《代数结构》
习题解答

——第3，6，9次作业

邵新洋

第3次作业

- 作业编号：

- 习题2　　40, 42
- 习题3　　8, 12

习题2.40

- **题目：求37的12个原根**
- 考察内容：原根/原根的性质

- 解答：查最小原根和指数表，得知37的最小原根=2。由于$\Phi(37) = 37 - 1 = 36$，所以37的原根都在缩系$\{2^1, 2^2, \cdots, 2^{36} \equiv 1\}$中。

- 如何找到其他的11个原根？

习题2.40

- $\{2^1, 2^2, \cdots, 2^{36} \equiv 1\}$

- 2^2？错误：$(2^2)^{18} \equiv 1$
- 2^3？错误：$(2^3)^{12} \equiv 1$
- 2^4？错误：$(2^4)^9 \equiv 1$
- 2^5？
- …
- 2^8？错误：$(2^8)^9 \equiv 1$

习题2.40

- 假设2^m也是一个原根。则使$(2^m)^n \equiv 1$的最小n=36。
- 假设$(m, 36) = k \neq 1$，则$m = k \times l$，则取$n = \frac{36}{k}$，即有$\left(2^{k \times l}\right)^{\frac{36}{k}} \equiv 2^{36l} \equiv 1$。
- 所以，m必须和36互素：$m \in \{1,5,7,11,13,17,19,23,25,29,31,35\}$
- 根据指数的定义：$n \equiv g^m$有$m = ind_g n$。举例：如何求2^{19}：$19 = ind_2 x$，去指数表内查得为35

习题2.40

- 观察$H = \{2^1, 2^2, \cdots, 2^{36} \equiv 1\}$。——36阶循环群
- 实际上在模37运算下，$< H, \times >$构成一个乘法群。

- 对于数m，令集合$G = \{0,1,2,\ldots,m-1\}$，则$< G, \times >$在模m乘法运算下构成群。

- 原根的意义：上述乘法群的所有$\Phi(m)$阶子群的所有生成元。

习题2.42

- **证明：若$\boldsymbol{a}$模$\boldsymbol{p}$的阶为3，则$\boldsymbol{a+1}$模$\boldsymbol{p}$的阶为6。**
- 考察内容：阶的定义

- 阶的定义：$a^n \equiv 1(mod\ p)$，

其中n是满足式子的<u>最小整数</u>。

- 所以，需要证明：

$$\begin{cases}(a+1)^6 \equiv 1(mod\ p) \\ a+1\text{阶不为}1,2,3\end{cases}$$

习题2.42

- 已知a的阶为3，所以$a^3 \equiv 1$。
- 因此，$0 \equiv a^3 - 1 \equiv (a-1)(a^2+a+1)$。由于$a$的阶为3不是1，因此$a-1 \not\equiv 0$。所以有：
$$a^2 + a \equiv -1 (mod\ p)$$
- 所以$(a+1)^6$
$\equiv (a^3 + 3a^2 + 3a + 1)^2$
$\equiv (1 + 3\times(-1) + 1)^2$
$\equiv 1$

习题2.42

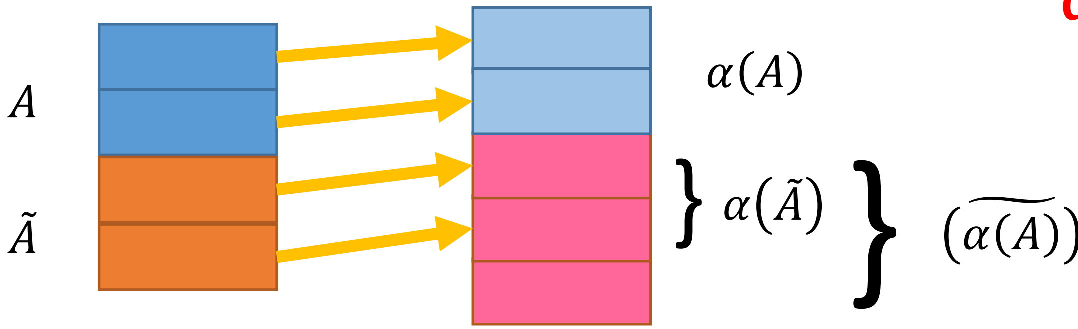
- $a + 1$的阶不为1，2，3：

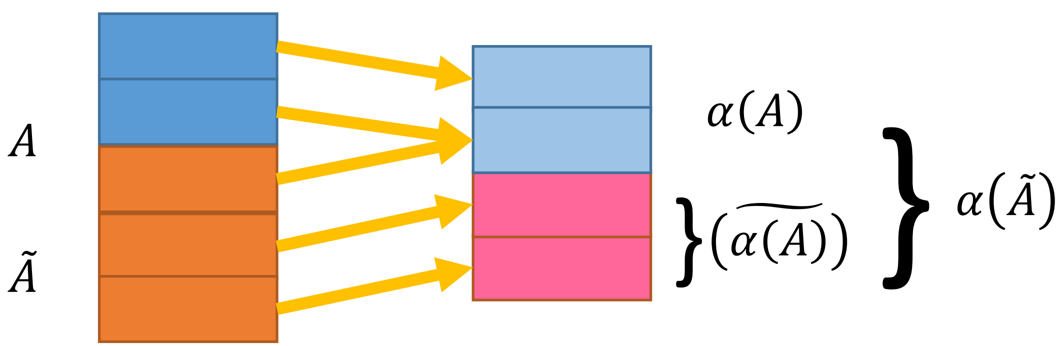
- 之前推导过程中可以看出阶不为3。
- 阶不为1：很简单
- 阶不为2：$a^2 + 2a + 1 \equiv (a^2 + a) + a + 1$

习题3.8

- 题目：令$\boldsymbol{\alpha}: \boldsymbol{S} \rightarrow \boldsymbol{T}, \boldsymbol{A}$是$\boldsymbol{S}$的子集，$\boldsymbol{A}$在$\boldsymbol{S}$中的补$\widetilde{\boldsymbol{A}} = \boldsymbol{S} - \boldsymbol{A}$。当$\boldsymbol{\alpha}$是单射或满射时，讨论$\boldsymbol{\alpha}\left(\widetilde{\boldsymbol{A}}\right)$和$\left(\widetilde{\boldsymbol{\alpha}(\boldsymbol{A})}\right)$的关系。
- 考察内容：集合的关系

$$\alpha(\tilde{A}) \subseteq (\widetilde{\alpha(A)})$$





$$(\widetilde{\alpha(A)}) \subseteq \alpha(\tilde{A})$$

习题3.8

- 严格证明：
- $\alpha(\tilde{A}) \subseteq \left(\widetilde{\alpha(A)}\right)$：任取$y \in \alpha(\tilde{A})$。设$y$的原像是$x$，则$x \in \tilde{A}$，即$x \notin A$。由于$\alpha$是单射，所以$y = \alpha(x) \notin \alpha(A)$，即$y \in \left(\widetilde{\alpha(A)}\right)$。
- $\left(\widetilde{\alpha(A)}\right) \subseteq \alpha(\tilde{A})$ ：任取 $y \in \left(\widetilde{\alpha(A)}\right)$，即$y \notin \alpha(A)$ 。由于α是满射，既然y不在A的像集里面，则一定在$\tilde{A}$的像集里，即 $y \in \alpha(\tilde{A})$。

习题3.12

- 设$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \end{pmatrix}$，$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix}$，求$\tau\sigma, \tau^2\sigma, \sigma^2\tau, \sigma^{-1}\tau\sigma$
- 考察内容：置换的运算
- $\sigma = (1\ 3\ 4\ 5\ 6\ 2), \tau = (1\ 2\ 4\ 3)(5\ 6)$
- $\tau\sigma = (1)(2)(3)(4\ 6)(5)$
- $\tau^2\sigma = (1\ 2\ 4\ 5\ 6\ 3)$
- $\sigma^2\tau = (1\ 3\ 4\ 5)(2\ 6)$
- $\sigma^{-1}\tau\sigma = (1\ 2\ 6\ 3)(4\ 5)$

习题3.12拓展：快速计算置换积

- $[(1\ 2)(3\ 4)][(1\ 3\ 4)(2)][(1\ 4)(2)(3)] = ?$

习题3.12拓展：快速计算置换积

- $[(1\ 2)(3\ 4)][(1\ 3\ 4)(2)][(1\ 4)(2)(3)] = (1$

习题3.12拓展：快速计算置换积

- $[(1\ 2)(3\ 4)][(1\ 3\ 4)(2)][(1\ 4)(2)(3)] = (1\ 2$
- $1 \rightarrow 4 \rightarrow 1 \rightarrow 2$

习题3.12拓展：快速计算置换积

- $[(1\ 2)(3\ 4)][(1\ 3\ 4)(2)][(1\ 4)(2)(3)] = (1\ 2)$

- $1 \rightarrow 4 \rightarrow 1 \rightarrow 2$
- $2 \rightarrow 2 \rightarrow 2 \rightarrow 1$

习题3.12拓展：快速计算置换积

- $[(1\ 2)(3\ 4)][(1\ 3\ 4)(2)][(1\ 4)(2)(3)] = (1\ 2)(3$

- $1 \rightarrow 4 \rightarrow 1 \rightarrow 2$
- $2 \rightarrow 2 \rightarrow 2 \rightarrow 1$

习题3.12拓展：快速计算置换积

- $[(1\ 2)(3\ 4)][(1\ 3\ 4)(2)][(1\ 4)(2)(3)] = (1\ 2)(3)$

- $1 \rightarrow 4 \rightarrow 1 \rightarrow 2$
- $2 \rightarrow 2 \rightarrow 2 \rightarrow 1$
- $3 \rightarrow 3 \rightarrow 4 \rightarrow 3$

习题3.12拓展：快速计算置换积

- $[(1\ 2)(3\ 4)][(1\ 3\ 4)(2)][(1\ 4)(2)(3)] = (1\ 2)(3)(4)$

- $1 \rightarrow 4 \rightarrow 1 \rightarrow 2$
- $2 \rightarrow 2 \rightarrow 2 \rightarrow 1$
- $3 \rightarrow 3 \rightarrow 4 \rightarrow 3$
- $4 \rightarrow 1 \rightarrow 3 \rightarrow 4$

第6次作业

- 作业编号：
- 习题5　　7，9，16，20

习题5.7

- **题目：如果群G中只有一个2阶元$\boldsymbol{a}$，那么$\boldsymbol{a}$与$\boldsymbol{G}$中任意元素都是交换的，即$\forall \boldsymbol{x} \in \boldsymbol{G}, \boldsymbol{a} * \boldsymbol{x} = \boldsymbol{x} * \boldsymbol{a}$.**
- 考察内容：群论中阶的定义

- 观察到$(x^{-1} * a * x)^2$
$$= (x^{-1} * a * x) * (x^{-1} * a * x) = \mathrm{e}$$
- $x^{-1} * a * x = a$（得证）或$x^{-1} * a * x = e$（不可能）

习题5.9

- $\boldsymbol{H}$是群$\boldsymbol{G}$的非空子集，$<\boldsymbol{H},*>$是$<\boldsymbol{G},*>$的子群当且仅当$\forall \boldsymbol{a},\boldsymbol{b}\in \boldsymbol{H},\boldsymbol{a}*\boldsymbol{b}'\in \boldsymbol{H}$
- 考察内容：子群的性质与证明

- （必要性）$b\in H$，则$b'\in H$（存在逆元），则$a*b'\in H$（运算封闭）

- （充分性）利用子群定义。（没有说集合有限，因此不可用定理5.9）

习题5.9

- （充分性）利用子群定义。（没有说集合有限，因此不可用定理5.9）
- $\forall a, b \in H, e = a * a' \in H,$
- $a' = e * (a)' \in H$（逆元）
- $a * b = a * (b')' \in H$（运算封闭）

习题5.16

- 证明：只有一个生成元的循环群至多含有两个元素。
- 考察内容：循环群、生成元

- 设生成元是g，若$g = e$，则$G = \{e\}$，一个元素
- 若$g \neq e$，则g的逆元g^{-1}也是生成元。由于生成元只有一个，则$g = g^{-1}$，即g的阶为2，此时$G = \{g, g^2 = e\}$

习题5.20

- **题目：A_4是全体4元偶置换构成的群，请列出它的全部元素。**
- 考察内容：置换的奇偶性

- 对换是奇置换，所以偶置换是含有偶数个对换的置换。
- (1)(2)(3)(4), (1 2 3), (1 3 2), (1 2 4), (1 4 2), (1 3 4), (1 4 3), (2 3 4), (2 4 3), (1 2)(3 4), (1 3)(2 4), (1 4)(2 3)

第9次作业

- 作业编号：
- 习题6　　15，16，18，20

习题6.15

- 题目：令$\boldsymbol{G}=\{\boldsymbol{A}|\boldsymbol{A}\in(\boldsymbol{Q})_{\boldsymbol{n}},|\boldsymbol{A}|\neq\mathbf{0}\}$, $\boldsymbol{G}$对于矩阵乘法构成群。$\boldsymbol{f}:\boldsymbol{G}\rightarrow\mathbf{R}^{*}$, $\boldsymbol{f}(\boldsymbol{A})=|\boldsymbol{A}|$证明：$\boldsymbol{f}$是从群$\boldsymbol{G}$到非零实数乘群$\boldsymbol{R}^{*}$的同态映射。求$\boldsymbol{f}(\boldsymbol{G})$和$\mathbf{Ker}\,\boldsymbol{f}$.
- 考察内容：同态关系、核

- $f(A*B)=|A*B|=|A|\cdot|B|=f(A)\cdot f(B)$
- $f(G)=\boldsymbol{Q}^{*}$
- $\mathrm{Ker}\,f=\{\boldsymbol{A}|\,|\boldsymbol{A}|=1\}$

习题6.16

- 题目：$\boldsymbol{G}$是交换群，$\boldsymbol{k}$是取定的正整数。$\boldsymbol{f}: \boldsymbol{G} \to \boldsymbol{G}, \boldsymbol{f}(\boldsymbol{a}) = \boldsymbol{a}^{\boldsymbol{k}}$.证明：$\boldsymbol{f}$是同态映射，求出$\boldsymbol{f}(\boldsymbol{G})$和$\mathbf{Ker}\,\boldsymbol{f}$。
- 考察内容：同态关系、核

- $f(a*b) = (a*b)^k = a^k * b^k = f(a)*f(b)$
- $f(G) = \{a^k | a \in G\}$
- $\mathrm{Ker}\, f = \{a \in G | a^k = e\}$

习题6.18

- 题目：$\boldsymbol{H}$是$\boldsymbol{G}$的正规子群，$[\boldsymbol{G}:\boldsymbol{H}] = \boldsymbol{m}$. 证明：对于$\boldsymbol{G}$中的任意元素$\boldsymbol{x}$，$\boldsymbol{x^m} \in \boldsymbol{H}$
- 考察内容：指数，正规子群，代表元

- 证明：考虑商群G/H。
- $[G:H] = m$意味着G/H的阶为m
- 根据推论6.1，G/H中任意元素Hx的阶是m的因子，所以$(Hx)^m = e = H$（单位元指G/H的）
- 所以$x^m \in H$

习题6.20

题目：在群G中，a, b是G中的元素，称$a' * b' * a * b$为G的换位元。证明：

(1) G的所有有限个换位元乘积构成G'，G'是G的正规子群。

(2) G/G'是交换群

(3) 若N是G的正规子群且G/N是交换群，那么G'是N的子群。

考察内容：正规子群、商群

习题6.20

(1) G的所有有限个换位元乘积构成G'，G'是G的正规子群。

- 先证明G'是群：封闭性、结合律、单位元、逆元
- G'是正规子群：$\forall g \in G, h = a' * b' * a * b \in G'$,
- $g' * h * g = g' * a' * b' * a * b * g$
  $= g' * a' * g * g' * b' * g * g' * a * g * g' * b * g$

$= (g' * a * g)' * (g' * b * g)' * (g' * a * g) * (g' * b * g) \in G'$

可类推h是多个换位元乘积时情况。

习题6.20

(2) G/G'是交换群

- 证明：任取$G'a, G'b \in G/G'$，则
- $G'a * G'b$
$= G'a * b$
$= G'a * b * (b' * a' * b * a)$
$= G'b * a$
$= G'b * G'a$

习题6.20

(3) 若N是G的正规子群且G/N是交换群，那么G'是N的子群。

- 只需证明G'是N的子集。任取元素$h \in G'$
- 对于一个换位元的简单情况$h = a' * b' * a * b$，由于G/N是交换群，所以$a * b \equiv b * a (mod\ N)$
- 所以$a' * b' * a * b \equiv e (mod\ N)$，即$h \in N$。
- 对于由多个换位元构成的元素h^*，由于N的运算封闭，所以一定有$h^* \in N$。

第12次作业

- 习题编号：

- 习题7 16，22
- 习题8 3，6

习题7.16

- 题目：$Q[x]$是有理数域Q上的一元多项式环，证明$(2, x)$是$Q[x]$的主理想。

- 考察内容：多项式主理想环。

- 证明：$(2, x)$是$Q[x]$上的理想（利用定义）
- 结合定理7.12，所以$(2, x)$是主理想

习题7.22

- 证明：$(3)/(6)$是$Z/(6)$的理想，并且
$$\frac{Z/(6)}{(3)/(6)} \cong Z/(3)$$

- 考察内容：环同态定理

- 证明：见书$P123$定理7.16

习题8.3

- 证明：在格中，如果$a \leq b, c \leq d$，则有$a * c \leq b * d$.

- 考察内容：格的基本性质

- 证明：$a * c \leq b * c \leq b * d$

习题8.6

- $<A,\leq>$ 为格。A中的元素$a,b,a<b.$ 令
$$B=\{x|x\in A且a\leq x\leq b\}$$
证明：$<B,\leq>$是格。

- 考察内容：格的定义

1. B是部分序集

2. B是格（最大下界和最小上界）

习题8.6

- 任取$x, y \in B$，即$a \leq x \leq b$且$a \leq y \leq b$，要证明，B中存在$x * y$和$x \oplus y$。
- 逻辑上要注意的点：（以最大下界为例）

1.A中的$x * y$一定在B中吗？

2.如果在，则A中的这个$x * y$元素仍然是B中x和y的最大下界吗？

3.如果不在，那么显然a是x, y的一个下界，那么为什么一定有最大下界？