MATH W4042 Prof. Deopurkar

Yichen Wang
yw2944

hw. 7

20/20

1. $\mathbb{F}_4^+ = \{a+bx \mid a, b \in \mathbb{Z}_2\} = \{0, 1, x, 1+x\}$

$1+1=2 \equiv 0$, $x+x = 2x \equiv 0$ $1+x+1+x = 2+2x \equiv 0$.

Each nonzero elt. has degree 2 in this group, so

5 $\mathbb{F}_4^+ \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, the klein-4 group ✓

2. By Thm. 15.7.3(6), $X^{16} - X = X^{2^4} - X$ splits as linear, quadratic, and quartic factors (irreducible) in $\mathbb{F}_2$.

$X^{16} - X = X(X+1)(X^2+X+1)(X^4+X+1)(X^4+X^3+1)(X^4+X^3+X^2+X+1)$ ✓

Similarly in $\mathbb{F}_2 < \mathbb{F}_{2^2} = \mathbb{F}_4$, the quadratic polynomial splits and quartic splits into quadratics: (say root of x^2+x+1 is α) ✓

$X^{16} - X = X(X+1)(X+1+\alpha)(X+\alpha)(X^2+X+\alpha)(X^2+X+\alpha+1)(X^2+\alpha X+1)(X^2+\alpha X+\alpha)$

In $\mathbb{F}_{2^3} = \mathbb{F}_8$, neither of quartic and quadratic split further, also by 15.7.3(6). so the factorization is the same as

5 in $\mathbb{F}_2$ ✓

$\cdot (X^2+(\alpha+1)X+\alpha(\alpha+1)) \cdot (X^2+(\alpha+1)X+1)$

3. $|K^\times| = q-1 = p^k - 1$ for some prime p and positive integer k. suppose the generator of $K^\times$ is α, then the product of all nonzero elt is

5 $1 \cdot \alpha \cdot \alpha^2 \cdot \alpha^3 \cdot \cdots \alpha^{q-2} = \alpha^{\frac{(q-1)q}{2}}$.

$(\alpha^{\frac{(q-1)q}{2}})^2 = (\alpha^{q-1})^q = 1$. ✓

$\alpha^{\frac{(q-1)q}{2}} = \pm 1$. $-1 = 1$.

case 1: K is of char 2: $-1 = 1$.

case 2: K is not of char 2: q is odd.

$\Rightarrow \frac{(q-1)q}{2} = \frac{(q-1)(2p+1)}{2} \bmod q-1 = (q-1)p + \frac{1}{2}(q-1) \bmod (q-1)$

$= \frac{q-1}{2} \bmod q-1 \Rightarrow \alpha^{\frac{(q-1)q}{2}} = \alpha^{\frac{q-1}{2}} \neq 1, = -1$.

4. Suppose $\exists\ G \subset K^*$ such that $|G| = n$ and G is not cyclic.

G is finite and abelian, but not cyclic

$\Rightarrow$ $G = \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_m}$ for some positive integers $d_1 | d_2 | d_3 \cdots | d_m$

$\Rightarrow$ $\forall\ g \in G$, $g^{d_m} = 1$, $d_m < n$.

$\Rightarrow$ but $x^{d_m} = 1$ has at most d_m solutions in K.

contradiction! ✓