NIS2312-01 Fall 2023-2024

信息安全的数学基础 (1)

Assignment 19

2023 年 12 月 15 日

Problem 1

设 α 是 $\mathbb{F}_{2^4}$ 的一个本原元, 且 α 是 $x^4+x+1 \in \mathbb{F}_2[x]$ 在 $\mathbb{F}_{16}$ 上的一个根. 计算 $\mathbb{F}_{2^4}^*$ 中全部元素的极小多项式, 并把 $x^{15}-1$ 分解成 $\mathbb{F}_2$ 上的不可约多项式的乘积.

Hint: 将有限域元素进行划分, 划分的依据为是同一个极小多项式的根; 考虑不同 (同一个) 极小多项式的根的关系, 用于计算极小多项式.

解: 如果 α 是 $x^4+x+1 \in \mathbb{F}_2$ 在 $\mathbb{F}_{16}$ 上的一个根, 那么 α^2 也是根:

$$\alpha^4+\alpha+1=0 \Rightarrow (\alpha^2)^4+(\alpha^2)+1=(\alpha^4+\alpha+1)^2=0.$$

同理 α^4, α^8, 故如果 f 是 α 的极小多项式, 那么 f 也是 $\alpha^2, \alpha^4, \alpha^8, \ldots$ 的极小多项式. 因此有划分

$$\begin{aligned}
&\alpha^0\\
&\alpha, \alpha^2, \alpha^4, \alpha^8\\
&\alpha^3, \alpha^6, \alpha^{12}, \alpha^9\\
&\alpha^5, \alpha^{10}\\
&\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}.
\end{aligned}$$

1. 显然 $\alpha^0=1$ 的极小多项式是 $x+1$;

2. 注意到 x^4+x+1 是 $\mathbb{F}_2$ 上的不可约多项式: (之前的作业有直接指出) 或者: x^4+x+1 显然无法被一次不可约多项式 $\{x, x+1\}$ 整除, 同时也无法被二次不可约多项式 x^2+x+1 整除, 故是一个不可约多项式. 注意到 x^4+x+1 在 $\mathbb{F}_{2^4}$ 上的一个根是 α, 则 $\alpha, \alpha^2, \alpha^4, \alpha^8$ 对应的极小多项式为 x^4+x+1; 又因为 $\alpha^{14}, \alpha^{13}, \alpha^{11}, \alpha^7$ 是 $\alpha, \alpha^2, \alpha^4, \alpha^8$ 的逆, 故其极小多项式是互反的, 即 x^4+x^3+1;

   互反多项式: 设 $f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n$, 则 $f(x)$ 的互反多项式为

   $$f^*(x)=a_n+a_{n-1}x+a_{n-2}x^2+\cdots+a_0x^n=x^nf(x^{-1}),$$

3. α^5, α^{10} 的极小多项式次数为 2, 所以只能是 x^2+x+1 (因为只有 $\mathbb{F}_2$ 上的 2 次不可约多项式只有这一个);

4. $\alpha^3, \alpha^6, \alpha^{12}, \alpha^9$ 本身是互反的 $(\alpha^3 * \alpha^{12} = 1, \alpha^6 * \alpha^9 = 1)$, 故其极小多项式是自反的, $\mathbb{F}_2$ 上 4 次自反多项式只有 $x^4+x^3+x^2+x+1$ 和 $x^4+x^2+1=(x^2+x+1)^2$, 故极小多项式为 $x^4+x^3+x^2+x+1$.

上述极小多项式的根的集合恰好是 $\mathbb{F}_{2^4}^*$, 故 $x^{15}-1$ 的分解就是上述极小多项式的乘积

$$x^{15}-1=(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1).$$