Graduate Algebra
Homework 9

Due 2015-04-15

1. Recall that on the last problem set you showed that $\mathrm{Aut}(K(x)/K) \cong \mathrm{PGL}(2, K)$. Suppose $H \subset \mathrm{PGL}(2, K)$ is a finite subgroup.

   (a) Define
   $$f_H(Y) = \prod_{h \in H} (Y - h(x)) \in K(x)[Y]$$
   Show that $f_H(Y) \in K(x)^H[Y]$.

   (b) Show that $K(x)^H$ is generated over K by the coefficients of $f_H(Y)$.

   (c) Suppose $K = \mathbb{F}_2$. Show that
   $$\mathbb{F}_2(x)^{\mathrm{Aut}(\mathbb{F}_2(x)/\mathbb{F}_2)} = \mathbb{F}_2\left(\frac{(x^2+x+1)^3}{x^2(x+1)^2}\right)$$
   [Hint: Recall from the midterm last semester that $\mathrm{PGL}(2, \mathbb{F}_2) = \mathrm{GL}(2, \mathbb{F}_2) \cong S_3$. You don't need the computationally intensive part (b), although it would lead to the same answer. Think of part (b) as an algorithm that can be executed on a computer, but not by hand.]

   This contrasts well with the setup of finite Galois extensions where the base field is the subfield invariant under the whole Galois group.

2. Let $m > 1$ be an integer and $\Phi_m(X)$ the m-th cyclotomic polynomial.

   (a) Let $a \in \mathbb{Z}$ and p a prime divisor of $\Phi_m(a)$. Show that either $p \mid m$ or $p \equiv 1 \pmod{m}$. [Hint: The polynomial $X^m - 1$ is separable modulo p if $p \nmid m$. What is the order of a mod p?]

   (b) Deduce that there exist infinitely many primes $p \equiv 1 \pmod{m}$.

3. Let $P(X) = X^4 - 2X^2 - 2 \in \mathbb{Q}[X]$.

   (a) Show that P is irreducible with roots $\alpha_{\pm,\pm} = \pm\sqrt{1 \pm \sqrt{3}}$.

   (b) Let $K_1 = \mathbb{Q}(\alpha_{+,+})$ and $K_2 = \mathbb{Q}(\alpha_{+,-})$. Show that $K_1 \cap K_2 = \mathbb{Q}(\sqrt{3})$ and $K_1 \neq K_2$.

   (c) Show that K_1, K_2, K_1K_2 are Galois over $\mathbb{Q}(\sqrt{3})$ and $\mathrm{Gal}(K_1K_2/\mathbb{Q}(\sqrt{3})) \cong (\mathbb{Z}/2\mathbb{Z})^2$.

   (d) Prove that the splitting field L of $P(X)$ over $\mathbb{Q}$ has $\mathrm{Gal}(L/\mathbb{Q}) \cong D_8$. [Hint: You need not do any computations for this.]

4. Let L/K be any finite Galois extension and $L/M/K$ a subextension. Let $\alpha \in M$.

   (a) Show that the set of embeddings $M \hookrightarrow L$ is in bijection with the quotient set $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/M)$ (which is not a group unless M/K is also Galois).

   (b) Define $P_{M/K,\alpha}(X) = \prod_{\sigma: M \hookrightarrow L}(X - \sigma(\alpha))$. Show that $P_{M/K,\alpha}(X) \in K[X]$. Find explicitly $P_{M/K,\alpha}(X)$ when M/K is quadratic.

   (c) Show that $P_{M/K,\alpha}(X) = P_{K(\alpha)/K,\alpha}(X)^{[M:K]/[K(\alpha):K]}$.

(d) Define the trace $\mathrm{Tr}_{M/K}(\alpha) = \sum_{\sigma: M \hookrightarrow L} \sigma(\alpha)$ and the norm $N_{M/K}(\alpha) = \prod_{\sigma: M \hookrightarrow L} \sigma(\alpha)$. Show that $\mathrm{Tr}_{M/K}(\alpha + \beta) = \mathrm{Tr}_{M/K}(\alpha) + \mathrm{Tr}_{M/K}(\beta)$ and $N_{M/K}(\alpha\beta) = N_{M/K}(\alpha) N_{M/K}(\beta)$.

(e) If α has minimal polynomial $X^d + a_{d-1}X^{d-1} + \cdots + a_0 \in K[X]$ show that $\mathrm{Tr}_{M/K}(\alpha) = -a_{d-1}[M : K]/d$ and $N_{M/K}(\alpha) = (-1)^d a_0^{[M:K]/d}$. [Hint: Use (c).]