2014 Algebra SEP $\sim$ Fields Day 3 Solutions, by E. Dummit

1. (Jan-08.3): Let ϵ be a primitive 16th root of unity and $\alpha = \epsilon\sqrt{2}$, with $E = \mathbb{Q}[\epsilon]$ and $f(x) = x^8 + 16$; observe that $f(\alpha) = 0$.

   (a) Show that $\sqrt{2} \in \mathbb{Q}[\epsilon^2]$.

   (b) Show that $f(x)$ splits in $E[x]$.

   (c) For $G = \mathrm{Gal}(E/\mathbb{Q})$, show that no nonidentity element of G fixes α. Conclude that $f(x)$ is irreducible in $\mathbb{Q}[x]$.

   Solution:

   a) Without loss of generality let $\epsilon = e^{i\pi/8}$; then $\epsilon^2 = \dfrac{\sqrt{2}}{2} + \dfrac{\sqrt{2}}{2}i$, so $\sqrt{2} = \epsilon^2 + \dfrac{1}{\epsilon^2} = \epsilon^2 + \epsilon^{14}$.

   b) By the usual, the 8 roots of $f(x)$ are $\epsilon^{2k+1}\sqrt{2}$, for $0 \leq k \leq 7$. Since $\sqrt{2} \in E$ by part (a) we see that all roots of f lie in E.

   c) Suppose $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ fixes $\alpha = \epsilon\sqrt{2}$. Observe that $\sigma(\sqrt{2}) = \pm\sqrt{2}$: if $\sigma(\sqrt{2}) = \sqrt{2}$, then $\sigma(\alpha) = \alpha$ implies $\sigma(\epsilon) = \epsilon$, but since ϵ generates E, σ fixes all of E hence is the identity. If it were true that $\sigma(\sqrt{2}) = -\sqrt{2}$, then we would need $\sigma(\epsilon) = -\epsilon$, but then $\sigma(\epsilon^2) = \epsilon^2$, so by part (a), σ would have to fix $\sqrt{2}$, contrary to the assumption that $\sigma(\sqrt{2}) = -\sqrt{2}$. Hence σ is the identity, and by the usual argument this implies f is irreducible.

   Remark Another approach to this problem is to show directly that the splitting field of f is $\mathbb{Q}[\alpha]$: this follows from the observation that the other roots of f are $\alpha \cdot \epsilon^{2k}$ for $0 \leq k \leq 7$ and from the fact that $\epsilon^2 = \dfrac{1}{2}\alpha^2 \in \mathbb{Q}[\alpha]$. Then in fact we can see that $\mathbb{Q}[\alpha] = \mathbb{Q}[\epsilon]$, since $\sqrt{2} \in \mathbb{Q}[\epsilon^2]$, meaning that $\sqrt{2}$ lies in both $\mathbb{Q}[\alpha]$ and $\mathbb{Q}[\epsilon]$. Since the minimal polynomial of ϵ has degree $\varphi(16) = 8$, we see that $|\mathbb{Q}[\epsilon] : \mathbb{Q}| = |\mathbb{Q}[\alpha] : \mathbb{Q}| = 8$, meaning that f is irreducible, and that $G = \mathrm{Gal}(E/\mathbb{Q})$ is simply the Galois group of f.

---

2. (Jan-11.3): Let E/F be an extension of char-0 fields with $E = F[\alpha]$ for some α with $\alpha^p \in F$ and some prime p. Let $E^* = E[\epsilon]$ where ϵ is a primitive pth root of unity.

   (a) Show that E^* is a Galois extension of F.

   (b) If E is Galois over F, show $E = F$ or $E = E^*$.

   (c) Show by example that it is possible to have $E = E^*$ without having $\epsilon \in F$.

   Solution:

   a) E^* is the splitting field of $x^p - \alpha^p \in F[x]$, since the roots of this polynomial are $\alpha \cdot \epsilon^k$ for $0 \leq k \leq p-1$. Hence it is Galois, since F has characteristic zero.

   b) Consider the action of $\mathrm{Gal}(E/F)$ on α: if every element fixes α, then $\alpha \in F$ hence $E = F$. Otherwise, if some element σ does not fix α, then since $x^p - \alpha^p \in F[x]$ we see that $\sigma(\alpha) \in E$ is also a root of $x^p - \alpha^p$, hence $\sigma(\alpha) = \alpha \cdot \epsilon^k$ for some $1 \leq k \leq p-1$. Hence $\epsilon^k = \dfrac{\sigma(\alpha)}{\alpha} \in E$, so since k is invertible mod p, we get $\epsilon \in E$, whence $E = E^*$.

   c) We can take $F = \mathbb{Q}$, $\alpha = \epsilon = \zeta_3$, $p = 3$: then $E^* = E = \mathbb{Q}(\zeta_3)$, but $\epsilon \notin F$.

---

3. (Jan-14.5): Let L/K be a field extension of degree 4. We say K' is intermediate between K and L if K' properly contains K and is properly contained in L.

   (a) Show that L/K has at most 3 intermediate fields.

   (b) Give an explicit example to show that there can be 3 intermediate fields between L and K.

   (c) Give an explicit example to show that there can be 0 intermediate fields between L and K.

Remark In fact, as it was stated on the qualifying exam, part (a) is false unless we also assume L/K is separable. A spectacular counterexample is the following: $K = k(x^2, y^2)$ and $L = k(x, y)$, where k is an infinite field of characteristic 2 and x and y are indeterminates. Then L/K has degree 4, but there are in fact infinitely many intermediate subfields, one family of which is given by $K_\alpha = K(x + \alpha y)$ for $\alpha \in k$. (It is reasonably easy to check that both L/K_α and K_α/K are degree-2 extensions.) The reason this example exists is due to the following theorem: A finite-degree extension L/K has finitely many intermediate fields if and only if L is a primitive extension of K – that is, if L is obtained by adjoining a single element to K (i.e., there exists an irreducible polynomial p such that $L \cong K[x]/p(x)$). The point here is that this inseparable extension cannot be generated by a single element.

Solution: If L/K is separable of degree 4, consider its normal closure $\hat{L}/K$, which is a Galois extension. Denote $G = \mathrm{Gal}(\hat{L}/K)$ and also let $\mathrm{Gal}(\hat{L}/L) = H$.

a) From its action on the roots of the minimal polynomial of a generator of L/K, we get an embedding of G as a transitive subgroup of the symmetric group S_4. There are five possibilities, up to conjugacy in G: (i) $G = \langle (1\,2\,3\,4) \rangle$ is cyclic of order 4, (ii) $G = \langle (1\,2)(3\,4), (1\,3)(2\,4) \rangle$ is the Klein 4-group, (iii) $G = \langle (1\,2\,3\,4), (1\,3) \rangle$ is the dihedral group of order 8, (iv) G is the alternating group A_4, (v) G is S_4. By the Galois correspondence, the intermediate fields K' correspond to index-2 subgroups of G containing a point stabilizer H (in other words: H is the subgroup of G that fixes 1). The cases have the following numbers of such subgroups: (i) one subgroup $\langle (1\,3)(2\,4) \rangle$, (ii) three subgroups each generated by an element of order 2, (iii) one subgroup $\langle (1\,2\,3\,4) \rangle$, (iv) no subgroups, (v) no subgroups. In each case, there are at most 3 intermediate fields.

a-alt) By hypothesis, H is a subgroup of G of index 4, and intermediate subfields correspond to subgroups containing H having index 2 in G. Such a subgroup is necessarily the union of H and another of the 3 left cosets of H, so there are at most 3 intermediate extensions.

b) From the analysis in (a), there can be 3 intermediate fields only when the extension L/K itself is Galois with Galois group the Klein 4-group. One such example over $K = \mathbb{Q}$ is $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

c) From the analysis in (a), there can be 0 intermediate fields when the extension L/K is a degree-4 extension with Galois closure the alternating group A_4 or S_4 – i.e., if $L = K[\alpha]$ where α is a root of an irreducible degree-4 polynomial in $K[x]$ whose Galois group is A_4 or S_4. It is not too likely that one would know a quartic whose Galois group is provably A_4 or S_4 offhand, but $p(x) = x^4 + 8x + 12$ has Galois group A_4 over $\mathbb{Q}$ and $q(x) = x^4 - x + 1$ has Galois group S_4 over $\mathbb{Q}$.

Remark One can prove these statements about p and q by observing that they are both irreducible, that the discriminant of p is $2^{12}3^4$ (a square), that the discriminant of q is 229 (not a square), and then factoring p and q modulo primes not dividing the discriminant to see that the irreducible-factor degrees yield all of the possible cycle types in A_n or S_n respectively. For example, q is irreducible modulo 2, and modulo 3 it has factors of degrees 1 and 3. By a standard result of number theory, this means the Galois group of q contains a 4-cycle and a 1,3-cycle, but the only such subgroup of S_4 is S_4 itself. Similarly, p modulo 5 has irreducible factors of degrees 1 and 3, and since its discriminant is a square, its Galois group must be A_4.

bc-alt) For (b) and (c) one can also use this general construction for an extension L/K with arbitrary Galois group G: let G be embedded as a subgroup of a symmetric group S_n, and let $L = \mathbb{C}(x_1, \cdots, x_n)$ and $F = \mathbb{C}(\sigma_1, \cdots, \sigma_n)$ where σ_i is the elementary symmetric function in the x_j of degree i. Then $\mathrm{Gal}(L/F) = S_n$: it contains S_n (each of the σ_i is fixed by index permutation on the x_j), but L is also the splitting field of the polynomial $p(x) = \prod_i (x - x_i) = \sum_j (-1)^{n-j} \sigma_{n-j} x^j$ of degree n, so $|L : F| \leq n!$, hence equality must hold. Now let K be the fixed field of G inside L; then by the Galois correspondence, L/K is Galois and $\mathrm{Gal}(L/K) \cong G$.

4. (Aug-05.3): Let p, q be distinct primes and let $\mu = q^{1/p}$ and $\nu = p^{1/q}$.

   (a) Let F be a subfield of $\mathbb{R}$ not containing μ. If $\mu^n \in F$ for some $n > 0$, show that $p|n$.

   (b) With F as in (a), show that $|F[\mu] : F| = p$.

   (c) Show that $|\mathbb{Q}[\mu + \nu] : \mathbb{Q}| = pq$.

   Solution:

   a) If $p|n$ we are done so assume n is invertible mod p, say with $mn = 1 + kp$ for some integers m and k. Then $q^{-k}\mu^{nm} = \mu \in F$, contradicting the assumption that $\mu \notin F$.

   b) Consider the minimal polynomial $q(x)$ of μ over F: it divides $x^p - q$, so its other roots must be of the form $\mu \cdot \zeta_p^k$ for some integers $1 \leq k \leq p-1$. Its constant term $q(0)$ is the product of some of these, hence is of the form $\pm\mu^d \cdot \zeta_p^f$. Since F is a subfield of $\mathbb{R}$ we see that ζ_p^f must be in $\mathbb{R}$, hence must be ± 1 – thus $\mu^d \in F$, so by part (a) we see $p|d$. Since $d \leq p$ we see $d = p$, and so $q(x)$ has degree p, and so $|F[\mu] : F| = p$.

   c) By Eisenstein, $x^p - q$ and $x^q - p$ are irreducible, so $|\mathbb{Q}(\mu) : \mathbb{Q}| = p$, $|\mathbb{Q}(\nu) : \mathbb{Q}| = q$, and then $|\mathbb{Q}(\mu, \nu) : \mathbb{Q}| = pq$ since the degrees are coprime, so it is enough to show that $\mathbb{Q}(\mu + \nu) = \mathbb{Q}(\mu, \nu)$. If one of μ, ν is in $F = \mathbb{Q}(\mu + \nu)$ then the other is also, so suppose neither is: then by part (b) applied to $F[\mu] = \mathbb{Q}(\mu, \nu)$ and then $F[\nu] = \mathbb{Q}(\mu, \nu)$, we would have $|\mathbb{Q}(\mu, \nu) : F| = p$ and also $|\mathbb{Q}(\mu, \nu) : F| = q$, which is impossible.

---

5. (Aug-06.3): Let $\mathbb{Q} \subseteq K \subseteq E \subseteq \mathbb{C}$ be fields with $E = \mathbb{Q}[\alpha]$ with $\alpha^n \in \mathbb{Q}$, and K is generated by all roots of unity in E. Assume E is Galois over $\mathbb{Q}$.

   (a) Show that $\mathrm{Gal}(E/K)$ is cyclic.

   (b) If the restriction τ of complex conjugation to E is in the center of $\mathrm{Gal}(E/\mathbb{Q})$, prove that $|\alpha|^2 \in \mathbb{Q}$.

   Solution:

   a) Let $\sigma \in \mathrm{Gal}(E/K)$ and observe that $\sigma(\alpha)^n = \sigma(\alpha^n) = \alpha^n$, since $\alpha^n \in \mathbb{Q}$, so $\sigma(\alpha) = \alpha \cdot \zeta_\sigma$ for some nth root of unity ζ_σ. Since E is Galois, all Galois conjugates of α lie in E, so $\zeta \in E$ hence by definition of K, $\zeta \in K$. But now we see that the map $\pi : \mathrm{Gal}(E/K) \mapsto \mu_n$ (the group of nth roots of unity) defined by sending $\sigma \mapsto \zeta_\sigma$ is a well-defined homomorphism from the Galois group to the group of nth roots of unity, which is cyclic. The map is also injective since if $\pi(\sigma) = 1$, then $\sigma(\alpha) = \alpha$, so that σ fixes E, hence is the identity in $\mathrm{Gal}(E/K)$. Since subgroups of cyclic groups are cyclic, we see that $\mathrm{Gal}(E/K)$ is cyclic.

   b) Let $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ and as above observe that $\sigma(\alpha) = \alpha \cdot \zeta_n$ for some nth root of unity. But then since τ is central, we have $\sigma(|\alpha|^2) = \sigma(\alpha \cdot \tau(\alpha)) = \sigma(\alpha) \cdot \sigma(\tau(\alpha)) = \sigma(\alpha) \cdot \tau(\sigma(\alpha)) = |\sigma(\alpha)|^2 = |\alpha\zeta_n|^2 = |\alpha|^2$. Hence σ fixes $|\alpha|^2$ for every σ, meaning $|\alpha|^2 \in \mathbb{Q}$.

---

6. (Jan-05.3): Let F be a field and $f(x) \in F[x]$ be irreducible. Suppose E/F is an extension containing a root α of $f(x)$ such that $f(\alpha^2) = 0$. Show that f splits over E.

Solution: The idea is: $\alpha \mapsto \alpha^2$ is morally an element of the Galois group, so the square of any root of f should also be a root of f. To show this without passing to a Galois closure (in case we are in positive characteristic, which could cause problems), we can let $g(x) = f(x^2)$ and observe that α is a root of both f and g. Since f is the minimal polynomial, we see that f divides g, and so we can write $f(x^2) = f(x) \cdot q(x)$, where q has the same degree as f. Then if β is any root of f, we see $f(\beta^2) = f(\beta) \cdot q(\beta) = 0$, so β^2 is also a root of f. Since f has only finitely many roots, by iterating this we see that $\beta^{2^a} = \beta^{2^b}$ for some a and b, so either $\beta = 0$ (in which case $f(x) = x$), or β is a primitive nth root of unity for some n. If any roots of f are primitive kth roots of unity for $k < n$, then $\gcd(f, x^k - 1)$ has positive degree and divides f; since f is irreducible, this means its roots are all primitive nth roots of unity. Then f splits over $F[\alpha] \subseteq E$ since the other roots are powers of α.

Remark The official solution assumes without explanation the fact that if α is an nth root of unity, then all other roots are also nth roots of unity. While this is true, it requires justification!

---

7. (Aug-11.3): Let $K \subseteq F \subseteq E$ be fields with $E = F[\alpha]$, $\alpha^n \in F$ for some n, and K containing a primitive nth root of unity. Let L be a field with $K \subseteq L \subseteq E$ with $L \cap F = K$.

   (a) If L is Galois over K, show that $L = K[\beta]$ for some β with $\beta^n \in K$.

   (b) Show by example that L need not be Galois over K.

Solution:

a) First observe that E is Galois over F, since E is the splitting field of the polynomial $x^n - \alpha^n \in F[x]$, as all its roots lie in E (since K contains a primitive nth root of unity). The Galois group $\mathrm{Gal}(E/F)$ is also cyclic: every element of the Galois group fixes $x^n - \alpha^n \in F[x]$, hence $\sigma(\alpha) = \alpha \cdot \zeta \in E$ where ζ is some nth root of unity (necessarily fixed by σ since K contains a primitive nth root of unity); conversely since α generates the extension E/F, any element $\sigma \in \mathrm{Gal}(E/F)$ is determined uniquely by its action on α. Then the map $\varphi : \mathrm{Gal}(E/F) \to \mu_n$ sending $\sigma \mapsto \dfrac{\sigma(\alpha)}{\alpha}$ is an injective homomorphism, so we conclude that $\mathrm{Gal}(E/F)$ is isomorphic to a subgroup of a cyclic group, hence is cyclic. We conclude that it is generated by an element $\tau : \alpha \mapsto \zeta\alpha$ where ζ is some (possibly non-primitive) nth root of unity.
Then by the "sliding-up" property of Galois extensions, $\mathrm{Gal}(L/K) = \mathrm{Gal}(L/L \cap F) \cong \mathrm{Gal}(E/F)$ because $L \cap F = K$. We conclude that $\mathrm{Gal}(L/K)$ is also a cyclic group generated by a map of the form $\varphi : \beta \mapsto \beta\zeta$ for some β, by standard Kummer theory (or Hilbert's theorem 90, or another method). This element β is necessarily a generator of L/K (since φ generates the Galois group), and $\varphi(\beta^n) = \beta^n$ hence β^n is fixed by all of $\mathrm{Gal}(L/K)$ hence is in K.

Remark It is a standard fact of Kummer theory that if K is a field containing the nth roots of unity and whose characteristic does not divide n, then any cyclic Galois extension of K of degree n has the form $K[\beta^{1/n}]$ for some $\beta \in K$. To prove this, if σ is a generator of the Galois group and $\alpha \in K$, one observes that the "Lagrange resolvent" $(\alpha, \zeta_n) = \alpha + \zeta_n\sigma(\alpha) + \zeta_n^2\sigma^2(\alpha) + \cdots + \zeta_n^{n-1}\sigma^{n-1}(\alpha)$ has the property that $\sigma(\alpha, \zeta_n) = \zeta_n^{-1}(\alpha, \zeta_n)$.

b) We can take $K = \mathbb{Q}$, $L = \mathbb{Q}(2^{1/3})$, $F = \mathbb{Q}(2^{1/3}\zeta_3)$, $E = \mathbb{Q}(2^{1/3}, \zeta_3) = F[\sqrt{-3}]$, for ζ_3 a primitive cube root of unity. Then L is not Galois (its Galois closure is E), and since $|L : \mathbb{Q}| = |F : \mathbb{Q}| = 3$ we see that $[L \cap F : \mathbb{Q}]$ divides 3: if it were 3, it would necessarily be equal to L and to F, but L and F are not equal (F contains a nonreal element while E does not) – hence we see $L \cap F = \mathbb{Q}$.
