MATH 121. HOMEWORK 6

1. 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 $G = \mathrm{Aut}(L/k) \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Show that the maps in (*i*) do give a bijection between the set of intermediate fields between L and k and the set of 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').

2. (*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 $\mathbf{F}_p[X]$.

3. 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 $\varphi(N) = |(\mathbf{Z}/N\mathbf{Z})^\times|$.

4. 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 $n(\sigma) \in \mathbf{Z}/N\mathbf{Z}$ so that $\sigma(\zeta) = \zeta^{n(\sigma)}$ for *every* Nth root of unity $\zeta \in L$.
(*ii*) Prove $n(\sigma) \in (\mathbf{Z}/N\mathbf{Z})^\times$ 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 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 $\mathrm{Aut}(\mathbf{Q}(\zeta_{p^n})/\mathbf{Q}) \to (\mathbf{Z}/p^n\mathbf{Z})^\times$ is an *isomorphism*.

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!