NIS2312-01 Fall 2023-2024

信息安全的数学基础 (1)

Answer 18

2023 年 12 月 8 日

证明: 多项式 $x^4+x^2+1\in\mathbb{Q}[x]$ 在有理数域 $\mathbb{Q}$ 上的分裂域是 $\mathbb{Q}[\sqrt{-3}]$.

解: 分解等式有

$$x^4+x^2+1=(x^2+x+1)(x^2-x+1),$$

因此多项式的根是

$$x=\frac{\pm1\pm\sqrt{-3}}{2}.$$

故分裂域 F 必定是 $\mathbb{Q}[\frac{\pm1\pm\sqrt{-3}}{2}]=\mathbb{Q}[\sqrt{-3}]$ 的子域. 又因为 $f(x)=x^2+3$ 是 $\mathbb{Q}$ 上的次数最低的不可约多项式, 故 $\left[\mathbb{Q}[\sqrt{-3}]:\mathbb{Q}\right]=2$, 因此有

$$\left[\mathbb{Q}[\sqrt{-3}]:\mathbb{Q}\right]=\left[\mathbb{Q}[\sqrt{-3}]:F\right][F:\mathbb{Q}]=2,$$

因为 $F\neq\mathbb{Q}$, 则 $[F:\mathbb{Q}]\geq2$, 故分裂域 $F=\mathbb{Q}[\sqrt{-3}]$.