NIS2312-1 2022-2023 Fall

信息安全的数学基础 (1)

Answer

2022 年 12 月 19 日

1

本次考试共有 6 道证明题, 共 $15 \times 4 + 20 \times 2 = 100$ 分, 其中 20 分的题会有 2/3 道小题, 15 分的题是相对基础的题.

考试知识点:

(1) 集合、等价关系、映射、群的定义、子群的判定、循环群、置换群、群的阶、群元素的阶、陪集、拉格朗日定理、正规子群、商群、同态、同构、同态基本定理、直积、直和;

(2) 环的定义、子环的判定、理想、商环、极大理想、素理想、单位、零因子、整环、多项式环、多项式的根;

(3) 域的定义、素域、扩域、有限域的结构、有限域的阶、有限域的乘法群、有限域的存在、唯一性

Problem 1

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

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, 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

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

显然 $\alpha^0 = 1$ 的极小多项式是 $x + 1$;

因为 x^4+x+1 在 $\mathbb{F}_2$ 上没有根, 在 $\mathbb{F}_4$ 上也没有根 (因为 x^2+x+1 不整除 x^4+x+1), 故 $x^4 + x + 1$ 是不可约多项式. 注意到 f 在 $\mathbb{F}_{16}$ 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 $\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}$ 是 $\alpha, \alpha^2, \alpha^4, \alpha^8$ 的逆, 故其极小多项式是互反的, 即 $x^4 + x^3 + 1$;

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一个);

$\alpha^3, \alpha^6, \alpha^{12}, \alpha^9$ 本身根是互反的 ($\alpha^3 * \alpha^{12} = 1, \alpha^6 * \alpha^9 = 1$), 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

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

Problem 2

有限域的例题 (仅给出部分例题, 考试绝对不会出现原题): 分解 $x^{p^n-1} - 1$, 解题方法如上;

写出乘法表, 习题已经做过了;

构造一个 p^n 阶有限域, 并找出乘法群的生成元: 构造方法 $\mathbb{F}_p[x]/ < f >$, 其中 f 是次数为 n 的首一不可约多项式, 乘法群的生成元就是寻找阶为 $p^n - 1$ 的元素;

证明多项式为 $\mathbb{F}_p$ 上的不可约多项式: 一般是反证;

有限域上的多项式的根: $x^3 + 2x + 1$ 在 $\mathbb{F}_3$ 上如果有根 α, 那么 $\alpha + 1$ 也是根: $(x + 1)^3 + 2(x + 1) + 1 = x^3 + 1 + 2x + 2 + 1 = 0$, 同理 $\alpha + 1 + 1$ 也是根.