LECTURE 2

Sept. 17/2003.

$GL_n(\mathbb{R}) = \{$ all invertible $n \times n$ matrices A with entries $a_{ij} \in \mathbb{R}\}$

$GL_n(\mathbb{C}) = \{$ ______________

______________ $\in \mathbb{C}\}$

$GL_n(\mathbb{Q}) = \{$ ______________

______________ $\in \mathbb{Q}\}$

rational numbers

All of these are groups G:

- a set with a product structure
  $a, b \in G \quad , \quad a \cdot b \in G$
- associative $\quad a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- existence of identity e
  $a \cdot e = e \cdot a = a$
- existence of inverses $\quad a \rightsquigarrow a^{-1}$
  $a \cdot a^{-1} = a^{-1} \cdot a = e$

Ur - group: $Sym(T) = \left\{ \begin{array}{c} \text{all bijections} \\ a: T \to T \end{array} \right\}$

set

w/ group operation being composition:
$a \cdot b(t) = a(b(t))$

identity:
$e(t) = t$

inverses exist since assumed bijective.

Notation: <u>morphism</u> = map
<u>automorphism</u> = bijective map from an object to itself

Why "ur group": groups arise as subgroups of groups of form $Sym(T)$

e.g. $GL_n(\mathbb{R}) \subset Sym(\mathbb{R}^n)$

This is an example of a subgroup:

Precisely: $H \subset G$ is subgroup if is subset closed under $\cdot$, contains e, closed under $a \mapsto a^{-1}$

$S_n := \mathrm{Sym}\{1, 2, 3, \dots, n-1, n\}$

= "permutation group on n letters"

or "symmetry group on n letters"

finite group of order $= n!$

<u>written</u>: $|S_n| = n!$

$S_1 = \{e\}$

$S_2 = \{\ e : \begin{matrix} 1 \to 1 \\ 2 \to 2 \end{matrix}\ ,$

$\tau : \begin{matrix} 1 \to 2 \\ 2 \to 1 \end{matrix}\ \}$

$\cdot$	e	τ
e	e	τ
τ	τ	e

in particular, $\tau^{-1} = \tau$.

<u>Recall</u>: if $ab = ba$ for all $a, b \in G$ then we say G is <u>Abelian</u> (or <u>commutative</u>)

So: S_2 is Abelian.

$$S_3 = \{ e ,$$

$$\tau : \begin{array}{l} 1 \to 2 \\ 2 \to 1 \\ 3 \to 3 \end{array} \quad ,$$

$\leftarrow$ "transposition" (exchanges 2 elements of T)

$$\tau' : \begin{array}{l} 1 \to 1 \\ 2 \to 3 \\ 3 \to 2 \end{array} \quad ,$$

$$\tau'' : \begin{array}{l} 1 \to 3 \\ 2 \to 2 \\ 3 \to 1 \end{array} \quad ,$$

$$\sigma : \begin{array}{l} 1 \to 2 \\ 2 \to 3 \\ 3 \to 1 \end{array}$$

$$\sigma' : \begin{array}{l} 1 \to 3 \\ 2 \to 1 \\ 3 \to 2 \end{array} \quad \}$$

Is this group Abelian?

$\tau\sigma(1) = \tau(\sigma(1)) = \tau(2) = 1$

(so $\tau\sigma$ is either e or τ'; it must be τ' because τ & σ cannot be inverses.

$\sigma\tau(1) = \sigma(2) = 3$

$\left(\begin{array}{l} \sigma\tau(2) = \sigma(1) = 2 \\ \therefore\ \sigma\tau = \tau'' \end{array} \right)$

note
$\tau^{-1} = \tau$
$\sigma^{-1} = \sigma'$)

In particular, $\sigma\tau \neq \tau\sigma$

<u>Corollary</u> The group S_n is <u>non-abelian</u> for all $n \geq 3$.

<u>Proof</u> $S_3 \subset S_n$ fixing the letters $\{4, 5, 6, \ldots, n\}$. $\boxtimes$

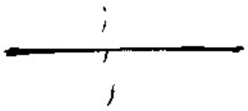
<u>Note</u>: transpositions are always their own inverse.

<u>Note</u>: For $k \leq n$, $S_k \subset S_n$

$\uparrow$ permutations in S_n fixing $\{k+1, \ldots, n\}$

Another example:

Q What is the subgroup of $GL_2(\mathbb{R})$ which stabilizes the line $y=0$?



(Note: immediately it is clear that this is a subgroup because composites stabilize, identity stabilizes, inverse stabilizes)

A $H = \left\{ A = \begin{pmatrix} a & c \\ 0 & d \end{pmatrix} : ad \neq 0 \right\}$

Some trivial examples of subgroups of a group G:

$\{e\}$ and all of G

Yet another example:

Proposition

The subgroups of $(\mathbb{Z}, +)$ are precisely given by $(b\mathbb{Z}, +)$ (b a fixed integer)

(Ex: $b = 0$ gives subgroup $\{0, +\}$
$b = 1$ gives subgroup $H = G$)

Proof * First those are all subgroups

- $bm + bn = b(m+n)$
- $-bm = b(-m)$
- $0 = b \cdot 0$ so $0 \in b\mathbb{Z}$

* To show these exhaust the subgroup, let $H \subset \mathbb{Z}$

① $H = \{0\}$ ✓

or ② $H \neq \{0\}$ so contains $m \neq 0$

Taking m or $-m \in H$, we see it contains $m > 0$.

Let $b > 0$ be smallest positive integer contained in H

Then clearly $H \supset b\mathbb{Z}$ by closure under addition & inversion

Suppose now $h \in H$

$h = mb + r$ with $0 \le r < b$

(can do this by Euclidean algorithm)

— Claim $r = 0$

Why? If not, then since

$r = h - mb \in H$,

we contradict the choice of r as smallest positive integer in H.

That's it! $\boxtimes$

G any group

$g \in G$

$H = \langle g \rangle$

= "cyclic subgroup generated by g"

This is the smallest subgroup containing g,

$\{e, g, g^{-1}, g^2, g^{-2}, \dots\}$

$= \{g^m : m \in \mathbb{Z}\}$.

(Note that $\cdot$ $g^m \cdot g^n = g^{m+n}$ for any $m, n \in \mathbb{Z}$

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

<u>Caveat</u>: Careful not to think that these elements need to be distinct.

For example, in S_2:

$\langle \tau \rangle = \{e, \tau\}$

since $\tau^2 = e$.

If $g^m = e$ and m is the smallest such power, we say m is the <u>order</u> of $g \in G$

If no power $g^m = e$ $(m > 0)$, we say g has infinite order.