NIS2312-01 Fall 2023-2024

信息安全的数学基础 (1)

Assignment 12

2023 年 10 月 27 日

Problem 1

假设 D 是一个有理数且不是完全平方数, 定义集合

$$\mathbf{Q}(\sqrt{D}) = \{a + b\sqrt{D} \mid a, b \in \mathbf{Q}\}.$$

那么集合 $\mathbf{Q}(\sqrt{D})$ 在通常数的加法乘法的运算下是否构成环, 如果构成环是否构成 $\mathbf{C}$ 的子环?

Problem 2

证明在任意无零因子有单位元的有限交换环中, 非零元素均是单位 (本质上是证明有限整环是域).

Problem 3

如果一个元素 $x \in R$ 满足等式 $x^n = 0, n \in \mathbf{Z}^+$, 那么称其幂零元 (简单的例子是线性代数中的幂零矩阵). 证明: 在交换环 R 中, 有 $x \in R$ 是幂零元, 那么:

(1) x 不是零元素就是零因子;

(2) rx 仍然是幂零元, 其中 $r \in R$;

(3) $1+x$ 是单位 (hint: 构造系数在 R 上的多项式 $f(x)$ 使得 $(1+x)f(x) = 1+g(x^n) = 1$ 即可).

Problem 4

证明: 如果环 R 的元素满足 $r^2 = r$, 其中 $r \in R$, 那么 R 是一个交换环 (hint: $r = x + y$ where $x, y, r \in R$ or $2xy = 0$ for all $x, y \in R$).