Review about fields:

- group $(G, \circ)$, $\circ : G \times G \to G$. + properties

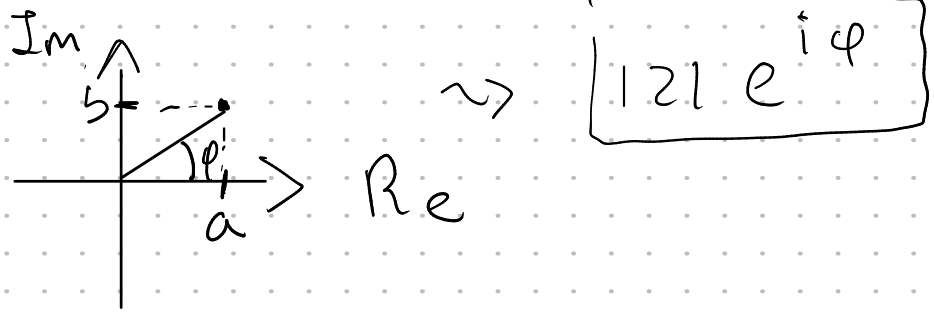
- $\mathbb{K}$ is a field: $\mathbb{K}$ is a set and it has two operations

  i) + $(\mathbb{K}, +)$ is an abelian group $\rightsquigarrow \exists\, 0$ neutral element for sum.

  ii) $\cdot$ $(\mathbb{K} \setminus \{0\}, \cdot)$ is an abelian group

  iii) $a \cdot (b + c) = a \cdot b + a \cdot c$.

- $\mathbb{R}$, $\mathbb{Q} = \left\{ \frac{n}{m} : n, m \in \mathbb{Z},\ m \neq 0 \right\}$, $\mathbb{C}$ = field of complex numbers.

- $\mathbb{C} = \{ a + ib : a, b \in \mathbb{R} \text{ and } i \text{ satisfy } \boxed{i^2 = -1} \}$.
  - $(a + ib) + (c + id) = (a + c) + i(b + d)$
  - $(a + ib) \cdot (c + id) = ac + i(ad + bc) + i^2 bd$
    $= (ac - bd) + i(ad + bc)$
  - in $\mathbb{R}$ there is no solution to $x^2 + 1 = 0$
  - 

    $\rightsquigarrow \boxed{|z| e^{i\varphi}}$

field:

- $\mathbb{Z}_p$ integers modulo p prime number.

$\{\overline{0}, \overline{1}, \dots, \overline{p-1}\}$

- $Ax = b$: until the solutions in $\mathbb{R} \rightsquigarrow \mathbb{Z}_p$

$\mathbb{Z}_7 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$

- $11 \equiv 4 \mod 7$
- $11 = k \cdot 7 + \text{remainder}$, $\text{remainder} = 4$

$11 \equiv 4 \mod 7$

iff $\overline{11} = \overline{4}$ in $\mathbb{Z}_7$

$\overline{n} = \{n + k \cdot 7 : k \in \mathbb{Z}\}$.

$$A = \begin{pmatrix} 1 & 2 & 4 & 0 \\ 0 & 1 & 2 & 4 \\ 3 & 1 & 2 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix}$$

solve $Ax = b$ over $\mathbb{Z}_7$, $x = (x_1, x_2, x_3, x_4)$ $x_i \in \mathbb{Z}_7$

$$\left(\begin{array}{cccc|c} 1 & 2 & 4 & 0 & 1 \\ 0 & 1 & 2 & 4 & 2 \\ 3 & 1 & 2 & 1 & 0 \end{array}\right) \xrightarrow{r_3 = r_3 - 3 \cdot r_1} \left(\begin{array}{cccc|c} 1 & 2 & 4 & 0 & 1 \\ 0 & 1 & 2 & 4 & 2 \\ 0 & 2 & 4 & 1 & 4 \end{array}\right) \xrightarrow{r_3 = r_3 - 2r_2} \rightarrow$$

$\overline{-5} = \{-5 + k \cdot 7 : k \in \mathbb{Z}\}$

$= \{(-5+7) + k7 : k \in \mathbb{Z}\}$

$= \{2 + k7\}$

$$\left(\begin{array}{cccc|c} 1 & 2 & 4 & 0 & 1 \\ 0 & 1 & 2 & 4 & 2 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

$2 - 2 \cdot 1 = 0$ $\quad$ $4 - 2 \cdot 2 = 0$ $\quad$ $1 - 2 \cdot 4 = -7 \equiv 0 \ (7)$

$\overline{2}$

$1 - 6 = -5 \equiv 2 \mod 7$

$2 - 12 = -10 \equiv 4 \mod 7$

$-3 \equiv 4 \mod 7$

- if we want to compute the inverse of a matrix over $\mathbb{Z}_5$, $A = \begin{pmatrix} 1 & 3 & 2 \\ 3 & 4 & 0 \\ 0 & 1 & 1 \end{pmatrix}$

$$\left(\begin{array}{ccc|ccc} 1 & 3 & 2 & 1 & 0 & 0 \\ 3 & 4 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|c} 1 & 0 & 0 & \\ 0 & 1 & 0 & A^{-1} \\ 0 & 0 & 1 & \end{array}\right)$$

- $\overline{0}$, can't multiply by 5.

- Fermat's little th: $\forall$ every p prime

$a \in \{1, \dots, p-1\}$ $a^{p-1} \equiv 1 \mod p$.

- $a^{1000} \mod p$ $\quad 1000 = K \cdot (p-1) + r$

$a^{1000} \equiv a^r \mod (r)$

- GCD(n, m)

- $\exists a, b \in \mathbb{Z}$ s.t. $an + bm = GCD(n, m)$

- n, m primes, $GCD(7, 17) = 1$

$\Rightarrow \exists a, b \in \mathbb{Z}$ $a \cdot 7 + b \cdot 17 = 1$

$\downarrow \mod 17, \mathbb{Z}_{17}$

$a \cdot 7 \equiv 1 \mod 17.$

- $17 - 2 \cdot 7 = 3$

- $7 - 2 \cdot 3 = 1 \rightsquigarrow 7 - 2 \cdot (17 - 2 \cdot 7) = 1$

$5 \cdot 7 - 2 \cdot 17 = 1.$