Solutions to Homework 10

1. Let $L_1/L_2/k$ be a tower of algebraic extensions, with L_i/k normal. Prove that there is a natural surjection of groups $\mathrm{Aut}(L_1/k) \to \mathrm{Aut}(L_2/k)$, with kernel $\mathrm{Aut}(L_1/L_2)$.

Using the given tower, we regard k and L_2 as subfields of L_1, with $k \subseteq L_2$. For any $\sigma \in \mathrm{Aut}(L_1/k)$, we have $\sigma(L_2) = L_2$ by normality of L_2/k, so we get a map $\mathrm{Aut}(L_1/k) \to \mathrm{Aut}(L_2/k)$ which is a map of groups. By an earlier handout on embeddings into a normal extension, for any k-automorphism σ_2 of L_2, we can fill in the top row of the commutative diagram

$$\begin{tikzcd} L_1 \arrow[r, "?"] & L_1 \\ L_2 \arrow[u] \arrow[r, "\simeq", "\sigma_2"'] & L_2 \arrow[u] \end{tikzcd}$$

where the columns are the given inclusion of L_2 into L_1. Pick a choice of σ_1 fitting into the top row. Since L_1 is algebraic over k, such a self-map σ_1 of L_1 over k must be an automorphism. Thus, the map $\mathrm{Aut}(L_1/k) \to \mathrm{Aut}(L_2/k)$ is surjective. By *definition*, the kernel is obviously $\mathrm{Aut}(L_1/L_2)$.

2. Let L/k be a finite normal extension, $G = \mathrm{Aut}(L/k)$. For each subgroup H in G, define

$$L^H = \{x \in L | h(x) = x \text{ for all } h \in H\}.$$

For each intermediate field k' between L and k, define $G_{k'} = \{g \in G | g(x) = x \text{ for all } x \in k'\}$.
(i) Show that L^H is an intermediate field between k and L and that $G_{k'}$ is a subgroup of G.
(ii) Let $k = \mathbf{Q}$ and let $L = \mathbf{Q}(\alpha, \beta)$ with $\alpha^2 = 2$, $\beta^2 = 3$. Show that $G = \mathrm{Aut}(L/k) \simeq \mathbf{Z}/2 \times \mathbf{Z}/2$. Show that the maps in (i) do give a bijection between intermediate fields between L and k and subgroups of $\mathrm{Aut}(L/k)$.

(i) Chase definitions.
(ii) Since $[L : \mathbf{Q}(\alpha)] = 2$ (why?), L is a splitting field for $X^2 - 3$ over $\mathbf{Q}(\alpha)$. Thus, there exists $\sigma \in \mathrm{Aut}(L/\mathbf{Q}(\alpha))$ with $\sigma(\beta) = -\beta$. Similarly, there exists $\tau \in \mathrm{Aut}(L/\mathbf{Q}(\beta))$ with $\tau(\alpha) = -\alpha$. Since an element of $\mathrm{Aut}(L/\mathbf{Q})$ is determined by its action of α and β, we see that there are at most 4 such automorphisms. Check 'by hand' that $1, \sigma, \tau, \sigma\tau = \tau\sigma$ are 4 distinct automorphisms. Thus, $\mathrm{Aut}(L/\mathbf{Q}) = \langle \sigma, \tau \rangle$. Since $\sigma^2 = \tau^2 = 1$, we see that $\mathrm{Aut}(L/\mathbf{Q}) \simeq \mathbf{Z}/2 \times \mathbf{Z}/2$.

Using the basis $1, \alpha, \beta, \alpha\beta$ of L over $\mathbf{Q}$ and our knowledge of all of the intermediate subgroups, it is easy to check $H = G_{L^H}$ for each H. For an intermediate field k' strictly between $\mathbf{Q}$ and L, we must have $[L : k'] = 2$, so $G_{k'}$ is an index 2 subgroup. Since $k' \subseteq L^{G_{k'}} \subsetneq L$, we must have that $k' = L^{G_{k'}}$. Such subfields are exactly one of the three "obvious" quadratic subfields $\mathbf{Q}(\alpha), \mathbf{Q}(\beta), \mathbf{Q}(\alpha\beta)$. Hence, it is not hard to check that $L^{G_{k'}} = k'$ for each k'.

3. (i) Let k be a field, G a finite subgroup of $k^\times$. Show that G is cyclic
(ii) Prove that if k is a finite field with characteristic p, then k is a quotient of $\mathbf{F}_p[X]$. Conclude that for every positive integer d, there exists an irreducible polynomial of degree d in $\mathbf{F}_p[X]$.

(i) Let G have order d. By the structure theorem for finite abelian groups we see that if $d'|d$ is the least common multiple of the orders of the factors in a cyclic decomposition of G, necessarily $x^{d'} = 1$ for all $x \in G$. Hence, $d' \geq d$, so $d' = d$. But clearly $d' = d$ if and only if G is cyclic.
(ii) Choosing a generator of the *finite* cyclic group $k^\times$, we get a surjection $\mathbf{F}_p[X] \to k$ as $\mathbf{F}_p$-algebras. The monic generator of the (non-zero!) kernel must therefore be irreducible and has degree equal to $[k : \mathbf{F}_p]$. Since we have shown previously that there exists an extension of $\mathbf{F}_p$ with any desired finite degree, we're done.

4. Choose a positive integer N. A *primitive Nth root of unity* over a field k an an element ζ in an extension of k so that $\zeta^N = 1$ and the multiplicative group generated by ζ has order exactly N.
(i) If N is divisible by the characteristic of k (in particular, k must have positive characteristic), then show that no primitive Nth root of unity exists over k.

(ii) If N is not divisible by the characteristic of k (always the case if k has characteristic 0), then prove that a primitive Nth root of unity exists over k. In addition, show that an extension L/k contains a primitive Nth root of unity over k if and only if it contains a splitting field for $X^N - 1 \in k[X]$. In this case, show that the number of primitive Nth roots of unity over k in L is $\varphi(N) = |(\mathbf{Z}/N)^\times|$.

(i) If $N = pN'$, then $x^N = 1$ if and only if $x^{N'} = 1$.
(ii) Since $X^N - 1$ is separable over k by the derivative test, it has N distinct roots in a splitting field. This set of roots is cyclic by Exercise 4(i), so since it has size N, a generator of this group is the same thing as a primitive Nth root of unity in the splitting field. We know from finite group theory that a cyclic group of order N has exactly $\varphi(N)$ generators. The rest is clear.

5. Let $L = \mathbf{F}_p(X, Y)$, $k = \mathbf{F}_p(X^p, Y^p)$.
(i) Show that L is the splitting field over k of $(T^p - X^p)(T^p - Y^p) \in k[T]$. Prove that $[L : k] = p^2$.
(ii) Show that L/k is *not* generated by a single element.
(iii) Exhibit an explicit list of *infinitely many* distinct intermediate fields between L and k!

(i) Certainly L is such a splitting field. Moreover, neither X^p nor Y^p lie in $k^p = \mathbf{F}_p(X^{p^2}, Y^{p^2})$ (proof?), so $[L : k] \le [L : k(X)][k(X) : k] \le p^2$. Since $[k(X) : k] = p$ and $[k(Y) : k] = p$, if $[L : k] < p^2$ then the degree is p and so $k(X) = k(Y)$. But $Y \notin k(X) = \mathbf{F}_p(X, Y^p)$ (proof?). Thus, $[L : k] = p^2$.
(ii) By (i), L/k is a finite normal extension. If $L = k(a)$, where a has minimal polynomial $f \in k[T]$, then f has degree p^2. But clearly for all $r \in L$ we have $r^p \in k$, so a satisfies a degree p polynomial over k, a contradiction.
(iii) Let $k_j = k(X + X^{pj}Y)$ for all positive integers j. Note that $r_j = X + X^{pj}Y$ is a root of $T^p - (X^p + X^{p^2 j}Y^p) \in k[T]$, with the constant term not a pth power in k (proof?), so $[k_j : k] = p$. If $k_j = k_{j'}$ with $j \neq j'$, and say we let k' denote this field, then k' contains $r_j - r_{j'} = ((X^p)^j - (X^p)^{j'})Y$. Since $(X^p)^j - (X^p)^{j'} \in k \subseteq k'$ is *non-zero*, k' contains Y. Then k' contains $r_j - (X^p)^j Y = X$, so k' must fill up all of L. But $[k' : k] \neq [L : k]$, a contradiction.

6. (**Extra Credit**) Let k be a field. Let I be the set of all non-constant monic polynomials in $k[T]$, and $\mathfrak{m}$ a maximal ideal in $R = k[X_f]_{f \in I}$ which contains $f(X_f)$ for all $f \in I$. As in class (via Zorn), $\mathfrak{m}$ exists and $L = R/\mathfrak{m}$ is an extension *field* of k in which all non-constant $f \in k[T]$ have a root.

(i) Let $x_f \in L$ be the image of $X_f \in R$. L is the composite of the subfields $k(x_f) = k[X_f]$, with x_f a root of $f \in k[T]$. Since each $k(x_f)$ is algebraic over k (as x_f is), L/k is algebraic.
(ii) Clearly $k \subseteq k_0 \subseteq L$. If k has positive characteristic p and $x^{p^n} \in k$ and $y^{p^m} \in k$, then for $r \ge m, n$, $(x + y)^{p^r} = x^{p^r} + y^{p^r} \in k$, so $x + y \in k_0$, etc. In this way, we see k_0 is a field. If k has characteristic 0, then $k_0 = k$ is perfect. If k has characteristic $p > 0$, then to show k_0 is perfect, we need to show that $k_0 = k_0^p$. For $x \in k_0$, with $a = x^{p^n} \in k$, the polynomial $T^{p^{n+1}} - a$ has a root $y \in L$. Since $(y^p)^{p^n} = a = x^{p^n}$, $y \in k_0$ and $y^p = x$.

Since L/k_0 is an algebraic extension (by (i)), the perfectness of k_0 forces the perfectness of L.
(iii) Let $f = \sum a_j T^j \in k_0[T]$ be non-constant. Choose n so large that $a_j^{p^n} \in k$ for all j (with $p = 1$ when k has characteristic 0). Thus, $g = \sum a_j^{p^n} T^j \in k[T]$ has a root $y \in L$. Since L is perfect, $y = z^{p^n}$ for some $z \in L$. Thus, $f(z)^{p^n} = g(y) = 0$, so $f(z) = 0$.
(iv) Supposing k is perfect, we choose $f \in k[T]$ non-constant and let k_f/k be splitting field of f. Since k_f/k is a finite *separable* extension, we may choose a primitive element a. Letting $g \in k[T]$ be the minimal polynomial of a over k, we may choose a root r to g in L and so get a k-embedding $k_f \simeq k[T]/g(T) \hookrightarrow L$ taking a to r. Since f splits completely over k_f, it splits completely over L.

Let $f \in L[T]$ be an irreducible monic, $L' = L[T]/f$ an extension generated by a root $t = T \bmod f$. Since L'/L and L/k are algebraic, so is L'/k, so t satisfies some minimal polynomial h over k. But h splits completely over L, so the root t of h lies in L. Hence, $L = L'$ and so f has degree 1. Therefore L is algebraically closed.
(v) By (iii), we can apply the arguments in (iv) to the extension L/k_0 to conclude that L is algebraically closed. By (i), L/k is an algebraic closure.