

第5章 群

计算证明

1. 判断下列函数关系中哪些是函数？哪些是满射？哪些是单射？对于其中的每一个函数写出逆函数.

(1) $f_1: \mathbb{Z}^+ \rightarrow \mathbb{Z}^+, f_1(x) = x^2 + 1;$

(2) $f_2: \mathbb{Z}^+ \cup \{0\} \rightarrow \mathbb{Q}, f_2(x) = \frac{1}{x};$

(3) $f_3: 1, 2, 3 \rightarrow \alpha, \beta, \gamma, f_3 = \{ \langle 1, \alpha \rangle, \langle 2, \beta \rangle, \langle 3, \gamma \rangle \}$

2. 给定实数域上的 n 阶方阵 \mathbf{A} , \mathbf{T} 为实数域上的任意 n 阶方阵, 证明: 映射 $f: \mathbf{T} \mapsto \mathbf{AT}$ 是单射当且仅当 $\det(\mathbf{A}) \neq 0$.

3. 给定任意集合 S , 定义 2^S 为所有 S 子集构成的集合, 称为 S 的幂集 (有时也记作 $\rho(S)$, 如取 $S = \{1, 2\}$, 则幂集 $2^S = \rho(S) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$), 证明:

(1) $(2^S, \cup)$ 和 $(2^S, \cap)$ 为半群;

(2) 若对 S 的子集定义运算 $A \Delta B = (A \setminus B) \cup (B \setminus A)$, 则 $(2^S, \Delta)$ 为群. (明确: $A \setminus B = \{x | x \in A \wedge x \notin B\}$)

4. 设群中每个非幺元的阶为2, 证明该群是Abel群.

5. 设 H 是 \mathbb{Z} 的子群, 证明必定存在整数 m 使得 $H = m\mathbb{Z}$.

6. 证明群 G 不能写成两个真子群的并.

nmd, 唯一一阶子群必是正规子群

7. 设 G 是群, $a \in G$, $\langle a \rangle$ 是 G 中唯一的二阶子群, 证明对 $\forall x \in G$, 有 $ax = xa$.

8. 设 G 为交换群. 幺元为 e . 定义 G 中的扭元为满足 $g^n = e (n \in \mathbb{Z}^+)$ 的元素 g , 扭元集合为 $G_{tor} = \{g \in G | \exists n \in \mathbb{Z}^+, g^n = e\}$. 证明 G_{tor} 是 G 的正规子群.

9. 设 G 是一个群, $N \triangleleft G$, $H < G$, $HN = \{hn | h \in H, n \in N\}$ (符号表示的含义与教材保持一致). 证明 H 与 HN/N 之间存在满同态映射.

10. 在DES分组对称加密算法的设计中，首先对分组的明文执行初始置换，初始置换是通过IP置换矩阵实现的. IP的定义如下:

$$IP = \begin{bmatrix} 58 & 50 & 42 & 34 & 26 & 18 & 10 & 2 \\ 60 & 52 & 44 & 36 & 28 & 20 & 12 & 4 \\ 62 & 54 & 46 & 38 & 30 & 22 & 14 & 6 \\ 64 & 56 & 48 & 40 & 32 & 24 & 16 & 8 \\ 57 & 49 & 41 & 33 & 25 & 17 & 9 & 1 \\ 59 & 51 & 43 & 35 & 27 & 19 & 11 & 3 \\ 61 & 53 & 45 & 37 & 29 & 21 & 13 & 5 \\ 63 & 55 & 47 & 39 & 31 & 23 & 15 & 7 \end{bmatrix}$$

- (1) 查阅资料，对IP置换的含义进行说明；
- (2) 对分组后得到的64 bit数据：507239AA7EA3B82E，进行IP置换后得到的数据（同样使用十六进制表示）；
- (3) 求IP置换的逆元 IP^{-1} （以同样的矩阵的形式给出）；
- (4) *(选做，不算分)考虑C/C++编程实现对数据的分组和初始置换等.