Math 835 Homework 5

Theo Koss

October 2024

Chapter 13

Section 5

2. Find all irred. polynomials of degree 1, 2, and 4 over $\mathbb{F}_2$ and prove their product is $x^{16} - x$

   - Degree 1: x and $x + 1$.
   - Degree 2: $x^2 + x + 1$.
   - Degree 4: $x^4 + x^3 + x^2 + x + 1$, $x^4 + x^3 + 1$, $x^4 + x + 1$.

   Product:

$$x(x+1)(x^2+x+1)(x^4+x^3+x^2+x+1)(x^4+x^3+1)(x^4+x+1)$$
$$= (x^4+x)(x^4+x^3+x^2+x+1)(x^4+x^3+1)(x^4+x+1)$$
$$= (x^8+x^7+x^6+x^3+x^2+x+1)(x^4+x^3+1)(x^4+x+1)$$
$$= (x^8+x^7+x^6+x^3+x^2+x+1)(x^8+x^7+x^5+x^4+x^3+x+1)$$
$$= (x^{16}+x) = (x^{16}-x)$$

3. Prove that d divides n iff $x^d - 1$ divides $x^n - 1$. Note that if $n = qd + r$ then $x^n - 1 = (x^{qd+r} - x^r) + (x^r - 1)$

   Proof. ($\implies$) Let $d \mid n$. Then $n = kd$ for some $k \in \mathbb{Z}$. We then have $x^n - 1 = x^{kd} - 1$. Let $y = x^d$ and substitute,

$$y^q - 1 = (y-1)(y^{q-1} + \cdots + y + 1)$$

So

$$x^n - 1 = (x^d - 1)(x^{dq-d} + x^{dq-2d} + \cdots + x^d + 1)$$

($\Longleftarrow$) Assume d does not divide n.

$$n = qd + r,\ r < d,\ r \neq 0$$

$$\begin{aligned} x^n - 1 &= (x^{qd+r} - x^r) + (x^r - 1) \\ &= x^r(x^{qd} - 1) + (x^r - 1) \end{aligned}$$

But x^d divides the first part, and not the second part. So we have $x^d - 1$ does not divide $x^n - 1$ contradiction. □

4. Let $a > 1$ be an integer. Prove for any positive integers n, d that d divides n if and only if $a^d - 1 \mid a^n - 1$ (cf. the previous exercise). Conclude in particular that $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$ if and only if $d \mid n$.

Proof. By above, the polynomial $x^d - 1 \mid x^n - 1$ iff $d \mid n$. So
($\Longrightarrow$) Let $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$ and $k \in \mathbb{F}_{p^d}$, then we have $k \in \mathbb{F}_{p^n}$. Then, the finite fields are determined by roots of $x^{p^d} - x$ and $x^{p^n} - x$ respectively. So k is a root of both $x^{p^d} - x$ and $x^{p^n} - x$, therefore

$$x^{p^d} - x \mid x^{p^n} - x \implies p^d \mid p^n \implies d \mid n$$

($\Longleftarrow$) Let $d \mid n$, then $n = dq$ for some $q \in \mathbb{Z}^+$. So

$$x^{p^d} - x \mid x^{p^{dq}} - x = x^{p^n} - x \implies \mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$$

□