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 $\det(A-xI)=(-1)^n\underbrace{\det(xI-A)}_{\substack{\text{monic:}\\ \text{its leading}\\ \text{term is } x^n.}}$

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 $m(x)$.

<u>Theorem</u> 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).

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

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

$yx^2 = x^{-2}y = x^2y$ $\quad$ $i=0$, $j=2$ 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. $1 \times 8 = 8$
$2 \times 4 = 4$.

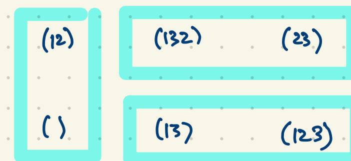
Cosets and Lagrange's Theorem

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 $H \leq G$ partition the elements of G.

Proof If $g \in G$, then gH is a coset containing 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: $|G| = \underbrace{(\text{no. of cosets of } H \text{ in } G)}_{\text{the index of } H \text{ in } G \text{ (denoted } [G:H])} \times \underbrace{(\text{size of each coset})}_{|H|}$

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. $\sigma_1 = ()$, $\sigma_2 = (1\,2)$, $\sigma_3 = (1\,3)$, $\cdots$, $\sigma_n = (1\,n)$
$\sigma_k H = \{\text{all } \sigma \in G : \sigma(1) = k\}$

<u>Proof</u> 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 $Hg = \{hg : h \in H\}$

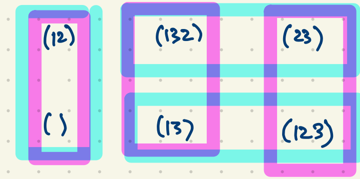
$[G:H]$ = index of H in G
= number of left cosets of H in G
= number of right cosets of H in G

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

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

Left cosets

Right cosets



$G_k = \{\sigma \in G : \sigma(k) = k\}$
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 $gKg^{-1} \subseteq K$. $\quad (gKg^{-1} = \{gkg^{-1} : k \in K\})$.

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 $h \longmapsto ghg^{-1}$.

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 $gHg^{-1} = G_2$.