第十四次习题课

2023.12 29

知识点

循环群：

设G是群，如果存在 $g\in G$ 使得 $G=\langle g\rangle$，则称 G是循环群 (cyclic group).

循环群的子群也是循环群.

设 $G=\langle g\rangle$ 为有限阶循环群 $|G|=n$.

g^k 是G的生成元 $\Longleftrightarrow (k,n)=1$

作业 1.(a) 写出群 $(\mathbb{Z}_{12},+,\bar{0})$ 的所有子群.

$\langle\bar{0}\rangle=\{0\}$.

$\langle\bar{1}\rangle=\mathbb{Z}_{12}$

对于12的每个正因子s，$\mathbb{Z}_{12}$ 有且存在一个s阶的循环群

$\langle\bar{2}\rangle=\{\bar{0},\bar{2},\bar{4},\bar{6},\bar{8},\overline{10}\}$

$\langle\bar{3}\rangle=\{\bar{0},\bar{3},\bar{6},\bar{9}\}$

$\langle\bar{4}\rangle=\{\bar{0},\bar{4},\bar{8}\}$

$\langle\bar{6}\rangle=\{\bar{0},\bar{6}\}$

(b) 证明 $\mathbb{Z}_{13}$ 中的乘法可逆元关于乘法构成循环群.

$\mathbb{Z}_{13}^*=\mathbb{Z}_{13}\setminus\{0\}$

$\langle\bar{2}\rangle\subset\mathbb{Z}_{13}^*$ 且 $\mathrm{ord}(\bar{2})=12$.

由 $2^{12}=(2^4)^3\equiv3^3\equiv1 \mod 13$，且 $\forall\, 1\le a<12$，$2^a\not\equiv1 \mod 13$.

故 $\mathbb{Z}_{13}^*=\langle\bar{2}\rangle$.

环：

$(R,+,0,\cdot,1)$ (i) $(R,+,0)$ 是交换群

(ii) $(R,\cdot,1)$ 含幺半群；

(iii) 对 $\forall\, x,y,z\in R$,

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

若 $xy=yx$ 则 R 称为交换环

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

环同态，环同构，子环，整环.

1. 定义：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 $x,y\in R$，

$$\phi(x+y)=\phi(x)+\phi(y),\quad \phi(xy)=\phi(x)\phi(y),\quad \phi(1_R)=1_S.$$

则称 ϕ 是环同态.
如果 ϕ 是双射，则称 ϕ 是环同构.

2. 定义：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).

零因子、可逆元.

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).

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.

命题：设 U_R 是环 R 中所有可逆元的集合，则 $(U_R,\cdot,1)$ 是群.

3. 设 D 是交换环，如果 D 中没有零因子，则称 D 是整环 (domain)

域：（子域）

定义：设 F 是交换环，如果 F 中任何非零元都可逆，则称 F 是域(field).

域的特征：

设 $(F,+,0,\cdot,1)$ 是域，如果加法群 $(F,+,0)$ 中 1 的阶有限，则 $\mathrm{ord}(1)$ 称为 F 的特征.

域的特征记为 $\mathrm{char}(F)$.

域上的线性代数：

前三章关于线性代数的结论（除了用到 $2\neq 0$）对任何域 F 和坐标空间 F^n 都成立.

ex: $A\in M_{2n+1}(\mathbb{R})$ 是斜对称矩阵，则 $|A|=0$

$A\in M_{2n+1}(\mathbb{Z}_2)$ 是斜对称矩阵，反例：(I)

$$\begin{pmatrix} \bar{1} & 0 & 0 \\ 0 & \bar{1} & 0 \\ 0 & 0 & \bar{1} \end{pmatrix}$$

Euler 函数 φ：

对 $m\in\mathbb{Z}^+$，$\varphi(m)$ 表示 $1,\cdots,m$ 中与 m 互素的数个数.

Euler 定理：

对任何与正整数 m 互素的整数 a，有

$$a^{\varphi(m)}\equiv 1 \pmod{m}.$$

Fermat 小定理：

设 p 为素数，则对任何 $a\in\mathbb{Z}$ 有 $a^p\equiv a \pmod{p}$.

亦即整数 a 不被 p 整除时 $a^{p-1}\equiv 1 \pmod{p}$

Fermat 大定理 (Last Theorem) 整数 $n>2$，关于 x,y,z 方程 $x^n+y^n=z^n$ 没有正整数解

2. 设 $(R,+,0,\cdot,1)$ 为一个环, $u\in R$. 若存在 $v\in R$ 使得 $uv=1$, 我们称 u 有右逆. 设 u 有右逆, 证明以下命题等价:

(a) u 不是 R 中的可逆元;

(b) u 有多于一个右逆;

(c) u 为左零因子.

证明: 已知 $\exists\, v\in R$, s.t. $uv=1$.

(a) $\Longrightarrow$ (b). 反证, 假设 u 只有一个右逆.

由 $uv=1$ 得:

$$u(v+(1-vu)) = uv+u-uvu = uv=1.$$

由假设可得:

$$v+(1-vu)=v$$

故 $vu=1 \Longrightarrow u$ 可逆 矛盾.

(a) $\Longrightarrow$ (c).

反证, 假设 u 不是左零因子

由 $uv=1$ 得:

$$u(vu-1)=uvu-u=u-u=0$$

故 $vu=1 \Longrightarrow u$ 可逆 矛盾.

(b) $\Longrightarrow$ (a). 反证 显然

(c) $\Longrightarrow$ (a) 反证. 显然

$\square$

(b) $\Longrightarrow$ (c)

$\because$ u 有多于一个右逆

$\therefore$ $\exists\, v_1,v_2\in R$ 且 $v_1\neq v_2$ 有 $uv_1=uv_2=1$

$\therefore$ $u(v_1-v_2)=0$ 故 u 为左零因子

(c) $\Longrightarrow$ (b) $\because$ u 为左零因子

$\therefore$ $\exists\, w\in R$ 且 $w\neq 0$ 有 $uw=0$

故 $1=uv+uw=u(v+w)$

而 $v\neq v+w$ 得 u 有多于一个右逆.

错误例子.

① $uv=1 \Rightarrow vuv=v$

$\cancel{\Rightarrow}\ vu=1$

② 若 $vu\neq 1 \cancel{\Rightarrow uv\neq v}$

③. 若 u 为左零因子

则 $\exists\, p\neq 0$. $up=0$

$u(p+1)v=upv+uv=1$

$\Rightarrow (p+1)v$ 是 u 的右逆.

$\cancel{\Rightarrow} (P+I)v \neq v.$

3. 设 $(R,+,0,\cdot,1)$ 为一个环, $a,b\in R$. 证明:

(a) 若存在 $n\in\mathbb{N}$ 使得 $a^n=\cancel{1}\,0$, 则 $\underline{1-a\text{ 可逆}}$; (注: $a^0=1 \Longleftrightarrow a=0$)

(b) (选做) 若 $1-ab$ 可逆, 则 $1-ba$ 可逆.

证明: (a). 设 $x^n=0$, 有 $1-x^n=1$. 分解可得

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

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

故 $(1-x)^{-1}=1+x+\cdots+x^{n-1}$,

(b). 令 $c=(1-ab)^{-1}$.

易证

$$(1-ba)(1+bca)=1$$
$$(1+bca)(1-ba)=1$$

故 $1-ba$ $\underline{\text{可逆}}$ 即 $(1-ba)^{-1}=1+b(1-ab)^{-1}a$

4. 证明: 含有有限个元素的整环是域.

需证. 任何非零元都可逆

5. 设 $A=\begin{pmatrix}\bar{1} & \bar{2} & \bar{0}\\ \bar{2} & \bar{1} & \bar{2}\\ \bar{2} & \bar{1} & \bar{2}\end{pmatrix}\in \mathrm{M}_3(\mathbb{Z}_3)$.

(a) 求线性方程组 $A\boldsymbol{x}=\mathbf{0}$ 的解空间;

(b) 求 A 的列空间中所含向量的个数.

解: (a) 记线性方程组 $A\vec{x}=\vec{0}$ 的解空间为 V_A.

利用 Gauss 消去法计算

$$A \to \begin{pmatrix} \bar{1} & \bar{2} & \bar{0} \\ \bar{2} & \bar{1} & \bar{2} \\ \bar{0} & \bar{0} & \bar{0} \end{pmatrix} \to \begin{pmatrix} \bar{1} & \bar{2} & \bar{0} \\ \bar{0} & \bar{0} & \bar{2} \\ \bar{0} & \bar{0} & \bar{0} \end{pmatrix}.$$

于是

$$\operatorname{rank}(A)=2 \Longrightarrow \dim(V_A)=1.$$

由方程组 $\begin{cases} x_1+\bar{2}x_2=\bar{0} \\ \bar{2}x_3=\bar{0} \end{cases}$ 得 $\begin{cases} x_1=x_2 \\ x_3=\bar{0} \end{cases}$

所以

V_A 的一组基是 $(\bar{1},\bar{1},\bar{0})^t$.

故

$$V_A=\left\{\lambda\begin{pmatrix}\bar{1}\\ \bar{1}\\ \bar{0}\end{pmatrix} \,\middle|\, \lambda\in\mathbb{Z}_3\right\}.$$

(b) 由 $\operatorname{rank}(A)=2$ 得 $\dim(V_c(A))=2$.

所以

$$V_c(A)=\langle \vec{A}^{(1)}, \vec{A}^{(2)}\rangle=\left\{\lambda\vec{A}^{(1)}+\mu\vec{A}^{(2)} \,\middle|\, \lambda,\mu\in\mathbb{Z}_3\right\}$$

所以 $|V_c(A)|=3\times 3=9$.

6. 设线性映射 $\phi:\mathbb{Z}_5^3\to\mathbb{Z}_5^2$ 由

$$\phi(\mathbf{e}_1)=\epsilon_1-\bar{2}\epsilon_2,\ \phi(\mathbf{e}_2)=\epsilon_1+\bar{3}\epsilon_2,\ \phi(\mathbf{e}_3)=\mathbf{0}_2$$

确定, 其中 $\mathbf{e}_1,\mathbf{e}_2,\mathbf{e}_3$ 是 $\mathbb{Z}_5^3$ 的标准基, ϵ_1,ϵ_2 是 $\mathbb{Z}_5^2$ 的标准基.

(a) 写出 ϕ 在 $\mathbf{e}_1,\mathbf{e}_2,\mathbf{e}_3;\epsilon_1,\epsilon_2$ 下的矩阵.

(b) 计算 $\dim(\ker(\phi))$ 的维数和 $\operatorname{im}(\phi)$ 的一组基.

解: $\phi(e_1, e_2, e_3) = (\varepsilon_1, \varepsilon_2)\begin{pmatrix} \bar{1} & \bar{1} & \bar{0} \\ -\bar{2} & \bar{3} & \bar{0} \end{pmatrix}$,

(a) 矩阵

$$A = \begin{pmatrix} \bar{1} & \bar{1} & \bar{0} \\ -\bar{2} & \bar{3} & \bar{0} \end{pmatrix} = \begin{pmatrix} \bar{1} & \bar{1} & \bar{0} \\ \bar{3} & \bar{3} & \bar{0} \end{pmatrix}.$$

(b) 对 A 利用 Gauss 消去法得

$$A \longrightarrow \begin{pmatrix} \bar{1} & \bar{1} & \bar{0} \\ \bar{0} & \bar{0} & \bar{0} \end{pmatrix}$$

故 $\operatorname{rank}(A) = 1$. 于是 $\dim(\operatorname{im}(\phi)) = 1$. 根据对偶定理 $\dim(\ker(\phi)) = 3 - 1 = 2$.

$\operatorname{im}(\phi)$ 的一组基为 $\begin{pmatrix} \bar{1} \\ \bar{3} \end{pmatrix}$.

注: $\ker(\phi) = \left\langle \begin{pmatrix} \bar{0} \\ \bar{0} \\ \bar{1} \end{pmatrix}, \begin{pmatrix} \bar{4} \\ \bar{1} \\ \bar{0} \end{pmatrix} \right\rangle = \left\{ \lambda \begin{pmatrix} \bar{0} \\ \bar{0} \\ \bar{1} \end{pmatrix} + \mu \begin{pmatrix} \bar{4} \\ \bar{1} \\ \bar{0} \end{pmatrix} \middle| \lambda, \mu \in \mathbb{Z}_5 \right\}$

$\operatorname{im}(\phi) = \left\langle \begin{pmatrix} \bar{1} \\ \bar{3} \end{pmatrix} \right\rangle = \left\{ \alpha \begin{pmatrix} \bar{1} \\ \bar{3} \end{pmatrix} \middle| \alpha \in \mathbb{Z}_5 \right\}$

这里像空间和核空间是在不同的坐标空间中.