Reminder: Midterm 1 next Monday!

Previously in math 203a: examples of groups.

$SL(2,F)$, $F = \mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}_n, \mathbb{Z}$

Special linear group $= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \begin{array}{l} a,b,c,d \in F \\ ad-bc=1 \end{array} \right\}$

Closed under matrix mult since

$$\det(AB) = \det(A)\det(B) = 1$$

if $A, B \in SL(2,F)$ $\therefore AB \in SL(2,F)$

Inverses: $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

$\det A = ad - bc$

Looking ahead: $SL(2,\mathbb{R}) \subset GL(2,\mathbb{R})$

both are groups!

This is an example of a subgroup (one group contained in another)

Basic properties of groups

Thm. G group

(1) G has a unique identity element

i.e. if e & e' are both identity elements, then $e = e'$

(2) Cancellation holds: $ab = ac \Rightarrow b = c$
$ba = ca \Rightarrow b = c$

(3) Inverses are unique: If $ab = e$ & $at = e$, then $b = c$.

Pf: Note first that (3) is a special case of (2) $ab = e$ & $ac = e \Rightarrow ab = ac$
$\Rightarrow b = c$ by (2). So we'll prove (1) & (2)

(1) If e & e' are identity elements, then

$$ea = e'a = a \quad (*) \qquad \forall\, a \in G$$
$$\& \quad ae = ae' = a \quad (**)$$

Take $a = e'$ in $(*)$ so that

$$ee' = e'e' = e' \Rightarrow ee' = e'$$

Take $a = e$ in $(**)$ so that

$$ee = ee' = e \Rightarrow ee' = e$$

$\therefore e = e'$ which proves (1)

(2) Cancellation. Suppose $ab = ac$.
Let a' be an inverse of a. (We're not assuming inverses are unique yet.)

$$a'(ab) = a'(ac)$$

By assoc. $(a'a)b = (a'a)c \Rightarrow b = c$ // this proves Thm.

Puzzle (Are we having fun yet?)

Suppose this is a Cayley table for a group $G = \{a, b, c, d, e = \text{identity}\}$ 5 elements

Fill in the missing entries

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

(Recall that the entry in the row labeled x and the column labeled y represents the element $xy \in G$)

Big clue: for the row x, the entries represent xe, xa, xb, xc, xd. By cancellation, these are all different, e.g. $xa = xd$ would mean $a = d$, not true.

∴ each row contains each of a, b, c, d, e exactly once.

Similarly, each column contains each of a, b, c, d, e exactly once

Also, the first row & column are obvious.

Let's do it on the blackboard!

The answer will be on the next page of the notes.

Some useful notation

Write g^{-1} for the inverse of g, g^{-2} for $(g^{-1})g^{-1}$, etc. Then G contains all elements of the form g^n, $n \in \mathbb{Z}$, where $g^0 = e$. By definition, $\boxed{g^n g^m = g^{n+m}}$

Also $\boxed{(g^n)^m = g^{nm}}$

Ex: Let $\boxed{G = U(5) = \{1, 2, 3, 4\}}$

Take $g = 4$. Then $g^2 = 16 \bmod 5 = 1$

$\therefore g^{-1} = g$ and $\{g^m : m \in \mathbb{Z}\} = \{1, 4\}$.

How to find inverses of products.

Caution, In general, $a^n b^n \neq (ab)^n$ unless G is abelian.

Thm (Socks - Shoe Property)
For $a, b \in G$, $\boxed{(ab)^{-1} = b^{-1}a^{-1}}$

Pf: By associativity

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = e \;//$$

Finite groups, subgroup

Def The order of a group G, written $|G|$, is the number of elements in the group.

Ex 1. $|GL(2,\mathbb{R})| = \infty$
2. $|D_n| = 2n$
3. $|U(16)| = |\{1, 3, 5, 7, 9, 11, 13, 15\}| = 8$

Def The order of an element $g \in G$, written $|g|$ is the smallest positive integer n for which $g^n = e$. If no such n exists, write $|g| = \infty$

Observation: If $|g| = \infty$, then $g^n \neq g^m$ if $n \neq m$

Reason: WLOG, suppose $n \geq m$.
$g^n = g^m \Rightarrow g^{n-m} = e$. Since $|g| = \infty$, $n - m = 0$.

Ex 1. $G = \mathbb{Z}$. $|m| = \infty$ $\forall$ m. operation = addition

Notation: m^2 is $m+m = 2m$

m^3 means $3m$, etc.

Ex 2. $G = GL(2, \mathbb{R})$ $\quad g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $g^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$

so $\left| \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right| = \infty$

Check: $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n+1 \\ 0 & 1 \end{pmatrix}$

Try $g = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$. $\quad g^2 = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e$

$\therefore \left| \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} \right| = 2.$

Ex 3. $G = U(5) = \{1, 2, 3, 4\}$ $\quad |U(5)| = 4$

Find $|2|$ $\quad 2^2 = 4$

$2^3 \bmod 5 = 8 \bmod 5 = 3$

$2^4 \bmod 5 = 6 \bmod 5 = 1$

$\therefore |2| = 4$

We've checked $|4| = 2$, since $4^2 \bmod 5 = 1$

Not surprising, since $4^n = 2^{2n}$.

---

	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

Subgroups

G group, $g \in G$

Observation: $\{g^m : m \in \mathbb{Z}\}$ is a group contained in G

$g^m g^n = g^{m+n}$

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

Notation:

Write $\langle g \rangle$ for $\{g^m : m \in \mathbb{Z}\}$

abelian group $\subset G$

called a subgroup of G

Ex: $G = U(5)$

$g = 2 \quad |\langle 2 \rangle| = 4$

Since $|U(5)| = 4$ & $\langle 2 \rangle \subset U(5)$

must have $\langle 2 \rangle = U(5)$.

For $g = 4 \quad |\langle 4 \rangle| = 2$

$\langle 4 \rangle = \{1, 4\} \subsetneq U(5)$.