Homework 3
due on Tuesday, March 26

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, Γ is a finite group. Let $M = K(u)^\Gamma$.

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

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

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

d) Prove that Γ is generated by Γ_m, Γ_a and the automorphism ϕ 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 K be a field and let $f \in K[x]$. Show that if $1 + f^2$ has a factor of odd degree in $K[x]$ then there is an $a \in K$ such that $a^2 = -1$.

Problem 5. Give an example of an irreducible polynomial $f \in K[x]$ which has roots a, b, c in its splitting field such that the fields $K(a, b)$ and $K(a, c)$ are not isomorphic over K.

Problem 6. Let Φ_n be the n-th cyclotomic polynomial, let $\mathbb{Q}(\zeta_n)$ be the $n-$th cyclotomic field (i.e. a splitting field of Φ_n), where ζ_n is a root of Φ_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 $\Phi_n(x^p) = \Phi_n(x)\Phi_{np}(x)$.