NIS2312-1 Spring 2021-2022

信息安全的数学基础 (1)

Final Exam

2022 年 6 月 13 日

Problem 1

假设 X 是一个非空集合, $\mathcal{P}(X)$ 是集合 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 $A - B = \{c \in X \mid c \in A, c \notin B\}$. 证明 $\mathcal{P}(X)$ 关于上述的加法运算构成群.

Problem 2

试证:

1. 群 G 的指数为 2 的子群 N 一定是 G 的正规子群;
2. 设 M, N 是群 G 的正规子群, 如果 $M \cap N = \{e\}$, e 是群 G 的单位元, 则对任意 $a \in M, b \in N$ 有 $ab = ba$.

Problem 3

1. 设 $N \triangleleft G$ 且 g 是群 G 中的任意一个元素. 若元素 g 的阶 $\mathrm{ord}(g)$ 和商群的阶 $|G/N|$ 互素, 试证 $g \in N$;
2. 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 是群 G 的正规子群.

Problem 4

设 R, S 是两个非零环, 证明 $R \times S$ 不可能是域.

Problem 5

设 R, S 是交换环, $f : R \to S$ 是环同态, I, J 分别是 R, S 的理想, 令 $\sqrt{I} = \{r \in R \mid$ 存在 $n \in \mathbf{Z}^+$ 使得 $r^n \in I\}$ 求证:

1. $f(\sqrt{I}) \subset \sqrt{f(I)}$;
2. $\sqrt{f^{-1}(J)} = f^{-1}(\sqrt{J})$.

Problem 6

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 $IJ \subseteq P$, 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;
2. p 为素元当且仅当 $\langle p \rangle$ 是 R 的非零素理想.