some $g \in G$.

Equivalence classes under "$\sim$" are orbits of this action.

Ex: $\mathbb{R} \circlearrowright \mathbb{R}^2$.

$$\mathbb{R} \times \mathbb{R}^2 \to \mathbb{R}^2$$
$$(a, (x,y)) \to (x+a, y)$$



Ex: Conjugacy classes.

Orbits of conjugation.

Ex: left cosets. G/H.

orbits under right multiplication.

Defn: If S consists of one orbit. the operation of G is called transitive

$\boxed{\text{Decompose the action into actions on different orbits.}}$

Defn: Stabilizer $G_s = \{g \in G \mid gs = s\}$

Prop: a) If $as = bs$, then $a^{-1}b \in G_s$

b). If $as = s'$. $G_{s'} = a G_s a^{-1}$

Operation on G/H.

Defn: $G \times G/H \to G/H$

$(g, aH) \mapsto gaH$.

Check: "well-defined":

If $aH = a'H$, then $gaH = ga'H$.

Prop: ① Transitive.

② Stabilizer. for $s = H$, is H.

for $s = aH$. $G_s = aHa^{-1}$

Prop: $G \curvearrowright S$, Let $s \in S$. $H = G_s$ stabilizer. O_s orbit

There is a bijection $f: G/H \to O_s$. Compatible with the group action. $aH \to as$.

$$\begin{tikzcd} G \times G/H \arrow[r] \arrow[d, "id \times f"] & G/H \arrow[d, "f"] \\ G \times O_s \arrow[r] & O_s \end{tikzcd}$$

$$f(g(aH)) = g \cdot f(aH).$$

Pf: "well-defined".

Check: $aH = a'H$, then $as = a's$.

f: injective. If $as = a's$, then $(a')^{-1}as = s$.

$h = (a')^{-1}a \in H$, $a = a' \cdot h$.

surjective: $s' \in O_s$, $s' = g \cdot s$.

so $f(gH) = s'$

compatible with G-operation.

$$f(g(aH)) = f(gaH) = gas$$

$$g \cdot f(aH) = g \cdot (as) = gas.$$

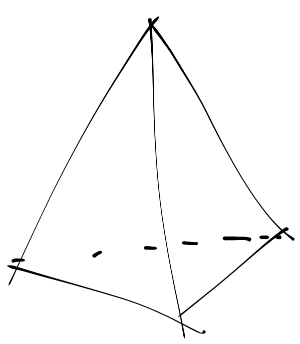
Counting formula.

Prop: $|G| = |G_s| \cdot |O_s|$

$$|S| = |O_1| + \cdots + |O_k|.$$

Ex: $S_n \curvearrowright \{1, \ldots, n\}$.

Ex: rotational symmetry of tetrahedron.



G

$$|G| = |G_s| \, |O_s| = 3 \cdot 4 = 12.$$

More examples of groups and group actions

① S_n acts on $\mathbb{R}^n$. (or $\mathbb{C}^n$). Conjugacy classes in S_n.

② Finite subgroups of $O(2)$, $SO(2)$.

Dihedral group D_n.

Cyclic group C_n.

③ Group action on set of subsets with fixed order.

①

S_n action on $\mathbb{R}^n$

$x \in S_n$. $x : \{1 \dots n\} \mapsto \{1 \dots n\}$

$i \mapsto x_i$.

$e_1 \dots e_n$ basis of $\mathbb{R}^n$.

$e_1 = (1, 0 \dots 0)^T$ $e_2 = (0, 1 \dots 0)^T$

$\vdots$

S_n acts on $e_1 \cdots e_n$. by

$$x(e_i) = e_{x(i)}.$$

then x extends to an action on

$$x(\sum a_i e_i) = \sum a_i \, x(e_i) = \sum a_i \, e_{x(i)}$$

So we have a homomorphism

$$\rho: S_n \to GL(n)$$

$$x \mapsto \begin{array}{r} x(2) \to \\ \\ x(1) \to \\ \\ \\ \end{array} \begin{bmatrix} 0 & \vdots & 0 & \vdots & 0 \\ \vdots & \vdots & \vdots & 1 & \vdots \\ 1 & \vdots & 1 & \vdots & 1 \\ \vdots & 1 & 1 & 1 & \vdots \\ 0 & 1 & & & \end{bmatrix}$$

each row has exactly one "1".

column has exactly one "1"

$$\rho(xy) = [\quad\quad][\quad\quad]$$

Determinant $\det : GL(n, \mathbb{R}) \to \mathbb{R}^\times$

Restriction to S_n.

$$S_n \to GL(n, \mathbb{R}) \to \mathbb{R}^\times$$

$$\text{sign} : S_n \to \mathbb{R}^\times$$

Question : (a) what is the image?

(b) what is the kernel?

(a) $\text{Im}(\text{sign}) = \{\pm 1\}$.

(b) $\ker(\text{sign}) = A_n$. (even permutations)

A_n is a <u>index 2</u> normal subgroup of S_n

Pf: (a) $x^N = 1$ for $N = n!$

$$(\text{sign}(x))^N = 1.$$

so $\text{sign}(x) = \pm 1$.

Take $x(1) = 2$

$x(2) = 1$

$x(i) = i \quad i \geq 3.$

$\text{sign}(x) = -1$

More structures on S_n.

Defn: cycle $x = (i_1 \cdots i_k)$ $i_1 \cdots i_k$ distinct.

$x(i_1) = i_2$, $x(i_2) = i_3, \cdots$

$x(i_k) = i_1$. $x(j) = j$ if $j \notin \{i_1 \cdots i_k\}$

Prop: If $x = (i_1 \cdots i_k)$ k is the length of x.

$y = (j_1 \cdots j_l)$

$\{i_1 \cdots i_k\} \cap \{j_1 \cdots j_l\} = \phi$.

then $xy = yx$. (disjoint cycles)

Thm (cycle decomposition).

Any $x \in S_n$ can be written as

$x = x_1 x_2 \cdots x_t$, x_i are disjoint cycles. $x_1 \cdots x_t$ is unique up to a permutation of index $1 \ldots t$.

Ex:

$$\begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 7 & 6 & 2 & 5 & 3 & 4 & 1 \end{matrix}$$

$x = (1\,8)(2\,7\,4)(3\,6)$

Pf: Existence. $S = \{i \mid x(i) \neq i\}$.

Induction on $|S|$ to prove $x = x_1 \cdots x_t$ and the union of elements appeared in x_i is S.

$\{i_1 \cdots i_k\} = \{i \mid x(i) \neq i\}$.

$i_1, x(i_1) \ldots x^m(i_1)$.

$\exists\ n_1 \leq n_2$, s.t. $x^{n_1}(i_1) = x^{n_2}(i_1)$.

Take n_2 to be the first number such that

$x^{n_1}(i_1) = x^{n_2}(i_1)$

Then $x^{n_2 - n_1}(i_1) = i_1$.

so $n_1 = 0$, and $\underbrace{i_1, x(i_1) \ldots x^{n_2-1}(i_1)}_{C}$

are distinct.

Let $x_1 = (i_1 \cdots x^{n_2-1}(i_1))$.

and $\tilde{x} = x_1^{-1} x$

$x(j) \notin \{i_1 \ldots x^{n_2-1}(i_1)\}$ if $j \notin C$.

$\{\tilde{x}(i) \neq i\} = S - C$

Use induction assumption on $\tilde{x}$.

$\tilde{x} = x_2 \cdots x_t$

Uniqueness. If $x = x_1 \cdots x_t$

$= y_1 \cdots y_m$.

$\{x(i) \neq i\}$ is the union of elements appeared in x_i, and also y_i.

so if $x_1(i_1) \neq i_1$, then i_1 must appear in some y_j.

recover y_j and x_1 use $i_1, x(i_1) \dots x^{n_2}(i_1)$

Each cycle decomposition corresponds to a partition of $n = k_1 + k_2 + \dots k_t + 1 \dots + 1$

$5 = 2+3$
$= 3+2$ same partition.

Thm: $x, y \in S_n$ are conjugate iff x, y corresponds to the same partition of n.

Pf: If $x = (i_1 \cdots i_k)$ is a cycle.

then $gxg^{-1} = (g(i_1) \dots g(i_k))$.

If $x = x_1 \cdots x_t$.

then $gxg^{-1} = gx_1g^{-1}gx_2g^{-1} \cdots gx_tg^{-1}$

gx_ig^{-1} are disjoint cycles

So all the elements conjugate to x correspond to the same partition of n.

Conversely, if x, y correspond to the same partition of n. then we have cycle decompositions

$x = x_1 x_2 \cdots x_t$

$y = y_1 y_2 \cdots y_t$.

such that the length of x_i is the same as length of y_i,

assume $x_i = (a_1^i \cdots a_{k_i}^i)$

$y_i = (b_1^i \cdots b_{k_i}^i)$

and let $\{c_1 \cdots c_\ell\} = \{i \mid x(i) = i\}$.

$\{d_1 \cdots d_\ell\} = \{i \mid y(i) = i\}$.

Define $g(a_m^i) = b_m^i$

$g(c_i) = d_i$.

Then $gxg^{-1} = y$.

$\square$.

conclusion.

$\#$ of conjugacy classes $= \#$ of partitions of n.

Infinite group. $GL(2,\mathbb{R})$ acting on $\mathbb{R}^2$.

$$gv = \begin{bmatrix} x & x \\ x & x \end{bmatrix} v.$$

Put more structure on $\mathbb{R}^2$.

$|v| = \sqrt{v_1^2 + v_2^2}$ or $\langle v, w \rangle = v^t w$.

Defn ($O(2)$, orthogonal group)

The following are equivalent. (TFAE).

① $|gv| = |v|$ for all $v \in \mathbb{R}^2$

② $\langle gv, gw\rangle = \langle v, w\rangle$.

③ $g^t g = I$.

$|v|$ and $\langle \cdot \rangle$ are related by
$|v| = \sqrt{\langle v, v\rangle}$
$\langle v, w\rangle = \frac{1}{2}\left(|v+w|^2 - |v|^2 - |w|^2\right)$
(parallelogram law)

Structure of $O(2)$.

$g = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ $\quad g^t g = I$

$\Rightarrow \begin{pmatrix} a & c \\ \hline b & d \end{pmatrix}\left(\begin{array}{c|c} a & b \\ c & d \end{array}\right) = \begin{pmatrix} a^2+c^2 & ab+cd \\ ab+cd & b^2+d^2 \end{pmatrix}$.

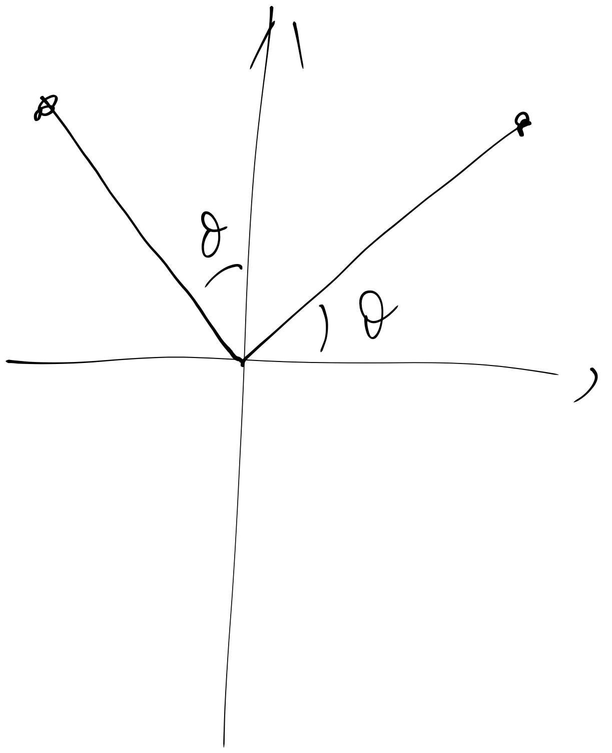
$a^2+c^2 = 1 = b^2+d^2$. $\quad \underline{ab+cd} = 0$.

$a = \cos\theta$, $\quad b = -\sin\theta$ $\quad$ or $\quad b = \sin\theta$

$c = \sin\theta$ $\quad d = \cos\theta$ $\quad\quad d = -\cos\theta$.

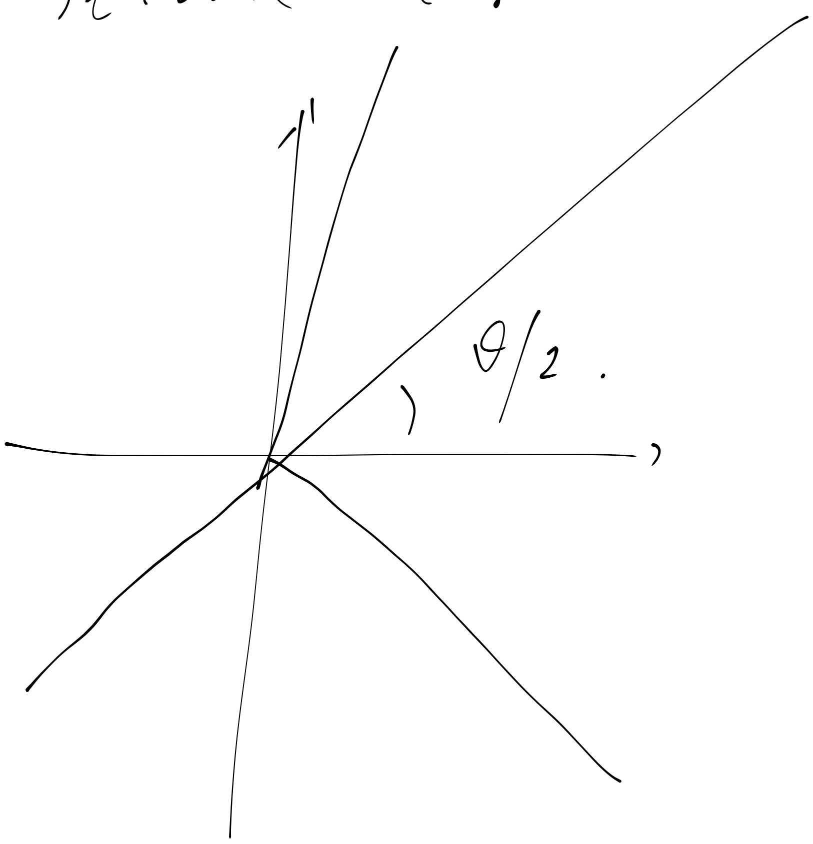
First case $\quad g = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$.

$g e_1 = \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}$ $\quad g(e_2) = \begin{pmatrix} -\sin\theta \\ \cos\theta \end{pmatrix}$



rotation.

second case.



reflection w.r.t $\theta/2$.

$\mathrm{Det} : O(2) \to \{\pm 1\}$.

$\ker(\mathrm{Det}) = SO(2) = \left\{ \underbrace{\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}}_{= \rho_\theta} \right\}$.

Finite subgroups of $SO(2)$.

Thm: $G \subset SO(2)$ a finite subgroup.

then $G = \langle \rho_\theta \rangle$ $\theta = \frac{2\pi}{n}$.

and $G \cong C_n$.

Pf: (Euclidean division).

Let $\theta_1 = \min \{ \rho_\theta \in G \mid 0 < \theta < 2\pi \}$.

Then $\rho_{\theta_1} \in G$, $\langle \rho_{\theta_1} \rangle \subset G$.

If $G \not\subset \langle \rho_{\theta_1} \rangle$, then $\exists\ \rho_\theta \in G$.

s.t. $\rho_\theta \notin \langle \rho_{\theta_1} \rangle$

Let $\theta = m\theta_1 + r$. $m \in \mathbb{Z}_{\geq 0}$.

$0 \leq r < \theta$.

Since $\rho_\theta \notin \langle \rho_{\theta_1} \rangle$.

then $r > 0$.

so $\rho_\theta \cdot \rho_{-m\theta_1} = \rho_r \in G$

contradiction with definition of θ_1.

So $G = \langle \rho_{\theta_1} \rangle$ and for any

$\rho_\theta \in G$, $\theta = m \cdot \theta_1$.

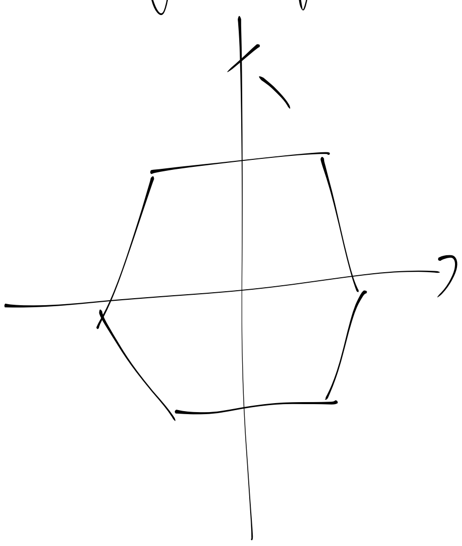
since ρ_{θ_1} has finite order.

$\theta_1 = \frac{2\pi}{n}$.

$\square$

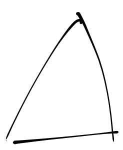
Finite subgroup of $O(2)$.

D_6



6 rotations
6 reflections.

D_3



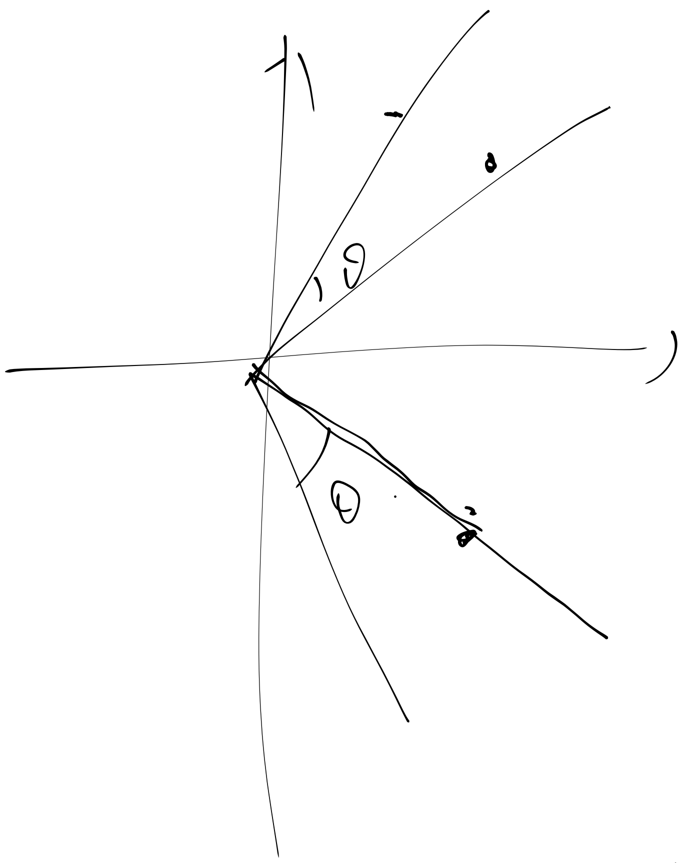
$D_3 \cong S_3$.

D_n symmetry of n-gon.

$x = \rho_\theta \qquad \theta = \frac{2\pi}{n}.$

y = reflection $\qquad y^2 = 1.$

$yxy^{-1} = x^{-1}.$



$$y = \begin{bmatrix} 1 & \\ & -1 \end{bmatrix}$$

or $$y = \begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{pmatrix}$$

$$y^2 = 1.$$

$$yxy^{-1} = x^{-1}.$$

elements in D_n $\quad 1, x, \ldots, x^{n-1}, y, xy, \ldots, x^{n-1}y$

Thm (6.4.1) any finite subgroup G of O_2 is

(1) C_4

(2) D_n. generated by ρ_θ and reflection about a line l through the origin.

Pf: $G \subset SO(2)$. then case (1)

$G \not\subset SO(2)$. then $\exists\, y \in G$. $y \notin SO(2)$.

Assume $y = \begin{bmatrix} 1 & \\ & -1 \end{bmatrix}$

$G \cap SO(2) = \langle \rho_\theta \rangle$.

Claim $D_n = \langle \rho_\theta, y \rangle = G$.

① $D_n \subset G$. obvious

② $D_n \supset G$. Any $g \in G$. if $g \notin SO(2) \cap G$.

then $gy \in G \cap SO(2)$.

so $g = (gy)y \in D_n$.

Conjugacy classes in D_n. $x = \rho_{\frac{2\pi}{n}}$, $y = \begin{bmatrix} 1 & \\ & -1 \end{bmatrix}$

n even: $\{1\}$, $\{x, x^{-1}\}$. $\{x^2, x^{-2}\}$, ... $\{x^{\frac{n}{2}}\}$.

$\{y, x^2y, x^4y, \dots x^{n-2}y\}$

$\{xy, x^3y, \dots x^{n-1}y\}$.

n odd: $\{1\}$, $\{x, x^{-1}\}$. $\{x^2, x^{-2}\}$, ... $\{x^{\frac{n-1}{2}}, x^{\frac{n+1}{2}}\}$

$\underbrace{\{y, x^2y, x^4y, \dots x^{n+1}y = xy, x^3y, \dots x^{n-2}y\}}_{\text{all the reflections}}$.

Pf: Use the equalities

$(x^k y) x (x^k y)^{-1} = x^k y x y x^{-k} = x^k x^{-1} y^2 x^{-k} = x^{-1}$.

$x^k y x^{-k} = x^{2k} y$. $\quad x^k (x^m y) x^{-k} = x^{2k+m} y$.

$(x^k y) y (x^k y)^{-1} = x^{2k} y$. $\quad (x^k y) x^m y (x^k y)^{-1} = x^{2k-m} y$.

$= x^{2(k-m)} x^m y$.

Generate new group actions by existing group actions.

① restrict to subgroup H

② act on set of subsets of a fixed order

Sylow's Thm

Defn: Center of G.
$Z(G) = \{g \in G \mid gh = hg \text{ for all } h \in G\}$
is a normal subgroup of G.

Defn: p-group. $|G| = p^n$.

Prop: Center of a p-group is nontrivial.

Consider the conjugate action of G on G.

$p^n = |G| = |O_1| + |O_2| \cdots |O_k|$.

$O_1 = \{1\}$. $\exists\ O_i$, s.t. $|O_i| = 1$.

Thm (Fix point Thm) $G \curvearrowright S$.

$p \nmid |S|$. then there is an element in S

s such that $G_s = G$. (s is fixed by G)

Prop: $|G| = p^2$, then G is abelian.

Pf: $G/Z(G) \neq \{1\}$. then $|Z(G)| = p$.

$\exists\ g \notin Z(G)$

Consider $Z(g) = \{h \in G \mid hgh^{-1} = g\}$.

centralizer.

then $Z(G) \subset Z(g)$.

and $g \in Z(g)$.

so $|Z(g)| > p$. $|Z(g)| = p^2 = |G|$

so $g \in Z(G)$. contradiction.

$\square$

Corollary: $|G| = p^2$, then $G \cong C_p \times C_p$

or $\cong C_{p^2}$

Pf: order of element in $G \mid p^2$.

① maximal order $= p^2$

$G = \langle g \rangle$ with $\operatorname{ord} g = p^2$

② maximal order $= p$.

then $G \supset \langle k \rangle$.

$G/\langle k \rangle \cong C_p$.

Choose $h \in G$, $h \notin \langle k \rangle$.

then $\underbrace{\langle h \rangle}_{= H} \cap \underbrace{\langle k \rangle}_{= K} = \{1\}$.

H, K both normal subgroups.

$|HK| > p$ $|HK| = p^2$, $HK = G$.

$G \cong H \times K$

How about $|G| = p^3$.

$$\left\{ \begin{bmatrix} 1 & x & z \\ & 1 & y \\ & & 1 \end{bmatrix} \right\} \quad x \in \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p.$$

subgroup of $GL(3, \mathbb{F}_p)$.

What is the center?

$$\begin{bmatrix} 1 & x & z \\ & 1 & y \\ & & 1 \end{bmatrix} \begin{bmatrix} 1 & x' & z' \\ & 1 & y' \\ & & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & x'+x & z'+xy'+z \\ & 1 & y'+y \\ & & 1 \end{bmatrix}$$

If $xy' \neq x'y$, then they don't commute.

So $\begin{bmatrix} 1 & 0 & z \\ & 1 & 0 \\ & & 1 \end{bmatrix}$ is the center.

Question: What are the possible G, such that $|G| = p^3$.

More familiar example $G = D_4$ $|G| = 8$. D_n is not Abelian when $n \geq 3$.

Question: Is $D_4 \cong \left\{ \begin{bmatrix} 1 & x & y \\ & 1 & z \\ & & 1 \end{bmatrix} \middle| \; x, y, z \in \mathbb{F}_2 \right\}$?

Normalizer. $N(H) = \{ g \in G \mid gHg^{-1} = H \}$.

Counting formula: $|G| = |N(H)| \,/\,$ number of conjugate subgroups of H. /

Prop: a) H is a normal subgroup of N.

b). H is normal in G iff $G = N(H)$

c). $|H| \mid |N|$. $|N| \mid G$.

Example: $p = (12)(34) \in S_5$.

gpg^{-1} has $\binom{5}{2}\binom{3}{2}/2 = \frac{5\times 4}{2\times 1} \times \frac{3\times 2}{2\times 1}/2$

$= 15$.

$|N(\langle p \rangle)| = \frac{120}{15} = 8$

$N(\langle p \rangle) = \{ 1, \begin{pmatrix} 1&2&3&4&5 \\ 2&1&3&4&5 \end{pmatrix}, \begin{pmatrix} 1&2&3&4&5 \\ 1&2&4&3&5 \end{pmatrix}, \begin{pmatrix} 1&2&3&4&5 \\ 2&1&4&3&5 \end{pmatrix}, \begin{pmatrix} 1&2&3&4&5 \\ 3&4&1&2&5 \end{pmatrix}, \begin{pmatrix} 1&2&3&4&5 \\ 3&4&2&1&5 \end{pmatrix}, \begin{pmatrix} 1&2&3&4&5 \\ 4&3&1&2&5 \end{pmatrix}, \begin{pmatrix} 1&2&3&4&5 \\ 4&3&2&1&5 \end{pmatrix} \}$

Defn: Sylow p-group $|G| = p^e \cdot m$. $p \nmid m$.

subgroup $H \subset G$ such that $|H| = p^e$ is called Sylow p-group.

$|G/H| = [G:H]$ = index of H in G.

1st Sylow thm: (Existence).

If $p \mid |G|$, then G contains a sylow p-group.

2nd : (conjugate)

① The Sylow p-groups are conjugate.

② H subgroup that is a p-group is contained in a Sylow p-group.

3rd. $|G| = p^e m$. s = number of sylow p-groups.

$s \equiv 1 \mod p$. $s \mid m$.

Application: $|G| = 15$. then $G \cong C_{15}$.

H sylow 3-group $H \cong C_3 = \langle h \rangle$

K Sylow 5-group $K \cong C_5 = \langle k \rangle$.

H, K normal subgroups $HK = G$.

$H \cap K = \{1\}$, so $G \cong H \times K$.

$|G| = 6$, H sylow-3 group

K sylow-2 group.

H normal subgroup.

K normal or K_1, K_2, K_3 3-Sylow group.

$G \curvearrowright \{[K_1], [K_2], [K_3]\}$ by conjugation.

$\rho : G \to S_3$. $\ker \rho = \{1\}$.

Pf of Sylow's Thms:

Lemma 1: U subset of G, $\mathrm{Stab}([U])$ of $[U]$ for the operation of left multiplication by G on the set of its subsets divides both $|U|$ an $|G|$.

Pf: $H = G_{[U]}$ then

$$U = \bigsqcup_{g \in U} Hg \quad \text{so} \quad |H| \,\big|\, |U|.$$

Lemma 2: $|\text{Set of subsets with order } p^e| = N$.

$|S| = p^e m$. $p \nmid m$.

$p \nmid N$.

Pf: $N = \binom{n}{p^e} = \frac{n(n-1)\cdots(n-p^e+1)}{p^e(p^e-1)\cdots 1}$.

$k = p^\ell k_0$. $p \nmid k_0$. define $\nu(k) = \ell$.

For $1 \le k \le p^e - 1$. $\nu(k) < e$.

$\nu(p^e - k) = \nu(k)$. $\left(\nu(m_1 + m_2) = \min\{\nu(m_1), \nu(m_2)\} \right)$

$\nu(p^e m - k) = \nu(k)$.

$\nu(m_1 m_2) = \nu(m_1) \cdot \nu(m_2)$.

So $\nu(N) = \nu(n) - \nu(p^e) + \nu(n-1) - \nu(p^e - 1) \cdots$

$= 0$.

Pf of 1st Sylow's Thm:

Consider $S = \{ U \subset G \mid |U| = p^e \}$.

$|S| = N = \binom{p^e m}{p^e} \not\equiv 0 \pmod p$

$N = |O_1| + |O_2| \cdots |O_k| \not\equiv 0 \pmod p$.

$p^e m = |G| = |O_i| \cdot |G_i|$. G_i = stabilizer of $[U_i] \in O_i$.

$\exists i$, s.t. $p^e \mid |G_i|$.

Lemma1 $\Rightarrow$ $|G_i| \mid V_i$.

so $|G_i| = p^e$

2nd Sylow's Thm: K p-subgroup. H Sylow p-subgroup.

Consider the action of K on G/H.

K fix some aH. by fixed point theorem (proved last time)

then $K \subset aHa^{-1}$

3rd Sylow's Thm: G action on

$S = \{$ Sylow p-subgroups $\}$.

is transitive.

$|S| \cdot |N(H)| = |G|$.

$H \subset N(H)$. so $|S| \mid m$.

Restrict to H, splits into orbits.

$$|S| = |O_1| + |O_2| + \cdots |O_k|$$

$$\{[H]\} = O_1.$$

$$|O_k| \,\Big|\, |H| = p^e.$$

$|O_i| = 1$ means $O_i = \{[K]\}$.

and $gKg^{-1} = K$ for all $g \in H$.

$H \subset N(K)$.

Both H, K are sylow p-subgroups of $N(K)$.

so H, K are conjugate in $N(K)$.

So $H = K$. because K is normal subgroup of $N(K)$

02/11.

More applications of Sylow's Thms and Semi-direct product.

Classify Finite group G of order 21.

\# of 7-sylow subgroup is 1.

\# of 3-sylow subgroup is 1 or 7.

Case 1. H unique sylow 7-group.

H normal subgroup. $H \trianglelefteq G$.

K unique Sylow 3-group

$H \cap K = \{1\}$. $HK \cong H \times K$.

$HK = G$.

$G \cong C_3 \times C_7 \cong C_{21}$

Case 2. $K_1 \cdots \cdots K_7$ Sylow 3-groups

Let $K = K_1$

$$G \not\cong H \times K.$$

H normal subgroup $\Rightarrow HK = KH$ subgroup

(Homework 2, problem 3)

$H \cap K = \{1\}$.

$H \times K \to G$. (Note not a morphism)

$(h, k) \mapsto hk$.

Injective because $h_1 k_1 = h_2 k_2$.

$\Rightarrow h_2^{-1} h_1 = k_2 k_1^{-1} \in H \cap K$.

Bijective because of the order $|H \times K| = |G|$.

Every element in G has a unique form

hk, $h \in H$, $k \in K$.

How to find the product structure?

$$hk\,h'k' = h(kh'k^{-1})kk'$$

Need to determine $kh'k^{-1}$

$$\varphi : K \longrightarrow \mathrm{Aut}(H).$$
$$k \longmapsto \varphi(k) : h \mapsto khk^{-1}$$

φ is a group morphism

$H = \langle x \rangle. \quad x^7 = 1.$

$K = \langle y \rangle \quad y^3 = 1.$

$y x y^{-1} = x^{i}?$

$\mathrm{Aut}(C_7) \cong (\mathbb{Z}/7\mathbb{Z})^{\times} \cong \mathbb{Z}/6\mathbb{Z}$

$yxy^{-1} = x^j$, $\quad y^2xy^{-2} = yx^jy^{-1}$

$= (x^j)^j = x^{j^2}$

$y^3xy^{-3} = x^{j^3} = 1$.

so $j^3 \equiv 1 \pmod 7$.

$\bar{0}$ $\bar{1}$ $\bar{2}$ $\bar{3}$ $\bar{4}$ $\bar{5}$ $\bar{6}$

cube $\bar{0}$, $\bar{1}$, $\bar{1}$, $\bar{6}$, $\bar{1}$, $\bar{6}$, $\bar{6}$

$j = 2$ or 4. (choose y^2 instead of y makes $j = 2$).

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

Defn (outer semi direct product). H, K groups.

$\varphi: K \to \mathrm{Aut}(H)$ is a homomorphism.

There is a group structure on $H \times K$ by

$$(h, k) \cdot (h', k') = (h \cdot \varphi(k) h', \; k k')$$

(Check this defines a group structure.)

It is denoted by $H \rtimes_\varphi K$.

Thm: If H is a normal subgroup of G,

K is a subgroup of G,

$H \cap K = \{1\}$, and $G = HK$,

then G is isomorphic with the semi direct product $H \rtimes_\varphi K$ with

$$\varphi: K \to \mathrm{Aut}\, H$$

$$k \mapsto \varphi(k): h \mapsto k h k^{-1}.$$

Review for 1st midterm:

Defn: Groups, subgroups, normal subgroups.
cyclic group, homomorphism, isomorphism,
Quotient group, 1st isomorphism thm.
Group operation orbits, stabilizer.
Conjugation centralizer, normalizer.
Conjugacy classes,
Counting formula.

p-groups, $|G|=p$, $G \cong C_p$.
.. $|G|=p^2$, $G \cong C_p \times C_p$, C_{p^2}.
$|G|=p^3$ can be non abelian.

Sylow's Thms

Ex: $A_n \subset S_n$, D_n,

$SL(n) \subset GL(n)$

$SO(2) \subset O(2)$

finite subgroups in $O(2)$ and $SO(2)$

Classify G of order 12.

$|G| = 12, = 2^2 \times 3$.

$|\{\text{Sylow 2-groups}\}| = s = 1$ or 3.

$|\{\text{Sylow 3-groups}\}| = s' = 1$ or 4,

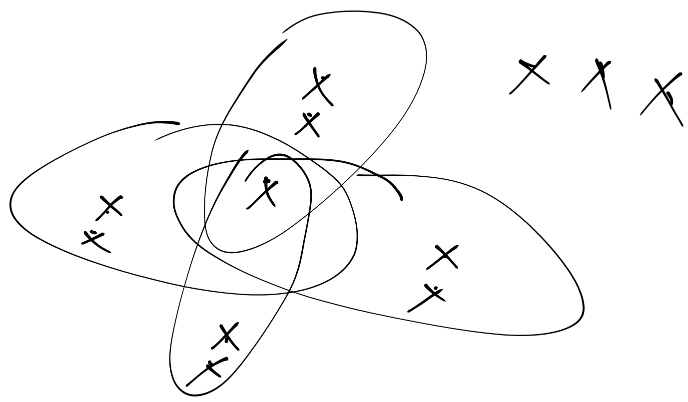
If $s = 3$, $s' = 4$,

there're 4 Sylow 3-groups.

K_1, K_2, K_3, K_4

$K_i \cap K_j = \{1\}$ for $i \neq j$ because they're cyclic.

so



Let H be Sylow-2group.

then $H \subset \{1\} \cup (K_1 \cup K_2 \cup K_3 \cup K_4)^c$

and $|H| = 4$

so H is unique.

Case 1 $H \lhd G$,

Case 2 $K \lhd G$.

1a $H \cong C_2 \times C_2$, $K = C_3 = \langle y \rangle$.

Let $H = \langle x_1, x_2 \rangle$ $x_1^2 = x_2^2 = 1$. $x_1 x_2 = x_2 x_1$

Let $f \in Aut(H)$

then $f\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}a_{11}\\a_{12}\end{pmatrix}$

$$f\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}a_{21}\\a_{22}\end{pmatrix}$$

$$\begin{pmatrix}a_{11}\\a_{12}\end{pmatrix} \neq \begin{pmatrix}0\\0\end{pmatrix} \quad \text{and} \quad \begin{pmatrix}a_{21}\\a_{22}\end{pmatrix} \neq \begin{pmatrix}0\\0\end{pmatrix} \text{ or } \begin{pmatrix}a_{11}\\a_{12}\end{pmatrix}$$

So $|Aut(H)| = (2^2-1)(2^2-2) = 6$

$$f = \left\{ \begin{pmatrix}1 & \\ & 1\end{pmatrix} \begin{pmatrix}1 & 1\\ & 1\end{pmatrix} \begin{pmatrix}1 & 0\\1 & 1\end{pmatrix} \begin{pmatrix}1 & 1\\1 & 0\end{pmatrix} \begin{pmatrix}0 & 1\\1 & 1\end{pmatrix} \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix} \right.$$

$$\varphi : K \to Aut(H)$$

$$y \mapsto \varphi(y) = f.$$

$f^3 = 1.$ $\Rightarrow$ $f = \begin{pmatrix}1 & 1\\1 & 0\end{pmatrix}$ or $\begin{pmatrix}0 & 1\\1 & 1\end{pmatrix}$

or $\begin{pmatrix}1 & \\ & 1\end{pmatrix}$

up to a choice of generators for H (or K).

we can assume $f = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ or $\begin{pmatrix} 1 & \\ & 1 \end{pmatrix}$

so $G = \langle x_1, x_2, y \rangle$.

$$x_1^2 = x_2^2 = 1. \quad x_1 x_2 = x_2 x_1$$

$$y x_1 y^{-1} = x_2, \quad y x_2 y^{-1} = x_1 x_2.$$

(actually isomorphic to A_4) or $G \cong C_2 \times C_2 \times C_3$.

1b. $H = C_4, \quad K = C_3$.

$$\mathrm{Aut}(H) = (\mathbb{Z}/4\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z}).$$

no nontrivial homomorphism from C_3 to

$\mathrm{Aut}(H)$

so $G \cong C_3 \times C_4$.

2a: $H = C_2 \times C_2$, $\quad \mathrm{Aut}(C_3) = (\mathbb{Z}/3\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z})$

$= \langle x_1, x_2 \rangle$. $\quad x_1^2 = x_2^2 = 1, x_1 x_2 = x_2 x_1$

$\varphi: H \to \mathrm{Aut}(C_3)$.

$x_1 y x_1^{-1} = y^{j_1}$. $x_2 y x_2^{-1} = y^{j_2}$.

$j_1^2 \equiv j_2^2 \equiv 1 \mod 3$,

So $(j_1, j_2) = (1, 1)$ $G \cong C_3 \times C_2 \times C_2$

$(j_1, j_2) = (1, 2)$ or $(2, 1)$.

$x_1 y x_1^{-1} = y$, $x_2 y x_2^{-1} = y^2$

In this case $G \cong D_6$.

$(j_1, j_2) = (2, 2)$. choose $x_1^{-1} x_2$, x_2 as generator for H. reduce to

$(j_1, j_2) = (1, 2)$

2b. $H = C_4$, $\mathrm{Aut}(K) = (\mathbb{Z}/3\mathbb{Z})^{\times}$

So $xyx^{-1} = y$ or y^2

If $xyx^{-1} = y$ then $G = C_4 \times C_3$

$xyx^{-1} = y^2$, then $G \cong C_3 \rtimes_\varphi C_4$.

$G = \langle x, y \rangle$, $x^4 = 1$, $y^3 = 1$, $xyx^{-1} = y^2$

In total, there are 5 isomorphism classes.