MATH 594. HOMEWORK 10 (DUE APRIL 2)

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 $\mathrm{Aut}(L_1/L_2)$. In particular, $\mathrm{Aut}(L_1/L_2) \lhd \mathrm{Aut}(L_1/k)$.

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, with $H \subseteq G_{L^H}$ and $k' \subseteq L^{G_{k'}}$. Thus, $H \mapsto L^H$ and $k' \mapsto G_{k'}$ give maps between the set of subgroups of G and the set of intermediate field extensions between k and L (these maps are not always bijections, since G can be trivial with $[L : k] > 1$; e.g., $k = \mathbf{Q}$, $L = \mathbf{Q}[T]/(T^3 - 2)$).
(*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 $\mathrm{Aut}(L/k)$ (hint: first prove $G_{L^H} = H$ for every subgroup H of G, then deduce that the intermediate fields k' between k and L are just the "obvious" ones, and show $L^{G_{k'}} = k'$ for each k').

3. (*i*) Let k be a field, G a finite subgroup of $k^\times$. Show that G is cyclic (hint: use the fact that a non-zero polynomial over k has no more roots than its degree). Is this "physically obvious" when $k = \mathbf{C}$?
(*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 $\mathbf{F}_p[X]$.

4. Choose a positive integer N. A *primitive Nth root of unity* over a field k is 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 $\varphi(N) = |(\mathbf{Z}/N)^\times|$.

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 (with proof!) an explicit list of *infinitely many* distinct intermediate fields between L and k!

6. (**Extra Credit**). Here we outline a more refined proof of *existence* of algebraic closures. Let k be a field. Let Σ be the set of all non-constant monics in $k[T]$, and consider the ideal J in $R = k[X_f]_{f \in \Sigma}$ generated by the elements $f(X_f)$ for $f \in \Sigma$. Because of the existence of simultaneous splitting fields for a finite set of non-constant polynomials, the ideal J cannot contain 1 (much as we argued some time ago in class). Hence, by Zorn's Lemma there exists a maximal ideal $\mathfrak{m}$ of R containing J, so $L = R/\mathfrak{m}$ is an extension *field* of k in which all non-constant $f \in k[T]$ have a root (since we noted that many arguments in class could be done for *finite* extensions using sufficiently large finite normal extensions of the ground field to bypass appealing to algebraic closures, the theory required to do this exercise does not depend on the existence of algebraic closures; using algebraic closures merely allowed proofs in lecture to avoid finiteness hypotheses).
(*i*) Show that L/k is an algebraic extension.
(*ii*) Let $p = 1$ if k has characteristic 0, and otherwise let p denote the characteristic of k. Let k_0 be the subset of elements $x \in L$ such that some $x^{p^n} \in k$ (with $n \geq 0$ allowed to depend on x). Show that k_0 is an intermediate field between k and L and that k_0 is a perfect field. Conclude that L is perfect.
(*iii*) Show that all non-constant $f \in k_0[T]$ have a root in L.
(*iv*) If k is perfect (so L/k is a separable extension), show that every $f \in k[T]$ splits completely over L. Conclude that L is algebraically closed if k is perfect.
(*v*) Without assuming k to be perfect, prove that L is algebraically closed and therefore is an algebraic closure of k.