第十六周习题课: 循环群, 环和域简介

郑晓鹏

中国科学院数学与系统科学研究院

目录

生成元 · 子群

定义 1

设 G 是群, 如果存在 $g \in G$, 使得 $G = \langle g \rangle$, 则称 G 为循环群.

$(\langle g \rangle, \cdot, 1)$

命题 1.1

循环群在同构意义下只有两种类型:

1. 如果 $\mathrm{card}(G) = \infty$, 则 $G \simeq (\mathbb{Z}, +, 0)$;
2. 如果 $\mathrm{card}(G) = n$, 则 $G \simeq (\mathbb{Z}_n, +, \bar{0})$.

$(a+a) = 2a$.

证明: (1) $\phi : \mathbb{Z} \to G$, $m \to g^m$; (2) $\phi : \mathbb{Z}_n \to G$, $\overline{m} \to g^m$.

循环群的生成元

注: 若 G 为循环群, G 的生成元指的是满足 $\langle a\rangle = G$ 的元素 a, 比如作为加法群 $\mathbb{Z}_6 = \langle 1\rangle = \langle 5\rangle$, 则 $\bar{1}$ 和 $\bar{5}$ 都是 $\mathbb{Z}_6$ 的生成元.

$$\mathbb{Z}_6 = \langle \bar{1}\rangle = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$$
$$= \bar{0}$$
$$= \langle \bar{5}\rangle = \{\bar{5}, \bar{4}, \bar{3}, \bar{2}, \cdots\}$$
$$= 2\cdot\bar{5} \quad = 3\cdot\bar{5} \quad = 4\cdot\bar{5}$$

循环群的生成元

注: 若 G 为循环群, G 的生成元指的是满足 $\langle a\rangle = G$ 的元素 a, 比如作为加法群 $\mathbb{Z}_6 = \langle 1\rangle = \langle 5\rangle$, 则 $\overline{1}$ 和 $\overline{5}$ 都是 $\mathbb{Z}_6$ 的生成元.

习题 1.

1. 写出 $G = (\mathbb{Z}_{12}, +, 0)$ 的所有生成元.
2. 设 $G = \langle a\rangle$ 为循环群且 $\mathrm{card}(G) = +\infty$, 证明: G 只有两个生成元.
3. 设 $G = \langle a\rangle$ 为有限阶循环群且 $n = \mathrm{card}(G)$. 证明: a^k 是 G 的生成元当且仅当 k 和 n 互素.

$G = \langle c\rangle$, $c = a$ 或 a^{-1}

$(\mathbb{Z}, +, 0)$, $1, -1$.

$\{a^k\}$

$=$

(2) 设 $G = \langle a \rangle$ 为循环群且 $\mathrm{card}(G) = +\infty$, 证明: G 只有两个生成元.

证: 设 $G = \langle a^k \rangle$, 因为 $a \in G$, 所以存在 $m \in \mathbb{Z}$, 使得

$$(a^k)^m = a, \text{ 即 } a^{km-1} = 1$$

由 $\mathrm{card}(G) = +\infty$, 得 $\mathrm{ord}(a) = +\infty$, 所以

$$a^{km-1} = 1 \Rightarrow km - 1 = 0.$$

所以 $k = \pm 1$. 显然 $\langle a \rangle = \langle a^{-1} \rangle = G$, 所以 G 有且只有两个生成元 a, a^{-1}.

显然 $a \neq a^{-1}$ □

(2) 设 $G = \langle a \rangle$ 为循环群且 $\mathrm{card}(G) = +\infty$, 证明: G 只有两个生成元.

证明: 当 $\mathrm{card}(G) = +\infty$ 时, $\mathrm{ord}(a) = +\infty$. 设 $G = \langle a^k \rangle$, 则存在 $m \in \mathbb{Z}$, 使得 $(a^k)^m = a$. 所以 $a^{km-1} = 1$. 由 $\mathrm{ord}(a) = +\infty$ 可得 $km - 1 = 0$, 即 $k = \pm 1$. 显然 a 和 a^{-1} 可以作为 G 的生成元, 且 $a \neq a^{-1}$, 所以 G 有且只有两个生成元.

$G = \langle a^k \rangle \Leftrightarrow \gcd(k, n)$.

(3) 设 $G = \langle a \rangle$ 为有限阶循环群且 $n = \mathrm{card}(G)$. 证明: a^k 是 G 的生成元当且仅当 k 和 n 互素.

证明: 因为 $\langle a^k \rangle \subset G$, 所以

$$\langle a^k \rangle = G \Leftrightarrow \mathrm{card}(G) = \mathrm{card}(\langle a^k \rangle)$$
$$\Leftrightarrow \mathrm{ord}(a^k) = n$$

又因为 $\mathrm{ord}(a^k) = \dfrac{n}{\gcd(n,k)}$, 所以

$$\mathrm{ord}(a^k) = n \Leftrightarrow \gcd(n,k) = 1$$
$$\Leftrightarrow n, k \text{ 互素}.$$

□

(3) 设 $G = \langle a \rangle$ 为有限阶循环群且 $n = \mathrm{card}(G)$. 证明: a^k 是 G 的生成元当且仅当 k 和 n 互素.

证明: 因为 a^k 是 G 的生成元当且仅当 $\mathrm{ord}(a) = n$. 所以根据 $\mathrm{ord}(a^k) = \frac{n}{\gcd(n,k)}$, 可知 $\mathrm{ord}(a) = n$ 当且仅当 n, k 互素.

(3) 设 $G = \langle a \rangle$ 为有限阶循环群且 $n = \mathrm{card}(G)$. 证明: a^k 是 G 的生成元当且仅当 k 和 n 互素.

证明: 因为 a^k 是 G 的生成元当且仅当 $\mathrm{ord}(a) = n$. 所以根据 $\mathrm{ord}(a^k) = \frac{n}{\gcd(n,k)}$, 可知 $\mathrm{ord}(a) = n$ 当且仅当 n, k 互素.

(1) 写出 $G = (\mathbb{Z}_{12}, +, 0)$ 的所有生成元.
解: $G = \langle \bar{1} \rangle = \langle \bar{5} \rangle = \langle \bar{7} \rangle = \langle \bar{11} \rangle$.

$\mathbb{Z}_{12} = \langle \bar{1} \rangle = \langle \bar{5} \rangle = \langle \bar{7} \rangle = \langle \bar{11} \rangle$,

$(\langle \bar{1} \rangle, +, 0)$ $\quad\quad$ $\langle \bar{1}, \bar{5} \rangle = \mathbb{Z}_{12}$

循环群的子群

命题 1.2

循环群的子群都是循环群.

习题2.

1. 写出 $(\mathbb{Z}_{12}, +, 0)$ 的所有子群;
2. 证明: 当 $G = \langle a \rangle$ 为 n 阶循环群时, 对于每个 n 的正因子 k (即 $k \mid n$, $k > 0$), G 有且只有一个 k 阶子群, 且这个子群就是 $\langle a^{\frac{n}{k}} \rangle$.

$(\mathbb{Z}_{12}, +, \bar{0})$, $\bar{12}$ 的生成元为 $\bar{1}, \bar{12}, \bar{2}, \bar{6}, \bar{3}, \bar{4}$

分别为 $\langle \bar{12} \rangle$ (= $\langle \bar{0} \rangle$), $\langle \bar{1} \rangle$, $\langle \bar{6} \rangle$, $\langle \bar{2} \rangle$, $\langle \bar{4} \rangle$, $\langle \bar{3} \rangle$,

(2) 当 $G=\langle a\rangle$ 为 n 阶循环群时, 对于每个 n 的正因子 k (即 $k \mid n$, $k>0$), G 有且只有一个 k 阶子群, 且这个子群就是 $\langle a^{\frac{n}{k}}\rangle$.

证明：存在性：因为 $\langle a^{\frac{n}{k}}\rangle$ 是 G 的子群，而且

$$ord(a^{\frac{n}{k}})=\frac{n}{gcd(\frac{n}{k},n)}=k,$$

所以 $card(\langle a^{\frac{n}{k}}\rangle)=ord(a^{\frac{n}{k}})=k$，所以 G 存在 k 阶子群 $\langle a^{\frac{n}{k}}\rangle$.

唯一性：设 H 为 G 的 k 阶子群，因为 G 的子群为循环群，

所以设 $H=\langle a^m\rangle$，因为 $card(H)=k$，所以

$ord(a^m)=k$. 于是

$(a^m)^k=e$

$=a^n=(a^{\frac{n}{k}})^k$

$$k=ord(a^m)=\frac{n}{gcd(n,m)} \Rightarrow k\cdot gcd(n,m)=n$$

又 $a^m=a^{\frac{n}{k}}$

所以 $gcd(n,m)=\frac{n}{k}$，所以 $\frac{n}{k}\mid m$，于是

$a^k=b^k \not\Rightarrow a=b$

$\Rightarrow (ab^{-1})^k=e$

$a^m\in\langle a^{\frac{n}{k}}\rangle \Rightarrow \langle a^m\rangle\subset\langle a^{\frac{n}{k}}\rangle$

又因为 $card(\langle a^m\rangle)=card(\langle a^{\frac{n}{k}}\rangle)$，所以 $H=\langle a^{\frac{n}{k}}\rangle$

(2) 当 $G = \langle a \rangle$ 为 n 阶循环群时, 对于每个 n 的正因子 k (即 $k \mid n$, $k > 0$), G 有且只有一个 k 阶子群, 且这个子群就是 $\langle a^{\frac{n}{k}} \rangle$.

证明: 设 $k \mid n$ 且 $n = kq$, 则 $\mathrm{ord}(a^q) = k$, 从而 $\langle a^q \rangle$ 是 G 的一个 k 阶子群. 又设 H 也是 G 的一个 k 阶子群, 则 H 是一个循环群, 设 $H = \langle a^m \rangle$, $\mathrm{ord}(a^m) = k$. 但 a^m 的阶是 $\frac{n}{(m,n)}$, 故

$$\frac{n}{\gcd(m,n)} = k, \quad n = k(m,n).$$

则 $\gcd(m,n) = q$. 所以 $q \mid m$, 即 $a^m \in \langle a^p \rangle$, 推出 $\langle a^m \rangle \subset \langle a^p \rangle$. 但由于 $\langle a^q \rangle$ 与 $\langle a^m \rangle$ 的阶相同,故

$$H = \langle a^m \rangle = \langle a^q \rangle = \left\langle a^{\frac{n}{k}} \right\rangle,$$

即 $G = \langle a \rangle$ 的 k 阶子群是唯一的.

(1) 写出 $(\mathbb{Z}_{12}, +, 0)$ 的所有子群;

(1) 写出 $(\mathbb{Z}_{12}, +, 0)$ 的所有子群;

解: 由于对于 12 的每个正因子 s, $\mathbb{Z}_{12}$ 有且存在一个 s 阶的循环子群, 因为 12 的因子有 $1, 12, 2, 6, 3, 4$, 所以 $(\mathbb{Z}_{12}, +, 0)$ 的子群有 $\langle\overline{12}\rangle$, $\langle\overline{1}\rangle$, $\langle\overline{6}\rangle$, $\langle\overline{2}\rangle$, $\langle\overline{4}\rangle$, $\langle\overline{3}\rangle$.

目录

环的定义

环的定义. 五元组 $(R, +, 0, \cdot, 1)$, 其中 R 是集合, $0, 1 \in R$ 且 $0 \neq 1$, $+$, $\cdot$ 是 R 上的二元运算, 称为 (含么)环 (ring), 如果

(i) $(R, +, 0)$ 是交换群;

环的定义

环的定义. 五元组 $(R, +, 0, \cdot, 1)$, 其中 R 是集合, $0, 1 \in R$ 且 $0 \neq 1$, $+$, $\cdot$ 是 R 上的二元运算, 称为 (含么)环 (ring), 如果

(i) $(R, +, 0)$ 是交换群;

(ii) $(R, \cdot, 1)$ 是含么半群; 且

结合律 + 1_R

环的定义

环的定义. 五元组 $(R, +, 0, \cdot, 1)$, 其中 R 是集合, $0, 1 \in R$ 且 $0 \neq 1$, $+$, $\cdot$ 是 R 上的二元运算, 称为 (含么)环 (ring), 如果

(i) $(R, +, 0)$ 是交换群;

(ii) $(R, \cdot, 1)$ 是含么半群; 且

(iii) 对于任意 $x, y, z \in R$,

"+" 一定交换.

"·" 不一定交换

$$x(y+z) = xy + xz \quad (x+y)z = xz + yz.$$

当 $(R, \cdot, 1)$ 是交换的含么半群时, R 称为交换环. 否则称之为非交换环.

环的定义

环的定义. 五元组 $(R,+,0,\cdot,1)$, 其中 R 是集合, $0,1\in R$ 且 $0\neq 1$, $+$, $\cdot$ 是 R 上的二元运算, 称为 (含么)环 (ring), 如果

(i) $(R,+,0)$ 是交换群;

(ii) $(R,\cdot,1)$ 是含么半群; 且 ← 乘法封闭.

(iii) 对于任意 $x,y,z\in R$,

$$x(y+z)=xy+xz \quad (x+y)z=xz+yz.$$

当 $(R,\cdot,1)$ 是交换的含么半群时, R 称为交换环. 否则称之为非交换环.

环的例子: 整数环 $\mathbb{Z}$, 模 n 剩余类环 $\mathbb{Z}_n$ ($+,\cdot$), 多项式环 $F[x]$, 矩阵环 $(\mathrm{M}_n(\mathbb{R}),+,O,\cdot,E)$ (非交换环).

环的性质

设 $(R, +, 0, \cdot, 1)$ 是环. 则

1. 对任意 $x \in R, 0x = x0 = 0$;
2. 对任意 $x, y \in R$,

$$(-x)y = x(-y) = -(xy) \quad \text{和} \quad (-x)(-y) = xy;$$

3. 对任意 $x \in R, (-1)x = x(-1) = -x$.
4. 设 $x_1, \ldots, x_m, y_1, \ldots, y_n$ 是环 R 中的元素. 则

$$\left(\sum_{i=1}^{m} x_i\right)\left(\sum_{j=1}^{n} y_j\right) = \sum_{i=1}^{m}\sum_{j=1}^{n} x_i y_j.$$

5. 设 $m, n \in \mathbb{Z}, x, y \in R$. 则 $(mx)(ny) = (mn)(xy)$.

子环

子环. 设 $(R,+,0_R,\cdot,1_R)$ 是环, $S\subset R$ 使得 $(S,+,0_R,\cdot,1_R)$ 也是环. 则称 S 是 R 的子环(subring).

判定

① $(S,+,0_R)$ 是交换群 $a-b\in S$.

② $(S,\cdot,1_R)$ 是幺半群

(1) "$\cdot$" 封闭

(2) 结合律显然. (3) $1_R\in S$

③ 左右分配律显然.

子环

子环. 设 $(R,+,0_R,\cdot,1_R)$ 是环, $S\subset R$ 使得 $(S,+,0_R,\cdot,1_R)$ 也是环. 则称 S 是 R 的子环(subring).

习题3. 设 $\mathbb{Z}[\sqrt{2}]=\{a+b\sqrt{2}:a,b\in\mathbb{Z}\}$. 验证 $(\mathbb{Z}[\sqrt{2}],+,0,\cdot,1)$ 是 $(\mathbb{R},+,0,\cdot,1)$ 的子环. 确定该子环中所有可逆元.
证明:

子环

$a,b\in H$, $ab^{-1}\in H$.

子环. 设 $(R,+,0_R,\cdot,1_R)$ 是环, $S\subset R$ 使得 $(S,+,0_R,\cdot,1_R)$ 也是环. 则称 S 是 R 的子环(subring).

习题3. 设 $\mathbb{Z}[\sqrt{2}]=\{a+b\sqrt{2}:a,b\in\mathbb{Z}\}$. 验证 $(\mathbb{Z}[\sqrt{2}],+,0,\cdot,1)$ 是 $(\mathbb{R},+,0,\cdot,1)$ 的子环. 确定该子环中所有可逆元.

证明: 显然 $\mathbb{Z}[\sqrt{2}]$ 非空. 设 $a+b\sqrt{2},c+d\sqrt{2}\in\mathbb{Z}[\sqrt{2}]$, 则

$$(a+b\sqrt{2})-(c+d\sqrt{2})=(a-c)+(b-d\sqrt{2})\in\mathbb{Z}[\sqrt{2}]$$

的子群

所以 $(\mathbb{Z}[\sqrt{2}],+,0)$ 是 $(\mathbb{R},+,0)$, 所以 $(\mathbb{Z}[\sqrt{2}],+,0)$ 是一个群, 而且显然为交换群.

又因为

$(\mathbb{Z}[\sqrt{2}],\cdot,1_R)$

$$(a+b\sqrt{2})\cdot(c+d\sqrt{2})=(ac+2bd)+(bc+ad)\sqrt{2}\in\mathbb{Z}[\sqrt{2}],$$

所以 $\cdot$ 是 $\mathbb{Z}[\sqrt{2}]$ 上的二元运算. 因为 $\cdot$ 在 $\mathbb{R}[\sqrt{2}]$ 中满足结合律以及对加法的左右分配律, 所以 $\cdot$ 在 $\mathbb{Z}[\sqrt{2}]$ 中也满足结合律以及对加法的左右分配律. 而且 $1\in\mathbb{Z}[\sqrt{2}]$. 所以 $(\mathbb{Z}[\sqrt{2}],+,0,\cdot,1)$ 是 $(\mathbb{R},+,0,\cdot,1)$ 的子环.

$\mathbb{Z}[\sqrt{2}]$ 可逆元.

设 $a+b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, $(a+b\sqrt{2})^{-1} \in \mathbb{R}$, 而且

$$(a+b\sqrt{2})^{-1} = \frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})}$$

$$= \frac{a-b\sqrt{2}}{a^2-2b^2}$$

$$= \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}.$$

$a+b\sqrt{2}$ 可逆 $\Leftrightarrow \frac{a}{a^2-2b^2} \in \mathbb{Z}$, $\frac{b}{a^2-2b^2} \in \mathbb{Z}$.

所以 $\mathbb{Z}[\sqrt{2}]$ 的可逆元为 $\{a+b\sqrt{2} \in \mathbb{Z}[\sqrt{2}] \mid \frac{a}{a^2-2b^2} \in \mathbb{Z}, \frac{b}{a^2-2b^2} \in \mathbb{Z}\}$

设 $a+b\sqrt{2}$ 可逆, 则存在 $c+d\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, 使得

$$(a+b\sqrt{2})(c+d\sqrt{2}) = 1$$

于是 $ac+2bd=1$, $bc+ad=0$. 变型

$$a(c^2-2d^2)=c, \quad c(a^2-2b^2)=a.$$

$\Rightarrow a|c, c|a, \Rightarrow a=\pm c$. (易得 $a=0$ 不可能)?

于是 $a^2-2b^2=\pm 1$,

$\{\text{可逆元}\} = \{a+b\sqrt{2} \in \mathbb{Z}[\sqrt{2}] \mid a^2-2b^2=\pm 1\}$

设 $a+b\sqrt{2}$ 可逆, 我们知道 $a+b\sqrt{2}$ 在 $\mathbb{R}$ 中的逆为

$$\frac{1}{a+b\sqrt{2}}=\frac{a-b\sqrt{2}}{a^2-2b^2}.$$

所以 $a+b\sqrt{2}$ 可逆当且仅当 $\frac{a}{a^2-2b^2}\in\mathbb{Z}$ 且 $\frac{b}{a^2-2b^2}\in\mathbb{Z}$.
进一步地, 存在 $c+d\sqrt{2}$, 使得

$$(a+b\sqrt{2})(c+d\sqrt{2})=1.$$

得 $ac+2bd=1$, $bc+ad=0$. 变型可得

$$a(c^2-2d^2)=c, c(a^2-2b^2)=a,$$

所以 $a=\pm c$. 当 $a=0$ 时, 得 $a+b\sqrt{2}=b\sqrt{2}$ 不可逆, 矛盾, 所以 $a\neq 0$, 则 $a^2-2b^2=\pm 1$. 因为当 $a^2-2b^2=\pm 1$ 时, $\frac{1}{a+b\sqrt{2}}=\frac{a-b\sqrt{2}}{a^2-2b^2}\in\mathbb{Z}[\sqrt{2}]$.
所以 $a^2-2b^2=\pm 1$ 是 $a+b\sqrt{2}$ 可逆的充要条件.
(注: 实际上所有可逆元可以写为 $\{\pm(1+\sqrt{2})^n \mid n\in\mathbb{Z}\}$)

$1+\sqrt{2}$ $-1-\sqrt{2}$ ± 1

环同态

环同态. 设 $(R,+,0_R,\cdot,1_R)$ 和 $(S,+,0_S,\cdot,1_S)$ 是两个环. 如果映射 $\phi: R \longrightarrow S$ 满足对任意 $x,y \in R$,

$$\phi(x+y)=\phi(x)+\phi(y), \phi(xy)=\phi(x)\phi(y), \text{ 和 } \phi(1_R)=1_S,$$

则称 ϕ 是环同态. 如果环同态 ϕ 是单射, 则称 ϕ 是环嵌入; 如果是双射, 则称环同构.

$(R,+,0_R)$ ϕ是群同态.

$\searrow (S,+,0_S)$

$\phi(0_R)=0_S$ ✓.

$\phi(-a)=-\phi(a)$.

零因子和可逆元

a是R的左零因子
$\Leftrightarrow$ $a\neq 0$, $\exists b\neq 0$, s.t
$ab=0$.

零因子. 设 a, b 是环 R 中的非零元素. 如果 $ab = 0$, 则称 a 是 R 的左零因子(left zero-divisor), b 是 R 的右零因子(right zero-divisor). 如果 $x \in R$ 满足 $x \neq 0$ 且 x 既非左零因子又非右零因子, 则称 x 是非零因子(non-zerodivisor). 当 R 交换时, 左右零因子统称为零因子.

可逆元. 设 $a \in R$, 如果存在 $b \in R$, 使得 $ab = ba = 1$, 则称 a 是 R 中的可逆元. (关于乘法可逆)

模 n 剩余类环: $(\mathbb{Z}_n, +, 0, \cdot, 1)$

命题 2.1

设 $\bar{a} \in \mathbb{Z}_n$. 则 $\bar{a}$ 关于乘法可逆当且仅当 a 和 n 互素.

命题 2.2

在 $\mathbb{Z}_n$ 中, $\bar{a}$ 是零因子当且仅当 $1 < \gcd(n, a) < n$.

矩阵环 $(\mathrm{M}_n(\mathbb{R}), +, O, \cdot, E)$ (非交换环).

命题 2.3

设 $A \in \mathrm{M}_n(\mathbb{R})$ 是非零矩阵. A 是左或右零因子当且仅当 $\mathrm{rank}(A) < n$.

命题 2.4

设 $A \in \mathrm{M}_n(\mathbb{R})$ 是非零矩阵. A 可逆当且仅当 $\mathrm{rank}(A) = n$.

$M_n(\mathbb{R}) = \{ O,$ 可逆元, 零因子 $\}$

$\mathrm{rank}(A) = n$ $\quad$ $\mathrm{rank}(A) < n,\ A \neq O$

$\exists A' \in M_n(\mathbb{R}),\ AA' = A'A = E$

设 $A \in M_n(\mathbb{R})$，设

$$\mathbb{R}[A] := \left\{ \sum_{i=0}^{k} \alpha_k A^k \mid k \in \mathbb{N}, \alpha_i \in \mathbb{R} \right\}.$$

则 $\mathbb{R}[A]$ 是 $\mathrm{M}_n(\mathbb{R})$ 的子环且 $\mathbb{R}[A]$ 是交换环.

命题 2.5

设 $B \in \mathbb{R}[A]$ 且非零. B 可逆当且仅当 $\mathrm{rank}(B) = n$.

命题 2.6 (自行思考)

设 $B \in \mathbb{R}[A]$ 且非零. B 是零因子当且仅当 $\mathrm{rank}(B) < n$.

定义. $B \in \mathbb{R}[A]$ 可逆 $\Leftrightarrow \exists B' \in \mathbb{R}[A]$, s.t $BB' = B'B = E$.

$\mathbb{R}[A] = \{ 0$, 可逆元, 零因子 $\}$.

可逆元 $\Leftrightarrow \mathrm{rank}(B) = n$

零因子 $\Leftrightarrow \mathrm{rank}(B) < n$, $B \neq 0$

习题4. 环 R 的非零元素 x 称为幂零的, 若存在 $n \in N$, 使得 $x^n = 0$. 证明:

1. 若 R 是任意有单位元的环, x 是幂零元, 则 $1 - x$ 是可逆元;
2. 环 $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ 包含幂零元当且仅当 m 可以被一个大于 1 的整数的平方整除.

证明: (1) $(1-x)(\quad) = 1$

$(\quad)(1-x) = 1$

因为 x 是幂零元, 所以 $\exists n \in \mathbb{N}$, $x^n = 0$, 于是

$$1 - x^n = (1-x)(x^{n-1} + x^{n-2} + \cdots + x + 1)$$

$$= (x^{n-1} + x^{n-2} + \cdots + x + 1)(1-x)$$

$$(1-x)^{-1} = x^{n-1} + x^{n-2} + \cdots + x + 1.$$

习题4. 环 R 的非零元素 x 称为幂零的, 若存在 $n \in N$, 使得 $x^n = 0$. 证明:

1. 若 R 是任意有单位元的环, x 是幂零元, 则 $1 - x$ 是可逆元;
2. 环 $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ 包含幂零元当且仅当 m 可以被一个大于 1 的整数的平方整除.

证明: (a) 设 $x^n = 0$, 则 $1 - x^n = 1$. 分解可得

$$(1-x)(x^{n-1} + \cdots + x + 1) = 1, \ (x^{n-1} + \cdots + x + 1)(1-x) = 1$$

所以 $(1-x)^{-1} = x^{n-1} + \cdots + x + 1$.

(b) 必要性: 设 $\bar{a} \in \mathbb{Z}_m$ 且 $\bar{a}$ 幂零, 存在 $n \in \mathbb{N}$, s.t. $\bar{a}^n = \bar{0}$

反证, 设 m 不能被任何大于1的整数的平方整除, 则 m 的素分解为 $m = p_1 p_2 \cdots p_s$, p_i 为素数, 由 $m \mid a^n$, 得

$$p_i \mid a^n \Longrightarrow p_i \mid a, \quad i = 1, \cdots, s.$$

于是 $m \mid a$, 得 $\bar{a} = \bar{0}$, 和 $\bar{a}$ 是幂零矛盾.

习题4. 环 R 的非零元素 x 称为幂零的, 若存在 $n \in N$, 使得 $x^n = 0$. 证明:

1. 若 R 是任意有单位元的环, x 是幂零元, 则 $1 - x$ 是可逆元;
2. 环 $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ 包含幂零元当且仅当 m 可以被一个大于 1 的整数的平方整除.

证明: (a) 设 $x^n = 0$, 则 $1 - x^n = 1$. 分解可得

$$(1-x)(x^{n-1} + \cdots + x + 1) = 1, \ (x^{n-1} + \cdots + x + 1)(1-x) = 1$$

所以 $(1-x)^{-1} = x^{n-1} + \cdots + x + 1$.

(b) 必要性: 设 $\bar{a} \in \mathbb{Z}_m$, $\bar{a} \neq 0$, $\bar{a}^n = 0$, 即 $m \mid a^n$, 所以 $a^n = mq$. 因为 $\bar{a} \neq 0$, 所以 $n \neq 1$. 反证. 假设 m 不能被任何整数的平方整除, 则 m 的素因子分解为 $m = p_1 \cdots p_s$, p_i 为素数, 所以 $p_i \mid a^n$, 则 $p_i \mid a$. 于是 $m \mid a$, 与 $\bar{a} \neq 0$ 矛盾.

充分性. 设 $m = a^2 p$, $a > 1$, $ap < m$, 取 $x = ap$, 得 $\bar{x}^2 = \overline{(ap)^2} = \overline{a^2 p^2} = \bar{0}$, 且 $\bar{x} \neq \bar{0}$, 所以 $\bar{x}$ 是幂零的.

习题4. 环 R 的非零元素 x 称为幂零的, 若存在 $n \in N$, 使得 $x^n = 0$. 证明:

1. 若 R 是任意有单位元的环, x 是幂零元, 则 $1 - x$ 是可逆元;
2. 环 $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ 包含幂零元当且仅当 m 可以被一个大于 1 的整数的平方整除.

证明: (a) 设 $x^n = 0$, 则 $1 - x^n = 1$. 分解可得

$$(1-x)(x^{n-1} + \cdots + x + 1) = 1,\ (x^{n-1} + \cdots + x + 1)(1-x) = 1$$

所以 $(1-x)^{-1} = x^{n-1} + \cdots + x + 1$.
(b) 必要性: 设 $\bar{a} \in \mathbb{Z}_m$, $\bar{a} \neq 0$, $\bar{a}^n = 0$, 即 $m \mid a^n$, 所以 $a^n = mq$. 因为 $\bar{a} \neq 0$, 所以 $n \neq 1$. 反证. 假设 m 不能被任何整数的平方整除, 则 m 的素因子分解为 $m = p_1 \cdots p_s$, p_i 为素数, 所以 $p_i \mid a^n$, 则 $p_i \mid a$. 于是 $m \mid a$, 与 $\bar{a} \neq 0$ 矛盾.
充分性. 设 $m = b^2 q$, $b > 1$, $b, q \in \mathbb{Z}^+$. 取 $a = bq$, 则 $\bar{a} \neq 0$, 且 $a^2 = b^2 q^2 = qm$. 即 $\bar{a}^2 = \bar{0}$. 所以 a 是幂零元.

环的特征

$n \in \mathbb{N}$.

$n \in F$

$(1+1+1+1+\cdots+1) = 0$

n

$n \cdot 1_R$ $n>0$. $n = (1_R + 1_R + \cdots + 1_R)$ (n个)

$n<0$ $n = (-1_R) + \cdots + (-1_R)$ ($-n$).

环的特征. 设 $(R, +, 0, \cdot, 1)$ 是环. 如果加法群 $(R, +, 0)$ 中 1 的阶有限, 则 ord(1) 称为 R 的特征. 否则, R 的特征定义为零. 环 R 的特征记为 char(R).

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$. ← 特征0.

注:

$(1+1+1+1+1+\cdots) \neq 0$

$\mathbb{Z}_3$. $(\bar{1}+\bar{1}+\bar{1}) = \bar{0}$ 特征3.

$\mathbb{Z}_2$. $(\bar{1}+\bar{1}) = \bar{0}$ 特征2

$2 = 0$

↑ ↑

$2 \cdot 1_R$ $0 \cdot 1_R$

$2 \cdot \bar{1} = \bar{2} = 0 \cdot \bar{1} = \bar{0}$ $\in \mathbb{Z}_2$

$\bar{2} = \bar{0}$

$n \in \mathbb{N}$ $n \in F$ $n \triangleq n \cdot 1_F$.

域 ⇒ 整环.

命题 2.7

设 D 是整环 (无零因子的交换环), 则 D 的特征是零或者素数. 特别地, 域的特征是素数或 0.

char(F)=4 ✗ char(F)=1 ✗

域和子域

域. 设 F 是交换环, 如果 F 中的任何非零元都可逆, 则称 F 是域.

命题 2.8

$\mathbb{Z}_p$ 是域当且仅当 p 为素数.

定义 2 (子域)

设 $(F, +, 0_R, \cdot, 1_R)$ 是域, $K \subset R$ 使得 $(K, +, 0_R, \cdot, 1_R)$ 也是域. 则称 S 是 R 的子域(subfield). 换句话说, $(K, +, 0_R, \cdot, 1_R)$ 是 $(F, +, 0_R, \cdot, 1_R)$ 的子环而且 $(K, +, 0_R, \cdot, 1_R)$ 的每个非零元都可逆.

习题5. 设 F 是一个域,

$$A=\begin{pmatrix}1&1&1&1\\1&1&-1&-1\\1&-1&1&-1\\1&-1&-1&1\end{pmatrix}\in M_4(F)$$

$1_F+1_F=0$

根据 F 的特征,

$(-1_F)=1_F$

1. 讨论 $\mathrm{rank}(A)$ 的取值;
2. 设 $\phi_A: F^4\to F^4$ 是以 A 为矩阵的线性映射, 求 $\ker(\phi_A)$ 和 $\mathrm{im}(\phi_A)$.

解: (1) $\det(F)=-16$ $(=16\cdot(-1_F))$

若 $\mathrm{char}(F)=2$, 则 $2=0$, 则 $-16=0$, 而且 $-1=1$, 则

($\mathrm{char}(F)$为素数)

$$A=\begin{pmatrix}1&1&1&1\\1&1&1&1\\1&1&1&1\\1&1&1&1\end{pmatrix}$$

所以 $\mathrm{rank}(A)=1$,

若 $\mathrm{char}(F)\neq 2$, $\det(F)=-16\neq 0$, $\mathrm{rank}(A)=4$.

习题5. 设 F 是一个域,

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \in M_4(F)$$

根据 F 的特征,

1. 讨论 $\mathrm{rank}(A)$ 的取值;
2. 设 $\phi_A : F^4 \to F^4$ 是以 A 为矩阵的线性映射, 求 $\ker(\phi_A)$ 和 $\mathrm{im}(\phi_A)$.

解: (1) 计算得 $\det(F) = -16$. 因为域的特征都是素数, 所以当 F 的特征不等于 2 时, $\det(F) \neq 0$, 则 $\mathrm{rank}(F) = 4$. 当 F 的特征为 2 时, 有 $1 = -1$, 则 A 的所有行都相等, 所以 $\mathrm{rank}(A) = 1$.

习题5. 设 F 是一个域,

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \in M_4(F)$$

根据 F 的特征,

char(F) = 4 ✗

1. 讨论 $\mathrm{rank}(A)$ 的取值;
2. 设 $\phi_A : F^4 \to F^4$ 是以 A 为矩阵的线性映射, 求 $\ker(\phi_A)$ 和 $\mathrm{im}(\phi_A)$.

解: (1) 计算得 $\det(F) = -16$. 因为域的特征都是素数, 所以当 F 的特征不等于 2 时, $\det(F) \neq 0$, 则 $\mathrm{rank}(F) = 4$. 当 F 的特征为 2 时, 有 $1 = -1$, 则 A 的所有行都相等, 所以 $\mathrm{rank}(A) = 1$.

(2) 当 F 的特征不等于 2 时, $\mathrm{rank}(A) = 4$. 所以 $\ker(\phi_A) = \{0\}$, $\mathrm{im}(\phi_A) = F^4$. 当特征等于 2 时, 所以 $\mathrm{im}(\phi_A) = V_c(A) = \{x(1,1,1,1)^t : x \in F\}$. 计算方程:

1 = -1

$$x_1 + x_2 + x_3 + x_4 = 0$$

的解空间为 $\{a(1,1,0,0)^t + b(1,0,1,0)^t + c(1,0,0,1)^t : a, b, c \in F\}$. 所以 $\ker(\phi_A) = \{a(1,1,0,0)^t + b(1,0,1,0)^t + c(1,0,0,1)^t : a, b, c \in F\}$.

(选做)

1. 偶数阶群必含有 2 阶元.
2. 若群 G 的阶为 $2n$, n 为奇数, 则存在阶为 n 的子群. (提示: 需要 G 嵌入 S_{2n}, 再运用 (a) 以及奇置换偶置换的性质)

证明:

(选做)

1. 偶数阶群必含有 2 阶元.
2. 若群 G 的阶为 $2n$, n 为奇数, 则存在阶为 n 的子群. (提示: 需要 G 嵌入 S_{2n}, 再运用 (a) 以及奇置换偶置换的性质)

证明: (a) 设群中二阶元的个数为 k, 设 $a \in G$ 且 a 的阶大于 2, 则 $a^{-1} \neq a$ 且 $a^{-1} \in G$, 即阶大于 2 的元素都是成对存在的. 所以 $\mathrm{card}(G) - 1 - k$ 为偶数 (单位元的阶为1). 因为 $\mathrm{card}(G)$ 为偶数, 所以 $k \neq 0$.

(选做)

1. 偶数阶群必含有 2 阶元.
2. 若群 G 的阶为 $2n$, n 为奇数, 则存在阶为 n 的子群. (提示: 需要 G 嵌入 S_{2n}, 再运用 (a) 以及奇置换偶置换的性质)

证明: (a) 设群中二阶元的个数为 k, 设 $a \in G$ 且 a 的阶大于 2, 则 $a^{-1} \neq a$ 且 $a^{-1} \in G$, 即阶大于 2 的元素都是成对存在的. 所以 $\mathrm{card}(G) - 1 - k$ 为偶数 (单位元的阶为1). 因为 $\mathrm{card}(G)$ 为偶数, 所以 $k \neq 0$.

(b) 思路如下:

1. 群 G 存在2阶元 a.
2. 把群 G 看成一个置换群(S_{2n}的子群).
3. 二阶元 τ_a 可以分解为两两不交的轮换的乘积, 特别的, 因为 τ_a 为二阶元, 所以这些轮换都是对换.
4. τ_a 把不同的元素映射成不同的元素, 所以τ_a是 n 个对换的乘积. 因为 n 为奇数, 所以τ_a为奇置换.
5. 置换群中若存在奇置换, 则奇置换和偶置换各占一半, 所有偶置换构成阶为n的子群.

谢谢!