MATH 121. HOMEWORK 8

1. Prove $\mathrm{Gal}(L/\mathbf{Q}) = D_4$ (order 8), with L the splitting field of $X^4 - 4X^2 - 1$ (hint: note the constant term -1). Give the "lattice" of subfields. Which ones are Galois over $\mathbf{Q}$?

2. Let $L = \mathbf{Q}(\zeta)$ where $\zeta^7 = 1, \zeta \neq 1$, so $\mathrm{Gal}(L/\mathbf{Q}) = (\mathbf{Z}/7\mathbf{Z})^\times$ is cyclic of order 6, with generator $\zeta \mapsto \zeta^3$ (since 3 generates $(\mathbf{Z}/7\mathbf{Z})^\times$).

(i) Prove L has unique subfields with degrees 2 and 3 over $\mathbf{Q}$, and no other intermediate fields.

(ii) Using that the elements $\sigma := 2 = 3^2 \bmod 7$ and $\tau := -1 = 3^3 \bmod 7$ generate the subgroups of $(\mathbf{Z}/7\mathbf{Z})^\times$ with respective orders 3 and 2, we are led to consider

$$a := \zeta + \sigma(\zeta) + \sigma^2(\zeta) = \zeta + \zeta^2 + \zeta^4, \;\; b = \zeta + \tau(\zeta) = \zeta + \zeta^{-1}$$

in L. Explain via the Fundamental Theorem (without messy explicit computations) why a must generate the quadratic subfield (in particular, $a \notin \mathbf{Q}$), and b must generate the cubic subfield.

(iii) Using that $\zeta + \zeta^2 + \zeta^3 + \cdots + \zeta^6 = -1$, check that $a^2 + a + 2 = 0$ and $b^3 - 2b + b^2 - 1 = 0$. Deduce that the quadratic subfield of L is $\mathbf{Q}(\sqrt{-7})$, and that $X^3 + X^2 - 2X - 1 \in \mathbf{Q}[X]$ is irreducible with splitting field $\mathbf{Q}(b)$.

(iv) Compute the two roots b' and b'' of $f = X^3 + X^2 - 2X - 1$ in $\mathbf{Q}(b)$ apart from b, expressed as quadratic polynomials in b over $\mathbf{Q}$, and explicitly verify that $(X - b)(X - b')(X - b'') = f$.

3. (*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* whereas $x \mapsto x^{|k|}$ often shows up in number theory.
(*ii*) Find the $\mathbf{F}_7$-degree of a splitting field for $X^{15} - 2$ over $\mathbf{F}_7$. (Hint: show that a splitting field is $\mathbf{F}_7(\zeta_{45})$, and note that $\mathbf{F}_{7^n}^\times$ is cyclic of order $7^n - 1$.)

4. Let L_1, L_2 be intermediate extensions in a finite extension $k \subseteq L$, with L_1/k Galois.
(*i*) Show L_1L_2/L_2 is Galois and there is a natural injective homomorphism $\mathrm{Gal}(L_1L_2/L_2) \to \mathrm{Gal}(L_1/k)$, 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 Galois, show there is a natural isomorphism of groups

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

5. This exercise illustrates new behavior with separable normal algebraic extensions of infinite degree. (Such considerations arise often in number theory and algebraic geometry.)

Let p be an *odd* prime, $k = \mathbf{Q}$, $L = \cup_{n \geq 1} \mathbf{Q}(\zeta_{p^n})$ the algebraic extension inside $\overline{\mathbf{Q}}$ generated by the p-power roots of unity. Let $L_n = \mathbf{Q}(\zeta_{p^n})$, so Exercise 4 in HW6 gives naturally $\mathrm{Gal}(L_n/\mathbf{Q}) \simeq (\mathbf{Z}/p^n\mathbf{Z})^\times$. Fix a generator a_2 of the cyclic group $(\mathbf{Z}/p^2\mathbf{Z})^\times$ (here we use that p is an odd prime), and for each $n > 2$ recursively choose $a_n \in (\mathbf{Z}/p^n\mathbf{Z})^\times$ satisfying $a_n \bmod p^{n-1} = a_{n-1}$. Let $g_n \in \mathrm{Gal}(L_n/k)$ correspond to a_n (i.e., $g_n(\zeta) = \zeta^{a_n}$ for all p^nth roots of unity ζ in L_n).

(i) If $m \geq n \geq 2$, prove the effect of g_m on L_n coincides with that of g_n. Deduce that there is a unique $g \in \mathrm{Aut}_k(L)$ satsifying $g(x) = g_n(x)$ for all $n \geq 2$ and $x \in L_n$. What is g^{-1} on L_n?

(ii) Let $H := g^{\mathbf{Z}}$ be the subgroup of $\mathrm{Aut}_k(L)$ generated by g. Check that $L^H = k$. (Hint: Show that the fixed field in L_n for g_n is k for each n by proving via induction on n that a_n generates $(\mathbf{Z}/p^n\mathbf{Z})^\times$ for all $n \geq 2$.)

(iii) Show there are uncountably many choices of g, and deduce that upon choosing one g we can choose another g' that is not in H. Conclude that there are uncountably many distinct subgroups of $\mathrm{Aut}_k(L)$ that each has fixed field in L equal to k (so the "Galois correspondence" breaks down for separable normal extensions with infinite degree; it is fixed by putting a topology on $\mathrm{Aut}_k(L)$).