群：一种二元运算，→再引入一种得环

环：① $\langle G, +, \times \rangle$

s.t
- $\langle G, + \rangle$ 是一个 Abel(交换)群　　交换群 × 含幺半群
- G 对 $\times$ 运算封闭
- $\times$ 结合律
- $\times$ 下有单位元　$\forall a \in G, \exists e \in G$, s.t $a \times e = e \times a = a$ } 含幺半群
- 分配律：$(a+b) \times c = a \times c + b \times c$, $a \times (b+c) = a \times b + a \times c$

若 $\langle G, \times \rangle$ 为群 则为域

$\langle \mathbb{Z}, +, \times \rangle$ 环

$\langle Even, +, \times \rangle$ 非环　$\langle Even, \times \rangle$ 无单位元

$\langle \mathbb{Q}, +, \times \rangle$ 环.

$\langle \mathbb{Z}_m, +\ (mod\ m), \times\ (mod\ m) \rangle$ 环

$\langle \mathbb{Z}[\sqrt{2}], +, \times \rangle$ 环

$\langle \mathbb{Z}[\sqrt{5}], +, \times \rangle$ 环

$\left\langle \left\{ a_0 + a_1 t^{\frac{1}{2}} + a_2 t^{\frac{2}{2}} + \cdots + a_{k-1} t^{\frac{k-1}{2}} \;\middle|\; a_i \in \mathbb{Z}^{(t \in N^+)} \right\}, +, \times \right\rangle$

$\langle \mathbb{Z}[x], +, \times \rangle$ 环

整系数多项式 $\{ a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k \mid a \in \mathbb{Z},\ k \in \mathbb{N} \}$

整环：环 R 被称作整环 若：R 对 $\times$ 可交换 $a, b \in R$, $a \times b = 0_R \Rightarrow a = 0_R$ or $b = 0_R$

整数环是整环

整系数多项式环是整环

非整环的例子：$\left\langle \begin{pmatrix} a & b \\ c & d \end{pmatrix}_{\in \mathbb{Z}}, +, \times \right\rangle$ 是环 有 $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ 都不是整环

环 $\langle Q, +, \times \rangle$
① $+$ 交换群
② $\times$ 含幺半群

$\xrightarrow{\langle Q \setminus \{0\}, \times \rangle \text{是群}}$

域 $\langle Q, +, \times \rangle$
$\langle Q, + \rangle$ 为交换群
$\langle Q \setminus \{0\}, \times \rangle$ 为群

$\langle \mathbb{Z}_m, +(mod\ m), \times (mod\ m) \rangle$ 是环，但不一定是域：eg $\langle \mathbb{Z}_4, +, \times \rangle$ $2 \times 2 = 0$ ×

m为素数的时候是域

域一定是整环.

证: $\forall a, b \in R$. $a \times b = 0$

$\begin{cases} a \neq 0, \text{则} \exists a^{-1}, a^{-1} \times a \times b = b = 0 \\ a = 0 \end{cases}$

整环不一定是域.

eg: 实矩阵.

有限整环一定是域

i) 整环有乘法消去律:

$\forall a \neq 0$, $a \times b = a \times c$

$\Rightarrow a \times (b-c) = 0 \Rightarrow b - c = 0$ 即 $b = c$

ii) 整环有乘法逆元:

记整环 $R = \{r_0, r_1, \cdots r_n\}$. $(r_0 = 0)$

$\forall r_i \in R$. $r_i \neq 0$. 构造 $r_i R = \{r_i \times r_0, r_i \times r_1, \cdots r_i \times r_n\}$

则 $r_i R$ 中 $\forall$ 两元素不同

$\rightarrow$ 反证 $\exists r_j \neq r_k$. s.t. $r_i \times r_j = r_i \times r_k \Rightarrow r_i \times (r_j - r_k) = 0$ 即 $r_i \neq 0$ 则 $r_j - r_k = 0$. 矛盾

由 $\forall r_i \cdot r \in r_i R$. $r_i \cdot r \in R \Rightarrow r_i R \subseteq R$

又 $|R| = |r_i R| \Rightarrow R = r_i R$ 故 $\forall r_i$ 均可构造 $r_i R = R$ 故 $\exists r_i \cdot r_i' \in R \Rightarrow r_i' r_i = 1_R$

即 $\forall r_i \neq 0$. r_i 有逆元

则直接 $r_i^1 r_i^2 \cdots r_i^n$, r_i^m 出现有两个相同 $\Rightarrow r^i = r^j \Rightarrow r^{|i-j|} = 1_R$ 则有逆元

则有限整环一定是域