NIS2312-1 2022-2023 Fall

信息安全的数学基础 (1)

Answer 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.

解: 设 α 为 x^3+2x+1 在 $\mathbb{Z}_3$ 某个扩域 E 上的根, 那么可以发现, $(\alpha+1)^3+2(\alpha+1)+1=0$ 仍然成立, 所以, 我们有 $x^3+2x+1=(x-\alpha)(x-(\alpha+1))(x-(\alpha+2))$.

Problem 2

求 x^4-x^2+1 在 $\mathbb{Z}_3$ 上的分裂域.

解: 有 $x^4-x^2+1=x^4+2x^2+1=(x^2+1)^2$, 故其分裂域使 x^2+1 可以分解, 显然有 $x^2+1=(x+\mathrm{i})(x-\mathrm{i})$, 则分裂域为 $\mathbb{Z}_3[\mathrm{i}]$.

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.

解: 显然 $f(x)$ 在 $\mathbb{Z}_2$ 上是不可约的, 设 α 为 x^3+x+1 在 $\mathbb{Z}_3$ 某个扩域 E 上的根, 那么 α^2 也是 $f(x)=0$ 的根: $f(\alpha^2)=\alpha^6+\alpha^2+1=(\alpha^3+\alpha+1)^2=0$, 同理 α^4 也是根. 同时 α, α^2 和 α^4 均不相同, 所以 $f(x)$ 在 $\mathbb{Z}_2$ 上的分裂域为 $\mathbb{Z}_2(\alpha)$, 此外, 可以根据 $\alpha^3+\alpha+1=0$ 得到 $\mathbb{Z}_2(\alpha) \cong \mathbb{F}_{2^3}$.