MATH 594. HOMEWORK 12 (DUE APRIL 16)

1. (*i*) Let k be a finite field, with k'/k a finite extension with degree d. Prove that $\mathrm{Gal}(k'/k)$ is a cyclic group of order d, with $x \mapsto x^{|k|}$ a generator. This generator is called the (arithmetic) *Frobenius map*; the *geometric Frobenius map* is its inverse $x \mapsto x^{1/|k|}$. The names are due to the fact that $x \mapsto x^{1/|k|}$ arises in algebraic *geometry* when computing étale cohomology on k-schemes, whereas $x \mapsto x^{|k|}$ often shows up in number theory.
(*ii*) What is the size of a splitting field for $X^{15} - 2$ over $\mathbf{F}_7$?

2. Let L_1, L_2 be intermediate extensions in an extension $k \subseteq L$, with L_1/k finite Galois.
(*i*) Show that L_1L_2/L_2 is finite Galois and that there is a natural injective group map $\mathrm{Gal}(L_1L_2/L_2) \to \mathrm{Gal}(L_1/k)$, with image $\mathrm{Gal}(L_1/L_1 \cap L_2)$.
(*ii*) If $L_1 \cap L_2 = k$, then prove that $[L_1L_2 : k] = [L_1 : k][L_2 : k]$.
(*iii*) If $L_1 \cap L_2 = k$ and L_2/k is finite Galois, show that there is a natural isomorphism of groups

$$\mathrm{Gal}(L_1L_2/k) \simeq \mathrm{Gal}(L_1/k) \times \mathrm{Gal}(L_2/k).$$

3. Let K be a field not of characteristic 2, and assume all odd degree polynomials in $K[T]$ have a root in K (thus, if K has positive odd characteristic p, taking $n = p$ shows K to be perfect; as characteristic 0 fields are also perfect, all extensions considered below are automatically separable). Let L be a quadratic extension of K with the magical property that all elements of L are squares.

(*i*) Prove that all finite extensions of K have degree a power of 2 (hint: consider the fixed field of the 2-Sylow subgroup of a finite Galois extension).

(*ii*) Using the fact that a non-trivial 2-group has an index 2 (normal) subgroup, prove that L has no non-trivial finite extensions which are Galois over K, and conclude that L is algebraically closed.

(*iii*) Using *only* calculus, explain why the hypothesis on K is satisfied for $K = \mathbf{R}$, and prove by explicit formulas that all elements of $L = \mathbf{R}[X]/(X^2 + 1)$ are squares. This is Artin's almost purely algebraic proof of the Fundamental Theorem of Algebra (one has to use *something* non-algebraic about $\mathbf{R}$ in the proof).

4. Determine $\mathrm{Gal}(L/\mathbf{Q})$, with L the splitting field of $X^4 - 4X^2 - 1$ (hint: pay careful attention to the constant term -1). Give the 'lattice' of subfields. Which ones are Galois over $\mathbf{Q}$? Do the same for $X^3 - 2$.

5. Let $k \subseteq L$ be a Galois extension, perhaps with infinite degree. For any intermediate F between L and k, define $G(F)$ to be the subgroup of $\mathrm{Gal}(L/k)$ fixing F, and for any subgroup H in $\mathrm{Gal}(L/k)$ define L^H to be the subfield of elements of L fixed by H.
(*i*) Show that $L^{G(F)} = F$.
(*ii*) Let $k = \mathbf{F}_p$, $L = \overline{\mathbf{F}}_p$ an algebraic closure (so L is a union of subfields $\mathbf{F}_{p^n}$ for all $n \geq 1$). Define $\varphi \in \mathrm{Gal}(L/k)$ by $\varphi(x) = x^p$, and let $H \subseteq \mathrm{Gal}(L/k)$ be the subgroup generated by φ (this is an infinite group). Define $e_n = 1! + 2! + \ldots (n-1)!$ and define $g_n \in \mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p)$ by $g_n(x) = x^{p^{e_n}}$ for all $x \in \mathbf{F}_{p^n}$ and $n \geq 1$. Check that if $x \in L$ lies in $\mathbf{F}_{p^n}$ and in $\mathbf{F}_{p^m}$, then $g_n(x) = g_m(x)$. Conclude that there exists a unique $g \in \mathrm{Gal}(L/k)$ so that $g(x) = g_n(x)$ for all $n \geq 1$ and $x \in \mathbf{F}_{p^n}$. In particular, conclude that $\mathrm{Gal}(L/k) \neq H$
(*iii*) Continuing with notation as in (*ii*), show that $L^H = k$, so $G(L^H) = \mathrm{Gal}(L/k)$ and thus $G(L^H) \neq H$. That is, the Galois correspondence is not generally bijective for Galois extensions with infinite degree.

Remark. For an arbitrary Galois extension of fields L/k of possibly infinite degree, the failure of the naive analogue of the Galois correspondence can be circumvented as follows. We define the *Krull topology* on $\mathrm{Gal}(L/k)$ to have a base of opens around $g \in \mathrm{Gal}(L/k)$ given by subsets $S_{K,g} = \{g' \in \mathrm{Gal}(L/k) \mid g'|_K = g|_K\}$ for subextensions K/k of *finite* degree over k. This topology is easily seen to be Hausdorff and to give $\mathrm{Gal}(L/k)$ a structure of topological group. In fact, this is just the subspace topology on $\mathrm{Gal}(L/k)$ as a subset of $\prod_K \mathrm{Gal}(K/k)$ where the product runs over finite Galois subextensions K/k with factors $\mathrm{Gal}(K/k)$ given the discrete (compact!) topology. Using Tychonoff's theorem, this topology is *compact*, and it is a pleasant exercise to prove in general that $G(F)$ is a *closed* subgroup and that the Galois correspondence sets up an inclusion-reversing bijection between intermediate fields and closed subgroups of $\mathrm{Gal}(L/k)$. See any graduate algebra text (e.g., Jacobson or Lang) for further discussion of this important construction.