Math 594. Homework 11 (due April 9)

1. Let k be a finite field with size q. Show that in $k[T]$, $T^{q^n} - T$ factors into the product of all monic irreducible polynomials of degree dividing n, each appearing exactly once in the factorization (hint: use what you already know about finite field theory). As a check on this, multiply together all monic irreducible cubics and linears in $\mathbf{F}_2[X]$ and see that you get $X^8 - X$.

2. Let $L/\mathbf{Q}$ be a splitting field for $X^5 - 2 \in \mathbf{Q}[X]$. Writing $L = \mathbf{Q}(a, \zeta)$ with $a^5 = 2$ and $\zeta^5 = 1$, $\zeta \neq 1$, describe generators of $\mathrm{Aut}(L/\mathbf{Q})$ in terms of their actions on a and ζ. Describe $\mathrm{Aut}(L/\mathbf{Q})$ as an abstract group (i.e., in terms of 'generators and relations'), and write out the diagrams of intermediate fields and intermediate subgroups, indicating all containments.

3. Let k be a field, N a positive integer not divisible by the characteristic of k. Let L/k be a splitting field for $X^N - 1$ over k. This is called the *Nth cyclotomic extension* of k. The case $k = \mathbf{Q}$ is very important (and one usually just speaks of *cyclotomic fields* when $k = \mathbf{Q}$).
(*i*) For each $\sigma \in \mathrm{Aut}(L/k)$, prove there is a unique $n(\sigma) \in \mathbf{Z}/N$ so that $\sigma(\zeta) = \zeta^{n(\sigma)}$ for *every* Nth root of unity $\zeta \in L$.
(*ii*) Prove that $n(\sigma) \in (\mathbf{Z}/N)^\times$ and that $\sigma \mapsto n(\sigma)$ is an injective group homomorphism $\mathrm{Aut}(L/k) \to (\mathbf{Z}/N\mathbf{Z})^\times$ (so $\mathrm{Aut}(L/k)$ is *abelian*).
(*iii*) For $n \geq 1$ and prime p, prove that the polynomial $\Phi_{p^n}(X) = \Phi_p(X^{p^{n-1}}) = (X^{p^n} - 1)/(X^{p^{n-1}} - 1) \in \mathbf{Z}[X]$ of degree $p^{n-1}(p-1)$ is *irreducible* over $\mathbf{Q}$, and deduce that $\mathrm{Gal}(\mathbf{Q}(\zeta_{p^n})/\mathbf{Q}) \to (\mathbf{Z}/p^n)^\times$ is an *isomorphism.*

4. Let k be a field containing a primitive Nth root of unity. Let $\mu_N \subseteq k^\times$ be the subgroup of Nth roots of 1 in $k^\times$ (a cyclic group of order N). For $a \in k^\times$, let F/k be a splitting field of $X^N - a$.
(*i*) Show that $F = k(\alpha)$ where α is any root to $X^N - a$ in F. Also, for any $\sigma \in \mathrm{Aut}(F/k)$, show that $\sigma(\alpha)/\alpha \in \mu_N$ and that this is *independent* of the choice of α.
(*ii*) Fix a choice of α as in (*i*). Show that the map $\mathrm{Aut}(F/k) \to \mu_N$ given by $\sigma \mapsto \sigma(\alpha)/\alpha$ is an injective group homomorphism. In particular, $\mathrm{Aut}(F/k)$ is *abelian.* Also, show that this map is an isomorphism if and only if $X^N - a$ is irreducible in $k[X]$.

5. Consider $f = 2X^5 - 10X + 5 \in \mathbf{Q}[X]$. Let $L/\mathbf{Q}$ be a splitting field of f. Show that $\mathrm{Gal}(L/\mathbf{Q})$ injects as a subgroup of S_5 which acts transitively on the set of 5 "letters" (i.e., roots of f) and that it contains an element of order 2 and an element of order 5 (you may use calculus to study the roots in $\mathbf{R}$). Deduce that $\mathrm{Gal}(L/\mathbf{Q}) \simeq S_5$.

6. Let $f = T^{p^2} + XT^p + Y \in k[T]$, with $k = \mathbf{F}_p(X, Y)$. Show that f is irreducible and let $L = k(a)$ be an extension generated over k by a single root of f. Show that $[L : k]_s = p$ and that there is a *unique* non-trivial intermediate extension k' between k and L. Conclude that L/k cannot be built up as a tower $L/E/k$ with E/k purely inseparable and L/E separable (this shows that one cannot 'reverse' the theorem that an algebraic extension can be built up as a separable extension followed by a purely inseparable one).

7. Let $f \in k[T]$ be an irreducible monic, L/k a splitting field. If k'/k is an extension generated by a single root of f (so $k' \simeq k[X]/f$), then show that in $L[T]$

$$f = \prod_{j=1}^{[k':k]_s} (T - r_j)^{[k':k]_i},$$

with all r_j's distinct.

$*$ 8. Let k be a field of positive characteristic p, and choose $a \in k$. Prove that $f_a(t) = t^p - t - a \in k[t]$ is either a product of linears or else is irreducible of degree p with splitting field k_a Galois of degree p over k (hint: see Exercise 7 on HW7, or rather its solution), and that $k_a \simeq k_{a'}$ over k if $a' - a = b^p - b$ for some $b \in k$ (in particular, when such an equation holds, show f_a is irreducible over k if and only if $f_{a'}$ is).

It is an important theorem of Artin-Schreier that *all* degree p Galois extensions of k arise by this construction, and that $k_a \simeq k_{a'}$ over k *only if* $a - a' = b^p - b$ for some $b \in k$.