NIS2312-1 Spring 2021-2022

信息安全的数学基础 (1)

Answer 2

2022 年 3 月 7 日

Problem 2

2 实际上是一个复数集合, 因为复数集合在乘法运算下去掉 0 才构成群, 所以此题不构成群.

4 注意到 $xS = Sx$ 仅仅能得到集合之间的相等关系, 也就是

$$xS = Sx \Rightarrow xa = bx, where\ a, b \in S$$

证明：如果集合 S 属于群 G, 那么 $N(S) \leq G$. 首先, 因为 $eS = Se$, 所以 $N(S)$ 不是空集. 然后假设 $a, b, c \in S$, 所以我们有

$$abS = a(bS) = a(Sb) = (aS)b = S(ab),$$

意味着 $ab \in S$. 并且, 还有

$$c^{-1}Sc = c^{-1}cS = S \Rightarrow c^{-1}S = Sc^{-1},$$

所以 $N(S) \leq G$.

5 不构成群, 因为运算不满足封闭性: 大家关于封闭性的证明都不严谨, 此证明需要的背景知识大家在此书中不学习, 在此仅给出反例 (需要线代的部分知识).

举例:

Let f be a polynomial in x, g be a polynomial in y and h be a polynomial in x, y, all with rational coefficients. Denote $m(f, g, h) = \begin{pmatrix} 1 & f(x) & h(x,y) \\ 0 & 1 & g(y) \\ 0 & 0 & 1 \end{pmatrix}$, and let G be the set of all such matrices. It's easy to verify G is a group under the matrix multiplication with the inverse of $m(f, g, h)$ is $m(-f, -g, -h + fg)$. Then commutator $[m(f_1, g_1, h_1), m(f_2, g_2, h_2)]$ is $[m(0, 0, f_1g_2 - f_2g_1)]$. Thus, we observe that $m(0,0,\sum a_{ij}x^iy^j) = \prod[m(a_{ij}x^i,0,0), m(0,y^j,0)]$ and $m(0,0,h_1)m(0,0,h_2) = m(0,0,h_1+h_2)$.

So let n be a positive integer and $h(x,y) = \sum_{i=0}^{2n+1} x^iy^i$. We confirm that $m(0,0,h)$ cannot be the product of n commutators. Otherwise, suppose

$$h(x,y) = \sum_{j=1}^{n} f_j(x)g_j(y) - h_j(x)k_j(y).$$

Write $f_j = \sum_i a_{ij}x^i$ and $h_j(x) = \sum_i b_{ij}x^i$ and from the coefficients of $1, x, \ldots, x^{2n+1}$ we have

$$\sum_{j=1}^{n} a_{ij}g_j(y) - b_{ij}k_j(y) = y^i \quad i = 1, \ldots, 2n+1.$$

Therefore we have $2n$ polynomials in y to generate $2n+1$ linear independent y^i, which is a contradiction.

6 注意使用书上的结论: 群 G 的任何子群的交集是子群.

Problem 4

因为 $e \in \bigcup_{i=1}^{\infty} H_i$, 此集合不是空集. 假设 $a \in H_j \subseteq \bigcup_{i=1}^{\infty} H_i$ 和 $b \in H_k \subseteq \bigcup_{i=1}^{\infty} H_i$, 不失一般性的可以假定 $j \leq k$, 因此有 $a \in H_j \leq H_k$, 又注意到 $b^{-1} \in H_k$, 所以有 $ab^{-1} \in H_k \subseteq \bigcup_{i=1}^{\infty} H_i$, 故证得是子群.

Problem 5

假设 $H \neq \{0\}$, 所以存在 $x = a/b \in H$, 其中 a, b 为整数, 因此有 $a = bx = \underbrace{x + x + \cdots + x}_{\text{b times}} \in H$. 得到 $1/a \in H$, 再使用同样的方法可以确定 $1 \in H$.

那么 $\mathbf{Z} \subseteq H$. 取 $\mathbf{Q}$ 中任意数 p/q 其中 p, q 是整数, 所以 $q \in \mathbf{Z} \subseteq H$, 同时也有 $1/q \in H$. 因此

$$\frac{p}{q} = \underbrace{\frac{1}{q} + \cdots + \frac{1}{q}}_{\text{p times}} \in H.$$

所以证得 $\mathbf{Q} \subseteq H$, 故 $H = \mathbf{Q}$.