Solutions to Homework 12

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 (called the *Frobenius map*).
(ii) What is the size of a splitting field of $X^{15} - 2$ over $\mathbf{F}_7$?

(i) The map $x \mapsto x^{|k|}$ clearly has order $[k' : k]$ in $\mathrm{Gal}(k'/k)$ (proof?). But $|\,\mathrm{Gal}(k'/k)| = [k' : k]$.
(ii) A splitting field contains a 15th root of 2 and 15th roots of unity. An extension $\mathbf{F}_{7^n}$ of degree n over $\mathbf{F}_7$ contains a primitive 15th root of unity if and only if $7^n - 1$ is divisible by 15. On the other hand, $2 \in \mathbf{F}_7^\times$ has order 3, so if $x^{15} = 2$, then x is a primitive 45th root of unity. Conversely, if $\mathbf{F}_{7^n}$ contains a primitive 45th root of unity, we see that from the cyclicity of $\mathbf{F}_{7^n}^\times$, 2 is a 45th power in $\mathbf{F}_{7^n}$. Thus, 2 is a 15th power in $\mathbf{F}_{7^n}$ if and only if $7^n - 1$ is divisible by $\mathrm{lcm}(15, 45) = 45$. From this, we conclude that $X^{15} - 2$ splits in $\mathbf{F}_{7^n}[X]$ if and only if 7 has order dividing n in $(\mathbf{Z}/45)^\times \simeq (\mathbf{Z}/5)^\times \times (\mathbf{Z}/9)^\times$. That is, n must be divisible by $\mathrm{lcm}(4, 3) = 12$, so a splitting field has size 7^{12}.

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

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

(i) Since L_1/k is the splitting field of a separable polynomial $f \in k[X]$, so is L_1L_2/L_2 (and view $f \in L_2[X]$). Any element $\sigma \in \mathrm{Gal}(L_1L_2/L_2)$ fixes k and so permutes the roots of f around (by unique factorization and the fact that $f \in k[X]$). Thus, σ induces a k-algebra map from L_1 back to itself. Such a map must be an automorphism (by degree considerations), so we get the desired group map, injective by looking at action on roots of f.

The image of $\mathrm{Gal}(L_1L_2/L_2) \to \mathrm{Gal}(L_1/k)$ clearly lies inside of $\mathrm{Gal}(L_1/L_1 \cap L_2)$. To prove equality, we need to show that $[L_1L_2 : L_2] = [L_1 : L_1 \cap L_2]$. For this, we may replace k by $L_1 \cap L_2$ and so can assume $L_1 \cap L_2 = k$. Write $L_1 = k(a)$, with a having minimal polynomial $g \in k[T]$. We need to show that g remains irreducible in $L_2[T]$. Any monic irreducible factor g_0 of g in $L_2[T]$ has coefficients which are symmetric functions in some subset of the roots of g. All of these roots lie in L_1, so the coefficients of g_0 lie in $L_1 \cap L_2 = k$. That is, the monic irreducible factorization of g in $L_2[T]$ is also one in $k[T]$, so g is irreducible in $L_2[T]$.
(ii) It suffices to show that $[L_1L_2 : L_2] = [L_1 : k]$. Since $L_1 \cap L_2 = k$, this was shown above.
(iii) There is certainly such a natural map of groups, visibly injective. Since both sides have the same size, it is bijective and thus an isomorphism.

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 in which all elements 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.

(i) To prove the result for a given extension, it suffices to treat any larger extension. Thus, we may pass to Galois closures (K is perfect!) to reduce to the case of F/K a finite Galois extension with Galois group G.

Let K' be the fixed field of a 2-Sylow subgroup P_2 of G, so $[K' : K] = [G : P_2]$ is odd. By the primitive element theorem, $K' = K(a)$, with a the root of an irreducible $f \in K[X]$, so f has degree equal to $[K' : K]$,

which is odd. By hypothesis, f must then have a root in K, so f is linear and therefore $K' = K$. Thus, $[F : K] = |G| = |P_2| = 2^n$ for some $n \geq 0$.
(*ii*) If L'/L is a non-trivial finite extension, then L'/K is separable and hence the Galois closure of L'/K provides another non-trivial finite extension of L which is even Galois over K. Hence, to prove L is algebraically closed it suffices to show that a finite extension L'/L which is Galois over K must be a trivial extension of L. By (*i*), $[L' : K]$ is a power of 2. Thus, $[L' : L]$ is a power of 2. Thus, $\mathrm{Gal}(L'/L)$ is a 2-group. If this group is non-trivial, it contains an index 2 subgroup (as p-groups admit solvability series whose successive quotients are cyclic of order p). By Galois theory, this gives rise to a quadratic extension of L. But since we are not in characteristic 2, such an extension has the form $L(\sqrt{a})$ for some $a \in L$ not a square. But all $a \in L$ are squares. Thus, $L' = L$.
(*iii*) By the Intermediate Value Theorem, all odd degree $f \in \mathbf{R}[X]$ have a root in $\mathbf{R}$. For $\mathbf{C} = \mathbf{R}(\sqrt{-1}) = \mathbf{R}[X]/(X^2+1)$, we have $x + y\sqrt{-1} = (u + v\sqrt{-1})^2$, with $u, v \in \mathbf{R}$ given by the formulas

$$u^2 = (x + \sqrt{x^2+y^2})/2, \quad v^2 = (-x + \sqrt{x^2+y^2})/2,$$

and the fact that all nonnegative elements of $\mathbf{R}$ have a unique nonnegative square root in $\mathbf{R}$ (and choose $u \geq 0$ and $\mathrm{sgn}(v) = \mathrm{sgn}(y)$). By the above, we may conclude that $\mathbf{C}$ is algebraically closed.

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

First consider $X^3 - 2$. This is irreducible and the splitting field $L = \mathbf{Q}(\alpha, \omega)$, with $\alpha^3 = 2$ and $\omega^3 = 1$, $\omega \neq 1$. We know $[L : \mathbf{Q}] = 6$ and so the natural injection $\mathrm{Gal}(L/\mathbf{Q}) \to S_3$ by action on the roots is an isomorphism. Writing down the subgroups of S_3 and the associated intermediate fields is easy (the cubic extensions are $\mathbf{Q}(\alpha\omega^i)$, $i = 0, 1, 2$, and the quadratic extensions are just $\mathbf{Q}(\omega)$, the latter being the only normal intermediate extension over $\mathbf{Q}$, aside from $\mathbf{Q}$ and L).

Now let $L/\mathbf{Q}$ be the splitting field of $X^4 - 4X^2 - 1$, which is clearly irreducible, with roots $\alpha, -\alpha, \beta, -\beta$, where α^2 and β^2 are the two roots to $Y^2 - 4Y - 1$ in L. Thus, $\mathbf{Q}(\alpha)$ is degree 4 over $\mathbf{Q}$ and $L = (\mathbf{Q}(\alpha))(\beta)$ is at worst quadratic over $\mathbf{Q}(\alpha)$. Clearly $Y^2 - 4Y - 1$ has roots $\alpha^2 = 2 + \sqrt{5}$ and $\beta^2 = 2 - \sqrt{5}$ (where we *define* $\sqrt{5} = \alpha^2 - 2$ to make the choice of $\sqrt{5} \in L$ unambiguous). Since α^2 and β^2 are squares in L, so is $-1 = (\alpha\beta)^2$, so we see that L does not have any real embeddings. However, $\mathbf{Q}(\alpha)$ does have a real embedding (i.e., $X^4 - 4X^2 - 1$ has a root in $\mathbf{R}$). Thus, $L \neq \mathbf{Q}(\alpha)$, so $[L : \mathbf{Q}] = 8$.

Since $(\alpha\beta)^2 = -1$, we see that $L = \mathbf{Q}(\alpha, i)$, with $i = \alpha\beta$ satisfying $i^2 = -1$. For any $g \in \mathrm{Gal}(L/\mathbf{Q})$, we have 4 choices for $g(\alpha)$ (namely $\alpha, -\alpha, \beta, -\beta$) and 2 choices for $g(i)$, for a total of 8 choices. But $|\mathrm{Gal}(L/\mathbf{Q})| = [L : \mathbf{Q}] = 8$, so all 8 possibilities actually occur. Define $\sigma, \tau \in \mathrm{Gal}(L/\mathbf{Q})$ by $\sigma(\alpha) = \beta$, $\sigma(i) = -i$ (so $\sigma(\beta) = -\alpha$, since $i = \beta\alpha$), and $\tau(\alpha) = \alpha$, $\tau(i) = -i$ (so $\tau(\beta) = -\beta$). Clearly $\sigma^4 = \tau^2 = 1$ and $\tau\sigma\tau^{-1} = \sigma^{-1}$, so $\mathrm{Gal}(L/\mathbf{Q}) = D_4$.

The subgroups of order 4 are $\langle\sigma\rangle$ (cyclic) and $\langle\sigma^2, \tau\rangle$, $\langle\sigma\tau, \sigma^3\tau\rangle$ ($\mathbf{Z}/2 \times \mathbf{Z}/2$). The only order 2 element in $\langle\sigma\rangle$ is σ^2, while $\langle\sigma^2, \tau\rangle$ contains the order 2 elements $\tau, \sigma^2\tau, \sigma^2$ and $\langle\sigma\tau, \sigma^3\tau\rangle$ contains the order 2 elements $\sigma\tau, \sigma^3\tau, \sigma^2$. From this we readily get the lattice for subgroups, and we see that the only normal subgroups are the ones of order 4 and the subgroup $\langle\sigma^2\rangle$ (which is the center).

It remains to determine the associated fields. We have $\alpha/\beta - \beta/\alpha$ is fixed by σ and is a square root of -20, so the fixed field of $\langle\sigma\rangle$ is $\mathbf{Q}(\sqrt{-5})$. The fixed field of $\langle\sigma^2\rangle$ is $\mathbf{Q}(\alpha/\beta)$ (indeed, note that α/β is fixed and $(\alpha/\beta)^2 = -9 - 4\sqrt{5}$ is not a square in $\mathbf{Q}(\sqrt{5})$, so $[\mathbf{Q}(\alpha/\beta) : \mathbf{Q}] = 4$). The fixed field of $\langle\sigma^2, \tau\rangle$ is $\mathbf{Q}((\alpha/\beta)^2) = \mathbf{Q}(\sqrt{5})$, the fixed field of $\langle\tau\rangle$ is $\mathbf{Q}(\alpha)$, and the fixed field of $\langle\sigma^2\tau\rangle$ is $\mathbf{Q}(\beta)$. Lastly, the fixed field of $\langle\sigma\tau, \sigma^3\tau\rangle$ is $\mathbf{Q}(i)$, the fixed field of $\langle\sigma\tau\rangle$ is $\mathbf{Q}(\alpha+\beta)$ (note that $\alpha + \beta$ does have 4 distinct conjugates under D_4 and so has degree 4 over $\mathbf{Q}$), and the fixed field of $\langle\sigma^3\tau\rangle$ is $\mathbf{Q}(\alpha - \beta)$.

Explicitly, the Galois subextensions over $\mathbf{Q}$ (aside from L and $\mathbf{Q}$) are $\mathbf{Q}(i)$, $\mathbf{Q}(\sqrt{5})$, $\mathbf{Q}(\sqrt{-5})$, and $\mathbf{Q}(\alpha/\beta)$.

5. Let $k \subseteq L$ be a Galois extension, perhaps with infinite degree. For any intermediate F between L and k, define $G(F)$ as usual, and for any subgroup H in $\mathrm{Gal}(L/k)$, define L^H as usual.
(*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 $e_n = 1! + 2! + \dots (n-1)!$ 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) 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.

(i) If $x \notin F$, then let K be the splitting field for x over F inside of the normal L/F. By finite Galois theory, there exists a non-trivial $g \in \mathrm{Gal}(K/F)$ with $g(x) \neq x$. Since $G(F) = \mathrm{Gal}(L/F) \to \mathrm{Gal}(K/F)$ is surjective, choose $g' \in G(F)$ mapping onto g, so $g'(x) \neq x$. That is, $L^{G(F)} \subseteq F$. The reverse inclusion is clear.
(ii) Since x generates a minimal field $\mathbf{F}_p(x)$, it suffices to show that if $\mathbf{F}_{p^n}$ lies inside of $\mathbf{F}_{p^m}$ (so $n|m$), then $g_n(x) = g_m(x)$. But $e_m \equiv e_n \bmod n$ since $m \geq n$, so $x^{p^{e_m}} = \varphi^{e_m}(x) = \varphi^{e_n}(x) = x^{p^{e_n}}$ (since φ has order n in $\mathrm{Gal}(\mathbf{F}_{p^n}/\mathbf{F}_p)$). Thus, the desired g exists by the given formula and clearly $g \notin H$ (proof?).