

**THE JOHNS HOPKINS UNIVERSITY**  
**Faculty of Arts and Sciences**  
**3 Homework - FALL SESSION 2007**  
**110.617 - Number Theory**

1. Let  $k = \mathbb{F}_q$  ( $q = p^r$ ) be a finite field and let  $K = \mathbb{F}_{q^n}$  denote the extension of degree  $n$  of  $k$ .

Let  $\sigma \in \text{Gal}(K/k)$  be the Frobenius automorphism  $\sigma(x) = x^q$ .

Let denote by  $T(x)$  and  $N(x)$  respectively, the trace and norm, relative to the extension  $K/k$  of an element  $x \in K$ .

- (a) Show that the mapping  $T : K \rightarrow k$  is surjective  
 (b) Let  $\theta \in K$  be an element of the form  $\theta = x - \sigma(x)$  ( $x \in K$ ). Show that  $T(\theta) = 0$ .  
 Conversely, let  $\theta \in K$  be an element satisfying  $T(\theta) = 0$ ; set

$$x = \frac{1}{T(u)}(\theta\sigma(u) + (\theta + \sigma(\theta))\sigma^2(u) + \cdots + (\theta + \sigma(\theta) + \cdots + \sigma^{n-2}(\theta))\sigma^{n-1}(u))$$

(where  $u \in K$  is an element such that  $T(u) \neq 0$ ). Verify that  $\theta = x - \sigma(x)$  and that every  $x_1 \in K$  such that  $\theta = x_1 - \sigma(x_1)$  is of the form  $x_1 = x + \lambda$ , where  $\lambda \in k$ .

- (c) Let  $\theta \in K$  be an element of the form  $\theta = \frac{x}{\sigma(x)}$  (where  $x \in K$  is a non-zero element); show that  $N(\theta) = 1$ .

Conversely, let  $\theta \in K$  be an element such that  $N(\theta) = 1$ , show that there exists an element  $x \in K$  such that  $\theta = \frac{x}{\sigma(x)}$ . Verify that every element  $x_1 \in K$  such that  $\theta = \frac{x_1}{\sigma(x_1)}$  is of the form  $x_1 = \lambda x$ , for  $0 \neq \lambda \in k$ .

- (d) Show that the mapping  $N : K \rightarrow k$  is surjective.  
 (e) Assume  $n|(q-1)$ . Let  $\mu_n$  denote the subgroup of the  $n$ -th roots of unity of  $k^*$ . Let  $A = \{a \in K^* : a^n \in k^*\}$ .  $A$  is a multiplicative subgroup of  $K^*$  containing  $k^*$ . Denote by  $\varphi : A \rightarrow \mu_n$  the mapping defined by  $\varphi(a) = \frac{a}{\sigma(a)}$ . Verify that  $\varphi$  is a group homomorphism and induces an isomorphism:  $A/k^* \simeq \mu_n$   
 (f) Under the above assumption on  $n$ , let  $a \in A$  and let  $d$  be the order of  $\varphi(a) \in \mu_n$ . Show that  $[k(a) : k] = d$ . Determine the factorization of the polynomial  $X^n - a^n$  as a product of irreducible factors in  $k[X]$ .  
 (g) Show that the mapping  $\psi : A \rightarrow k^*$  defined by  $\psi(a) = a^n$  is a group homomorphism which induces an isomorphism  $A/k^* \simeq k^*/(k^*)^n$ . Show that every element of  $k$  is a  $n$ -th power of an element of  $K$ .

2. Let  $k$  be a field of characteristic  $p \neq 0$  and let  $\mathbb{F}$  be its prime subfield.. Let  $P(X) = X^p - X - a$ , where  $a \in \mathbb{F}$ .

- (a) Let  $\alpha$  be a root of  $P(X)$  in an algebraic closure of  $K$ . Express all the roots of  $P(X)$  as a function of  $\alpha$ .  
 (b) Assume  $P(X)$  to be irreducible on  $k$ . Let  $\alpha$  be a root of  $P(X)$ . Show that  $K = k(\alpha)$  is a cyclic extension of  $k$  of degree  $p$ .  
 (c) Let  $K$  be a cyclic extension of  $k$  of degree  $p$ . Show that there exists an element  $\alpha \in K$  such that  $K = k(\alpha)$ ,  $\alpha$  being a root of a polynomial  $P(X) = X^p - X - a$  (where  $a \in k$ ).

3. Let  $k$  be a non-Archimedean local field (that is a complete, non-Archimedean valued field with discrete valuation and finite residue field) and let  $K$  denotes a finite extension of  $k$ , furnished with the absolute value extending that of  $k$ , that is unramified. Let denote by  $\bar{k}$ , resp  $\bar{K}$  the residue fields.

- (a) Verify that  $[\bar{K} : \bar{k}] = [K : k]$

- (b)  $\bar{K}/\bar{k}$  is Galois, its Galois group is cyclic and generated by the element  $\sigma$  defined by:  $\sigma(c) = c^q$ , where  $q = \text{card}(\bar{k}) = p^r$ .
- (c) Show that  $K$  is a splitting field over  $k$  of the polynomial  $X^{q^n} - X$  and that there exists a root  $\xi$  of this polynomial such that  $K = k(\xi)$ . From this deduce that the extension  $K/k$  is Galois.
- (d) Show that the mapping  $\text{Gal}(K/k) \rightarrow \text{Gal}(\bar{k}/\bar{k})$  defined by  $\sigma \mapsto \bar{\sigma}$  is an isomorphism.
- (e) From the above question deduce that  $\text{Gal}(K/k)$  is cyclic and generated by the element  $\sigma^*$  determined uniquely by  $|\sigma^*(x) - x^q| < 1$ , for all  $x \in \mathcal{O}_K := \{x \in K : |x| \leq 1\}$ .