 11/16/2018>

# Chapter 3 Vector spaces over fields

§3.2 Fields: are the things like $\mathbb{R}, \mathbb{C}, \mathbb{Q}, \ldots$
where one can do linear algebra & matrices just as before!

DEF'N: A field $(F, +, \times)$ is a set $F$ with two laws of composition

$$F \times F \to F \qquad\Big|\qquad F \times F \to F$$
$$(a, b) \mapsto a+b \qquad\Big|\qquad (a,b) \mapsto a \cdot b$$

such that (i) $F^+ := (F, +)$ is an abelian group, whose (additive) identity is called 0

(ii) $F^\times := (F \setminus \{0\}, \times)$ is an abelian group, whose (multiplicative) identity is called 1

(iii) $\times$ distributes over $+$ : $a(b+c) = ab + ac$

EXAMPLES:

① $\underbrace{\mathbb{C} \supset \mathbb{R} \supset \mathbb{Q}}_{\text{fields}} \left( \supset \underset{\text{not a field; Why?}}{\mathbb{Z}} \right)$

$\left( \begin{array}{l} \cap \\ \mathbb{H} := \{a + bi + cj + dk : a,b,c,d \in \mathbb{R}\} \\ \text{quaternions} \quad i^2 = j^2 = k^2 = -1 \\ \qquad ij = k = -ji \mid jk = i = -kj \mid ki = j = -ik \end{array} \right)$

are called a skew field or noncommutative field

② $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{p-1}\}$ for $p$ a prime is a field,

since $(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} : \gcd(a,n) = 1\}$
$= \mathbb{Z}/n\mathbb{Z} - \{\bar{0}\}$ if and only if $n$ is prime

e.g. $\mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ is not a field, since
$(\mathbb{Z}/6\mathbb{Z})^\times = \{\bar{1}, \bar{5}\} \not\ni \bar{2}, \bar{3}, \bar{4}$
$\neq \mathbb{Z}/6\mathbb{Z} - \{\bar{0}\}$

but $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$ is a field

(117) Note that $1 \neq 0$ in any field $F$ (since $F^\times = F - \{0\}$ needs to have 1 in it),

so $\mathbb{F}_2 = \{\bar{0}, \bar{1}\}$ is as small as a field can get!

A couple of other loose ends:

**PROPOSITION** (LEMMA 3.2.3) In any field $F$,

(i) $0 \cdot a = a \cdot 0 \quad \forall a \in F$

(ii) $\times$ is associative and 1 is a two-sided identity for $\times$ on all of $F$, not just on $F^\times = F - \{0\}$.

proof: For (i), note $0 + 0 = 0$ since $F^+$ is a group

$$\Big\downarrow \text{ mult. by } a \text{ on left}$$

$$\underbrace{a(0+0)}_{a0 + a0 \text{ (distributivity)}} = a \cdot 0$$

$$\Big\downarrow \text{ add } -a \cdot 0 \text{ to both sides}$$

$$a \cdot 0 = 0$$

Similarly for $0 \cdot a = 0$.

For (ii), note (i) shows $1 \cdot 0 = 0 \cdot 1 = 0$

and if any of $a, b, c$ are 0 then checking

$$\underbrace{(ab)c = a(bc)}_{0}$$

is easy via (i) ∎

---

Crucial point: Everything that we did about systems of equations $AX = B$

row-reduction $A \rightsquigarrow A'$ row-echelon form

determinants and invertibility

in Chapter 1 only relied on working with matrices $A \in F^{m \times n}$

where $F$ was a field (e.g. $F = \mathbb{R}$ or $\mathbb{C}$ there, but now $F = \mathbb{F}_p$ is ok)

because we needed the elementary matrices $E = \begin{bmatrix} 1 & & & & 0 \\ & \ddots & & & \\ & & \boxed{c} & & \\ & & & \ddots & \\ 0 & & & & 1 \end{bmatrix}$

with $c \in F - \{0\} = F^\times$ to have an inverse $E^{-1} = \begin{bmatrix} 1 & & & & 0 \\ & \ddots & & & \\ & & \boxed{c^{-1}} & & \\ & & & \ddots & \\ 0 & & & & 1 \end{bmatrix}$!

(118) **EXAMPLE**: Let's count the solutions to the systems

$$\begin{aligned} x+y&=1\\ x+z&=1\\ y+z&=1 \end{aligned} \quad \text{and} \quad \begin{aligned} x+y&=1\\ x+z&=1\\ y+z&=0 \end{aligned},$$

interpreted over $F = \mathbb{F}_2, \mathbb{F}_5, \mathbb{R}$

Equivalently,

$$\underbrace{\begin{bmatrix} 1&1&0\\1&0&1\\0&1&1 \end{bmatrix}}_{A} \underbrace{\begin{bmatrix} x\\y\\z \end{bmatrix}}_{X} = \underbrace{\begin{bmatrix} 1\\1\\1 \end{bmatrix}}_{Y_1} \qquad \underbrace{\begin{bmatrix} 1&1&0\\1&0&1\\0&1&1 \end{bmatrix}}_{A} \underbrace{\begin{bmatrix} x\\y\\z \end{bmatrix}}_{X} = \underbrace{\begin{bmatrix} 1\\1\\0 \end{bmatrix}}_{Y_2}$$

Augmented matrix:

$$[A|Y_1] = \left[\begin{array}{ccc|c} 1&1&0&1\\1&0&1&1\\0&1&1&1 \end{array}\right] \xrightarrow{\text{row ops}} \left[\begin{array}{ccc|c} 1&1&0&1\\0&-1&1&0\\0&1&1&1 \end{array}\right] \rightsquigarrow \left[\begin{array}{ccc|c} 1&1&0&1\\0&-1&1&0\\0&0&2&1 \end{array}\right]$$

If $F=\mathbb{F}_5$ or $\mathbb{R}$:

$$\left[\begin{array}{ccc|c} 1&1&0&1\\0&-1&1&0\\0&0&1&2^{-1} \end{array}\right]$$

where $2^{-1} = \frac{1}{2}$ in $\mathbb{R}$
$= 3$ in $\mathbb{F}_5$

Unique solution:

$z = 2^{-1}$
$y = z = 2^{-1}$
$x = 1-y = 1-2^{-1}$

$$\begin{bmatrix} x\\y\\z \end{bmatrix} = \begin{bmatrix} 2^{-1}\\2^{-1}\\1-2^{-1} \end{bmatrix}$$

If $F=\mathbb{F}_2$:

$$\left[\begin{array}{ccc|c} 1&1&0&1\\0&1&1&0\\0&0&0&1 \end{array}\right]$$

No solutions!

$$[A|Y_2] = \left[\begin{array}{ccc|c} 1&1&0&1\\1&0&1&1\\0&1&1&0 \end{array}\right] \xrightarrow{\text{row ops}} \left[\begin{array}{ccc|c} 1&1&0&1\\0&-1&1&0\\0&1&1&0 \end{array}\right] \rightsquigarrow \left[\begin{array}{ccc|c} 1&1&0&1\\0&-1&1&0\\0&0&2&0 \end{array}\right]$$

If $F=\mathbb{F}_5$ or $\mathbb{R}$:

$$\left[\begin{array}{ccc|c} 1&1&0&1\\0&-1&1&0\\0&0&1&0 \end{array}\right]$$

Unique solution:

$z=0$
$y=z=0$
$x=1-y=1$

$$\begin{bmatrix} x\\y\\z \end{bmatrix} = \begin{bmatrix} 0\\0\\1 \end{bmatrix}$$

If $F=\mathbb{F}_2$:

$$\left[\begin{array}{ccc|c} 1&1&0&1\\0&1&1&0\\0&0&0&0 \end{array}\right]$$

non-pivot variable $z$ can be chosen arbitrarily in $F=\mathbb{F}_2$, so two solutions,

and $y = -z = z$
$x = 1-y = 1+y = 1+z$

$$\begin{bmatrix} x\\y\\z \end{bmatrix} = \begin{bmatrix} 1+z\\z\\z \end{bmatrix}$$

Note that $\det A = \det\begin{bmatrix} 1&1&0\\1&0&1\\0&1&1 \end{bmatrix} = 1\cdot\det\begin{bmatrix} 0&1\\1&1 \end{bmatrix} - 1\cdot\det\begin{bmatrix} 1&1\\0&1 \end{bmatrix} = 1(-1)-1\cdot 1$
$= -2$ $\begin{cases} \neq 0 \text{ if } F=\mathbb{F}_5,\mathbb{R} \\ = 0 \text{ if } F=\mathbb{F}_2 \end{cases}$

Hence $A$ is invertible over $F=\mathbb{F}_5,\mathbb{R}$, but not over $F=\mathbb{F}_2$