Math 121. Homework 7

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 $\mathrm{Gal}(L/\mathbf{Q})$ in terms of their actions on a and ζ. Describe $\mathrm{Gal}(L/\mathbf{Q})$ as an abstract group (i.e., in terms of 'generators and relations').

3. 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 $\sigma \in \mathrm{Gal}(F/k)$, 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 $\mathrm{Gal}(F/k) \to \mu_N$ given by $\sigma \mapsto \sigma(\alpha)/\alpha$ is an injective group homomorphism. In particular, $\mathrm{Gal}(F/k)$ is *abelian*. Also, show that this map is an isomorphism if and only if $X^N - a$ is irreducible in $k[X]$.

4. Consider $f = 2X^5 - 10X + 5 \in \mathbf{Q}[X]$. Let $L/\mathbf{Q}$ be a splitting field of f.

(i) Show that $\mathrm{Gal}(L/\mathbf{Q})$ injects as a subgroup of S_5 which contains an element of order 5 (look at $[L : \mathbf{Q}]$) and contains an element of order 2 (you may use calculus to study the roots in $\mathbf{R}$).

(ii) For any *prime* $p > 2$, show that the symmetric group S_p is generated by any p-cycle σ and transposition τ. (Hint: arrange labels so that $\sigma = (1, 2, \ldots, p)$ and $\tau = (1, i)$ with $1 < i \leq p$. Pass to σ^{i-1} and rename the letters to reduce to the case $i = 2$.) Deduce that $\mathrm{Gal}(L/\mathbf{Q}) \simeq S_5$ in (i).

5. 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).

6. 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 separable and either totally split or irreducible of degree p with splitting field Galois of degree p over k (hint: see Exercise 7 on HW3). Letting k_a/k be its splitting field (Galois of degree 1 or p), prove 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 $b \in k$.