Algebra I

Group Theory

Book 2

Transpositions $(i\,j)$ are odd permutations.

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

A k-cycle is a product of $k-1$ transpositions.
If k is even, this is odd; and vice versa.
A cycle of odd length is an even permutation;
〃 〃 〃 even 〃 〃 〃 odd 〃 .

If α is a product of an even numbers of transpositions, then α is an even permutation.
〃 〃 〃 〃 〃 〃 〃 odd 〃 〃 〃 〃, 〃 〃 〃 〃 odd 〃 .

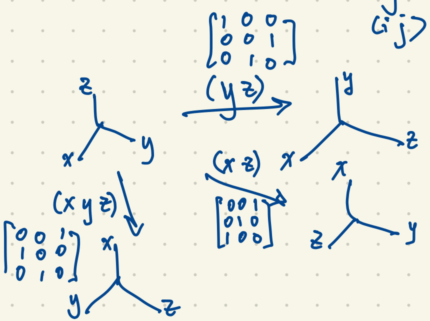
Permutations in S_5:

Even		Odd	
$()$	1	$(i\,j)$	10
$(i\,j\,k)$	20	$(i\,j\,k\,l)$	30
$(i\,j\,k\,l\,m)$	24	$(i\,j\,k)(l\,m)$	20
$(i\,j)(k\,l)$	15		
	60		60

$|S_5| = 120$

$A_5 = \{$ even permutations in $S_5 \}$

$|A_5| = 60$



An even permutation of the coordinate axis in $\mathbb{R}^n$ is an orientation-preserving transformation.
An odd permutation of the coordinate axis in $\mathbb{R}^n$ is an orientation-reversing transformation.
If $T: \mathbb{R}^n \to \mathbb{R}^n$ is a linear transformation then

$$\det T \begin{cases} = 0 & \text{if } T \text{ is not invertible} \\ > 0 & 〃 〃 \text{ preserves orientation} \\ < 0 & 〃 〃 \text{ reverses } 〃 \end{cases}$$

A permutation $\alpha \in S_n$ can be expressed as a product of transpositions.
If α is a product of an even number of transpositions, then α is even.
 " " " " " " odd " " " " " " " " " " odd.

In S_3:
$(13)(12)(13)(23)(23)(23)(12)(23) = (1\,2\,3)$ says (123) is an even permutation.

$S_3 \cong \left\langle \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} \right\rangle \cong$ dihedral group of order 6 (symmetry group of an equilateral triangle)

n	no. of groups of order n up to isomorphism
1	1
2	1
3	1
4	2
5	1
6	2
7	1
8	5

Groups of order 2

$S_2 \cong \{0, 1\} \bmod 2$ under addition $\cong \langle -1 \rangle$ under multiplication

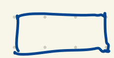
$\circ$	$()$	(12)
$()$	$()$	(12)
(12)	(12)	$()$

$+$	0	1
0	0	1
1	1	0

$\cdot$	1	-1
1	1	-1
-1	-1	1

Cayley tables of groups of order 2 all "look the same"

has a cyclic symmetry group of order 4



has an abelian symmetry group of order 4 which is not cyclic (the Klein four-group)

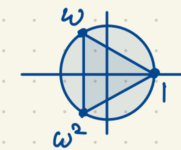
Theorem Any two groups of prime order p are isomorphic; they are cyclic of order p.

Eg. $\mathbb{Z}/3\mathbb{Z} = \{0,1,2\}$ (under addition mod 3) is isomorphic to $A_3 = \langle (123) \rangle = \{(), (123), (132)\}$ and $\{1, \omega, \omega^2\}$ under multiplication, $\omega = \frac{-1+i\sqrt{3}}{2} = e^{2\pi i/3}$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\circ$	()	(123)	(132)
()	()	(123)	(132)
(123)	(123)	(132)	()
(132)	(132)	()	(123)

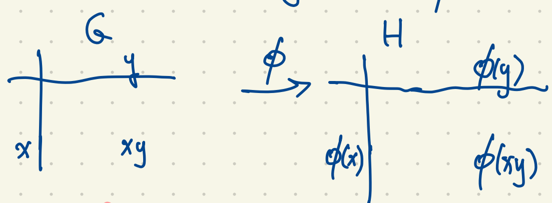
$\cdot$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω



We say two groups G, H are isomorphic ($G \cong H$) if there exists a bijection $\phi: G \to H$ such that $\phi(xy) = \phi(x)\phi(y)$

operation in G

operation in H



An isomorphism $\phi: \mathbb{Z}/3\mathbb{Z} \to A_3$ is a bijection satisfying $\phi(x+y) = \phi(x)\circ\phi(y)$

An isomorphism $\phi: \mathbb{R} \longrightarrow (0,\infty)$, $\phi(x+y) = \phi(x)\phi(y)$ is defined by $\phi(x) = e^x$

under addition

under multiplication (subgroup of $\mathbb{R}^\times = (-\infty,0)\cup(0,\infty)$)

$e^{x+y} = e^x \cdot e^y$.

$\ln = \phi^{-1}: (0,\infty) \longrightarrow \mathbb{R}$

$\mathbb{R} \not\cong \mathbb{R}^\times$

since $\mathbb{R}$ (reals under addition) has only one element of finite order whereas $\mathbb{R}^\times$ has two elements of finite order: ± 1.

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\mathbb{Z}/3\mathbb{Z}$

is isomorphic to

*	a	b	c
a	b	c	a
b	c	a	b
c	a	b	c

$\phi(0) = c$
$\phi(1) = a$
$\phi(2) = b$

*	c	a	b
c	c	a	b
a	a	b	c
b	b	c	a

or $\phi(0) = c$
$\phi(1) = b$
$\phi(2) = a$

*	c	b	a
c	c	b	a
b	b	a	c
a	a	c	b

+	0
0	0

Every group of order 1 is isomorphic to

·	1
1	1

(trivial group $\{1\}$)

" " " " " " 2 " " " " $\mathbb{Z}/2\mathbb{Z}$

+	0	1
0	0	1
1	1	0

	c
a	ac
b	bc

If $ac = bc$ then multiply both sides by c^{-1} on the right to get

$$(ac)c^{-1} = (bc)c^{-1}$$
$$a(cc^{-1}) = b(cc^{-1})$$
$$a1 = b1$$
$$a = b$$

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Every group of order 3 is cyclic (isomorphic to $\mathbb{Z}/3\mathbb{Z}$ under addition).

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Klein four-group

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Cyclic group of order 4

Two cases: either all non-identity elements of G have order 2, or G has an element not of order 2.

<u>Theorem</u>: There are exactly two groups of order 4 up to isomorphism: the Klein four-group and the cyclic group of order 4.

	e	a	b	c	d
e	e	a	b	c	d
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c

cyclic group of order 5

$$\langle a \rangle = \{e, a, \underset{b}{a^2}, \underset{c}{a^3}, \underset{d}{a^4}\}$$

	e	a	b	c	d
e	e	a	b	c	d
a	a	e	c	d	b
b	b	c	d	a	e
c	c	d	e	b	a
d	d	b	a	e	c

is not a group!

It is a quasigroup, in fact since it has an identity e, it is a loop (its Cayley table is a Latin square: each row/column is a permutation of e, a, b, c, d).

This loop is not associative

eg. $(ca)d = dd = c$

$c(ad) = cb = e$

c is a left inverse ~~for~~ b ($cb = e$) but not a right inverse ~~for~~ b ($bc = a$).

<u>Theorem</u> If every non identity element of a group G has order 2, then G is abelian.

<u>Proof</u> (Note: $x^2 = e$ = identity for every $x \in G$.)

Let $x, y \in G$. Then $(xy)^2 = xyxy = e$ so

$$yx = \underbrace{\cancel{x}(x}_{x^2=e}y x \underbrace{y)\cancel{y}}_{y^2=e} = xey = xy.$$

$\square$

In such groups, $x^{-1} = x$ for all $x \in G$.

Shoe-Sock Theorem

In every group G, with identity 1, for $x, y \in G$ we have $(xy)^{-1} = y^{-1}x^{-1}$.

Proof $(y^{-1}x^{-1})(xy) = y^{-1} 1 y = 1$ and $(xy)(y^{-1}x^{-1}) = 1$. $\square$

Warning: $(xy)^{-1} \neq x^{-1}y^{-1}$ in general.

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Klein four-group

Write the rows of the Cayley table as permutations of $\overset{1}{e}, \overset{2}{a}, \overset{3}{b}, \overset{4}{c}$:
$\{(\,), (12)(34), (13)(24), (14)(23)\}$ is a Klein ~~four~~ group as a subgroup of S_4.

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Cyclic group of order 4

Gives $\{(\,), (1234), (13)(24), (1432)\}$ as a subgroup of S_4.

Theorem (Cayley Representation Theorem)
Every finite group G is isomorphic to a subgroup of S_n where $n = |G|$.

By the way, every finite group G is also isomorphic to a group of matrices under multiplication.

Theorem If G is a finite group of order n, then every element $g \in G$ has order dividing n.
(If $g \in G$ then $|g| \mid n$.)

Eg. S_4 has elements of order $1,2,3,4$. These orders of elements divide $|S_4| = 24$.
S_5 has elements of order $1,2,3,4,5,6$ (divisors of $|S_5| = 120$).

Proof In the general case this follows from a later theorem, Lagrange's Theorem.
Here let's prove the theorem in the special case that G is abelian. (We have already proved the result for cyclic groups.)
Consider the product of all the group elements $\pi = g_1 g_2 g_3 \cdots g_n$ where $G = \{g_1, g_2, \dots, g_n\}$, $g_1 = 1$.
Note: since G is abelian, π is well-defined; it doesn't depend on what order we list the elements $g_1, \dots, g_n \in G$. Pick $a \in G$. (So $a \in \{g_1, \dots, g_n\}$.) The elements $ag_1, ag_2, \dots, ag_n$ are again all the elements of G so

$$\begin{array}{c|cccc} & g_1 & g_2 & \cdots & g_n \\ \hline a & ag_1 & ag_2 & ag_3 \cdots & ag_n \end{array}$$

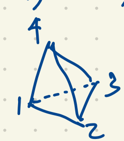
$$(ag_1)(ag_2)(ag_3)\cdots(ag_n) = \pi = a^n g_1 g_2 \cdots g_n = a^n \pi$$

So $a^n = 1$ and $k = |a|$ must divide n. $\square$

Lagrange's Theorem If G is any finite group of order n, and $H \leq G$ (i.e. H is a subgroup of G) then $|H| \mid n$.
This generalizes the previous statement: if $g \in G$ then by Lagrange's Theorem, $|g| = |\langle g \rangle| \mid |G|$.

eg. $|A_4| = \frac{1}{2}|S_4| = 12$, $A_4 = \{(), (123), (124), (132), (134), (142), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}$.

The symmetry group of a regular tetrahedron



is isomorphic to S_4.

The rotational symmetry group of the regular tetrahedron (the direct isometry group, consisting of those symmetries that preserve orientation) is isomorphic to A_4.

$A_4 = \{(),\ (123),\ (124),\ (132),\ (134),\ (142),\ (143),\ (234),\ (243),\ (12)(34),\ (13)(24),\ (14)(23)\}.$

Subgroups of A_4 have order $1, 2, 3, 4$.

Elements of A_4 have order $1, 2, 3$.

Divisors of $|A_4| = 12$ are $1, 2, 3, 4, 6, 12$.

$\langle (243), (12)(34) \rangle = \{(),\ (243),\ (12)(34),\ (234),\ (142),\ (124),\ \cdots\} = A_4.$

$(243)(12)(34) = (142)$

$\{(),\ (12)(34),\ (13)(24),\ (14)(23)\}$ is the Klein four-group, a subgroup of A_4.

Question: How many subgroups of $\mathbb{Z}$ are there containing 4? (Note: $\mathbb{Z}$ is an additive group.)

$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, 4, 5, \cdots\}$

$2\mathbb{Z} = \{\ldots, -6, -4, -2, 0, 2, 4, 6, 8, \ldots\}$

$4\mathbb{Z} = \{\ldots, -8, -4, 0, 4, 8, 12, \cdots\}$

$-4\mathbb{Z} = \{\ldots, -8, -4, 0, 4, 8, 12, \cdots\}$

Answer: There are three subgroups of $\mathbb{Z}$ containing 4, namely $\mathbb{Z}$, $2\mathbb{Z}$, $4\mathbb{Z}$.

$\mathbb{Z}$ has infinitely subgroups: one finite subgroup $\{0\}$ and all the other subgroups are infinite.

There are infinite subgroups of $\mathbb{Z}$ containing 4 but not infinitely many subgroups of $\mathbb{Z}$ containing 4.

Note: For every cyclic group G, all subgroups of G are cyclic; they are generated by powers of the generator of G.

Eg. $G = \langle g \rangle$ where $|g| = \infty$ i.e. $|G| = |\langle g \rangle| = |g| = \infty$.

$= \{\ldots, g^{-3}, g^{-2}, g^{-1}, 1, g, g^2, g^3, \ldots\}$ with no repeats.

1 is the identity

$g^i g^j = g^{i+j} = g^j g^i$

How many subgroups of $G = \langle g \rangle$ contain g^4? Three: $\langle g \rangle$, $\langle g^2 \rangle$, $\langle g^4 \rangle$.

$\langle g \rangle = \langle g^{-1} \rangle$, $\quad \langle g^2 \rangle = \langle g^{-2} \rangle = \langle g^6, g^{10} \rangle$, $\quad \langle g^4 \rangle = \langle g^{-4} \rangle$

$G = \{\ldots, g^{-3}, g^{-2}, g^{-1}, 1, g, g^2, g^3, g^4, \ldots\}$

$\langle g^2 \rangle = \{\ldots, g^{-6}, g^{-4}, g^{-2}, 1, g^2, g^4, g^6, \ldots\}$

$\langle g^4 \rangle = \{\ldots, g^{-8}, g^{-4}, 1, g^4, g^8, g^{12}, \ldots\}$

$\langle g^6, g^{10} \rangle \leq \langle g^2 \rangle$

$\langle g^2 \rangle \leq \langle g^6, g^{10} \rangle$

since $g^2 = (g^6)^2 (g^{10})^{-1}$

So $\langle g^2 \rangle = \langle g^6, g^{10} \rangle$

$\underset{\substack{\text{multiplicative} \\ \text{cyclic group}}}{G} \cong \underset{\substack{\text{additive} \\ \text{cyclic group}}}{\mathbb{Z}}$

$\phi : \mathbb{Z} \to G$ is an isomorphism

$\phi(i) = g^i$

Theorem If G is a group of even order, then G has an element of order 2 (i.e. at least one element of order 2). Note: G is not necessarily abelian.

Proof Pair up each group element with its inverse giving pairs $\{g, g^{-1}\}$ for $g \in G$. Note that $g = g^{-1}$ iff g has order 1 or 2. ($g = g^{-1} \Leftrightarrow g^2 = 1 \Leftrightarrow |g|$ divides 2). So G is partitioned into subsets $\{g, g^{-1}\}$ having size 1 or 2. If G has no elements of order 2 then we have partitioned a set G of even cardinality into one subset $\{1\}$ of size 1, and a collection of pairs $\{g, g^{-1}\}$ of size 2, a contradiction. $\square$

what we actually showed is that in a group of even order, the number of elements of order 2 is odd. (In a group of odd order, there are no elements of order 2 although we haven't proved this yet except in the abelian case.)

Eg. Direct Products: Given groups G, H (say, multiplicative) we form the <u>direct product</u> of G and H as $G\times H = \{(g,h) : g\in G,\ h\in H\}$ (the cartesian product of the sets G and H) which becomes a group under <u>coordinatewise multiplication</u> i.e.

$$(g,h)(g',h') = (gg', hh')$$

and coordinatewise inverses i.e. $(g,h)^{-1} = (g^{-1}, h^{-1})$
and the coordinatewise identity $1\in G\times H$ is $1 = 1_{G\times H} = (1_G, 1_H)$. or $e_{G\times H} = (e_G, e_H)$.

Eg. $\mathbb{Z}/2\mathbb{Z} = \{0,1\}$ under addition mod 2

+	0	1
0	0	1
1	1	0

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(x,y) : x,y\in \mathbb{Z}/2\mathbb{Z}\} = \{(0,0), (0,1), (1,0), (1,1)\}$$

$(x,y) + (x',y') = (x+x', y+y')$. The identity $0 = (0,0)$.

This is the Klein four-group since it has 3 elements of order 2.

Note: Many books write $\mathbb{Z}_2$ or Z_2 in place of $\mathbb{Z}/2\mathbb{Z}$

If $|G| = m$ and $|H| = n$ then $|G\times H| = mn$.

If G and H are abelian then so is $G\times H$.

In fact, the converse holds: G and H are both abelian, iff $G\times H$ is abelian.

$G\times H \cong H\times G$

$\phi: G\times H \to H\times G$

$\phi(g,h) = (h,g)$ is an isomorphism.

$G\times H$ has a subgroup $G\times\{1_H\} = \{(g,1_H) : g\in G\} \cong G$

An isomorphism $G\times\{1_H\}\longrightarrow G$ is given by $(g,1_H)\longmapsto g$.

Likewise, $G\times H$ has a subgroup $\{1_G\}\times H \cong H$

$$\underbrace{(g,1_H)}_{\substack{\uparrow\\ G\times\{1_H\}\\ \cong\\ G}}\underbrace{(1_G,h)}_{\substack{\uparrow\\ \{1_G\}\times H\\ \cong\\ H}} = (g,h) = (1_G,h)(g,1_H)$$

Eg. $\underset{\text{multiplicative group}}{\mathbb{R}^\times = (-\infty,0)\cup(0,\infty)} \cong \underbrace{\mathbb{R}}_{\substack{\text{additive}\\ \text{group}}} \times \underbrace{\mathbb{Z}/2\mathbb{Z}}_{\text{additive}}$

An isomorphism $\phi:\mathbb{R}^\times\longrightarrow\mathbb{R}\times\mathbb{Z}/2\mathbb{Z}$ is $\phi(a) = \begin{cases}(\ln|a|,0) & \text{if } a>0\\ (\ln|a|,1) & \text{if } a<0\end{cases}$

It's easy to see that ϕ is one-to-one and onto.

We show that $\phi(ab) = \phi(a)+\phi(b)$ for all $a,b\in\mathbb{R}^\times$.

We argue in ~~four~~ cases. If $a,b>0$ then

$\phi(ab) = (\ln|ab|,0)$ since $ab>0$

$= (\ln|a|+\ln|b|,0) = (\ln|a|,0)+(\ln|b|,0) = \phi(a)+\phi(b)$

If $a>0>b$ then $ab<0$ so

$\phi(ab) = (\ln|ab|,1) = (\ln|a|,0)+(\ln|b|,1) = \phi(a)+\phi(b)$

Similarly if $a<0<b$.

If $a,b<0$ then $ab>0$ so

$\phi(ab) = (\ln|ab|,0) = (\ln|a|,1)+(\ln|b|,1)$
$= \phi(a)+\phi(b)$

Every cyclic group is abelian.

Not every abelian group is cyclic but every abelian group is a direct product of cyclic groups.

eg. the Klein four-group is a direct product of two groups of order 2 i.e. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

There are five groups of order 8 up to isomorphism:

$\left.\begin{array}{l} \mathbb{Z}/8\mathbb{Z} \quad \text{(cyclic)} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} = \{(a,b) : a \in \mathbb{Z}/2\mathbb{Z},\ b \in \mathbb{Z}/4\mathbb{Z}\}. \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(a,b,c) : a,b,c \in \mathbb{Z}/2\mathbb{Z}\} \text{ under addition} \end{array}\right\}$ three abelian groups of order 8

dihedral group of order 8 $\cong$ symmetry group of square, D_4 (sometimes D_8)

quaternion group of order 8, Q or Q_8

$Q = \{1, \underset{\substack{\uparrow \\ \text{order } 2}}{-1}, \underbrace{i, -i, j, -j, k, -k}_{\text{order } 4}\}$

$ij = k,\ ji = -k,\quad i^2 = j^2 = k^2 = -1$

$jk = i,\ kj = -i$

$ki = j,\ ik = -j$

For any field F (eg. $\mathbb{R}, \mathbb{C}, \mathbb{Q}$) $GL_n(F) = \{\text{invertible } n\times n \text{ matrices over } F\}$ i.e. having entries in F.

Also $F = \mathbb{F}_3 = \{0,1,2\}$ works with addition mod 3. $2+2 = 1 = 2\times 2$

$\frac{1}{2} = 2$

In $\mathbb{F}_7 = \{0,1,2,\dots,6\}$, $\frac{1}{5} = 3$.

$\mathbb{F}_p = \{0,1,2,\dots,p-1\}$ is a field whenever p is prime.

$GL_2(\mathbb{F}_3) = \{\text{invertible } 2\times 2 \text{ matrices over } \mathbb{F}_3\}$ is a group of order 48.

$GL_2(\mathbb{R}) = \{\text{invertible } 2\times 2 \text{ matrices over } \mathbb{R}\} = \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{R},\ ad-bc \neq 0\right\}$

$GL_n(F) = \{\text{invertible } n\times n \text{ matrices over } F\}$ = general linear group of degree n over F

also denoted $GL(n,F)$ in the textbook

$SL_n(F)$ is the special linear group of degree n over F; $SL_n(F) \le GL_n(F)$
or $SL(n,F)$ $SL_n(F) = \{n\times n \text{ matrices over } F \text{ having determinant } 1\}$.

If $F = \mathbb{F}_p = \{0,1,2,\cdots,p-1\} \bmod p$ (field of prime order p) then we can count elements in $GL_n(\mathbb{F}_p)$ or $SL_n(\mathbb{F}_p)$.

(For 2×2 matrix over $\mathbb{F}_3$, $\underline{33}$ matrices have $\det A = 0$, $\underline{24}$ matrices have $\det A = 1$, $\underline{24}$ ... " $\det A = 2$).

$|GL_2(\mathbb{F}_3)| = 48$.

The number of 2×2 matrices over $\mathbb{F}_3 = \{0,1,2\}$ is 81. How many of them are invertible?
We count invertible matrices $\begin{bmatrix} a & b \\ c & d\end{bmatrix}$, $a,b,c,d \in F = \mathbb{F}_3$ with linearly independent columns.
There are $\underline{8}$ ← $9-1=8$ choices for the first column $\begin{bmatrix} a \\ c\end{bmatrix} \neq \begin{bmatrix} 0 \\ 0\end{bmatrix}$.
Having chosen the first column $\begin{bmatrix} a \\ c\end{bmatrix}$, there are $\underline{6}$ ← $9-3=6$ choices for the second column $\begin{bmatrix} b \\ d\end{bmatrix}$ which are not a scalar multiple of the first column. So $|GL_2(\mathbb{F}_3)| = 8\times 6 = 48$.
In fact, for $A \in GL_2(F)$, $F = \mathbb{F}_3$, there are 24 choices with determinant 1, and 24 choices with determinant $-1=2$.

$$|GL_n(\mathbb{F}_p)| = \underbrace{(p^n-1)}_{\text{no. of choices of first column}}\underbrace{(p^n-p)}_{\text{no. of choices of second column}}\underbrace{(p^n-p^2)}_{\text{no. of choices of third column}}\cdots\underbrace{(p^n-p^{n-1})}_{\text{no. of choices of last column}}$$

$|GL_2(\mathbb{F}_p)| = (p^2-1)(p^2-p)$

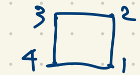
For $A \in GL_n(\mathbb{F}_p)$, $\det A \in \{1,2,\cdots,p-1\}$ and there equally many matrices with each possible nonzero determinant in $\{1,2,\cdots,p-1\}$ so

$|SL_n(\mathbb{F}_p)| = \frac{1}{p-1}|GL_n(\mathbb{F}_p)|$. We'll explain later.

For any group G, the center of G is $Z(G) = \{$all elements in G which commute with everything in $G\}$

Zentrum ↑ not Z Zahlen $= \{z \in G : zx = xz \text{ for all } x \in G\}$

Eg. if G is the symmetry group of a square (a dihedral group of order 8) then $|Z(G)| = 2$ and $Z(G)$ consists of the identity and the half-turn ($180°$ rotation about the center).



If we represent G using permutations on the vertices 1,2,3,4 then

$$G = \{(),\ (1234),\ (13)(24),\ (1432),\ (12)(34),\ (14)(23),\ (13),\ (24)\}$$

then $Z(G) = \langle (13)(24) \rangle = \{(),\ (13)(24)\}$.

Alternatively, G can be represented as a subgroup of $GL_2(\mathbb{R})$:

$$G = \left\{ \begin{bmatrix}1&0\\0&1\end{bmatrix}, \begin{bmatrix}0&-1\\1&0\end{bmatrix}, \begin{bmatrix}-1&0\\0&-1\end{bmatrix}, \begin{bmatrix}0&1\\-1&0\end{bmatrix}, \begin{bmatrix}1&0\\0&-1\end{bmatrix}, \begin{bmatrix}-1&0\\0&1\end{bmatrix}, \begin{bmatrix}0&1\\1&0\end{bmatrix}, \begin{bmatrix}0&-1\\-1&0\end{bmatrix} \right\}$$

$$Z(G) = \left\langle \begin{bmatrix}-1&0\\0&-1\end{bmatrix} \right\rangle = \left\{ \begin{bmatrix}1&0\\0&1\end{bmatrix}, \begin{bmatrix}-1&0\\0&-1\end{bmatrix} \right\}$$

In general, $Z(G) \leq G$ (a subgroup of G).

$Z(G) = G$ iff G is abelian.

For many groups, $Z(G) = \{1\}$ ← identity eg. $Z(S_3) = \{()\}$.

e = identity of G

Theorem If G is a group and $z \in G$, then $Z(G) \leq G$ (the center of G is a subgroup of G).

Proof Since $eg = g = ge$ for every $g \in G$, $e \in Z(G)$. If $z, z' \in Z(G)$ then

$$(zz')g = z(z'g) = z(gz') = (zg)z' = (gz)z' = g(zz')$$

so $zz' \in Z(G)$. Also if $z \in Z(G)$ then for every $g \in G$ we have $zg = gz$ so $z^{-1}g = z^{-1}(gz)z^{-1} = z^{-1}(zg)z^{-1} = gz^{-1}$

so $z^{-1} \in Z(G)$. □

Let $S \subseteq G$. The centralizer of S in G is $C_G(S)$ = the set all all elements of G commuting with every element of S, i.e. $C_G(S) = \{g \in G : gs = sg \text{ for all } s \in S\}$.

eg. $C_G(e) = G$, $C_G(G) = Z(G)$. If $z \in Z(G)$ then $C_G(z) = G$.

In S_4, $C_{S_4}((12)) = \{(), (34), (12), (12)(34)\}$

In general, $C_G(S) \leq G$ (the centralizer of a subset of G is always a subgroup of G).
The proof of this is virtually identical to the proof above; just quantify over $g \in S$ rather than $g \in G$.

If $G = GL_n(F)$ = invertible $n \times n$ matrices over F, then $Z(G) = \{\lambda I : \lambda \neq 0 \text{ in } F\}$
$I = I_n$ = $n \times n$ identity matrix.

$$\begin{bmatrix}1&0\\0&2\end{bmatrix}\begin{bmatrix}1&1\\0&1\end{bmatrix} = \begin{bmatrix}1&1\\0&2\end{bmatrix}, \quad \begin{bmatrix}1&1\\0&1\end{bmatrix}\begin{bmatrix}1&0\\0&2\end{bmatrix} = \begin{bmatrix}1&2\\0&2\end{bmatrix} \quad \text{so } \begin{bmatrix}1&0\\0&2\end{bmatrix} \notin Z(GL_2(\mathbb{R}))$$

Let $E_{ij}(a) = \begin{array}{c|c} & j \\ \hline i & \begin{bmatrix}1 & & a\\ & \ddots & \\ & & 1\end{bmatrix}\end{array}$ for $i \neq j$. (This is the elementary matrix obtained from the identity matrix by adding an "a" in the (i,j) position.)

If $A = [a_{ij} : 1 \leq i, j \leq n] \in Z(GL_n(F))$ then $AE_{ij}(1) = E_{ij}(1)A$ so $a_{ij} = 0$. So A is diagonal.
Continue using other elementary matrices to show $A = \lambda I$.

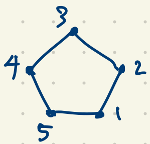
$G = GL_n(F)$ is generated by elementary matrices so $A \in Z(G)$ iff A commutes with all elementary matrices.

$Z(G)$ might be trivial e.g. $Z(S_3) = \{()\}$.

Another construction of subgroups: Suppose $G \leq S_n$. So G permutes $[n] = \{1, 2, \dots, n\}$.

The <u>stabilizer</u> of a point $x \in [n]$ is $\mathrm{Stab}_G(x) = \{g \in G : g(x) = x\} \leq G$.

Eg.



The symmetry group ~~of~~ of a regular pentagon is a group G which is dihedral of order 10 (sometimes denoted D_5 or D_{10}).

$$G = \{(), \underbrace{(12345), (13524), (14253), (15432)}_{5\text{ rotations}}, \underbrace{(12)(35), (13)(45), (14)(23), (15)(24), (25)(34)}_{5\text{ reflections}}\}$$

$G \leq S_5$ permuting $[5] = \{1, 2, 3, 4, 5\}$, the five vertices.

$\mathrm{Stab}_G(3) = \{(), (15)(24)\}$.

$()(x) = x$

If $g, h \in \mathrm{Stab}_G(x)$ then

$(gh)(x) = g(h(x)) = g(x) = x$

If $g \in \mathrm{Stab}_G(x)$ then $g(x) = x$ so

$x = g^{-1}(g(x)) = g^{-1}(x)$ so $g^{-1} \in \mathrm{Stab}_G(x)$.

Elements of order 2 in a group are called <u>involutions</u>.

If G is abelian then the product of any two involutions in G has order ≤ 2. If $|a| = |b| = 2$ then $(ab)^2 = abab = a^2b^2 = 1\cdot 1 = 1$ so $|ab| = 1$ or 2. If $ab = 1$ then $b = a$; otherwise $ab \ne 1$, $(ab)^2 = 1$ so ab is an involution so $\{1, a, b, ab\} = \langle a, b\rangle$ is a Klein four-subgroup of G. Any two distinct involutions in an abelian group G generate a Klein four-subgroup.

$(12)(13) = (132)$ in S_3.

How many involutions can a finite abelian group G have?

If G has k involutions then every involution lies in exactly $\frac{k-1}{2}$ Klein four-subgroup

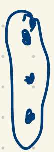
How many Klein four-subgroups does G have altogether?

Count subgroups of the form $\langle a,b\rangle = \{1, a, b, ab\}$ where $a, b \in G$ are distinct involutions

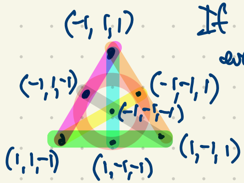
k choices for a

$k-1$ choices for b

$\frac{k(k-1)}{6}$ is the number of Klein four-subgroups in G.



If $k = 7$ then we have 7 involutions, 7 Klein four-subgroups, every Klein four-group has 3 involutions. every involution is in 3 Klein four-groups,



In a direct product of three groups of order two e.g. $\langle -1\rangle \times \langle -1\rangle \times \langle -1\rangle$
$= \{(x, y, z) : x, y, z \in \langle -1\rangle\}$

$\langle -1\rangle = \{1, -1\}$

Certainly $k \equiv 1$ or $3 \mod 6$

In general if a, b are distinct involutions in a group G then what can they generate?

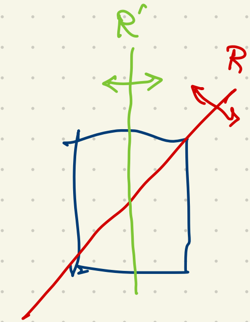
$\langle a,b\rangle = \{1, a, b, ab, ba, aba, bab, abab, baba, \ldots\}$ with possible duplicates.

The symmetry group of an infinite string $\cdots T\,T\,T\,T\,T\,T\,T \cdots$ is generated by two reflections a, b in vertical axes l, l' as shown

ab is a translation (shift) one step to the right
ba is a translation one step to the left.

$\langle ab\rangle = \{\ldots, baba, ba, 1, ab, abab, ababab, \ldots\}$ is an infinite cyclic group, a subgroup of $\langle a,b\rangle$

$\langle a,b\rangle$ itself is an infinite dihedral group.



The symmetry group of a square is a dihedral group $\langle R, R'\rangle$ generated by two reflections

$$\langle R,R'\rangle = \{I, R, R', RR', R'R, RR'R, R'RR', \underset{\substack{\parallel \\ R'RR'R}}{RR'RR'}\}$$

Comments on HW2:

Recall in class we used the product π of elements in a finite abelian group.

#5(a) Show that π has order ≤ 2.

<u>Proof</u> If $G = \{g_1, g_2, \cdots, g_n\}$ is abelian of order n then $\pi = g_1 g_2 \cdots g_n = g_1^{-1} g_2^{-1} \cdots g_n^{-1}$ so

$\pi^2 = (\cancel{g_1}\cancel{g_2}\cdots\cancel{g_n})(\cancel{g_1^{-1}}\cancel{g_2^{-1}}\cdots\cancel{g_n^{-1}}) = e$ (the identity element of G).

Eg. G is cyclic of order 4.

In multiplicative notation, $G = \langle g \rangle = \{1, g, g^2, g^3\}$ where $g^4 = 1$; $\pi = 1 \cdot g \cdot g^2 \cdot g^3 = g^2$ of order 2.

In additive notation, $G = \mathbb{Z}/4\mathbb{Z} = \{0,1,2,3\} = \langle 1 \rangle$; $\pi = 0+1+2+3 = 2$ of order 2. 0 is the identity.

In S_4, $G = \langle (1\,2\,3\,4) \rangle \le S_4$, $\pi = () \circ (1234) \circ (13)(24) \circ (1432) = (13)(24)$ of order 2.

$\lim_{x \to \infty} \frac{\sin x}{x} = 0$. $\lim_{\varepsilon \to \infty} \frac{\sin \varepsilon}{\varepsilon} = 0$ is problematic in its unorthodox choice of variable $\varepsilon \to \infty$.

$\lim_{\varepsilon \to 0} \frac{\sin \varepsilon}{\varepsilon} = 1$ is natural.

$G = SL_2(\mathbb{F}_3) = \{2\times 2$ matrices of $\mathbb{F}_3$ having determinant $1\}$. $|G| = 24$.

Is $G \cong S_4$? G as only one involution whereas S_4 has 9 involutions. (An involution in any group element of order 2.)

If $G = SL_2(\mathbb{R})$ or $SL_2(\mathbb{C})$ then G has only one involution, $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = -I$. $GL_2(\mathbb{R})$ has <u>many</u> involutions.

eg. $\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$ is a reflection in the y-axis.

Does $GL_2(\mathbb{R})$ have an element of order 11? Yes; in fact $SL_2(\mathbb{R})$ does:

$$\begin{bmatrix} \cos\frac{2\pi}{11} & -\sin\frac{2\pi}{11} \\ \sin\frac{2\pi}{11} & \cos\frac{2\pi}{11} \end{bmatrix} \in SL_2(\mathbb{R})$$

$A = \begin{bmatrix} \cos\theta & -\sin\theta \\ -\sin\theta & -\cos\theta \end{bmatrix} \in GL_2(\mathbb{R})$ has determinant -1.

$A^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ A is a reflection

(Infinitely many involutions in $GL_2(\mathbb{R})$.)

why is $-I$ the only involution in $SL_2(\mathbb{R})$?

Conjugacy in groups

Two elements $g, h \in G$ are <u>conjugate</u> if $h = aga^{-1}$ for some $a \in G$. We write $h \sim g$ in this case.

This is an equivalence relation on G:

- For every $g \in G$, $g \sim g$. $(g = ege^{-1})$
- $g \sim h$ iff $h \sim g$. If $h \sim g$ then $h = aga^{-1}$ for some $a \in G$ so $g = a^{-1}ha = (a^{-1})h(a^{-1})^{-1}$
- If $h \sim g \sim w$ then $h \sim w$. If $h = aga^{-1}$ and $g = bwb^{-1}$ then $h = a(bwb^{-1})a^{-1} = (ab)w(ab)^{-1}$.

(Look up equivalence relations in the textbook, Math 2800, my videos)

Eg. in $GL_n(F)$, conjugacy is just similarity. Look in linear algebra textbook. Two matrices $A, B \in GL_n(F)$ are similar iff they represent the same linear transformation with respect to a different choice of basis.

In general, conjugate elements in G have the same order. Why?

If $h = aga^{-1}$ then $h^n = \underbrace{(aga^{-1})(aga^{-1})\cdots(aga^{-1})}_{n \text{ times}} = ag^na^{-1}$. If $g^n = 1$ then $h^n = 1$. Conversely, if $h^n = 1$ then $g^n = 1$.

It follows that $|h| = |g|$ whenever h, g are conjugate in G.

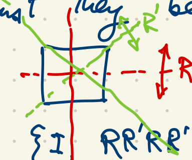
Is the converse true? If two elements have the same order, must they be conjugate in G?

No; e.g. in the symmetry group of a square, $G = \langle R, R' \rangle$ where

$R'RR' = R'R(R')^{-1} \sim R$

$R'RR'$ is conjugate to R

$RR'R$ is conjugate to R'



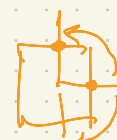
$G = \{ I, R, R', \boxed{RR', R'R}, RR'R, R'RR', RR'RR' \}$, $Z(G) = \langle RR'RR' \rangle = \{I, RR'RR'\}$

90° rotations

reflections

$RR'RR' = R'RR'R$

half-turn about the center



The two elements of order 4 are conjugate: $R'R = (R)RR'(R)$

The dihedral group of order 8 has conjugacy classes as follows:

$\{I\}$, $\{RR'RR'\}$, $\{R, R'RR'\}$, $\{R', RR'R\}$, $\{RR', R'R\}$.

order 1, order 2, order 2, order 2, order 4

If $z \in Z(G)$ then $\{z\}$ is a conjugacy class by itself $(aza^{-1} = aa^{-1}z = ez = z)$

Conjugacy in S_n

eg. $\sigma = (1\,5\,7)(2\,4)$, $\tau = (1\,2\,3)(5\,6\,8)(4\,7)$ in S_8

$\sigma \sim \tau\sigma\tau^{-1} = (1\,2\,3)(5\,6\,8)(4\,7)(1\,5\,7)(2\,4)(1\,3\,2)(5\,8\,6)(4\,7) = (2\,6\,4)(3\,7)$

$|\sigma| = 6$, $|\tau\sigma\tau^{-1}| = 6$.

In S_n, two elements (i.e. permutations) are conjugate iff they have the same cycle structure.

In S_8, $(1\,7\,6\,8\,3\,5)$ has order 6 but it cannot be conjugate to σ since its cycle structure is different.

A faster way to compute $\tau\sigma\tau^{-1}$:

$$\begin{array}{c} \sigma = (1\ 5\ 7)(2\ 4) \\ \downarrow\ \downarrow\ \downarrow\quad \downarrow\ \downarrow\ \tau \\ \tau\sigma\tau^{-1} = (2\ 6\ 4)(3\ 7) \end{array}$$