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.

   Proof. (1): If $g \in H$ then $g(f_H(Y)) = \prod(Y - gh(x)) = f_H(Y)$ as multiplication by g permutes H. Thus $f_H(X) \in K(x)[Y]^H = K(x)^H[Y]$.

   (2): Write L for the field generated by the coefficients of $f_H(X)$. Part (1) gives $L \subset K(x)^H$. Then $K(x)$ is the splitting field of $f_H(Y)$ over L. Clearly H acts transitively on the roots of $f_H(Y)$ (by definition) and so $f_H(Y)$ is irreducible over L. Indeed, otherwise H would permute the roots of the irreducible factors of $f_H(Y)$ but would not be able to take the root of one irreducible factor to a root of another. Thus $K(X)$ is the splitting field of the irreducible polynomial $f_H(Y)$ over L.

   Now $[K(x) : L] = \deg f_H(Y)$ since $K(x)$ is generated by a single root. But also H is finite so $[K(x) : K(x)^H] = |H|$ from the theorem proven in class. Since these two orders are equal we deduce $K(x)^H = L$ as desired.

   (3): Since $\mathrm{GL}(2, \mathbb{F}_2) \cong S_3$ it is generated by $\begin{pmatrix} & 1 \\ 1 & 1 \end{pmatrix}$ and $\begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$. These correspond to $x \mapsto 1/(x+1)$ and $x \mapsto 1/x$. Certainly $R(x) = \frac{(x^2+x+1)^3}{x^2(x+1)^2}$ is invaried by both and so $K(R(x)) \subset K(x)^{\mathrm{Aut}}$. From the technical theorem in class we deduce that $[K(x) : K(x)^{\mathrm{Aut}}] = |\,\mathrm{Aut}\,| = 6$ and from the homework $[K(x) : K(R(x))] = 6$ (the max degree of numerator and denominator) and so we conclude that $K(R(x)) = K(x)^{\mathrm{Aut}}$. □

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 $p \equiv 1 \pmod{m}$.

Proof. (1): Suppose $p \nmid m$. Then $(X^m - 1)' = mX^{m-1}$ which is coprime to $X^m - 1$ mod p and so $X^m - 1$ is separable mod p. Recall that $X^m - 1 = \prod_{d|m} \Phi_d(X)$ and so $a^m - 1 = \Phi_m(a) \prod_{d|m, d<m} \Phi_d(a) \equiv 0 \pmod{p}$. But all the roots of $X^m - 1$ are distinct and $\Phi_m(a) \equiv 0 \pmod{p}$ and so $p \nmid \Phi_d(a)$ for $d \mid m, d < m$. Thus a is a primitive m-th root mod p and so $\mathrm{ord}(a) = m \mid p - 1$ as desired.

(2): It suffices to show that $\Phi_m(a)$ have infinitely many prime divisors as a varies. Suppose this is not true and list all such primes $p_1, \ldots, p_s$. Then for each $r \in \mathbb{Z}$, $\Phi_m(rp_1 \cdots p_s) \in \mathbb{Z}$ is coprime to $p_1 \cdots p_m$ as it divides $(rp_1 \cdots p_s)^m - 1$. Therefore it must have a prime factor not among the p_i as long as $\Phi_m(rp_1 \cdots p_s) \neq \pm 1$. But $\Phi_m(rp_1 \cdots p_s)$ is a polynomial in r and so for some choice of r we have $\Phi_m(rp_1 \cdots p_s) > 1$. $\square$

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.]

Proof. (1): It's irreducible by Eisenstein. Note that $P(X) = (X^2 - 1)^2 - 3$ and the roots are now obvious.

(2): Certainly $\alpha_{+,\pm}^2 \in \mathbb{Q}(\sqrt{3})$ and so $\mathbb{Q}(\sqrt{3}) \subset K_1 \cap K_2$. Since $[K_1 : \mathbb{Q}] = [K_2 : \mathbb{Q}] = 4$ the only way the intersection is not $\mathbb{Q}(\sqrt{3})$ is if $K_1 = K_2$. But $\alpha_{\pm,+} \in \mathbb{R}$ while $\alpha_{\pm,-} \in \mathbb{C} - \mathbb{R}$ and so we get a contradiction.

(3): K_1, K_2 are quadratic over $\mathbb{Q}(\sqrt{3}) = K_1 \cap K_2$ and so are Galois with Galois group $\mathbb{Z}/2\mathbb{Z}$, the only group of order 2. The result from class gives that $K_1K_2/\mathbb{Q}(\sqrt{3})$ is also Galois and since $K_1 \cap K_2 = \mathbb{Q}(\sqrt{3})$ we have $\mathrm{Gal}(K_1K_2/\mathbb{Q}(\sqrt{3})) \cong \mathrm{Gal}(K_1/\mathbb{Q}(\sqrt{3})) \times \mathrm{Gal}(K_2/\mathbb{Q}(\sqrt{3})) \cong (\mathbb{Z}/2\mathbb{Z})^2$.

(4): Since $\alpha_{\pm,\pm} = \pm\alpha_{+,\pm}$ it follows that $L = K_1K_2$ which is then Galois over $\mathbb{Q}$. We need to compute $\Gamma = \mathrm{Gal}(K_1K_2/\mathbb{Q})$. We know that $\mathrm{Gal}(K_1K_2/\mathbb{Q}(\sqrt{3}))$ is a normal subgroup of Γ as $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ is clearly Galois. Moreover we know that Γ has order 8.

From the first semester we know that Γ is one of $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^3$, D_8 and Q_8. We can eliminate the abelian groups and Q_8 because their subgroups are all normal (for abelian clear; for Q_8 homework from last semester) and that would imply that $K_1/\mathbb{Q}$ is Galois (main theorem B form class), which it clearly is not as it is not normal (not all roots of P are in K_1).

Thus $\Gamma = \mathrm{Gal}(K_1K_2/\mathbb{Q}) \cong D_8$. $\square$

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).]

Proof. (1): Since L/K is normal and separable from class we know that every embedding $M \hookrightarrow L$ extends to $L \hookrightarrow L$ which is then an element of $\mathrm{Gal}(L/K)$. Two such automorphisms f and g restrict to the same embedding $M \hookrightarrow L$ if and only if fg^{-1} restricts to the identity $M \cong M \subset L$, i.e., iff $fg^{-1}\,\mathrm{Gal}(L/M)$. The result follows.

(2): Let $\tau \in \mathrm{Gal}(L/K)$. Part (1) shows that multiplication by τ permutes the set of embedding $M \hookrightarrow L$ as it permutes the quotient set $\mathrm{Gal}(L/K)/\,\mathrm{Gal}(L/M)$. Thus

$$\tau(P_{M/K,\alpha}(X)) = \prod_\sigma (X - \tau\sigma(\alpha)) = \prod_\sigma (X - \sigma(\alpha)) = P_{M/K,\alpha}(X)$$

and so $P_{M/K,\alpha}(X) \in L[X]^{\mathrm{Gal}(L/K)} = K[X]$ from main theorem A.

If M/K is quadratic then $\mathrm{Gal}(L/M)$ has index 2 in $\mathrm{Gal}(L/K)$ and so it is Galois. We deduce that there are two embeddings $M \hookrightarrow L$ namely $\mathrm{Gal}(M/K) \cong \mathrm{Gal}(L/K)/\,\mathrm{Gal}(L/M)$. Explicitly, if $M = K(\beta)$ where β satisfies a quadratic equation $X^2 - aX + b = 0$ with distinct roots $\beta, a - \beta$ then the two automorphisms are the identity and the map taking β to $a - \beta$. Write $\alpha = u + v\beta \in K[\beta]$ with $u, v \in K$. Then

$$P_{M/K,\alpha}(X) = (X - (u + v\beta))(X - (u + v(a - \beta))) = X^2 - (2u + av)X + u^2 + uva + v^2 b$$

In characteristic not 2 we can write $M = K(\sqrt{d})$ for some $d \in K - K^2$ in which case $P_{M/K,u+v\sqrt{d}}(X) = X^2 - 2uX + u^2 - dv^2$.

(3): From the definition

$$P_{M/K,\alpha}(X) = \prod_{\sigma \in \mathrm{Gal}(L/K)/\,\mathrm{Gal}(L/M)} (X - \sigma(\alpha))$$

but $\sigma(\alpha) = \tau(\alpha)$ iff $\sigma\tau^{-1} \in \mathrm{Gal}(L/K(\alpha))$. If $K \subset H \subset G$ are groups then $G/K = \sqcup_{H/K} G/H$ as a disjoint union of sets. Indeed, writing $H = \sqcup h_i K$ and $G = \sqcup g_i H$ then $G = \sqcup g_i h_j K$ and $\{g_i h_j\} = \sqcup_{h_j} \{g_i\} \cdot h_j$. Apply to $G = \mathrm{Gal}(L/K)$, $H = \mathrm{Gal}(L/K(\alpha))$ and $K = \mathrm{Gal}(L/M)$ (sorry for the double use of K) then

$$\begin{aligned}
P_{M/K,\alpha}(X) &= \prod_{\sigma \in \mathrm{Gal}(L/K)/\,\mathrm{Gal}(L/K(\alpha)), \tau \in \mathrm{Gal}(L/K(\alpha))/\,\mathrm{Gal}(L/M)} (X - \sigma\tau(\alpha)) \\
&= \prod_{\sigma \in \mathrm{Gal}(L/K)/\,\mathrm{Gal}(L/K(\alpha)), \tau \in \mathrm{Gal}(L/K(\alpha))/\,\mathrm{Gal}(L/M)} (X - \tau(\alpha)) \\
&= P_{K(\alpha)/K,\alpha}(X)^{|\,\mathrm{Gal}(L/K(\alpha))/\,\mathrm{Gal}(L/M)|} \\
&= P_{K(\alpha)/K,\alpha}(X)^{[M:K(\alpha)]}
\end{aligned}$$

as desired.

(4): Since σ is additive it follows trivially that Tr is additive. Since σ is multiplicative it follows trivially that N is multiplicative.

(5): Since L/K is Galois all the roots of $\min_\alpha(X)$ are in L and each root yields an embedding $K(\alpha) \hookrightarrow L$. Let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_d$ be the roots of $\min_\alpha(X)$. Then

$$P_{K(\alpha)/K,\alpha}(X) = (X - \alpha_1) \cdots (X - \alpha_d) = \min_\alpha(X)$$

This implies that $P_{M/K,\alpha}(X) = \min_\alpha(X)^{[M:K(\alpha)]}$. But if

$$P_{M/K,\alpha}(X) = X^n + s_1 X^{n-1} + \cdots + s_n$$

then $-s_1 = \sum \sigma(\alpha) = \mathrm{Tr}_{M/K}(\alpha)$ and $(-1)^n s_n = \prod \sigma(\alpha) = N_{M/K}(\alpha)$.
Finally,

$$X^n + s_1 X^{n-1} + \cdots + s_n = (X^d + a_{d-1} X^{d-1} + \cdots + a_0)^{n/d}$$

and breaking up the parantheses we get $s_1 = (n/d) a_{d-1}$ and $s_n = a_0^{n/d}$. The result follows. $\square$