Solutions to Homework 11

1. Let k be a finite field with size q. Show that in $k[T]$, $T^{q^n} - T$ factors into the product of all monic irreducible polynomials of degree dividing n, each appearing exactly once in the factorization.

Since $T^{q^n} - T$ is separable over k (by the derivative test), it is a product of distinct monic irreducibles. If an irreducible f divides $T^{q^n} - T$, then $k[T]/f$ injects into a splitting field of $T^{q^n} - T$ over k, with the latter a degree n extension of k. Thus, $[k[T]/f : k]$ would have to divide n, so the degree of f divides n. Conversely, assume the degree d of f divides n. Since $[k[T]/f : k]$ is a degree d extension of k, the image t of T in $k[T]/f$ satisfies $t^{q^d} = t$. Thus, f divides $T^{q^d} - T$. Since $d|n$ implies that $T^{q^d} - T$ divides $T^{q^n} - T$ (proof?), we see that f divides $T^{q^n} - T$. Hence, $T^{q^n} - T$ is the product of all monic irreducibles in $k[T]$ with degree dividing n.

2. Let $L/\mathbf{Q}$ be a splitting field for $X^5 - 2 \in \mathbf{Q}[X]$. Writing $L = \mathbf{Q}(a, \zeta)$ with $a^5 = 2$ and $\zeta^5 = 1$, $\zeta \neq 1$, describe generators of $\mathrm{Aut}(L/\mathbf{Q})$ in terms of their actions on a and ζ. Describe $\mathrm{Aut}(L/\mathbf{Q})$ as an abstract group (i.e., in terms of 'generators and relations').

Let $G = \mathrm{Aut}(L/\mathbf{Q})$. For $g \in G$, we have $g(a) = a\zeta^i$ for some $\zeta^i \in \mu_5$ (with $\mu_5 = \langle \zeta \rangle$ the group of 5th roots of unity in L) and $g(\zeta) = \zeta^j$ for some $j \in (\mathbf{Z}/5)^\times$. Thus, there are at most 20 possibilities for g. Since $\mathbf{Q}(a)$ and $\mathbf{Q}(\zeta)$ are subfields of L with relatively prime degrees over $\mathbf{Q}$, we have $[L : \mathbf{Q}(a)] = 4$ and $[L : \mathbf{Q}(\zeta)] = 5$. Thus, $X^4 + X^3 + X^2 + X + 1$ is irreducible over $\mathbf{Q}(a)$ with $L/\mathbf{Q}(a)$ a splitting field, and $X^5 - 2$ is irreducible over $\mathbf{Q}(\zeta)$, with $L/\mathbf{Q}(\zeta)$ a splitting field. Hence, there exist $\sigma \in \mathrm{Aut}(L/\mathbf{Q}(a))$ with $\sigma(\zeta) = \zeta^2$ and $\eta \in \mathrm{Aut}(L/\mathbf{Q}(\zeta))$ with $\eta(a) = a\zeta$. Clearly $\mathrm{Aut}(L/\mathbf{Q}(a)) = \langle \sigma \rangle$ is cyclic of order 4 and $\mathrm{Aut}(L/\mathbf{Q}(\zeta)) = \langle \eta \rangle$ is cyclic of order 5.

By group theory, it then follows from $|G| \leq 20$ that in fact $|G| = 20$, so all 20 possibilities actually occur, and G is generated by σ and η. Since $\mathbf{Q}(\zeta)/\mathbf{Q}$ is normal, we know that $\mathrm{Aut}(L/\mathbf{Q}(\zeta)) = \langle \eta \rangle$ is a normal subgroup, with quotient $\mathrm{Aut}(\mathbf{Q}(\zeta)/\mathbf{Q})$. Since σ surjects onto a generator of this cyclic order 4 quotient, we see that G is 'generalized dihedral' of order 20. More explicitly, we check $\sigma\eta\sigma^{-1} = \eta^2$. This relation, together with $\sigma^4 = 1$ and $\eta^5 = 1$, determines the group structure: it is a semi-direct product $\mu_5 \rtimes (\mathbf{Z}/5)^\times$.

There is a unique subgroup of order 5, namely the 5-Sylow μ_5, and between this and G is a unique intermediate group of order 10 corresponding to the unique index 2 subgroup of the cyclic group $G/\mu_5 \simeq (\mathbf{Z}/5)^\times$ of order 4. Thus, there is a unique intermediate field of degree 4 over $\mathbf{Q}$ (i.e., "index 5" beneath L), visibly $\mathbf{Q}(\zeta)$, and within this is a unique quadratic subfield which is $\mathbf{Q}(\sqrt{5})$ since $z = \zeta + \zeta^{-1}$ is invariant under the index 2 subgroup $\langle -1 \rangle$ in $(\mathbf{Z}/5)^\times \simeq \mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$ and

$$0 = 1 + \zeta + \zeta^2 + \zeta^{-2} + \zeta^{-1} = 1 + z + z^2 - 2 = z^2 + z - 1$$

(so $z = (-1 \pm \sqrt{5})/2$).

It remains to work out the subgroups of orders 2 and 4, along with the associated intermediate fields (of degree 10 and 5 over $\mathbf{Q}$ respectively). The subgroup $(\mathbf{Z}/5)^\times = \langle \sigma \rangle$ is a 2-Sylow and it fixes $\mathbf{Q}(a)$. Since $[\mathbf{Q}(a) : \mathbf{Q}] = 5$ is the index of this 2-Sylow, $\mathbf{Q}(a)$ must be the entire fixed field of this 2-Sylow. Conjugating the 2-Sylow corresponds to other abstractly isomorphic copies of this subfield embedded into L (over $\mathbf{Q}$), so the degree 5 subfields are $\mathbf{Q}(a\zeta^j)$ for some $j \in \mathbf{Z}/5$. These are all *distinct* as subfields since the 2-Sylow has 5 distinct conjugates (it is not normal and the number n_2 of conjugates is odd and divides 20).

To handle subfields K of degree 10, we note that it must contain a subfield of degree 5 (as any order 2 subgroup lies in a 2-Sylow). Pick such a subfield, necessarily some $\mathbf{Q}(a\zeta^j)$. In fact, this subfield is *unique* because each order 2 subgroup lies in a *unique* 2-Sylow. Indeed, by conjugacy of 2-Sylows and the uniqueness of the element of order 2 within each 2-Sylow it suffices to check that the centralizer of the order 2 element σ^2 is $\langle \sigma \rangle$. This is clear since $\eta^j \sigma^2 \eta^{-j} = \eta^{2j}\sigma^2$ is equal to σ^2 if and only if $j \equiv 0 \bmod 5$. Since $\mathrm{Gal}(L/\mathbf{Q}(a\zeta^j)) \to \mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$ was seen to be an isomorphism above (working with the subfield $\mathbf{Q}(a)$, but the same goes for all subfields $\mathbf{Q}(a\zeta^j)$), we must have $K = \mathbf{Q}(a\zeta^j, \sqrt{5})$. This degree 10 extension has $\mathbf{Q}(a\zeta^j)$ as its unique subfield of degree 5 over $\mathbf{Q}$ and has $\mathbf{Q}(\sqrt{5})$ as its unique subfield of degree 2 over $\mathbf{Q}$ (as this is even the unique quadratic subfield of L over $\mathbf{Q}$).

Here is the field diagram, with field degrees indicated and j running over $\mathbf{Z}/5$ (there are no containments among the fields for different j's):

$$\begin{tikzcd}
& L & \\
\mathbf{Q}(a\zeta^j, \sqrt{5}) \arrow[ur, "2"] & & \mathbf{Q}(\zeta) \arrow[ul, "5"'] \\
\mathbf{Q}(a\zeta^j) \arrow[u, "2"] & & \mathbf{Q}(\sqrt{5}) \arrow[u, "2"'] \\
& \mathbf{Q} \arrow[ul, "5"] \arrow[ur, "2"'] &
\end{tikzcd}$$

The group diagram is readily given in a similar manner.

3. 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.
(i) For each $\sigma \in \mathrm{Aut}(L/k)$, prove there is a unique $n(\sigma) \in \mathbf{Z}/N$ so that $\sigma(\zeta) = \zeta^{n(\sigma)}$ for *every* Nth root of unity $\zeta \in L$.
(ii) Prove that $n(\sigma) \in (\mathbf{Z}/N)^\times$ 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 that 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 $\mathrm{Gal}(\mathbf{Q}(\zeta_{p^n})/\mathbf{Q}) \to (\mathbf{Z}/p^n)^\times$ is an *isomorphism*.

(i) The set of solutions to $X^N - 1 = 0$ in L is a cyclic group of order N, and the automorphism group of such a group is $(\mathbf{Z}/N)^\times$. Since the action of $\mathrm{Aut}(L/k)$ on L induces automorphisms of this cyclic group, the existence and uniqueness of $n(\sigma)$ drops out (even that it is a unit mod N, as required in (ii).
(ii) This was essentially shown in the solution to (i), up to some standard checks.
(iii) Recall that $\Phi_p(Y+1) \equiv Y^{p-1} \bmod p$. Since $\Phi_{p^n}(X) = \Phi_p(X^{p^{n-1}})$, we compute

$$\Phi_{p^n}(X+1) = \Phi_p((X+1)^{p^{n-1}}) \equiv \Phi_p(X^{p^{n-1}} + 1) \equiv X^{p^{n-1}(p-1)} \bmod p.$$

Since the monic $\Phi_{p^n}(X+1)$ has degree $p^{n-1}(p-1)$, we conclude that its lower degree coefficients are all divisible by p. Its constant term is $\Phi_{p^n}(X+1)|_{X=0} = \Phi_{p^n}(1) = p$, which is not divisible by p^2, so Eisenstein applies to establish irreducibility over $\mathbf{Q}$. Thus, $[\mathbf{Q}(\zeta_{p^n}) : \mathbf{Q}] = \deg \Phi_{p^n} = p^{n-1}(p-1) = |(\mathbf{Z}/p^n)^\times|$. Hence, the inclusion of $\mathrm{Gal}(\mathbf{Q}(\zeta_{p^n})/\mathbf{Q})$ into $(\mathbf{Z}/p^n)^\times$ must be an isomorphism.

4. Let k be a field containing a primitive Nth root of unity. Let $\mu_N \subseteq k^\times$ be the subgroup of Nth roots of 1 in $k^\times$. For $a \in k^\times$, let F/k be a splitting field of $X^N - a$.
(i) Show that $F = k(\alpha)$ where α is any root to $X^N - a$ in F. Also, for any $\sigma \in \mathrm{Aut}(F/k)$, show that $\sigma(\alpha)/\alpha \in \mu_N$ and that this is *independent* of the choice of α.
(ii) Fix a choice of α as in (i). Show that the map $\mathrm{Aut}(F/k) \to \mu_N$ given by $\sigma \mapsto \sigma(\alpha)/\alpha$ is an injective group homomorphism. In particular, $\mathrm{Aut}(F/k)$ is *abelian*. Also, show that this map is an isomorphism if and only if $X^N - a$ is irreducible in $k[X]$.

(i) Since $X^N - a = \prod_{\zeta \in \mu_N}(X - \alpha\zeta)$, clearly $F = k(\alpha)$. Since any $\zeta \in \mu_N$ lies in k, we see $\sigma(\zeta\alpha)/\zeta\alpha = \sigma(\alpha)/\alpha$. Since $\sigma(\alpha)$ and α are both Nth roots of a, their ratio must lie in μ_N.
(ii) The fact that the map is an injective group homomorphism is straightfoward (since $F = k(\alpha)$). If $X^N - a$ is irreducible, then there exist elements of $\mathrm{Aut}(F/k)$ moving α to any desired root of $X^N - a$, so we see the map must also be surjective. Conversely, if $\mathrm{Aut}(F/k) \simeq \mu_N$, then all $\alpha\zeta$ must satisfy the same minimal polynomial over k (why?). There are N such distinct elements, yet α already satisfies $X^N - a$, so this must be the minimal polynomial and so is irreducible in $k[X]$.

5. Consider $f = 2X^5 - 10X + 5 \in \mathbf{Q}[X]$. Let $L/\mathbf{Q}$ be a splitting field of f. Show that $\mathrm{Gal}(L/\mathbf{Q})$ injects (as a group) into S_5 and that it contains an element of order 2 and an element of order 5. Deduce that $\mathrm{Gal}(L/\mathbf{Q}) \simeq S_5$.

By Eisenstein (with $p = 5$), f is irreducible (note the leading coefficient of 2 does not causes a problem here!). Thus, $[L : \mathbf{Q}]$ is divisible by $[\mathbf{Q}(a) : \mathbf{Q}] = 5$, with a a root of f in L. Since $L/\mathbf{Q}$ is normal and separable, $\mathrm{Aut}(L/\mathbf{Q}) = [L : \mathbf{Q}]$ is divisible by 5 and so contains an element of order 5. On the other hand, by calculus we see f has exactly 3 real roots, so there are exactly two non-real roots inside of a splitting field within $\mathbf{C}$. Complex conjugation therefore gives rise to an element of order 2 in $\mathrm{Aut}(L/\mathbf{Q})$ which is a transposition.

The group injection $\mathrm{Aut}(L/\mathbf{Q}) \to S_5$ is just the permutation action on the roots (after they are labelled). But by elementary group theory, for a prime p the group S_p is generated by any transposition and any element of order p. Thus, we conclude $\mathrm{Aut}(L/\mathbf{Q}) \simeq S_5$. In particular, this group is *not* solvable. When combined with refinements of Exercises 3 and 4, this will show that f cannot be solved 'in radicals' (since a radical tower will essentially give rise to a solvability series for $\mathrm{Gal}(L/\mathbf{Q})$, an impossibility).

6. Let $f = T^{p^2} + XT^p + Y \in k[T]$, with $k = \mathbf{F}_p(X, Y)$. Show that f is irreducible and let $L = k(a)$ be an extension generated over k by a single root of f. Show that $[L : k]_s = p$ and that there is a *unique* non-trivial intermediate extension k' between k and L. Conclude that L/k cannot be built up as a tower $L/E/k$ with E/k purely inseparable and L/E separable.

Viewing f in $\mathbf{F}_p(X)[Y, T]$ and then in $\mathbf{F}_p(X, T)[Y]$, we see that f is irreducible in $k[T]$ (one could argue more naturally if we knew that $\mathbf{F}_p[X, Y]$ is a UFD, but we haven't proved that and so I avoid using it). Thus, $[L : k] = p^2$. Since $f = g(T^p)$ with g separable of degree p, we see that $[L : k]_s = p$. Thus, there is a unique degree p intermediate extension k'/k which is separable over k, namely $k' = k(a^p)$.

Now let E/k be some degree p extension inside of L/k (viewing k as a subfield of L). If $E \neq k'$, then E/k must be purely inseparable (why?), so $[L : E]_s = [L : k]_s/[E : k]_s = p$, whence L/E is separable of degree p, with primitive generator a. Thus, the minimal polynomial g of a over E divides f and is separable of degree p. In a splitting field of f over E, f is a product of pth powers of monic linear factors and g is the product of just these monic linear factors (why?), so we see that over this splitting field, $g^p = f$. But this latter equality then must hold in $E[T]$ as well (why?). It then follows that we must have $g = T^p + xT + y$, with $x, y \in E$ satisfying $x^p = X$, $y^p = Y$. Hence, the degree p extension E contains a splitting field for $(U^p - X)(U^p - Y) \in k[U]$. But we saw on a previous homework (up to changing notation) that such a splitting field has degree p^2 over k and so cannot lie inside of E/k. This is a contradiction, so no such $E \neq k'$ exists.

7. Let $f \in k[T]$ be an irreducible monic, L/k a splitting field. If k'/k is an extension generated by a single root of f (so $k' \simeq k[X]/f$), then show that in $L[T]$

$$f = \prod_{j=1}^{[k':k]_s} (T - r_j)^{[k':k]_i},$$

with all r_j's distinct.

We know that in $L[T]$, we have

$$f = \prod_{j=1}^{d} (T - r_j)^{p^e}$$

with some d and p^e; we need to show that $d = [k' : k]_s$ and $p^e = [k' : k]_i$. Since $[k' : k] = [k' : k]_s[k' : k]_i$ and $[k' : k]$ is also the degree of f, which is equal to $d \cdot p^e$, it suffices to show that $d = [k' : k]_s$. We may choose $k' = k(r_1)$, so for $a = r_1^{p^e}$, a is separable over k and k' is purely inseparable over $k(a)$ (since it is obtained by adjoining a p^eth root to a). Thus, $[k' : k]_s = [k' : k(a)]_s[k(a) : k]_s = [k(a) : k]$. Since $f = g(X^{p^e})$ with g a separable monic *irreducible* in $k[T]$, and $g(a) = 0$, we see that $[k(a) : k]$ is equal to the degree of g, yet g clearly has degree d by construction. Hence, $[k' : k]_s = d$, as desired.

8. Let k be a field of positive characteristic p, and choose $a \in k$. Prove that $f_a(t) = t^p - t - a \in k[t]$ is either a product of linears or else is irreducible of degree p with splitting field k_a Galois of degree p over k (hint: see Exercise 7 on HW7, or rather its solution), and that $k_a \simeq k_{a'}$ over k if $a' - a = b^p - b$ for some $b \in k$ (in particular, when such an equation holds, show f_a is irreducible over k if and only if $f_{a'}$ is).

If r is a root in a splitting field of f_a, the set of all roots is $r + c$ for $c \in \mathbf{F}_p \subseteq k$ since the $s^p - s - a = 0 = r^p - r - a$ forces $s - r = s^p - r^p = (s-r)^p$ and the solutions to $T^p = T$ in k are the elements of $\mathbf{F}_p$. Hence, once an extension contains one root of f_a, it contains all roots.

If $f_a = gh$ with $g, h \in k[t]$ monic of degree $< p$, then g has roots of the form $r + c_i$ (in an extension of k) for various $c_i \in \mathbf{F}_p$, so if $\deg(g) = \delta < p$ then the $t^{\delta-1}$ coefficient in g is $\delta r + c$ for some $c \in \mathbf{F}_p$ and $\delta \in \mathbf{Z}$ not divisible by p. But this coefficient lies in k (as $g \in k[t]$), so we see that r also lies in k and hence f_a splits over k. Thus, either f_a is irreducible over k or else it splits over k.

Since f_a has distinct roots (or by computing its derivative), it follows that when f_a is irreducible then its splitting field is a Galois extension of degree p over k. If $a' - a = b^p - b$ for some $b \in \mathbf{F}_p$, then it is easy to compute that $r \mapsto r + b$ is a bijection from the roots of f_a onto the roots of $f_{a'}$ (in a common splitting field for both). But $b \in k$, so it follows that an extension containing the roots of f_a also contains the roots of $f_{a'}$ and vice-versa. Hence, within a common splitting field for both we see that the splitting subfields of f_a and $f_{a'}$ coincide. Thus, f_a is irreducible over k if and only if $f_{a'}$ is, and in such cases $k_a \simeq k_{a'}$ over k.