

上海交通大学试卷 (A 卷)

(2021 至 2022 学年 第 2 学期)

班级号 NIS2312 课程名称 信息安全的数学基础 (1)

1. (15 分) 设 X 是一个非空集合, $\mathcal{P}(X)$ 是由 X 的全部子集构成的集合。定义 $A, B \in \mathcal{P}(X)$ 的加法如下

$$A + B = (A - B) \cup (B - A),$$

其中 $A - B = \{c \in X | c \in A, c \notin B\}$ 。证明 $\mathcal{P}(X)$ 关于上述加法运算构成群。

2. (15 分) 利用群同态基本定理证明 $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$, 其中 \mathbb{Z} 是整数集, m 是任意一个正整数, \mathbb{Z}_m 是 m 次剩余类构成的加法群。

3. (20 分) 证明:

(1) 设 H 是群 G 的子群, 如果对任意 $x \in G$ 都有 $x^2 \in H$, 试证 $H \triangleleft G$; (10 分)

(2) 设 $N \triangleleft G$ 且 g 是群 G 中的任意一个元素。若元素 g 的阶 $\text{ord}(g)$ 和商群 G/N 的阶互素, 试证 $g \in N$ 。(10 分)

4. (15 分) 已知 $I = \langle 10 \rangle, J = \langle 15 \rangle$ 都是整数环 \mathbb{Z} 的理想, 求以下理想的生成元:

(1) $I + J$; (7 分)

(2) $I \cap J$ 。(8 分)

5. (15 分) 设 R 是一个有单位元的交换环, I, J 是 R 的两个理想, 满足 $I + J = R$ 。证明:

(1) $\phi: R \rightarrow R/I \times R/J, \phi(r) = (r + I, r + J)$ 是环同态映射; (7 分)

(2) 利用环同态基本定理证明 $R/I \cap J \cong R/I \times R/J$ 。(8 分)

6. (20 分) 设 P 是交换环 R 的一个真理想, 那么 P 是 R 的素理想的充分必要条件是: 对任意两个理想 I, J , 如果有 $IJ = \{\sum_{i=1}^n x_i y_i | n \in \mathbb{N}^+, x_i \in I, y_i \in J\} \subseteq P$, 则有 $I \subseteq P$ 或者 $J \subseteq P$ 。设 R 是整环, 证明:

(1) 若 $\langle p \rangle$ 是 R 的非零极大理想, 则 p 是不可约元; (10 分)

(2) p 是素元当且仅当 $\langle p \rangle$ 是 R 的非零素理想。(10 分)