Übungen zur Informationstheorie und Komplexität

Blatt 7

SS '98

Throughout the following exercises K denotes a finite field with $q = |K|$.

1. (a) Show $q = p^\nu$ (for some prime number p and $\nu \in \mathbb{N}_1$).

   (b) For $a \in K^*$ let $n = n(a) \in \mathbb{N}_1$ its order (the smallest number such that $a^n = 1$). Show that n divides $q-1$ (so: $a^{q-1} = 1$).

   (Hint: Use substructures !)

2. Let $f \in K[X]$ an irreducible polynomial of degree $m = \deg f > 1$. Show:

$$f \mid X^{q^m-1} - 1 \ .$$

   (Hint: Show that $K[X]/(f)$ is a field (the field of polynomials modulus (f)), using $f \mid g \cdot h \;\Rightarrow\; f \mid g \vee f \mid h$ for polynomials $g, h \in K[X]$.)

3. We specialize: Here $K = GF(2)$ denotes the field with $|K| = 2$. Show:

   (a) For polynomials $f \in K[X]$:

$$f \text{ has an even number of terms} \qquad \Leftrightarrow \qquad X + 1 \mid f \ .$$

   (b) $f(X)^{2^\nu} = f(X^{2^\nu})$ for $f(X) \in K[X]$ and $\nu \in \mathbb{N}_0$.

   (c) $X^4 + X + 1 \in K[X]$ is an irreducible polynomial.

   (d) $X^3 + X + 1 \mid X^7 + 1$ in $K[X]$.

Übung: Di 12^{30}-14, V2-216
Abgabe: bis 15.6.98 (Mo.)