(1)

Math 5285 Fall 2018 Vic Reiner

9/5/18 Honors Fundamental Structures of Algebra

- Go through some syllabus items, course structure, etc.
- Set tentative office hours

Course content: (Fall 2018) Groups + Linear algebra , (Spring 2019) rings & fields

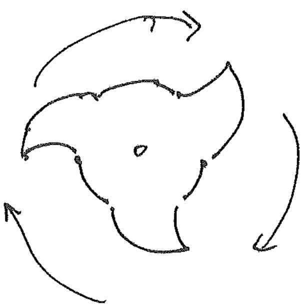
e.g. $\mathbb{Z}$ integers, e.g. $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ (rationals, reals, complexes)

$\mathbb{Z}/m\mathbb{Z}$ = "integers modulo m", $\mathbb{Z}/p\mathbb{Z}$ for p prime

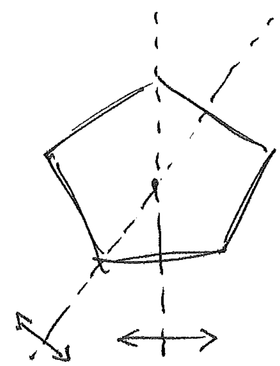
$\underbrace{\qquad\qquad\qquad}_{\text{more familiar at first}}$

Groups are about symmetry, e.g. linear symmetry like

rotational



or reflective



They can be represented as linear maps by matrices,

and matrix groups (= subsets of invertible matrices that form a group)

will be our best examples.

Also the invertible elements of $\mathbb{Z}/m\mathbb{Z}$ will form a group,

important for (public-key) cryptography and error-correcting codes.

Chapter 1 Matrices

§ 1.1, 1.2 Matrices & row-reduction

Recall some notations / definitions...

$$\mathbb{R}^{m\times n} \overset{\text{DEF'N}}{:=} \Big\{ \text{all } \underset{\text{rows}}{m} \times \underset{\text{columns}}{n} \text{ matrices } A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \text{ with } a_{ij} \in \mathbb{R} \Big\}$$

sometimes I'll write $A = (a_{ij})$ or $a_{ij} = A_{ij}$

e.g. $$A = \underbrace{\begin{bmatrix} -2 & -6 & -5 & -11 \\ 1 & 3 & 4 & 4 \\ 1 & 3 & 6 & 2 \end{bmatrix}}_{n=4} \Big\} m=3 \quad \in \mathbb{R}^{3\times 4}$$

$$\left(\text{Actually, } A \in \mathbb{Z}^{3\times 4} \subset \mathbb{Q}^{3\times 4} \subset \mathbb{R}^{3\times 4} \subset \mathbb{C}^{3\times 4} \right)$$

One can add matrices of same dimensions: $A+B$ for $A, B \in \mathbb{R}^{m\times n}$ has (i,j)-entry $(A+B)_{ij} = A_{ij} + B_{ij}$

e.g. $$\begin{bmatrix} 1 & 0 & -1 \\ 2 & 3 & 0 \end{bmatrix} + \begin{bmatrix} 5 & 6 & 7 \\ 8 & 9 & 10 \end{bmatrix} = \begin{bmatrix} 6 & 6 & 6 \\ 10 & 12 & 10 \end{bmatrix}$$

One can scale $A \in \mathbb{R}^{m\times n}$ by a scalar $c \in \mathbb{R}$ giving cA with $(cA)_{ij} = c \cdot A_{ij}$

e.g. $$(-10) \cdot \begin{bmatrix} 5 & 6 & 7 \\ 8 & 9 & 10 \end{bmatrix} = \begin{bmatrix} -50 & -60 & -70 \\ -80 & -90 & -100 \end{bmatrix}$$

One can multiply $\underset{(a_{ij})}{A} \in \mathbb{R}^{m\times n}$, $\underset{(b_{ij})}{B} \times \mathbb{R}^{n\times p}$ giving $AB \in \mathbb{R}^{m\times p}$ with

$$(AB)_{ij} \overset{\text{DEF'N}}{:=} \sum_{k=1}^{n} a_{ik} b_{kj}$$

$$= a_{i1}b_{1j} + a_{i2}b_{2j} + \dots + a_{in}b_{nj}$$

= dot product

$$\underbrace{[a_{i1} \cdots a_{in}]}_{i^{\text{th}} \text{ row of } A} \bullet \underbrace{[b_{1j} \cdots b_{nj}]}_{j^{\text{th}} \text{ column of } B}$$

$$= [a_{i1} \cdots a_{in}] \begin{bmatrix} b_{1j} \\ \vdots \\ b_{nj} \end{bmatrix}$$

$$m\Big\{ \overbrace{\begin{bmatrix} - A_1 - \\ \vdots \\ - A_m - \end{bmatrix}}^{A} \overbrace{\underbrace{\begin{bmatrix} | & & | \\ B_1 & \cdots & B_p \\ | & & | \end{bmatrix}}_{p}}^{B} = m\Big\{ \underbrace{\begin{bmatrix} A_1 \bullet B_1 & \cdots & A_1 \bullet B_p \\ \vdots & & \\ A_m \bullet B_1 & \cdots & A_m \bullet B_p \end{bmatrix}}_{p}$$

e.g. $$\underset{2\times 3}{\overset{A}{\begin{bmatrix} 1 & 0 & -1 \\ 2 & 3 & 0 \end{bmatrix}}} \underset{3\times 1}{\overset{B}{\begin{bmatrix} 5 \\ 6 \\ 7 \end{bmatrix}}} = \underset{2\times 1}{\overset{AB}{\begin{bmatrix} -2 \\ 10 \end{bmatrix}}}$$

(3)

Matrix addition, scaling, multiplication satisfy lots of properties that are easy to check, usually following from properties of $+, \times$ in $\mathbb{R}$, e.g.

$$A+B = B+A \qquad c(A+B) = cA + cB \qquad (cA)B = c(AB) = A(cB)$$

$$(A+B)+C = A+(B+C) \qquad A(B+C) = AB + AC$$

$$\boxed{A(BC) = (AB)C} \qquad (A+B)C = AC + BC$$

associativity is not to be taken for granted – it has implications!

Note commutativity fails in general: $AB \neq BA$

sometimes for obvious dimension reasons, e.g.

$$\underset{1\times 2}{\overset{A}{\begin{bmatrix} 1 & 1 \end{bmatrix}}} \underset{2\times 1}{\overset{B}{\begin{bmatrix} 1 \\ 1 \end{bmatrix}}} \neq \underset{2\times 1}{\overset{B}{\begin{bmatrix} 1 \\ 1 \end{bmatrix}}} \underset{1\times 2}{\overset{A}{\begin{bmatrix} 1 & 1 \end{bmatrix}}}$$

$$\underset{1\times 1}{[2]} \qquad\qquad \underset{2\times 2}{\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}}$$

but also even when A, B are square $\mathbb{R}^{n\times n}$

e.g.

$$\overset{A}{\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}} \overset{B}{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}} \neq \overset{B}{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}} \overset{A}{\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}}$$

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \qquad\qquad \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$$

9/7/18

The addition of matrices has $0_{m\times n} := \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & & \\ \vdots & & \ddots & \\ 0 & & & 0 \end{bmatrix}$ as (additive) identity $0 + A = A = A + 0 \quad \forall A \in \mathbb{R}^{m\times n}$

and $-A = (-1)A$ is the (additive) inverse of A

For multiplication, the $(n\times n)$ identity matrix $I_n = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & 0 \cdots & 0 \\ \vdots & 0 & \ddots & \\ 0 & 0 & & 1 \end{bmatrix}$ has $I_n A = A \quad \forall A \in \mathbb{R}^{n\times m}$

$$A I_m = A$$

and ~~[illegible]~~ inverses are more subtle:

Call $L \in \mathbb{R}^{m\times n}$ with $LA = I_m$ a left-inverse for A

$R \in \mathbb{R}^{m\times n}$ with $AR = I_n$ a right-inverse for A

- A might have neither, e.g. $A = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ or $A = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ or $A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$
- A might have one but not the other, e.g. $A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$ has any $R = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ r_1 & r_2 \end{bmatrix}$ as a right-inverse $AR = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2$

but check it has no left-inverse.