Algebra I

Group Theory

Book 3

A matrix in $GL_2(\mathbb{R})$ is conjugate to $\begin{bmatrix}1&0\\0&-1\end{bmatrix}$ iff it has trace 0 and determinant -1.

If $A=\begin{bmatrix}a&b\\c&d\end{bmatrix}\in GL_2(\mathbb{R})$ then A has characteristic polynomial $f(x)=\det(xI-A)=\det\left(\begin{bmatrix}x&0\\0&x\end{bmatrix}-\begin{bmatrix}a&b\\c&d\end{bmatrix}\right)$

$$=\begin{vmatrix}x-a&-b\\-c&x-d\end{vmatrix}=(x-a)(x-d)-bc=x^2-\underbrace{(a+d)}_{\operatorname{tr}A}x+\underbrace{(ad-bc)}_{\det A}.$$

Some books define the characteristic polynomial of A as $\det(A-xI)=(-1)^n\underbrace{\det(xI-A)}$
monic: its leading term is x^n.

Cayley-Hamilton Theorem (look it up in any linear algebra book)

If $f(x)$ is the characteristic polynomial of an $n\times n$ matrix A, then $f(A)=0$.

In the 2×2 case, $A^2-(\operatorname{tr}A)A+(\det A)I=0$ holds as we compute here:

$$A^2=\begin{bmatrix}a&b\\c&d\end{bmatrix}\begin{bmatrix}a&b\\c&d\end{bmatrix}=\begin{bmatrix}a^2+bc&ab+bd\\ac+cd&bc+d^2\end{bmatrix}$$

$$A^2-(\operatorname{tr}A)A+(\det A)I=\begin{bmatrix}a^2+bc&ab+bd\\ac+cd&bc+d^2\end{bmatrix}-(a+d)\begin{bmatrix}a&b\\c&d\end{bmatrix}+(ad-bc)\begin{bmatrix}1&0\\0&1\end{bmatrix}=\begin{bmatrix}\cancel{a^2}+\cancel{bc}-(\cancel{a}+\cancel{d})a+(\cancel{ad}-\cancel{bc})&\cancel{ab}+\cancel{bd}-(\cancel{a}+\cancel{d})b\\ac+cd-(a+d)c&bc+d^2-(a+d)d+(ad-bc)\end{bmatrix}=\begin{bmatrix}0&0\\0&0\end{bmatrix}$$

If $A\in GL_2(\mathbb{R})$ has trace 0 and determinant -1 then it satisfies $A^2-\underline{0}A-1I=0$ so $A^2=I$

So in the group $GL_2(\mathbb{R})$, A has order ~~1 or~~ 2. ($\operatorname{tr}I=2$, not 0)

$f(x)=\det(xI-A)$ may or may not be the smallest degree polynomial that has A as a root.

The <u>minimal polynomial</u> of A, $m(x)$, is the monic polynomial of smallest degree satisfying $m(A)=0$.

Facts (see a linear algebra book):

Roots of $f(x)$ are eigenvalues of A.

$m(x)$ divides $f(x)$ i.e. $f(x)=h(x)\,m(x)$ for some monic polynomial $h(x)$ (often $h(x)=1$, $m(x)=f(x)$).

Every eigenvalue of A is a root of $m(x)$.

__Theorem__ Let $A \in GL_2(\mathbb{R})$. Then the following are equivalent:

(i) $\operatorname{tr} A = 0$, $\det A = -1$

(ii) A has order 2 but $A \neq -I$.

(iii) A is conjugate to $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

We have proved (i) $\Rightarrow$ (ii). And (iii) $\Rightarrow$ (i) is easy. Assume $A = M\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}M^{-1}$ for some $M \in GL_2(\mathbb{R})$.

Then $\operatorname{tr} A = \operatorname{tr}\left(M\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}M^{-1}\right) = \operatorname{tr}\left(M^{-1}M\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\right) = \operatorname{tr}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = 0$.

$\operatorname{tr} AB = \operatorname{tr} BA$ if A is $m \times n$, B is $n \times m$ (short proof: see linear algebra. Both equal to $\sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij} b_{ji}$)

$\det A = \det M \det\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \underbrace{\det M^{-1}}_{(\det M)^{-1}} = -1$.

$MM^{-1} = I$

$\det(M)\underbrace{\det(M^{-1})}_{1/\det M} = \det I = 1$

We must prove (ii) $\Rightarrow$ (iii). If A has order 2 then $A^2 = I$, $A \neq I$. A is a root of $x^2 - 1 = (x+1)(x-1)$

so the minimal poly. of A divides $x^2 - 1$: $m(x) = x^2 - 1$ or $x+1$ or $x-1$ or 1.

If $m(x) = 1$ then $m(A) = I = 0$. No!.

If $m(x) = x - 1$ then $m(A) = A - I = 0$ then $A = I$ (No! I has order 1, not order 2)

If $m(x) = x+1$ then $m(A) = A + I = 0$ so $A = -I$ (No! by assumption).

So $m(x) = x^2 - 1$ divides $f(x)$, so $f(x) = x^2 - 1$. $\Rightarrow \operatorname{tr} A = 0$, $\det A = -1$. $\Rightarrow$ (i) holds

So ± 1 are eigenvalues of A. Let u, v be eigenvectors corresponding to $1, -1$ i.e. $Au = u$, $Av = -v$.

Let $M = [u \mid v]$ (2×2 matrix having u, v as columns)

$AM = [Au \mid Av] = [u \mid -v] = [u \mid v]\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = M\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \Rightarrow A = M\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}M^{-1}$ i.e. (iii) holds. $\square$

There are two conjugacy classes of elements of order 2 in $G = GL_2(\mathbb{R})$:

- $\{-I = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\}$ is in a class by itself since $-I \in Z(G)$
- All matrices conjugate to $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ i.e. all matrices with trace 0 and determinant -1.
  This includes $\begin{bmatrix} 1 & a \\ 0 & -1 \end{bmatrix}$, $a \in \mathbb{R}$

Consider the dihedral group G of order 8 (the symmetry group of a square), so $|G| = 8$.
Let's pick generators x, y for G where x is an element of order 4 and y is a reflection (order 2).

$G = \{1, x, x^2, x^3, y, xy, x^2y, x^3y\}$, $yx = x^3y$ i.e. $yxy^{-1} = yxy = x^{-1} = x^3$,

$$\left.\begin{aligned} x^i \cdot x^j &= x^{i+j} \\ x^i \cdot x^j y &= x^{i+j} y \\ x^i y \cdot x^j &= x^{i-j} y \\ x^i y \cdot x^j y &= x^{i-j} \end{aligned}\right\}$$

"If you move y past x^i, it inverts $x^i \mapsto x^{-i}$"

$$x^i y x^j y = x^i \underbrace{(yxy)(yxy)\cdots(yxy)}_{(yxy)^j} = x^i (x^j)^{-1} = x^i x^{-j} = x^{i-j}$$

Presentation for G: $G = \langle \underbrace{x, y}_{\text{generators}} : \underbrace{x^4 = y^2 = 1,\ yx = x^3y}_{\text{relations}} \rangle$

$x^2 \cdot y = x^2 y$

$yx^2 = x^{-2}y = x^2 y$ $\quad$ $i=0,\ j=2$ in the rule $x^i y \cdot x^j = x^{i-j}y$

g	$\lvert g\rvert$	$C_G(g)$	
1	1	G,	$\lvert G\rvert = 8$
x	4	$\langle x\rangle$	$\lvert\langle x\rangle\rvert = 4$
x^3	4	$\langle x\rangle$	$\lvert\langle x\rangle\rvert = 4$
x^2	2	G,	$\lvert G\rvert = 8$
y	2	$\langle x^2, y\rangle$	$\lvert\langle x^2, y\rangle\rvert = 4$
x^2y	2	$\langle x^2, y\rangle$	$\lvert\langle x^2, y\rangle\rvert = 4$
xy	2	$\langle x^2, xy\rangle$	$\lvert\langle x^2, xy\rangle\rvert = 4$
x^3y	2	$\langle x^2, xy\rangle$	$\lvert\langle x^2, xy\rangle\rvert = 4$

Centralizer of $g \in G$:

$$C_G(g) = \{x \in G : xg = gx\}$$

$Z(G) = \langle x^2\rangle = \{1, x^2\}$.

$C_G(y) = \{1, x^2, y, x^2y\}$ is a Klein four-group

$\mathcal{O}(x) = \{x, x^3\}$

$\mathcal{O}(1) = \{1\}$

$\mathcal{O}(x^2) = \{x^2\}$

$C_G(xy) = \{1, x^2, xy, x^3y\}$ is a Klein four-group

If $\mathcal{O}(g)$ is the conjugacy class of $g \in G$ then $|\mathcal{O}(g)||C_G(g)| = |G|$. eg. $1 \times 8 = 8$, $2 \times 4 = 4$.

Cosets and Lagrange's Theorem

If H is a subgroup of G (multiplicative, at least generically) then a coset of H in G is a subset of the form $gH = \{gh : h \in H\}$. Note: $gH \subseteq G$, not a subgroup in general.

Eg. take $H = \langle (12) \rangle$ in $G = S_3$. List all cosets of H in G. There are exactly three cosets of H in G: H, $(13)H$, $(23)H$.

$()H = ()\{(), (12)\} = \{(), (12)\}$

$(12)H = (12)\{(), (12)\} = \{(), (12)\}$

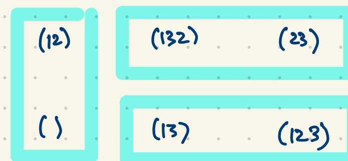
$(13)H = (13)\{(), (12)\} = \{(13), (123)\}$

$(23)H = (23)\{(), (12)\} = \{(23), (132)\}$

$(123)H = (123)\{(), (12)\} = \{(123), (13)\}$

$(132)H = (132)\{(), (12)\} = \{(132), (23)\}$

G is partitioned into three cosets, each of size 2.



$|G| = [G:H]\,|H|$

$6 = 3 \times 2$

(Recall: A partition of G is a collection of subsets that covers all of G without any overlap.)

Theorem The cosets of a subgroup $H \le G$ partition the elements of G.

Proof If $g \in G$, then gH is a coset containg g (since $e \in H$). Suppose two cosets aH and bH overlap i.e. $g \in aH \cap bH$ so $g = ah_1 = bh_2$ for some $h_1, h_2 \in H$, so $aH = gh_1^{-1}H = gH$ and $bH = gh_2^{-1}H = gH$. $\square$

$(a = gh_1^{-1}$ and $b = gh_2^{-1})$

If $h \in H$ then $h = h_1^{-1}h_1h \in h_1^{-1}H$ so $H \subseteq h_1^{-1}H$. Conversely, $h_1^{-1}H \subseteq H$

Theorem All cosets of H in G have cardinality $|gH| = |H|$.

Proof A bijection $H \longrightarrow gH$ is given by $h \longmapsto gh$. An inverse map $gH \to H$ is given by $x \longmapsto g^{-1}x$.

As a corollary, we obtain Lagrange's Theorem: $|G| = \underbrace{(\text{no. of cosets of } H \text{ in } G)}_{\substack{\text{the index of } H \text{ in } G \\ (\text{denoted } [G:H])}} \times \underbrace{(\text{size of each coset})}_{|H|}$

i.e. $|G| = [G:H]\,|H|$

Eg. In S_n, the set of all even permutations is a subgroup A_n. $(n \geq 2)$
The set of all odd permutations is a coset of A_n

S_n has two cosets of A_n : $( )A_n = A_n = \{\text{even permutations}\}$
$(12)A_n = \{\text{odd permutations}\}$

$$|S_n| = n! = \underbrace{[S_n : A_n]}_{2}\underbrace{|A_n|}_{\frac{n!}{2}}$$

Eg. In the additive group of $\mathbb{R}^3$, a line through the origin is a subgroup.
A coset of this line l is a line parallel to the original line.
The parallel lines to l give a partition of $\mathbb{R}^3$.

Eg. $G = S_n$ is partitioned into cosets of $H = G_1 \cong S_{n-1} = \{\text{permutions of } 2, 3, \cdots, n \text{ while fixing } 1\}$
$G = \sigma_1 H \cup \sigma_2 H \cup \sigma_3 H \cup \cdots \cup \sigma_n H$ where $\sigma_k \in G$ is any permutation mapping $1 \mapsto k$ $(k = 1, 2, \cdots, n)$.
eg. $\sigma_1 = ()$, $\sigma_2 = (12)$, $\sigma_3 = (1\ 3)$, $\cdots$, $\sigma_n = (1\ n)$
$\sigma_k H = \{\text{all } \sigma \in G : \sigma(1) = k\}$

Proof If $\sigma \in G$, $\sigma(1) = k$ then $\sigma^{-1}\sigma_k(1) = \sigma^{-1}(k) = 1$ so $\sigma^{-1}\sigma_k \in H = G_1$ so $\sigma^{-1}\sigma_k H = H$ so $\sigma_k H = \sigma H$.

$|H| = (n-1)!$, $[G : H] = n$, $|G| = |H|\,[G : H]$
$n! = (n-1)! \times n$.

Left cosets vs. Right cosets of $H \leq G$

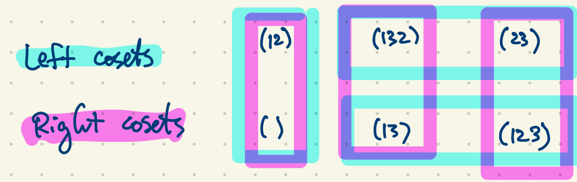
Left cosets $gH = \{gh : h \in H\}$, $g \in G$

Right cosets $Hg = \{hg : h \in H\}$

$[G:H]$ = index of H in G
= number of left cosets of H in G
= number of right cosets of H in G

All cosets of H in G have size $|gH| = |Hg| = |H|$.

Eg. $G = S_3$, $H = S_2 = G_3$



$G_k = \{\sigma \in G : \sigma(k) = k\}$ stabilizer of G

$H = \{(), (12)\}$

$H() = \{(), (12)\}() = \{(), (12)\}$

$H(12) = \{(), (12)\}(12) = \{(12), ()\}$

$H(13) = \{(), (12)\}(13) = \{(13), (132)\}$

$H(23) = \{(), (12)\}(23) = \{(23), (123)\}$

$H(123) = \{(), (12)\}(123) = \{(123), (23)\}$

$H(132) = \{(), (12)\}(132) = \{(132), (13)\}$

If G is abelian, then $gH = Hg$.

We say $H \leq G$ is <u>normal</u> if $gH = Hg$ for all $g \in G$ (left and right cosets are the same).

Eg. $G = S_4$, $K = \langle (12)(34), (13)(24) \rangle = \{(), (12)(34), (13)(24), (14)(23)\}$ is a Klein four-subgroup of G.

<u>Theorem</u> $K \trianglelefteq G$.

<u>Proof</u> If $g \in G$ and $k \in K$ then $gkg^{-1} \in K$ so $gKg^{-1} \subseteq K$. $(gKg^{-1} = \{gkg^{-1} : k \in K\})$.
so $gKg^{-1}g \subseteq Kg$ ie. $gK \subseteq Kg$. Similarly, $gK \supseteq Kg$ so $gK = Kg$. $\square$

In general if $H \leq G$ then gHg^{-1} is a subgroup of G, called a conjugate of H. (conjugating by $g \in G$)

<u>Proof</u> Given $h_1, h_2 \in H$, so $gh_1g^{-1}, gh_2g^{-1} \in gHg^{-1}$, we have $(gh_1g^{-1})(gh_2g^{-1}) = g\underline{h_1h_2}g^{-1} \in gHg^{-1}$. Take $e \in G$ as the identity, so $e \in H$ and $geg^{-1} = e \in gHg^{-1}$. Also if $h \in H$, so $ghg^{-1} \in gHg^{-1}$, then $(ghg^{-1})^{-1} = gh^{-1}g^{-1} \in gHg^{-1}$.

Conjugate subgroups are isomorphic to each other. Given $g \in G$, $H \leq G$, an isomorphism $H \longrightarrow gHg^{-1}$ is given by $h \mapsto ghg^{-1}$.

A subgroup $H \trianglelefteq G$ is <u>normal</u> ($H \trianglelefteq G$) iff every conjugate of H is H itself i.e. $gHg^{-1} = H$ for all $g \in G$.

<u>Example</u> $G = S_4$, $H = G_1 = \{(), (23), (24), (34), (234), (243)\} \cong S_3$, $g = (124) \notin H$.

$g^{-1} = (142)$

$gHg^{-1} = G_2 = \{(), (13), (14), (34), (134), (143)\} \cong S_3$

$= \langle (13), (14) \rangle$

why? Given $h \in H = G_1$, $ghg^{-1}(2) = gh(1) = g(1) = 2$. so $ghg^{-1} \in G_2$. This shows $gHg^{-1} \subseteq G_2$.

In fact $gHg^{-1} = G_2$.

Theorem Every conjugacy class in G has size (cardinality) dividing $|G|$.

Eg. A_4 has four conjugacy classes $\{()\}$, $\{(12)(34), (13)(24), (14)(23)\}$, $\{(124), (132), (143), (234)\}$, $\{(142), (123), (134), (243)\}$.

$$(123)(12)(34)\underbrace{(123)^{-1}}_{(132)} = (23)(14) = (14)(23), \quad (132)(12)(34)(132)^{-1} = (31)(24) = (13)(24).$$

$$(123)(124)(123)^{-1} = (234)$$

In S_4, (124) is conjugate to (142) since they have the same cycle structure:

$$(24)(124)(24)^{-1} = (142)$$

$$(14)(124)(14)^{-1} = (421)$$

Eg. **Theorem** A_4 has no subgroup of order 6.

Proof Suppose $G = A_4$ has a normal subgroup $K \trianglelefteq G$ of order $|K| = 6$. Partitioning G into left cosets $G = K \cup gK$ where $g \notin K$ $\left([G:K] = \frac{|G|}{|K|} = \frac{12}{6} = 2 \right)$ and partition G into right cosets as $G = K \cup Kg$ so $gK = Kg$. So $gKg^{-1} = K$.

Let G, H be groups (assumed to be multiplicative with identity elements $e_G \in G$, $e_H \in H$).

A <u>homomorphism</u> $G \to H$ is a map satisfying $\phi(gg') = \phi(g)\phi(g')$ for all $g, g' \in G$.

Note: An isomorphism is the same thing as a bijective homomorphism.

<u>Eg.</u> $\underset{\substack{\text{invertible}\\ n\times n \text{ matrices}\\ \text{over a field } F}}{\phi : \underbrace{GL_n(F)}} \to \underset{\substack{\text{multiplicative}\\ \text{group of nonzero}\\ \text{elements of } F}}{\underbrace{F^\times}}$, $\phi = \det$.

Properties: $\phi(e_G) = e_H$. $\quad (\phi(e_G) = \phi(e_G e_G) = \phi(e_G)\phi(e_G) \Rightarrow \phi(e_G) = e_H)$.

If $g \in G$ has order n then $|\phi(g)|$ divides $n = |g|$. $\quad$ eg. if $|g| = 6$ then $|\phi(g)|$ has order 1, 2, 3 or 6.

$g^n = e_G \Rightarrow \underset{\phi(g)^n}{\underset{\parallel}{\phi(g^n)}} = \phi(e_G) = e_H$

$\phi(g^{-1}) = \phi(g)^{-1}$ since $gg^{-1} = e_G \Rightarrow \underset{\phi(g)\phi(g^{-1})}{\underset{\parallel}{\phi(gg^{-1})}} = \phi(e_G) = e_H$

The <u>kernel</u> of a homomorphism $\phi: G \to H$ is $\ker\phi = \{g \in G : \phi(g) = e_H\}$. (Compare: the null space of a linear transformation)

<u>Theorem</u>: $\ker\phi$ is a subgroup of G.

<u>Proof</u> If $g, g' \in \ker\phi$ then $\phi(g) = \phi(g') = e_G$ then $\phi(gg') = \phi(g)\phi(g') = e_G e_G = e_G$ so $gg' \in \ker\phi$.

Since $\phi(e_G) = e_H$, $e_G \in \ker\phi$.

If $g \in \ker\phi$ then $\phi(g) = e_H$ so $\phi(g^{-1}) = \phi(g)^{-1} = e_H^{-1} = e_H$ so $g^{-1} \in \ker\phi$. $\quad$ So $\ker\phi \leq G$.

Note: If ϕ is one-to-one then $\ker\phi = \{e_G\}$. Conversely, if $\ker\phi = \{e_G\}$ then we show ϕ is one-to-one:

If $\phi(g) = \phi(g')$ then $\phi(g^{-1}g') = \phi(g^{-1})\phi(g') = \phi(g)^{-1}\phi(g') = e_H$ i.e. $g^{-1}g' \in \ker\phi = \{e_G\}$ so $g^{-1}g' = e_G$ so $g' = g$. $\quad\square$

The image of a homomorphism $\phi: G \to H$ then the image $\phi(G) = \{\phi(g) : g \in G\}$ is a subgroup of H.

Proof Given two elements in $\phi(G)$, say $\phi(g), \phi(g')$ for some $g, g' \in G$, then $\phi(g)\phi(g') = \phi(gg') \in \phi(G)$. Also $e_H = \phi(e_G) \in \phi(G)$. If we take any element in $\phi(G)$, say $\phi(g)$ where $g \in G$, then $\phi(g)^{-1} = \phi(g^{-1}) \in \phi(G)$. So $\phi(G) \leq H$. $\square$

Note: $\phi: G \to H$ is onto iff $\phi(G) = H$.

Eg. Define $\phi: S_4 \to S_3$ as follows: Take $\pi_1 = (12)(34)$, $\pi_2 = (13)(24)$, $\pi_3 = (14)(23)$ in S_4. These form a conjugacy class in S_4 $\{\pi_1, \pi_2, \pi_3\} = X$. (Really $\phi(\sigma) \in \mathrm{Sym}\, X = \mathrm{Sym}\{\pi_1, \pi_2, \pi_3\}$).

Given $\sigma \in S_4$, we have a map $X \to X$, $\pi_i \xmapsto{\phi(\sigma)} \sigma \pi_i \sigma^{-1}$.

Eg. $\phi((13))$:
$$\pi_1 \mapsto (13)\pi_1(13)^{-1} = (13)(12)(34)(13)^{-1} = (32)(14) = (14)(23) = \pi_3$$
$$\pi_2 \mapsto (13)\pi_2(13)^{-1} = (13)(13)(24)(13)^{-1} = (3\ 1)(24) = (13)(24) = \pi_2$$
$$\pi_3 \mapsto (13)\pi_3(13)^{-1} = (13)(14)(23)(13)^{-1} = (34)(2\ 1) = (12)(34) = \pi_1$$
$\phi((13)) = (13)$

$\phi((142))$:
$$\pi_1 \mapsto (142)\pi_1(142)^{-1} = (142)(12)(34)(142)^{-1} = (4\ 1)(3\ 2) = (14)(23) = \pi_3$$
$$\pi_2 \mapsto (142)\pi_2(142)^{-1} = (142)(13)(24)(142)^{-1} = (4\ 3)(1\ 2) = (12)(34) = \pi_1$$
$$\pi_3 \mapsto (142)\pi_3(142)^{-1} = (142)(14)(23)(142)^{-1} = (4\ 2)(13) = (13)(24) = \pi_2$$
$\phi((142)) = (132)$

ϕ is onto S_3. (why? $\phi(S_4)$ is a subgroup of S_3. By Lagrange's Theorem, $|\phi(S_4)|$ is divisible by $|\phi((13))| = |(13)| = 2$ and $|\phi((142))| = |(132)| = 3$ so $\phi(S_4) = S_3$.)

$\ker\phi = C_{S_4}(X) = \langle \pi_1, \pi_2 \rangle = \{(), \pi_1, \pi_2, \pi_3\}$ is a Klein four subgroup of order 4 in S_4.
$(\pi_3 = \pi_1\pi_2)$

ϕ is a homomorphism; it is 4-to-1.

The image of a homomorphism $\phi: G \to H$ i.e. the subgroup $\phi(G) = \{\phi(g) : g \in G\} \leq H$ is a <u>homomorphic image</u> of G.

Fractional Linear Transformations (or Linear Fractional Transformations)

A map $\mathbb{R}\cup\{\infty\} \to \mathbb{R}\cup\{\infty\}$ (actually a permutation) of the form $\begin{bmatrix} a & b \\ c & d \end{bmatrix} : x \longmapsto \dfrac{ax+b}{cx+d}$ where $ad-bc \neq 0$.

$GL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad-bc \neq 0 \right\}$ for actual invertible 2×2 real matrices.

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}(x) = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\left(\frac{\alpha x+\beta}{\gamma x+\delta}\right) = \frac{a\left(\frac{\alpha x+\beta}{\gamma x+\delta}\right)+b}{c\left(\frac{\alpha x+\beta}{\gamma x+\delta}\right)+d} = \frac{a(\alpha x+\beta)+b(\gamma x+\delta)}{c(\alpha x+\beta)+d(\gamma x+\delta)} = \frac{(a\alpha+b\gamma)x+(a\beta+b\delta)}{(c\alpha+d\gamma)x+(c\beta+d\delta)}$$

$$= \begin{bmatrix} a\alpha+b\gamma & a\beta+b\delta \\ c\alpha+d\gamma & c\beta+d\delta \end{bmatrix}(x)$$

Compare with multiplication of actual 2×2 invertible matrices:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} a\alpha+b\gamma & a\beta+b\delta \\ c\alpha+d\gamma & c\beta+d\delta \end{pmatrix}$$

We denote by $PGL_2(\mathbb{R})$ the group of all fractional linear transformations $\mathbb{R}\cup\{\infty\} \to \mathbb{R}\cup\{\infty\}$ i.e.

$$PGL_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{R},\ ad-bc \neq 0 \right\}.$$

This is a homomorphic image of $GL_2(\mathbb{R})$ under the homomorphism $\phi: GL_2(\mathbb{R}) \to PGL_2(\mathbb{R})$, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \begin{bmatrix} a & b \\ c & d \end{bmatrix}$. This map is a homomorphism: $\phi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\right) = \phi\left(\begin{pmatrix} a\alpha+b\gamma & a\beta+b\delta \\ c\alpha+d\gamma & c\beta+d\delta \end{pmatrix}\right)$

$$= \begin{bmatrix} a\alpha+b\gamma & a\beta+b\delta \\ c\alpha+d\gamma & c\beta+d\delta \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \phi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right)\phi\left(\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\right).$$

This homomorphism is <u>onto</u> $PGL_2(\mathbb{R})$ by definition but it's not onto because $\phi\left(\begin{pmatrix} \lambda a & \lambda b \\ \lambda c & \lambda d \end{pmatrix}\right) = \begin{bmatrix} \lambda a & \lambda b \\ \lambda c & \lambda d \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

since $\begin{bmatrix} \lambda a & \lambda b \\ \lambda c & \lambda d \end{bmatrix}(x) = \dfrac{\lambda a x + \lambda b}{\lambda c x + \lambda d} = \dfrac{ax+b}{cx+d} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}(x)$

$$\begin{bmatrix}3&4\\1&7\end{bmatrix}(5) = \frac{3\times5+4}{1\times5+7} = \frac{19}{12}.$$

$$\begin{bmatrix}3&4\\1&7\end{bmatrix}(\infty) = \frac{3\times\infty+4}{1\times\infty+7} = 3$$

$$\begin{bmatrix}3&4\\1&7\end{bmatrix}(-7) = \frac{3\times(-7)+4}{1\times(-7)+7} = \frac{-17}{0} = \infty$$

$$\begin{bmatrix}3&4\\0&7\end{bmatrix}(\infty) = \frac{3\times\infty+4}{\cancel{0\times\infty}+7} = \infty.$$

In $GL_2(\mathbb{R})$, $\begin{pmatrix}a&b\\c&d\end{pmatrix}^{-1} = \frac{1}{ad-bc}\begin{pmatrix}d&-b\\-c&a\end{pmatrix}$. $(ad-bc\neq 0)$

$\mathbb{F}_q$: field of order q

$|GL_2(\mathbb{F}_q)| = (q^2-1)(q^2-q)$ divide by $q-1$.

$|SL_2(\mathbb{F}_q)| = (q^2-1)q$

Every fractional linear transformation is a permutation of $\mathbb{R}\cup\{\infty\}$

$PGL_2(\mathbb{R})$ is a group. $\begin{bmatrix}a&b\\c&d\end{bmatrix}^{-1} = \frac{1}{ad-bc}\begin{bmatrix}d&-b\\-c&a\end{bmatrix} = \begin{bmatrix}d&-b\\-c&a\end{bmatrix}.$

The identity $\begin{bmatrix}1&0\\0&1\end{bmatrix}(x) = \frac{1\times x\cancel{+0}}{\cancel{0\times x}+1} = x.$

You can think of $PGL_2(\mathbb{R})$ as the same as 2×2 invertible matrices but where we identify nonzero scalar multiples i.e. $\lambda\begin{bmatrix}a&b\\c&d\end{bmatrix} = \begin{bmatrix}\lambda a&\lambda b\\\lambda c&\lambda d\end{bmatrix} = \begin{bmatrix}a&b\\c&d\end{bmatrix}.$

$GL_2(\mathbb{F}_2) = \{\begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}, \begin{pmatrix}0&1\\1&0\end{pmatrix}, \begin{pmatrix}1&1\\1&0\end{pmatrix}, \begin{pmatrix}0&1\\1&1\end{pmatrix}, \begin{pmatrix}1&0\\1&1\end{pmatrix}\} = SL_2(\mathbb{F}_2).$

$|GL_2(\mathbb{F}_2)| = (2^2-1)(2^2-2) = 3\times2 = 6.$

$\mathbb{F}_2 = \{0,1\}$ is the field of order 2:

$PGL_2(\mathbb{F}_2) = \{\begin{bmatrix}1&0\\0&1\end{bmatrix}, \begin{bmatrix}1&1\\0&1\end{bmatrix}, \begin{bmatrix}0&1\\1&0\end{bmatrix}, \begin{bmatrix}1&1\\1&0\end{bmatrix}, \begin{bmatrix}0&1\\1&1\end{bmatrix}, \begin{bmatrix}1&0\\1&1\end{bmatrix}\} \cong GL_2(\mathbb{F}_q) \cong SL_2(\mathbb{F}_2) \cong S_3$

why? $PGL_2(\mathbb{F}_2)$ is a group of permutations of $\{\underbrace{0, 1}_{\mathbb{F}_2}, \infty\}$

$Sym\{0,1,\infty\} = \{$all permutations of $0,1,\infty\}$

so $PGL_2(\mathbb{F}_2)$ is isomorphic to a subgroup of S_3.

$|GL_2(\mathbb{F}_3)| = (3^2-1)(3^2-3) = 8\times6 = 48$

$\mathbb{F}_3 = \{0,1,2\}$ $\quad \frac{1}{2} = 2 = -1$ $\quad |PGL_2(\mathbb{F}_3)| = \frac{48}{2} = 24$ $\quad PGL_2(\mathbb{F}_3) \cong S_4.$

The map $GL_2(\mathbb{F}_3) \to PGL_2(\mathbb{F}_3)$ is 2-to-1.

$PGL_2(\mathbb{F}_3)$ is a group of permutations of $\mathbb{F}_3\cup\{\infty\} = \{0,1,2,\infty\}.$

$\begin{pmatrix}a&b\\c&d\end{pmatrix} \longmapsto \begin{bmatrix}a&b\\c&d\end{bmatrix}$

$\mathbb{F}_4 = \{0, 1, \alpha, \beta\}$ field of order 4

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\times$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

$|GL_2(\mathbb{F}_4)| = (4^2-1)(4^2-4) = 15 \times 12 = 180$

$|SL_2(\mathbb{F}_4)| = \frac{180}{3} = 60$

$|A_5| = \frac{5!}{2} = 60$

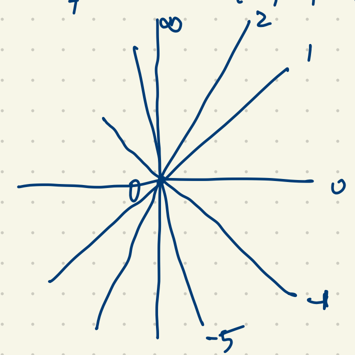
$SL_2(\mathbb{F}_4) \cong A_5$.

$PSL_2(\mathbb{F}_4) = \{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : ad-bc = 1, \quad a, b, c, d \in \mathbb{F}_4 \} \cong SL_2(\mathbb{F}_4)$

The map $SL_2(\mathbb{F}_4) \longrightarrow PSL_2(\mathbb{F}_4)$ acting as all even permutations of $\mathbb{F}_4 \cup \{\infty\} = \{0, 1, \alpha, \beta, \infty\}$

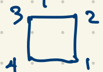
$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}(x) = \frac{1 \times x + 1}{0 \times x + 1} = x + 1 \quad : \quad (0, 1)(\alpha, \beta)(\infty)$



$\mathbb{R} \cup \{\infty\} = \{$all possible slopes of lines through the origin in $\mathbb{R}^2\}$

Orbits and Stabilizers for Group Actions

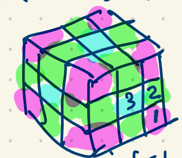
Eg. $G =$ symmetry group of 

, $G < S_4$, $G = \langle (1234), (13) \rangle$ a dihedral group of order 8.

G permutes the four vertices transitively (meaning if $x, y \in \{1,2,3,4\}$ then there exists $g \in G$ such that $g(x) = y$).

For legal moves of a Rubik's cube, the group of all moves does not permute the 26 small cubes (the group has three orbits of size 12, 8, 6)

$12 + 8 + 6 = 26.$



$\mathcal{O}(1) = \{\text{all small corner cubes}\}$, $|\mathcal{O}(1)| = 8$

$|\mathcal{O}(2)| = 12$

$|\mathcal{O}(3)| = 6$

A group action is transitive if there is only only one orbit.

The stabilizer of x is $\mathrm{Stab}_G(x) = G_x = \{ g \in G : g(x) = x \} \leq G$. (a subgroup)

eg. in the dihedral group above, $\mathrm{Stab}_G(2) = G_2 = \{\text{all elements of } G \text{ fixing } 2\} = \{(), (1\ 3)\}$

$= \langle (13) \rangle$

$\mathrm{Stab}_G(1) = \{(), (24)\} = \mathrm{Stab}_G(3) = \langle (24) \rangle$

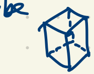
The orbit of x is $\mathcal{O}(x) = \{ g(x) : g \in G \}$. In this case there is only one orbit

$\mathcal{O}(1) = \{1, 2, 3, 4\} = \mathcal{O}(2) = \mathcal{O}(3) = \mathcal{O}(4)$

Theorem If G permutes $X = [n] = \{1, 2, \ldots, n\}$ then for every $x \in X$, $|\mathrm{Stab}_G(x)|\,|\mathcal{O}(x)| = |G|$.

In our dihedral group of order 8:

$|\mathrm{Stab}_G(x)| = 2$, $|\mathcal{O}(x)| = 4$, $|G| = 8$

We have implicitly used this! eg. when calculating the symmetry group G of a cube 

$|G| = |\mathrm{Stab}(v)||\mathcal{O}(v)|$ where v is a vertex

$= 6 \times 8 = 48$

or

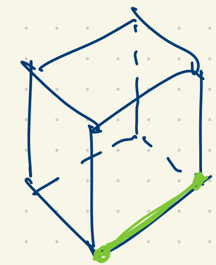
$|G| = |\mathrm{Stab}(F)||\mathcal{O}(F)|$ where F is a face

$= 8 \times 6 = 48$

or

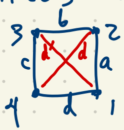
$|G| = |\mathrm{Stab}(e)||\mathcal{O}(e)|$

$= 4 \times 12 = 48$



More examples of stabilizers and orbits

$G = \langle (1234), (13) \rangle$



G also permutes the four edges a, b, c, d transitively

$\mathrm{Stab}_G(a) = \langle (12)(34) \rangle = \{(\,), (12)(34)\}$

$\mathcal{O}(a) = \{a, b, c, d\}$

$|G| = |\mathrm{Stab}(a)|\,|\mathcal{O}(a)|$

$8 = 2 \times 4$

G also permutes the two diagonals d, d'

$\mathcal{O}(d) = \{d, d'\}$

$\mathrm{Stab}(d) = \{(\,), (13), (24), (13)(24)\}$, a Klein four-group

$|G| = \underline{|\mathrm{Stab}(d)|}\,\underline{|\mathcal{O}(d)|}$

$8 = 4 \times 2$

$\mathrm{Stab}_G(x) \leq G$ is a subgroup

$\mathcal{O}(x) \subseteq X$ is not a group, just a set of points

$G = GL_3(F)$ where F is a field

G acts on F^3, permuting vectors

The stabilizer of $e_1 = \begin{pmatrix}1\\0\\0\end{pmatrix}$ is $\mathrm{Stab}_G(e_1) = \{ g \in G : ge_1 = e_1 \}$

$ge_1 = e_1$ says $\begin{bmatrix}1 & b & c\\ 0 & e & f\\ 0 & i & j\end{bmatrix}\begin{bmatrix}1\\0\\0\end{bmatrix} = \begin{bmatrix}1\\0\\0\end{bmatrix}$

$= \left\{ \begin{bmatrix}1 & b & c\\ 0 & e & f\\ 0 & i & j\end{bmatrix} : b,c,e,f,i,j \in F,\ ej - fi \neq 0 \right\}$

$\mathcal{O}(e_1) = \{\text{all nonzero vectors}\} = F^3 - \left\{\begin{bmatrix}0\\0\\0\end{bmatrix}\right\}$

F^3 has two orbits: $\Big\{\underbrace{\begin{bmatrix}0\\0\\0\end{bmatrix}}_{0}\Big\}$, $F^3 - \left\{\begin{bmatrix}0\\0\\0\end{bmatrix}\right\}$.

$\mathrm{Stab}_G(0) = G$

<u>Theorem</u> If G acts on X (i.e. G permutes X i.e. $G \leq \underset{(\mathrm{Perm}\,X)}{\mathrm{Sym}\,X}$) and $x \in X$ (any point)

then $|\mathrm{Stab}_G(x)| \cdot |\mathcal{O}(x)| = |G|$.

<u>Proof</u> Let $H = \mathrm{Stab}_G(x)$ and $\mathcal{O}(x) = \{\underset{x}{\overset{\|}{x_1}}, x_2, \ldots, x_k\} \subseteq X$. Then there exist $g_1, \ldots, g_k \in G$ such that $g_i(x) = x_i$ (by definition). (Note: $g_1, \ldots, g_k$ are not uniquely determined.)

Then $G = g_1H \sqcup g_2H \sqcup g_3H \sqcup \cdots \sqcup g_kH$. ($A \sqcup B$ denotes disjoint union i.e. $A \cup B$ with no overlap, $A \cap B = \varnothing$)

Why? If $g \in G$ then $g(x) \in \mathcal{O}(x)$ so $g(x) = x_i$ for ~~some~~ $i \in \{1, 2, \ldots, k\}$ and $g_i(x) = x_i$ so $g_i^{-1}(g(x)) = g_i^{-1}(x_i) = x$ so $g_i^{-1}g \in H = \mathrm{Stab}(x)$

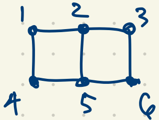
so $g_i^{-1}gH = H$ i.e. $g \in gH = g_iH$.

In fact $g_iH = \{g \in G : g(x) = x_i\}$.

Now $k = |\mathcal{O}(x)| = [G : H]$ and

$|G| = |H|\,[G:H] = |\mathrm{Stab}(x)|\,|\mathcal{O}(x)|$.

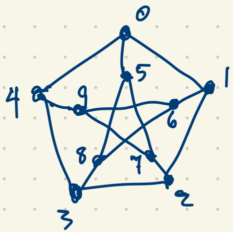
Application to graph theory: computing the number of automorphisms of a graph.

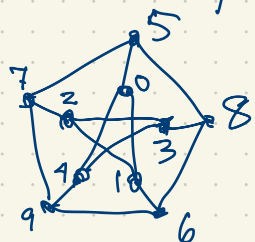
Eg. $\Gamma =$ 

has four automorphisms. Its automorphism group is a Klein four-group

$G = \langle (13)(46),\ (14)(25)(36) \rangle = \{(),\ (13)(46),\ (14)(25)(36),\ (16)(25)(34)\}$

G has two orbits on vertices: $\{1,3,4,6\}$, $\{2,5\}$.

Eg. $P =$ 

$=$ 

has automorphisms including $(0\ 1\ 2\ 3\ 4)(5\ 6\ 7\ 8\ 9)$,

$(0\ 5)(1\ 8\ 4\ 7)(2\ 6\ 3\ 9)$

$(0\ 5)(1\ 7\ 4\ 8)(2\ 9\ 3\ 6)$

P is the <u>Petersen graph</u>

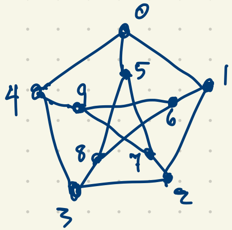
How many automorphisms does P have?

$\operatorname{Aut} P = \{\text{automorphisms of } P\} \leqslant S_{10}$ actually $\operatorname{Sym}\{0,1,2,\dots,9\}$

<u>Theorem</u> $|\operatorname{Aut} P| = 120$. Is $\operatorname{Aut} P \cong S_5$?

<u>Proof</u> First enumerate orbits of $G = \operatorname{Aut} P$ on the vertex set $\{0,1,2,\dots,9\}$.

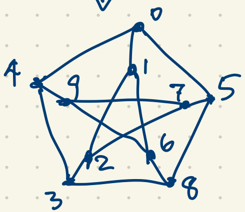
There is only one orbit by considering the dihedral subgroup of order 10 and $(0\ 5)(1\ 8\ 4\ 7)(2\ 6\ 3\ 9)$. So G is transitive on vertices $|G| = 10|G_0| = 10 \times 12 = 120$. where $G_0 = \operatorname{Stab}_G(0)$.



$G_0 = \mathrm{Stab}_G(0)$

We show $\{1,4,5\}$ is an orbit of G_0. Clearly $1,4$ are in the same orbit of G_0 since $(14)(23)(69)(78) \in G_0$.

Also 5 is in the same orbit as 1 (under G_0) since $(15)(28)(67) \in G_0$.

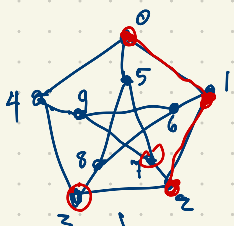


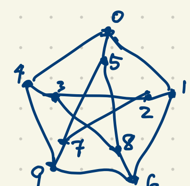
Since $\{1,4,5\}$ is an orbit of G_0, $\mathcal{O}_{G_0}(1) = \{1,4,5\}$

$$|G_0| = \Big|\overbrace{\mathrm{Stab}_{G_0}(1)}^{G_{0,1}}\Big|\,\big|\mathcal{O}_{G_0}(1)\big| = 3\,|G_{0,1}| = 3\times 4 = 12$$

where $G_{0,1} = \{g \in G : g(0)=0 \text{ and } g(1)=1\}$.

Does $G_{0,1}$ fix $2,6$ or can it interchange them?



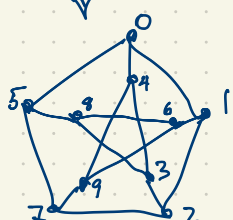


$(26)(39)(78) \in G_{0,1}$

$\mathcal{O}_{G_{0,1}}(2) = \{2,6\}$ is an orbit of $G_{0,1}$

$$|G_{0,1}| = \big|\underbrace{\mathrm{Stab}_{G_{0,1}}(2)}\big|\,\big|\mathcal{O}_{G_{0,1}}(2)\big| = 2\,|G_{0,1,2}| = 2\times 2 = 4$$

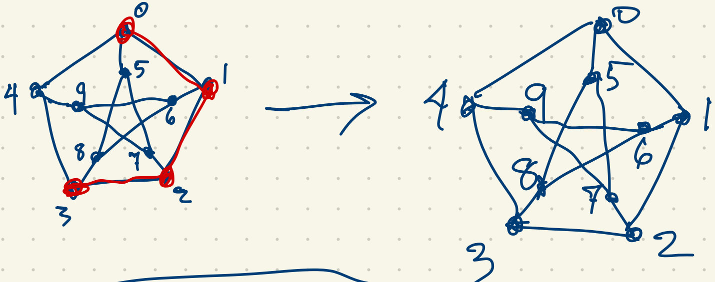
$G_{0,1,2} = \{g \in G : g(0)=0,\ g(1)=1,\ g(2)=2\}$



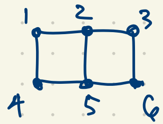
$(37)(45)(89) \in G_{0,1,2}$

$\mathcal{O}_{G_{0,1,2}}(3) = \{3,7\}$

$$|G_{0,1,2}| = \big|\mathrm{Stab}_{G_{0,1,2}}(3)\big|\,\big|\mathcal{O}_{G_{0,1,2}}(3)\big| = 2\,\big|\underset{\mathrm{Stab}_{G_{0,1,2}}(3)}{G_{0,1,2,3}}\big| = 2\times 1 = 2$$



$$G_{0,1,2,3} = \{()\}$$

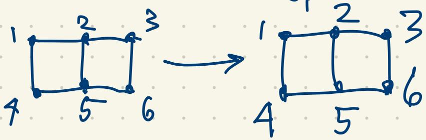
In the same way $\Gamma =$ 

has automorphism group $G = \mathrm{Aut}\,\Gamma$ which is the Klein fourgroup $\langle (13)(46), (14)(25)(36) \rangle$.

Proof: $\underbrace{\{1,3,4,6\}}_{= O(1)}$ is an orbit of G on the six vertices. So $|G| = |G_1|\,|O(1)|$

$$= 4|G_1| = 4 \times 1 = 4.$$

$$G_1 = \mathrm{Stab}_G(1) = \{()\}$$



In $GL_n(F)$, any two conjugate matrices (i.e. similar) have the same trace and determinant (but not conversely in general).

eg. in $GL_2(F)$, $\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$, $\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}$ are not similar (the only group element conjugate to the identity is itself).

$$tr(AB) = tr(BA) = \sum_{i,j} a_{ij} b_{ji}$$

If $A = MBM^{-1}$ then $AM = MB$, $\underbrace{\det(AM)}_{\det(A)\det(M)} = \det(MB) = \det(M)\det(B)$.

$$A - \lambda I = M(B - \lambda I)M^{-1} = MBM^{-1} - \lambda MIM^{-1} = A - \lambda I.$$

Theorem Every conjugacy class in G has size (cardinality) dividing $|G|$.

Eg. A_4 has four conjugacy classes $\{()\}$, $\{(12)(34), (13)(24), (14)(23)\}$, $\{(124), (132), (143), (234)\}$, $\{(142), (123), (134), (243)\}$.

Proof G permutes $\underset{X}{\overset{\shortparallel}{G}}$ by conjugation: if $g \in G$ and $x \in G$ then $\underbrace{g(x)}_{\text{new operation: conjugation.}} = \underbrace{gxg^{-1}}_{\text{multiplication in } G \text{ as usual}}$.

eg. in A_4, let $x = (12)(34)$, $g = (124)$. Then

$$g(x) = (124)(12)(34)(142) = (13)(24)$$

Alternatively: $(12)(34) \to (24)(31)$

The orbits of G acting on G by conjugation are just the conjugacy classes, by definition.

The stabilizer of any point $x \in G$ is $\mathrm{Stab}_G(x) = \{g \in G : g(x) = x\}$.

$g(x) = x$ iff $gxg^{-1} = x$ iff $gx = xg$ iff g commutes with x i.e. $\mathrm{Stab}_G(x) = C_G(x)$.

$$|G| = \underbrace{|C_G(x)|}_{|\mathrm{Stab}_G(x)|} \cdot \underbrace{(\text{no. of conjugates of } x \text{ in } G)}_{|\mathcal{O}_G(x)|.}$$

$\square$

The textbook writes $\mathcal{O}_X(x)$ for the orbit of G acting on X. I've been writing $\mathcal{O}(x)$ or

Eg. $C_{A_4}((12)(34)) = \langle (12)(34), (13)(24) \rangle = \{(), (12)(34), (13)(24), (14)(23)\}$.

The conjugacy class of (124) in S_4 is

$$\mathcal{O}_{S_4}((124)) = \{(124), (123), (134), (142), (132), (143), (234), (243)\}$$

The conjugacy class of (124) in A_4 is

$$\mathcal{O}_{A_4}((124)) = \{(124), (132), (143), (234)\}.$$

$$C_{S_4}((124)) = \langle (124) \rangle = \{(), (124), (142)\}$$

$$C_{A_4}((124)) = \langle (124) \rangle$$

In S_4, $|S_4| = |C_{S_4}((124))| \cdot |\text{conjugacy class of } (124)|$

$$24 = 3 \times 8$$

In A_4, $|A_4| = |C_{A_4}((124))| \cdot |\text{conjugacy class of } (124)|$

$$12 = 3 \times 4.$$

History of Group Theory (finite vs. infinite groups) (Arthur Cayley)

Historically, before we had axioms for group theory, we considered permutation groups (subgroups of S_n). This was motivated by the problem of finding roots of polynomials.

Roots of $x^2+5x+2=0$ are $\frac{-5\pm\sqrt{17}}{2}$ where $\sqrt{17}$ is the positive root of $x^2-17=0$.

Similar forumlas exist for finding roots of cubics $ax^3+bx^2+cx+d=0$ and quartics $ax^4+bx^3+cx^2+dx+e=0$. No such formula exists for roots of a general quintic $ax^5+bx^4+cx^3+dx^2+ex+f=0$.

$\left\{\begin{array}{l}\text{Evariste Galois}\\ \text{Niels Abel}\end{array}\right.$

The roots of a polynomial $f(x)$ of degree n can be expressed "explicitly" (using $+, \times, -, \div, \sqrt[n]{\cdot}$) iff the Galois group of $f(x)$ is solvable.

The Galois group is the group of permutations of the roots of $f(x)$ found using field automorphisms.

eg. $x^2+5x+2 = (x-\alpha)(x-\beta)$, $\alpha = \frac{-5+\sqrt{17}}{2}$, $\beta = \frac{-5-\sqrt{17}}{2}$.

There is an automorphism of $\mathbb{C}$ interchanging α, β.

Solving systems of PDE's (specifically, explicit/exact/analytic solutions rather than approximate solutions).

Axioms of Group Theory came after all these examples.

Sophus Lie
Lie groups/algebras
Emmy Noether

In HW 3 #3, $G = GL_2(\mathbb{F}_5)$ is permuting the 25 vectors of $\mathbb{F}_5^2 = \{\binom{x}{y} : x, y \in \mathbb{F}_5\}$.
$0 = \binom{0}{0}$ is the zero vector.

If $v = \binom{0}{1}$ then $G_v = \left\{ \begin{bmatrix} a & 0 \\ c & 1 \end{bmatrix} : a, c \in \mathbb{F}_5 \text{ with } a \neq 0 \right\}$.

(Similar to #3(c).) where $0 = \binom{0}{0}$.

$|G_v| = 20$. $|G| = 480$. (do this in (a)).

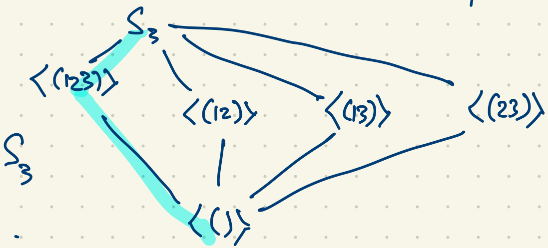
$|\mathcal{O}_G(v)| = 24$. If $w = \binom{b}{d}$ is any nonzero vector in $\mathbb{F}_5^2$ then there exists $u \in \mathbb{F}_5^2$ which is not a scalar multiple of w (there are $\underset{25-5}{} = 20$ possible choices for $u = \binom{a}{c}$). So u, w form a basis for $\mathbb{F}_5^2$. Then $A = [u|w] = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is invertible and $Av = w = \binom{b}{d}$.

$$|G| = |G_v||\mathcal{O}_G(v)| = 20 \times 24 = 480.$$

What is a solvable group?

A subgroup $K \leq G$ is <u>normal</u> if $gK = Kg$ for every $g \in G$. ($K \trianglelefteq G$)
(Equivalently, K is the kernel of a group homomorphism i.e. there exists a group homomorphism $\phi: G \to H$ such that $\ker\phi = \{g \in G : \phi(g) = 1\}$ is $\ker\phi = K$).

Eg. S_3 has subgroups



The only normal subgroups of S_3 are $\langle()\rangle$, $\langle(123)\rangle = A_3$, S_3.

$\langle(12)\rangle$, $\langle(13)\rangle$, $\langle(23)\rangle$ are not normal. $\langle(12)\rangle(13) \neq (13)\langle(12)\rangle$

$$\langle(123)\rangle(13) = (13)\langle(123)\rangle = \{(12), (13), (23)\}.$$

S_3 decomposes as

$$\langle()\rangle \triangleleft \langle(123)\rangle \triangleleft S_3 \qquad \text{(a composition series for } S_3\text{)}$$

$$1 \mid 3 \mid 6$$

S_4 has a composition series

$$\langle()\rangle \triangleleft \langle(12)(34)\rangle \triangleleft \langle(12)(34), (13)(24)\rangle \triangleleft A_4 \triangleleft S_4$$

$$1 \mid 2 \mid 4 \mid 12 \mid 24$$

Warning: $H \triangleleft K \triangleleft G$ does <u>not</u> imply $H \triangleleft G$.

eg. $\langle(12)(34)\rangle \ntriangleleft A_4$ or S_4.

S_5 has composition series

$$\langle () \rangle \lhd A_5 \lhd S_5 \qquad |S_5/A_5| = 2$$

$$1 \quad | \quad 60 \quad | \quad 120 \qquad |A_5/\langle () \rangle| = 60$$

A_5 has only two normal subgroups : $\langle () \rangle$, A_5 .

If G is any group then G has a composition series

$$1 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_k = G$$ where G_i/G_{i-1} is a simple group

i.e. we cannot find any normal subgp between G_{i-1} and G_i.

The simple groups are:

- the cyclic groups of prime order. These are the only abelian simple groups.
- the nonabelian simple groups. Classification of the finite simple groups (CFSG) was the main goal of group theory prior to the 1980's. This is the biggest proof in the history of mathematics.

Roughly, the finite nonabelian simple groups are

- A_n, $n \geq 5$ (important: polynomials of degree $n \geq 5$ cannot be explicitly solved in general)
- certain matrix groups over finite fields
- 26 exceptional simple groups, up to and including the Monster M, $|M| = 808{,}017{,}424{,}794{,}512{,}875{,}886{,}459{,}904{,}961{,}710{,}757{,}005{,}754{,}368{,}000{,}000{,}000$.

Officially our exam is 8–10 am Fri Dec 15 here (BU 209).
Optional afternoon time: 1:15 – 3:15 pm BU 209
3:30 – 5:30 pm CASM
If a room is taken, look for a note on the door.

If G is any finite group then G decomposes into a composition series

$1 \triangleleft G_1 \triangleleft G_2 \triangleleft \cdots \triangleleft G_k = G$ where $G_{i-1} \triangleleft G_i$ with no normal subgroups between G_{i-1} and G_i.

There are 'quotient groups' G_i / G_{i-1} and these are simple groups (no nontrivial normal subgroup).
These quotient groups are the composition factors of G.
G is <u>solvable</u> if all its composition factors are cyclic of prime order.

Abelian groups are solvable.

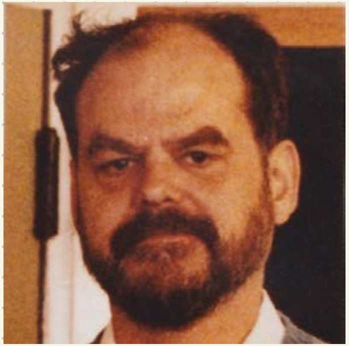
S_n is solvable for $n \leq 4$; S_n is nonsolvable for $n \geq 5$ eg. $1 \underbrace{\triangleleft\, A_5}_{A_5} \underbrace{\triangleleft\, S_5}_{\substack{\text{cyclic of order 2} \\ S_5/A_5}}$

Simple groups are important building blocks of all finite groups.
Just like prime numbers are building blocks of integers.

The first major result (before CFSG):

<u>Theorem</u> (Walter Feit, John <u>Thompson</u>) Every group of odd order is solvable.

John G. Thompson



Homomorphisms, Automorphisms

A group homomorphism is a map $\phi: G \to H$ such that $\phi(xy) = \phi(x)\phi(y)$ for all $x,y \in G$.

If $\phi: G \to G$ is a homomorphism and it is bijective then it is an isomorphism, hence an automorphism.

Eg. If we fix $g \in G$ then conjugation by g gives an automorphism $\psi_g(x) = gxg^{-1}$ $(x \in G)$ of G.

$\psi_g(xy) = g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) = \psi_g(x)\psi_g(y)$. (so ψ_g is a homomorphism).

$\psi_{g^{-1}}$ is the inverse function of ψ_g since $\psi_{g^{-1}}(\psi_g(x)) = g^{-1}(gxg^{-1})(g^{-1})^{-1} = x$ and similarly $\psi_g(\psi_{g^{-1}}(x)) = x$. So $\psi_{g^{-1}} = (\psi_g)^{-1}$ so ψ_g is bijective.

If G is abelian then G can have many automorphisms but only one of them has the above form since $\psi_g(x) = gxg^{-1} = gg^{-1}x = x$.

<u>Definition</u> An automorphism of G of the form $\psi_g(x) = gxg^{-1}$ is called an <u>inner</u> automorphism.

If G is abelian then the only inner automorphism of G is the identity $x \mapsto x$.

<u>Eg.</u> If G is a Klein four-group, $G = \langle a, b \rangle = \{1, a, b, c\}$, $c = ab$, $a^2 = b^2 = c^2 = 1$ then G has ~~four~~ automorphisms permuting a, b, c in all $3! = 6$ possible ways. These are outer automorphisms (not inner).

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

Eg. Consider S_n which is about as nonabelian as possible.
For $n \neq 2, 6$, S_n has $\underline{n!}$ automorphisms, and they are all inner.

S_3 has exactly 6 automorphisms permuting the three involutions in all $3! = 6$ possible ways.

eg. $\phi : S_3 \longrightarrow S_3$, $\phi((12)) = (12)$, $\phi((13)) = (23)$, $\phi((23)) = (13)$.
This defines an automorphism of S_3, namely $\phi = \psi_{(12)}$.
So $\phi((123)) = \psi_{(12)}((123)) = (2\,1\,3) = (1\,3\,2)$

$S_2 = \langle (12) \rangle$ is abelian. The only automorphism of S_2 is the identity

$$\phi(()) = () \qquad \phi = \psi_{()} = \psi_{(12)}$$
$$\phi((12)) = (12)$$

Every automorphism of S_2 is inner but there is only one automorphism, not two.

$|S_6| = 6! = 720$. S_6 has 1440 automorphisms, half of which are inner (they come from $\{\psi_g : g \in S_6\}$.) Look at Test.
We gave an automorphism ϕ of S_6 that maps a 3-cycle to another element not a 3-cycle.