代数结构：研究一些集合及其上的运算

群论 Group Theory

def：集合 G：定义运算 $*$

① 封闭 $\forall a, b \in G,\ a*b \in G$

② 结合律：$\forall a, b, c \in G,\ (a*b)*c = a*(b*c)$

③ 有单位元(幺元) e：$\forall a,\ a*e = e*a = a$

④ 可逆 $\forall a \in G,\ \exists b \in G,\ a*b = e = b*a$，$b$ 称为 a 的逆

满足①②：半群；满足①②③：含幺半群；满足①②③④：群

注：i) 以上没有定义换律、交换律是非常特殊的

ii) 单位元可拆为3条性质：
1) $\exists e_1,\ \forall a \in G,\ a*e_1 = a$ 右单位元
2) $\exists e_2\ \forall a \in G\ \ e_2*a = a$ 左单位元
3) $e_1 = e_2$

iii) 可逆可拆为2条：右逆、左逆、左逆=右逆

eg：
- $\langle Q, + \rangle$ 群
- $\langle Q, \times \rangle$ 含幺半群 → $\langle Q/\{0\}, \times \rangle$ 群
- $\langle R^{2\times 2}, + \rangle$ 交群
- $\langle R^{2\times 2}, \times \rangle$ 含幺半群
- $\langle R^{2\times 2}, det = 1, \times \rangle$ 交群
- $\langle R^{2\times 2}, det = \pm 1, \times \rangle$ 交群
- $\langle Z_m, + \rangle$ 交群。Z_m 表模 m 的余数
- $\langle Z_m/\{0\}, \times \rangle$ 含幺半群 $(ak \equiv 1 \bmod m \Leftrightarrow (a,m)=1)$
  - $\langle Z_p/\{0\}, \times \rangle$ p 为素数，交群。
- $\langle Z_m^*, \times \bmod m \rangle$ $Z_m^* = \{a \in Z_m \mid (a,m)=1\}$ 交群
  - $\forall a, b \in Z_m^*, (a,m)=1, (b,m)=1 \Rightarrow (ab, m)=1$ 封闭
- $\langle \{0\}, \times \rangle$ 交群　$\langle \{\pm 1, \pm i\}, \times \rangle$ 交群
- $\langle \{x \in \mathbb{C} \mid x^n = 1\}, \times \rangle$ 交群
  - 可构造一个群和 $\langle Z_n, + \rangle$ 之间建立同构关系

群的性质

1. 消去律

左消去：$a\times b=a\times c \Rightarrow b=c$

右消去：$b\times a=c\times a \Rightarrow b=c$

证：右/左乘同乘 a^{-1}（靠借助结合律）

回顾：$\begin{cases} a\cdot b=a\cdot c \mod m \\ (a,m)=1 \end{cases} \Rightarrow b\equiv c \mod m$（用整数说明）

群论角度：$a,b,c\in \mathbb{Z}_m^*$　$a\times b=a\times c$ 用消去律 $b=c$

（不太严谨，但确实是这个意思）

2. "线性方程组"有唯一解

$\forall a,b\in G$

$\exists!$（唯一的）$x\in G$ s.t. $a\times x=b$

$\exists!\ y\in G$ s.t. $y\times a=b$

证：希望先证左逆元、右逆元唯一。

$ax_1\times a=ax_2\times a$，由消去律，$ax_1=ax_2$ 故左、右逆元分别唯一

见"3"

eg：$\langle \mathbb{Z}_m^*,\times\rangle$ $\forall a,b\in \mathbb{Z}_m^*$，$ax\equiv b \mod m$ 有唯一解

3 单位元，逆元唯一

设有单位元 e_1,e_2，由定义 $e_1=e_1\times e_2=e_2$.

逆元唯一：左逆 a_1，右逆 a_2：　$a_1=a_1\times e=a_1\times a\times a_2=e\times a_2=a_2$

4. $(a^{-1})^{-1}=a$.　$(a\times b)^{-1}=b^{-1}\times a^{-1}$

$a^{-1}\times a=e=a^{-1}\times (a^{-1})^{-1}$

$(a\times b)\times (b^{-1}\times a^{-1})=a\times[(b\times b^{-1})\times a^{-1}]=a\times a^{-1}=e$