Math 122 Wednesday, September 21

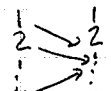
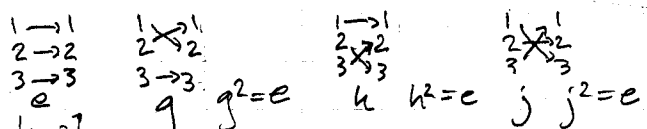
Recall a group G has a map $g,h \mapsto g\cdot h \in G$ associative, e identity, $g \mapsto g^{-1}$

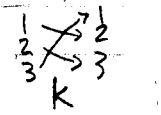
ex: $G = GL_n(\mathbb{R})$ = invertible $n\times n$ real matrices
↳ "general linear" group

ex: T a set $G = Aut(T) = \{$ bijections $g: T \to T\}$ multiplication = composition
e = identity map inverse = inverse map

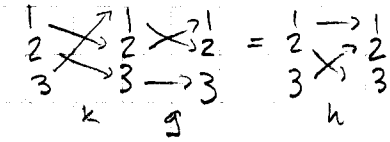
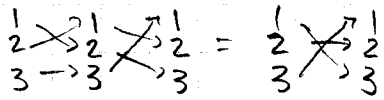
$T = \mathbb{R}^n = \{(x_1,\dots,x_n) : x_i \in \mathbb{R}\}$ $GL_n(\mathbb{R}) \subset Aut(T)$ subset of linear bijections $A\begin{pmatrix}x_1\\ \vdots \\ x_n\end{pmatrix} = \begin{pmatrix}y_1\\ \vdots \\ y_n\end{pmatrix}$

$T = \{1,2,\dots,n\}$ finite set then $Aut(T) = S_n$, the symmetric group on n letters

$g \in S_n$ works by  e.g. in S_3 

recall $\#S_n = n!$ So this is all of S_3. 

Claim S_3 is a non-abelian group.

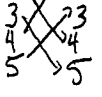
$g\cdot k = h$  but $k\cdot g = j$ 

defn The number of elements of a finite group (written $\#G$ or $|G|$) is called the order of G.

Cycle notation for S_n

e.g. $\begin{matrix}1\to1\\2\to2\\3\to3\end{matrix} = e = (1)(2)(3)$ $\begin{matrix}1\to1\\2\to2\\3\to3\end{matrix} = g = (12)(3)$  $= k = (123)$

for shorthand can write (12) for $(12)(3)$ etc
so $S_3 = \{e, (12), (23), (13), (123), (132)\}$

generally the cycle notation for $g \in S_n$ $g = (1\ g(1)\ g(g(1))\ \cdots)$ e.g.  $= (124)(35)$

defn Given $g \in G$ the order of g is the smallest $n \in \mathbb{N}$ such that $g^n = e$.

e.g. (12) has order 2, (123) has order 3

Given an object (group, set, rng, vector space, ...) we are also interested in

sub-object, quotient-object, map between objects = homomorphism

def Subgroup $H \subset G$ is
1) a subset
2) closed under multiplication
3) contains e
4) contains h^{-1} for all $h \in H$

ex: in S_3, $H = \{e, (12)\}$ is a subgroup

$H = \{e, (123)\}$ is not closed under multiplication or inverses but $H' = \{e, (123), (132)\}$ is.

other subgroups: $\{e, (13)\}, \{e, (23)\}, \{e\}, G$

ex: $GL_n(\mathbb{R}) \subset Aut(\mathbb{R}^n)$ is a subgroup
because matrix multiplication is the same as composition of linear transformations.
Closed because composition of two linear maps is linear.

General theme: often subgroups arise by preserving something (eg. linearity)

also $H = \{e, (12)\}$ is the subgroup of S_3 that fixes "3".
$H = \{e, (123), (132)\}$ fixes something too but this is harder to see

Let $H \subset S_n$ be all permutations that fix n, a subgroup of order $(n-1)!$
[next time we'll say H is isomorphic to S_{n-1}]

Consider the abelian group $\mathbb{Z}$ under addition [note: here "multiplication" is written "+"]
$e = 0$ $(n)^{-1} = -n$

Goal: classify all $H \subset \mathbb{Z}$ obvious subgroups: $H = \mathbb{Z}$, $H = \{0\}$
$H = \{\ldots, -4, -2, 0, 2, 4, 6, \ldots\}$ even numbers
note $H = \{\text{odd numbers}\}$ not closed, doesn't contain 0.
more generally take $H = n\mathbb{Z} = \{\text{numbers divisible by } n\} = \{nk \mid k \in \mathbb{Z}\}$
note: $n\mathbb{Z} = (-n)\mathbb{Z}$ so assume $n \geq 0$

Thm Any subgroup $H \subset \mathbb{Z}$ has the form $n\mathbb{Z}$ with $n \geq 0$ uniquely determined by H.

Pf: Let H be a subgroup. If $H = \{0\}$ take $n = 0$. Otherwise H contains some positive integers. Let n be the smallest positive integer contained in H. Then claim: $H = n\mathbb{Z}$. Clearly $H \supset n\mathbb{Z}$ by closure under addition and inverses. Take any $h \geq 1$ in H, and write $h = nk + r$ with $0 \leq r < n$. Claim $r = 0$. Note $h, nk \in H$ so $h - nk \in H$ by closure under addition and inversion. So $r \in H$. If $r \neq 0$ this contradicts minimality of n. So $h = nk \Rightarrow h \in n\mathbb{Z}$. For negative h consider the inverse so we're done.

More generally given $g \in G$ there is a subgroup H generated by g which is the smallest subgroup which contains g

$$\langle g \rangle = \{e, g, g^{-1}, g^2, g^{-2}, g^3, \ldots\} \qquad g^0 = e,\ g^a \cdot g^b = g^{a+b},\ (g^a)^{-1} = g^{-a}$$

in S_3 every subgroup other than S_3 is generated by one element

in $\mathbb{Z}$ every subgroup $n\mathbb{Z} = \langle n \rangle$ is generated by one element