Introduction:

- groups
- fields

$\Big\} \Rightarrow$ $\boxed{\text{vector space}}$

$\boxed{(G, *) \text{ is a group}}$: G = set and "$*$" is an operation on G

$$*: G \times G \to G$$
$$(g_1, g_2) \to g_1 * g_2$$

with the following properties:

(G1) $g_1 * g_2 = g_2 * g_1$ (commute)

(G2) $g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$ (associative)

(G3) There exists an unity element (e) in G such that
$$g * e = g \text{ , for all } g \in G$$

(G4) For every $g \in G$, there exists an "inverse" $h \in G$
such that
$$g * h = h * g = e$$

Field (see Appendix C)

$(F, +, \cdot)$ is called a field if F is a set endowed with two operations ("+" = addition, "·" multiplication)

"$+$" : $F \times F \to F$ and "$\cdot$" : $F \times F \to F$

$(a, b) \mapsto a + b$ $\qquad$ $(a, b) \to a \cdot b$

with the following properties

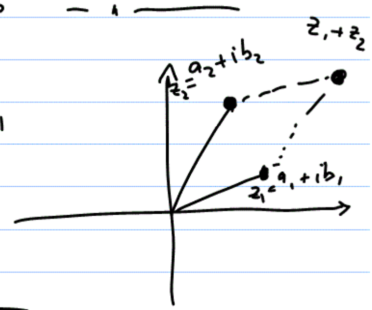
(F1) : $a+b=b+a$	$-\ a\cdot b = b\cdot a$
(F2) : $a+(b+c)=(a+b)+c$	$-\ a\cdot(b\cdot c)=(a\cdot b)\cdot c$
(F3) : There exists $0\in F$ $a+0=0+a=a$ for all $a\in F$	- There exists $1\in F$ $a\cdot 1=1\cdot a=a$ for all $a\in F$
(F4) : For each $a\in F$, there is $c\in F$ such that $a+c=0$	- For each $b\in F$, $b\neq 0$ there exists $d\in F$ such that $b.d=1$
$(F,+)$ is a group	$(F\setminus\{0\},\cdot)$ is a group

(F5) $a\cdot(b+c)=a\cdot b+a\cdot c$ (distributive property)

Ex.: $\mathbb{R}$ = ~~set~~ field of real numbers with usual addition and multiplication

Ex: $\mathbb{C}$ = ~~set~~ field of complex numbers

$\mathbb{C}=\{z=a+ib \mid a,b\in\mathbb{R}\}$ $\quad i=\sqrt{-1}$



"+" is as follows $\quad z_1=a_1+ib_1$

$$z_2=a_2+ib_2$$

$$z_1+z_2=a_1+a_2+i(b_1+b_2)$$

"$\cdot$" is as follows $\quad z_1\cdot z_2=(a_1+ib_1)(a_2+ib_2)$

$$= a_1a_2 - b_1b_2 + i(a_1b_2 + a_2b_1)$$

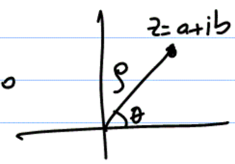
$1 \in \mathbb{C}$

Is it true that for any $z \in \mathbb{C}$, $z \neq 0$, there is $w \in \mathbb{C}$ such that $z \cdot w = 1$?

YES! Use polar form: $z = a + ib = \rho e^{i\theta}$, $\rho > 0$, $\theta \in [0, 2\pi)$

ρ = modulus of z = $|z|$ $\qquad \rho = \sqrt{a^2+b^2}$

θ = argument of z $\qquad \tan\theta = \frac{b}{a}$, $a \neq 0$

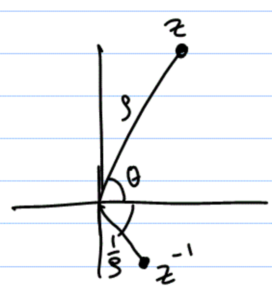


$$\left(e^{i\theta} = \cos\theta + i\sin\theta \right)$$

$$\left.\begin{aligned} z_1 &= \rho_1 e^{i\theta_1} \\ z_2 &= \rho_2 e^{i\theta_2} \end{aligned}\right\} \Rightarrow z_1 \cdot z_2 = \rho_1\rho_2\, e^{i(\theta_1+\theta_2)}$$

$\Rightarrow z = \rho e^{i\theta} \neq 0 \Rightarrow w = \rho^{-1} e^{-i\theta}$ satisfies

$$z \cdot w = \rho e^{i\theta} \rho^{-1} e^{-i\theta} = \rho\rho^{-1} e^{i(\theta-\theta)} = 1$$



$$z = 1 + 2i = \sqrt{5}\, e^{i\theta}$$

$$\Downarrow$$

$$w = z^{-1} = \frac{1}{\sqrt{5}} e^{-i\theta}$$

Other examples of fields: $\mathbb{Z}_2 = \{0, 1\}$

$\mathbb{H}$ = field of quaternions

Vector Spaces

Definition: Given a field $\mathbb{F}$ (called field of scalars) and a set V endowed with two operations "+" (vector addition) and "$\cdot$" (scalar multiplication)

$$"+": V \times V \to V \qquad "\cdot": \mathbb{F} \times V \to V$$

then $(V, +, \cdot)$ is called vector space (over $\mathbb{F}$) provided

the following properties hold:

$(V, +)$ is group

(V1) $x + y = y + x$, $x, y \in V$

(V2) $x + (y + z) = (x + y) + z$, $x, y, z \in V$

(V3) There is $0 \in V$, such that $0 + x = x + 0 = x$, $x \in V$

(V4) For every $x \in V$, there is $y \in V$: $x + y = y + x = 0$

(V5) $1 \cdot x = x$, for $x \in V$ $(1 \in \mathbb{F})$

(V6) $(ab) \cdot x = a \cdot (b \cdot x)$, for $x \in V$, $a, b \in \mathbb{F}$

(V7) $a \cdot (x + y) = a \cdot x + a \cdot y$, for $a \in \mathbb{F}$, $x, y \in V$

(V8) $(a + b) \cdot x = a \cdot x + b \cdot x$, $a, b \in \mathbb{F}$, $x \in V$

Ex. ① $\mathbb{F}^n$ = set of n-tuples with entries in $\mathbb{F}$

$$= \{ a = (a_1, \dots, a_n) \mid a_i \in \mathbb{F},\ i = \overline{1,n} \}$$

$$(\underbrace{\mathbb{R}^2, \mathbb{R}^3}_{\text{over } \mathbb{R}},\ \underbrace{\mathbb{C}^2, \mathbb{C}^3, \dots}_{\text{over } \mathbb{C}})$$

Ex: ② $\mathcal{M}_{m\times n}(\mathbb{F})$ = set of all $m\times n$ matrices with entries in $\mathbb{F}$

$$A \in \mathcal{M}_{m\times n}(\mathbb{F}) \qquad A = (a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ - & - & \cdot & \cdot \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}_{m\times n}$$

$a_{ij} \in \mathbb{F}$ for $i = \overline{1,m}$, $j = \overline{1,n}$

with usual matrix addition and scalar multiplication.

Ex: ③ $\mathbb{P}(\mathbb{F})$ = set of all polynomials with coefficients $\in \mathbb{F}$

$$= \{ a_0 + a_1 X + a_2 X^2 + \dots + a_n X^n \mid a_i \in \mathbb{F},\ i = 1,n,\ n \in \mathbb{N} \}$$

Ex: ④ $\mathbb{P}_n(\mathbb{F})$ = set of all polynomials with coeff in $\mathbb{F}$ of degree $\le n$

$$= \{ a_0 + a_1 X + a_2 X^2 + \dots + a_n X^n \mid a_i \in \mathbb{F},\ i = \overline{1,n} \}$$

(all are examples of vector spaces over $\mathbb{F}$)