**Homework 3**

due on Friday, March ??

Solve the following problems.

**Problem 1.** Let $\mathbb{F}_p$ be a filed with $p$ elelemts, $p$ a prime. Consider the polynomial $f(x) = x^{p^n} - x + 1$ and let $L$ be its splitting field.

a) Prove that $L$ contains $\mathbb{F}_{p^n}$.

b) Prove that $[L : \mathbb{F}_{p^n}] = p$.

c) Prove that $f$ is irreducible over $\mathbb{F}_p$ iff either $n = 1$ or $n = p = 2$.

**Problem 2.** Let $K = \mathbb{F}_q$ be a finite field of order $q = p^n$ and let $K(u)/K$ be a simple transcendental extension. In the previous homework it was proved that $\Gamma = \mathrm{Aut}(K(u)/K)$ is isomorphic to $\mathrm{PGL}_2(K)$. Since $K$ is finite, $\Gamma$ is a finite group. Let $M = K(u)^\Gamma$.

a) Prove that $\Gamma$ has $q^3 - q$ elements.

b) Every $a \in K^\times$ defines an automorphism $\sigma_a$ in $\Gamma$ defined by $\sigma_a(u) = au$. Prove that all such automorphisms form a cyclic subgroup $\Gamma_m$ of $\Gamma$ of order $q - 1$. Prove furthermore that $K(u)^{\Gamma_m} = K(u^{q-1})$.

c) Every $c \in K$ determines an automorphism $\tau_c$ in $\Gamma$ defined by $\tau_c(u) = u + c$. Prove that all such automorphisms form a subgroup $\Gamma_a$ of $\Gamma$ of order $q$. Prove furthermore that $K(u)^{\Gamma_a} = K(u^q - u)$.

d) Prove that $\Gamma$ is generated by $\Gamma_m$, $\Gamma_a$ and the automorphism $\phi$ given by $\phi(u) = u^{-1}$. Prove that $K(u)^\Gamma = K(w)$, where $w = (u^{q^2} - u)^{q+1}/(u^q - u)^{q^2+1}$. Hint: Prove that $u$ is a root of the polynomial $((x^q - x)^{q-1} + 1)^{q+1} - w(x^q - x)^{q^2-q}$.

**Problem 3.** Let $K$ be a field and let $f \in K[x]$ be an irreducible polynomial of degree $n$. Let $L$ and $M$ be subfields of an algebraic closure of $K$ such that $L$ is the splitting field of $f$ over $K$ and $M/K$ is Galois. Let $u$ be a root of $f$ in $L$. Prove that in $M[x]$ the polynomial $f$ splits into a product of $m = [K(u) \cap M : K]$ irreducible polynomials, each of degree $d = [M(u) : M] = [(L \cap M)(u) : L \cap M]$. Hint: Solve first under the assumption that $f$ is separable.

**Problem 4.** Let $\Phi_n$ be the $n$-th cyclotomic polynomial, let $\mathbb{Q}(\zeta_n)$ be the $n-$th cyclotomic field (i.e. a splitting field of $\Phi_n$), where $\zeta_n$ is a root of $\Phi_n$.

a) Prove that $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_n)$ for $m \leq n$ iff either $m = n$ or $m$ is odd and $n = 2m$.

b) Prove that $\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_n)$ iff either $m|n$ or $n$ is odd and $m|2n$.

c) Prove that the composite $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n)$ is equal to $\mathbb{Q}(\zeta_N)$ where $N = \mathrm{lcm}(m, n)$.

d) Prove that $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_d)$, where $d = \gcd(m, n)$.

e) Prove that if $n > 1$ is odd then $\Phi_{2n}(x) = \Phi_n(-x)$.

f) Prove that $\Phi_n(1) = p$ if $n$ is a power of a prime $p$ and $\Phi_n(1) = 1$ for all other $n$.

g) Prove that if $p$ is a prime and $p|n$ then $\Phi_{pn}(x) = \Phi_n(x^p)$.

h) Prove that if $p$ is a prime and $p \nmid n$ then $\Phi_n(x^p) = \Phi_n(x)\Phi_{np}(x)$.

**Problem 5.** a) Let $L/K$ be an algebraic extension. Prove that if $L/K$ is normal and separable (but not necessarily finite) and $\Gamma = \mathrm{Aut}(L/K)$ then $L^\Gamma = K$.

b) Suppose that $L/K$ and $M/L$ are finite. Prove that $[M : K]_s = [M : L]_s[L : K]_s$. Hint: Let $\phi : K \longrightarrow F$ be an embedding into algebraically closed field $F$. We proved that $[L : K]_s$ is the number of extensions of $\phi$ to an embedding of $L$ into $F$.

**Problem 6.** This problem outlines the Artin-Schreier theory of exponent $p$ extensions in characteristic $p$. Let $K$ be a field of characteristic $p > 0$. Let $f(x) = x^p - x$. Then $f : K \longrightarrow K$ is an endomorphism of $K$ considered as an additive group. By $\mathbb{F}_p$ we denote the prime subfield of $K$.

a) Let $L/K$ be a cyclic extension of degree $p$ and let $\sigma$ be a generator of $\mathrm{Gal}(L/K)$. Prove that there is $w \in L$ such that $w + \sigma(w) + \sigma^2(w) + \ldots + \sigma^{p-1}(w) \neq 0$. Conclude that there is $u \in L$ such that $u + \sigma(u) + \sigma^2(u) + \ldots + \sigma^{p-1}(u) = -1$. Let $a = \sum_{k=0}^{p-1}(k+1)\sigma^k(u)$. Prove that $\sigma(a) = a + 1$.

b) This part is an alternate approach to a). Let $T : L \longrightarrow L$ be given by $T(x) = \sigma(x) - x$. Think of $T$ as $K$-linear endomorphism of the $K$-vector space $L$. Prove that $T^p = 0$ and that the kernel of $T$ coincides with $K$ (so it has dimension 1). Conclude that the kernel of $T$ is contained in the image of $T$. Conclude that there is $a \in L$ such that $\sigma(a) = a + 1$.

c) Let $L/K$ be a cyclic extension of degree $p$ and let $\sigma$ be a generator of $\mathrm{Gal}(L/K)$. Let $a \in L$ be such that $\sigma(a) = a + 1$. Let $t = a^p - a$. Prove that $t \in K$. Prove that $L = K(a)$ and that $x^p - x - t$ is the minimal polynomial of $a$ over $K$.

d) Let $t \in K$. Prove that the polynomial $x^p - x - t \in K[x]$ is either irreducible over $K$ or splits over $K$. Prove that in the former case, any splitting field $L$ of this polynomial is a cyclic extension of $K$ of degree $p$. Prove that the latter case holds if and only if $t = s^p - s$ for some $s \in K$, i.e. t belongs to the image $f(K)$ of $f$.

e) Consider now any subgroup $W$ of the (additive) group $K/f(K)$ (we do not assume that $W$ is finite here) and let $U_W$ be the preimage of $W$ in $K$. Let $L_W$ be a splitting field of the set of polynomials $x^p - x - t$, where $t \in U_W$. Prove that $L_W/K$ is normal and separable. Let $\Gamma = \mathrm{Aut}(L_W/K)$. Define a pairing $< , >: \Gamma \times W \longrightarrow \mathbb{F}_p$ as follows: given $\tau \in \Gamma$ and $w \in W$ choose a preimage $u$ of $w$ in $U_W$ and choose a root $a$ of $x^p - x - u$ in $L_W$. Then set $< \tau, w >= \tau(a) - a$. Prove that $< , >$ is well defined and that it is a non-degenerate bilinear map. Conclude that $W$ is finite if and only if $\Gamma$ is finite and then the groups $\Gamma$ and $W$ are isomorphic (non-canonically).

e) Suppose now that $L/K$ is a normal and separable extension (not necessarily finite) such that $\Gamma = \mathrm{Aut}(L/K)$ is abelian of exponent $p$. Let $U = \{u \in K : x^p - x - u \text{ splits in } L\}$. Prove that $U$ is a subgroup of $K$ which contains $f(K)$. Set $W = U/f(K)$. Prove that $L = L_W$.

**Remark.** We have established a bijection between abelian extensions of $K$ of exponent $p$ and subgroups of $K/f(K)$. This correspondence can be nicely described as follows. Fix an algebraic closure of $K$. All extensions of $K$ will be assumed to be inside $F$. We can easily see that there is the largest extension $K(p)$ of $K$ which is abelian of exponent $p$. It corresponds to $W = K/f(K)$, i.e. it is the splitting field of all polynomials $x^p - x - t$, where $t \in K$. Let $\Gamma(p) = \mathrm{Aut}(K(p)/K)$. We need to consider a natural topology on $\Gamma(p)$ which makes it a compact, totally disconnected group (i.e. a profinite group) (I am not going to describe this topology here). We also consider $K/f(K)$ as a topological group with discrete topology and we identify $\mathbb{F}_p$ with the unique cyclic subgroup of order $p$ of

the group $\mathbb{Q}/\mathbb{Z}$, with discrete topology. Then the bilinear map considered above becomes a continuous map $< , >: \Gamma(p) \times K/f(K) \longrightarrow \mathbb{Q}/\mathbb{Z}$ and it gives natural isomorphisms $\Gamma(p) \simeq \mathrm{Hom}_{cont}(K/f(K), \mathbb{Q}/\mathbb{Z})$ and $K/f(K) \simeq \mathrm{Hom}_{cont}(\Gamma(p), \mathbb{Q}/\mathbb{Z})$. The subscript *cont* indicates that only continuous homomorphisms are considered and the Hom groups are appropriately topologized so the isomorphisms are of topological groups. Now according to the problem, every subgroup $W$ of $K/f(K)$ corresponds to a subfield $L_W$ of $K(p)$. It is not hard to see that if $\Gamma_W = \{\tau \in \Gamma(p) :< \tau, w >= 0 \text{ for all } w \in W\}$ then $\Gamma_W = \mathrm{Aut}(K(p)/L_W)$ is a closed subgroup of $\Gamma(p)$ and $L_W = K(p)^{\Gamma_W}$. Moreover, $\mathrm{Aut}(L_W/K) \simeq \Gamma(p)/\Gamma_W$ (recall that $\Gamma(p)$ is abelian). Conversely, if $\Gamma$ is a closed subgroup of $\Gamma(p)$ then $L = K(p)^{\Gamma}$ is a subfield of $K(p)$, hence $L = L_W$ for some $W$. It is not hard to see that $W = \{w \in W :< \tau, w >= 0 \text{ for all } \tau \in \Gamma\}$.

**Remark.** A similar global picture can be stated for Kummer theory.

**Remark.** There is extension of the above ideas, due to Witt, to abelian extensions of exponent dividing $p^k$. However, the group $K/f(K)$ needs to be replaced by a significantly more complicated group (related to Witt vectors). The theory is outlined in exercises in the book "Algebra" by S. Lang.