Math 122 Monday, September 19

understanding a <u>group</u> G

matrices under multiplication (invertible)

$n \times n$ matrices over $\mathbb{R} = M_n(\mathbb{R})$ $\quad n=1$ $A=(a)$ $\quad n=2$ $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

more generally $A = (a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots \\ a_{21} & & & \\ a_{23} & & \ddots & \\ \cdots & & & a_{nn} \end{pmatrix}$ $\quad$ i row, j column

$a, b \in \mathbb{R}$ then
$a+b=b+a$, $ab=ba$, $a(b+c)=ab+ac$
$0+a=a$, $1 \cdot a = a$

addition and multiplication of $n \times n$ matrices

$A+B=B+A$ $\quad$ ij-th entry is $a_{ij}+b_{ij}$

$A \cdot B$ $\quad$ $\begin{array}{c} \\ i^{th} \end{array}\begin{pmatrix} \\ \text{———} \\ \\ \end{pmatrix}\begin{pmatrix} | \\ | \\ | \end{pmatrix}_{j^{th}}$ $\quad$ ij-th entry is $\sum_{k=1}^{n} a_{ik} b_{kj}$

$A \cdot B \neq B \cdot A$ in some cases, when $n > 1$ $\quad$ [for $n=1$ $(a)\cdot(b)=(ab)$ like in $\mathbb{R}$]

e.g. $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ $\quad$ $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

for $n \times n$ use $\begin{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} & & 0 \\ & 1 & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix}$ $\quad$ $\begin{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} & & 0 \\ & 1 & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix}$

special matrices: $0 =$ all $a_{ij}=0$; $I = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$

$0+A=A+0=A$ $\quad$ $I \cdot A = A \cdot I = A$ $\quad$ <u>check this</u>

also: $A(B+C) = AB + AC$ $\quad$ <u>check this</u>

<u>associative law</u> $A\cdot(B\cdot C) = (A \cdot B)\cdot C$ $\quad$ ij-th entry of both sides is $\sum_{x,y=1}^{n} a_{ix} b_{xy} c_{yj}$

so $A^2 = A \cdot A$ and $A^3 = A^2 \cdot A = AA^2$ etc make sense more generally $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$

$$p(A) = a_n A^n + a_{n-1}A^{n-1} + \cdots + a_1 A + a_0 I$$

$cA = (c \cdot a_{ij})$

Invertibility: A is <u>invertible</u> if $\exists$ B such that $AB = BA = I$

e.g. $A = (a)$ is invertible $\iff a \neq 0$ $\quad B = (1/a)$

$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is invertible $\iff ad - bc \neq 0$ $\quad B = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

$0 \cdot A = A \cdot 0 = 0$ so 0 is never invertible. I is invertible, $I \cdot I = I$.

<u>Prop</u> There is a function $\det : M_n(\mathbb{R}) \to \mathbb{R}$ with the properties.

1) $\det(I) = 1$
2) A is invertible $\iff \det A \neq 0$.
3) $\det(AB) = \det A \cdot \det B$

Really $\det A = \sum_{n! \text{ terms}} \pm (n \text{ terms})$ see Artin for a precise definition

There is always another $n \times n$ matrix A^* called the <u>adjoint</u> such that $A \cdot A^* = A^* A = (\det A) \cdot I$
When $\det A \neq 0$ then $A^{-1} = \frac{1}{\det A} \cdot A^*$.

Our first interesting group $G = GL_n(\mathbb{R}) \subset M_n(\mathbb{R})$ the set $\{A$ which are invertible$\}$

This has these properties

1) I is an element of G
2) closed under multiplication $A \cdot B$
3) multiplication is associative $(AB)C = A(B \cdot C)$
4) inverses exist $AA^{-1} = A^{-1}A = I$

[5) Note $AB \neq BA$ sometimes]

Note: If a matrix inverse exists, it is unique. $AB = AB' = I \Rightarrow B = B'$ (multiply by A^{-1} on the left)

<u>group</u> G in general

0) G is a set
1) there is a law of composition or multiplication $G \times G \to G$ (need <u>not</u> have $gh = hg$)
$(g, h) \mapsto g \cdot h$
2) associative $g(h \cdot j) = (g \cdot h) \cdot j$
3) Identity element e such that $ge = eg = g$
4) $\exists!$ Inverse g^{-1} such that $gg^{-1} = g^{-1}g = e$.

Note given $g \in G$ can define g^n for any $n \in \mathbb{Z}$

defn If for all $g, h \in G$ $gh = hg$ then we say G is abelian after Norwegian mathematician Abel.

ex: abelian group $G = M_n(\mathbb{R})$ under addition $e = 0$ $g = A \Rightarrow g^{-1} = -A$

Now for in some sense the most general group

S = set $G = \mathrm{Aut}(S) = \{$ all maps $S \xrightarrow{g} S$ that are one-to-one and onto $\}$
$g \cdot h$ = composition of g and h $g \circ h(s) = g(h(s))$

$$\begin{tikzcd} S \arrow[r, "h"] \arrow[rr, bend right, "gh"'] & S \arrow[r, "g"] & S \end{tikzcd}$$

Note: composition is always associative e = identity map $e(s) = s$
g^{-1} = inverse map.

If S = finite $= \{1, 2, \ldots, n\}$ then $\mathrm{Aut}(S)$ = symmetric group on n letters
this group $\mathrm{Aut}(S)$ is also finite with $n!$ elements

Note: $GL_n(\mathbb{R}) \subset \mathrm{Aut}(\mathbb{R}^n)$ What is the difference? GL_n is the set of linear, 1-to-1 onto maps