

NIS2312-1 2022-2023 Fall

信息安全的数学基础 (1)

Assignment 20

2022 年 12 月 19 日

Problem 1

将 $x^3 + 2x + 1 \in \mathbb{Z}_3[x]$ 写成 \mathbb{Z}_3 的某个扩域中的一次因式的乘积.

Problem 2

求 $x^4 - x^2 + 1$ 在 \mathbb{Z}_3 上的分裂域.

Problem 3

求 $f(x) = x^3 + x + 1$ 在 \mathbb{Z}_2 上的分裂域, 并将 $f(x)$ 在该分裂域上分解为一次因式的乘积.