NIS2312-01 Fall 2023-2024

信息安全的数学基础 (1)

Midterm Exam

2023 年 11 月 10 日

问题一

假设 $p > 3$ 是一个素数. 考虑乘法群 $G = \mathbb{Z}_p^*$:

(1) 证明集合 $S = \{x^2 : x \in G\}$ 是群 G 的子群;

(2) 计算指数 $[G : S]$;

(3) 如果 $-1 \notin S$, 证明对任意 $a \in G$, 有 $a \in S$ 或者 $-a \in S$.

问题二

设 R 是一个没有单位元的环, 证明: 存在一个有单位元的环 R', 使 R 为 R' 的子环.