Technische Universität Kaiserslautern

Fachbereich Mathematik
Wintersemester 2010/11

Mohamed Barakat
Simon Hampe

Cryptography
Homework assignment 7

Due date: Wednesday 15/12 at 13:45

Exercise 1.

(1) Let U be a finite Abelian group. Prove:

$$\max\{\operatorname{ord} g \mid g \in U\} = \operatorname{lcm}\{\operatorname{ord} g \mid g \in U\}.$$

(2) Prove Proposition 3.3.29:
Let K be a field and U a *finite* subgroup of K^*. Then U is cyclic.
(3) Show that the condition "finite" cannot be dropped in (2).

Exercise 2. Let $K \leq L$ be a finite field extension, i.e. with $[L : K] < \infty$. Denote by $\mathrm{Aut}_K(L)$ the group of all K-linear automorphisms of L, i.e. all field automorphisms $\varphi : L \to L$ which fix the elements of K: $\varphi(x) = x$ for all $x \in K$. Now let $f \in K[x]$ and $\varphi \in \mathrm{Aut}_K(L)$ arbitrary. Prove:

(1) $\varphi(f(\alpha)) = f(\varphi(\alpha))$ for all $\alpha \in L$.
(2) Is $\alpha \in L$ a root of f then so is $\varphi(\alpha)$. Hence, $\mathrm{Aut}_K(L)$ acts on the roots of α.

Exercise 3. Let $q = p^n$ and $K = \mathbb{F}_q$ the finite field with q elements and L a finite field extension. Consider the Frobenius map $\varphi : L \to L, x \mapsto x^q$. Prove:

(1) $\varphi \in \mathrm{Aut}_K(L)$.
(2) $\mu_{\alpha,K} = \mu_{\alpha^q,K}$ for all $\alpha \in L$.
(3) Let $f \in K[x]$ be an irreducible divisor of $x^{q^d} - x$. Then $\deg f \mid d$.
(4) Let $f \in K[x]$ be an irreducible polynomial over K of degree d and α a root of f in L. Then the d roots of f are $\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}$.

Exercise 4. The primitive polynomial $f := x^4 + x + 1$ over $\mathbb{F}_2$ can be used to construct the field $\mathbb{F}_{16} := \mathbb{F}_2[x]/\langle f \rangle$. Represent elements of $\mathbb{F}_{16}$ by their "4-bit" coefficient row vectors with respect to the basis $(1, \bar{x}, \bar{x}^2, \bar{x}^3)$, e.g. $1+\bar{x}^2$ is represented by 1010 as a shorthand for $(1, 0, 1, 0)$. Set $a := \bar{x} = 0100$. Since f is primitive we know that a is primitive.

(1) List all powers of a by giving their 4-bit representation in a table.

Use the table for the rest of the exercise:

(2) Compute (or lookup) a^{-1} and a^{-7}.
(3) Compute the orbits of the Frobenius automorphism $\varphi : \mathbb{F}_{16} \to \mathbb{F}_{16}, x \mapsto x^2$.
(4) Which elements of $\mathbb{F}_{16}$ are contained in $\mathbb{F}_4$.

(5) Group the elements of $\mathbb{F}_{16}$ with equal minimal polynomial over $\mathbb{F}_2$. What do you observe?
(6) Group the elements of $\mathbb{F}_{16}$ with equal minimal polynomial over $\mathbb{F}_4$.

Hint for (5) and (6): Use Exercise 3.(4).