LECTURE 1 Sept. 15, 2003

Review of linear algebra

$n \times n$ matrices

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ & \ddots & & \\ & & a_{ij} & \\ a_{n1} & & \cdots & a_{nn} \end{pmatrix}$$

For now: $a_{ij} \in \mathbb{R}$

— Notation: $M_n(\mathbb{R})$ = set of such matrices.

Can add them:

$$\underset{(a_{ij})}{A} + \underset{(b_{ij})}{B} = (a_{ij} + b_{jj})$$

Can scalar multiply:
$\alpha \in \mathbb{R}$

$$\alpha \cdot A = (\alpha \cdot a_{ij})$$

So: $\mathbb{R}$-vectorspace of dim'n n^2

Multiplication of matrices

$$A \cdot B = (c_{ij})$$

$$c_{ij} = \sum_k a_{ik} b_{kj}. \leftarrow i^{th}\begin{pmatrix} \text{—} \end{pmatrix} \overset{j^{th}}{\begin{pmatrix} | \end{pmatrix}}$$

If A represents $T: \mathbb{R}^n \to \mathbb{R}^n$
and B represent $S: \mathbb{R}^n \to \mathbb{R}^n$

then $A \cdot B$ respresents the composition $T \circ S$

<u>Remember</u> $A+B = B+A$

but not necessarily true that $A \cdot B = BA$.

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

$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

denoted by O

$O + A = A + O = A.$ (it is the zero-element of $M_n(\mathbb{R})$ as a vectorspace)

$I = \begin{pmatrix} 1 & & O \\ & \ddots & \\ O & & 1 \end{pmatrix}$ has property $A \cdot I = I \cdot A = A$

Distributive law: $A(B+C) = AB + AC$

Associativity: $A(BC) = (AB)C$ (so can forget brackets!)

Note: to prove associativity, reinterpret matrices as linear transformations. The result then follows from associativity of composition.

We say A is invertible

$$\Updownarrow$$

$\exists$ a matrix B s.t. $AB = BA = I$.

Notes: • not all matrices are invertible
e.g. 0 cannot be invertible
since $0 \cdot A = 0 = A \cdot 0$.

• I is invertible (take $B = I$).

• 1×1 matrices: (a) is invertible $\Leftrightarrow$ $a \neq 0$
$(B = (1/a))$

• 2×2 matrices: $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is

invertible $\Leftrightarrow$ $ad - bc \neq 0$.

$\left(\text{then } A^{-1} = B = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \right)$

$\uparrow$ notation

can verify this explicitly.

- In general:

$$\text{determinant} = \det : M_n(\mathbb{R}) \longrightarrow \mathbb{R}.$$

$$\left(\text{e.g. } \det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc\right)$$

$$\det A = \sum_{n! \text{ terms}} (\pm 1)\,(\text{product of } n \text{ matrix entries})$$

<u>Fact:</u> A is invertible $\Leftrightarrow \det(A) \neq 0$.

In fact: $\exists$ canonical B s.t. $AB = BA = \det(A) \cdot I$

"matrix of cofactors"

We are more interested in subset

$$GL_n(\mathbb{R}) \subset M_n(\mathbb{R})$$

$$= \{A : \det A \neq 0\}$$

$$= \{A \text{ s.t. there is an inverse matrix } A^{-1}\}$$

Note: if inverse exists it is <u>unique</u>

Suppose $A \cdot B = A \cdot C = I$

Then
$$\begin{array}{ccc} B(A\cdot B) & = & B(AC) \\ \| & & \| \\ (BA)B & = & (BA)C \\ \| & & \| \\ I\cdot B & & I\cdot C \\ \| & & \| \\ B & & C \end{array}$$

By restricting to $GL_n(\mathbb{R})$ we gain some things but lose others:

- there is no addition law on $GL_n(\mathbb{R})$ (i.e. is not closed under addition from $M_n(\mathbb{R})$)
- also not closed under multiplication by 0
- <u>but</u> it is closed under multiplication.

<u>two proofs of ↑</u>:

① Suppose A & B invertible then $A \cdot B$ is invertible since

$$(B^{-1}A^{-1})(A\cdot B) = B^{-1}(A^{-1}A)B$$
$$= B^{-1} I B = I.$$

② Determinant identity:

$$\det(AB) = \det A \cdot \det B.$$

then use

$$GL_n(\mathbb{R}) = \{A : \det A \neq 0\}$$

More properties of $GL_n(\mathbb{R})$:

- has multiplication identity I
- has inverses A^{-1}
- product is associative
  $(AB)C = A(BC)$

These are the properties that define the notion of <u>group</u>.

<u>More precisely:</u>

A <u>group</u> G is a set with a product operation $g \cdot h \in G$ which is

1) associative
2) has an identity element e
3) has inverses g^{-1}:
$$g \cdot g^{-1} = g^{-1} g = e$$

Note: if $gh = hg$ for all pairs,
we say G is <u>commutative</u>
or <u>Abelian</u>

- An example of an Abelian group:

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \cdots\}$$

"product" is addition:

$$a + b = b + a$$

$$e = 0 \qquad a + 0 = a$$

$$\text{"}a^{-1}\text{"} = -a.$$

- Another example of a (Abelian) group is any vectorspace.
(Just forget scalar mult.)

Most "general" example of a group

T a set

$G = \{\text{all bijections } g : T \to T\}$
1-to-1, onto maps

$= \mathrm{Sym}(T)$

is a group under composition of transformations.

Identity: $e =$ identity map
$x \mapsto x$

Inverses: exist by bijectivity

Associativity: follows by def'n

In some sense this is most general because groups arise as bijections of a set which preserve the structure of a set ("symmetries")

T a set $\quad T = \{1, \ldots, n\}$

$$S_n := \mathrm{Sym}(T)$$

finite group of order $n!$

("order" = # of elements)

notation

<u>Ex:</u> S_3 is not Abelian