2014 Algebra SEP ∼ Fields Day 2 Solutions, by E. Dummit

1. (Jan-10.3) Let $F \subseteq E$ be finite fields where $|F| = q$ and $[E : F] = n$.

   (a) Show that every monic irreducible polynomial in $F[x]$ of degree dividing n is the minimal polynomial over F of some element of E.

   (b) Compute the product of all the monic irreducible polynomials in $F[x]$ of degree dividing n.

   (c) If $|F| = 2$, find the number of monic irreducible polynomials of degree 10 in $F[x]$.

Solution:

a) If $\alpha \in E$ then $[F(\alpha) : F]$ divides $[E : F] = n$. We also know the Frobenius map $\varphi : x \to x^q$ is an automorphism of E/F, so it is therefore a generator for the Galois group: the degree of the extension hence the order of the Galois group is n and σ is also order n (because $x^{q^{n-1}} - x$ only has q^{n-1} roots in E). In particular, we see that the intermediate fields between E and F are the fixed fields of powers of σ, and are thus the fields whose orders are q^k where k divides n. Then if $p(x)$ is any monic irreducible polynomial over F of degree dividing n, the extension $F[x]/p(x)$ is a field of $q^{\deg(p)}$ elements, hence is isomorphic to $F(\alpha)$ for $\alpha \in E$.

Note This argument assumes the well-known fact that there is a unique finite field (up to isomorphism) of any prime-power order. This in fact follows from the argument in part (b), if one wishes to be especially pedantic.

b) The product is $x^{q^n} - x$. To see this observe that every element of E is a root of this polynomial, since $|E^\times| = q^n - 1$ so by Lagrange every $x \in E^\times$ satisfies $x^{q^n - 1} = 1$; multiplying by x adds 0 as a root. Since this polynomial is degree q^n, we have found all the roots. Now we observe that every monic irreducible in $F[x]$ of degree dividing n must divide this polynomial (since by part (a) all of its roots lie in E), and conversely this polynomial can have no other type of irreducible factors over F (because it is separable, all its roots lie in E, and the minimal polynomial of every element of E has degree dividing n).

c) The product of all of the irreducibles of degree dividing n is $x^{2^n} - x$. By inclusion-exclusion (or Mobius inversion) the degree of the product of the irreducibles of exact degree 10 is $2^{10} - 2^5 - 2^2 + 2^1 = 990$, and since each has degree 10, there are 99 of them.

---

2. (Jan-09.3): Suppose $f(x) = x^m + 1$ is irreducible over $\mathbb{F}_p[x]$ where p is an odd prime.

   (a) Show that every root of f in a splitting field of f has multiplicative order $2m$.

   (b) Show that $2m$ divides $p^m - 1$ but does not divide $p^n - 1$ for any n with $0 < n < m$.

   (c) Show that $m \neq 4$.

Solution:

a) If $\alpha^m + 1 = 0$ then $\alpha^{2m} - 1 = 0$ so $\alpha^{2m} = 1$. Thus the order of any root divides $2m$. It cannot be equal to m since then $\alpha^m - 1 = 0$ whence $2 = 0$ and the characteristic is not 2. It also cannot be less than m since then α would satisfy a polynomial of degree less than that of $x^m + 1$, and hence taking the polynomial gcd would give a nontrivial factor of $x^m + 1$.

b) An irreducible polynomial of degree m over $\mathbb{F}_p$ has splitting field $\mathbb{F}_{p^m}$. Since by part (a) every root of $x^m + 1$ has multiplicative order $2m$, we see that $2m$ must divide $\left|\mathbb{F}_{p^m}^\times\right| = p^m - 1$. If $2m$ were to divide $p^n - 1$ for $0 < n < m$, then since over $\mathbb{F}_{p^m}$ the polynomial factors as $(x - \alpha)(x - \alpha^3) \cdots (x - \alpha^{2m-1})$ where α is any root (since if $\alpha^m = -1$ then $\alpha^{(2k+1)m} = -1$ for any integer k), we see that $\mathbb{F}_{p^n}$ would contain an element of multiplicative order $2m$ hence contain a root of $x^m + 1$ hence contain all roots of $x^m + 1$. But this would contradict the irreducibility of $x^m + 1$, since it would only generate an extension of degree $n < m$.

c) Suppose $m = 4$. Then if $p = 2k + 1$ we have $p^2 - 1 = (2k + 1)^2 - 1 = 8 \cdot \binom{k}{2}$, so $p^2 - 1$ is divisible by $2m = 8$, violating the condition of (b).

---

3. (Jan-13.2): Let k be a field. We say a polynomial $f(x) \in k[x]$ is "consecutive-root" if it has two roots x_0, x_1 (not necessarily in k) such that $x_1 - x_0 = 1$.

   (a) Show that there is no irreducible consecutive-root polynomial in $\mathbb{Q}[x]$.

   (b) Let p be a prime. Show that $x^p - x - 1$ is consecutive-root and irreducible in $\mathbb{F}_p[x]$.

   (c) Characterize all irreducible monic consecutive-root polynomials in $\mathbb{F}_p[x]$ of degree $\leq p$.

   Note Compare to Jan-92.3.

   Solution: Suppose $f(x)$ is consecutive-root. By hypothesis, $f(x)$ and $f(x+1)$ have a common root (namely, x_1), so their gcd has positive degree. If f is irreducible, then this forces the gcd to be equal to f, but since $f(x)$ and $f(x+1)$ have the same degree, we see $f(x) = f(x+1)$. Conversely, if $f(x) = f(x+1)$, then f is clearly consecutive-root.

   a) From the above observation we see immediately that there are no irreducible consecutive-root polynomials in $\mathbb{Q}[x]$, since it is not possible for $f(x)$ to equal $f(x+1)$, as the second-highest-degree terms are not equal.

   b) For $x^p - x - 1$ we see that $f(x) = f(x+1)$, since $(x+1)^p - (x+1) - 1 = (x^p + 1) - (x+1) - 1 = x^p - x - 1$ in characteristic p. Hence f is consecutive-root. To see it is irreducible, observe that the Galois action of $\mathbb{F}_p[x]/(x^p - x - 1)$ over $\mathbb{F}_p$ in this extension of finite fields is Frobenius, the pth power, but since $x \mapsto x^p = x + 1$ is the same as addition by 1. But now the Galois action is transitive on the roots, so the polynomial is irreducible. (Alternatively, if $q(x)$ is a divisor of $x^p - x - 1$, and α is any root, then the sum of the roots of $q(x)$ is $\deg(q)\alpha + r$ where $r \in \mathbb{F}_p$; since this term is also in $\mathbb{F}_p$ we see that α would necessarily be in $\mathbb{F}_p$ but it is easy to see that f has no roots in $\mathbb{F}_p$.)

   c) From the criterion at the beginning, we see that $f(x) = f(x+1) = \cdots = f(x+p-1)$, and so we see $f(0) = f(1) = \cdots = f(p-1) = a$. Hence $f(x) - a$ is identically zero on $\mathbb{F}_p$, so it is divisible by $x(x-1)\cdots(x-(p-1))$, which by standard finite field facts is $x^p - x$. Hence since f has degree $\leq p$ and is monic, we necessarily have $f(x) - a = x^p - x$, so $f(x) = x^p - x + a$ for some $a \in \mathbb{F}_p$. We see that, by the same argument in part (b), this polynomial is irreducible as long as $a \neq 0$.

   Remark These extensions are called Artin-Schreier extensions, and they characterize all (cyclic) degree-p Galois extensions of $\mathbb{F}_p$.

---

4. (Jan-89.3) Prove that $x^9 - 2$ is an irreducible factor of $x^{27} - 1$ over $\mathbb{F}_7$.

   Solution: We have $(x^9 - 2)(x^{18} + 2x^9 + 4) = x^{27} - 8$ (over $\mathbb{Z}$, even). For the irreducibility, let E be the splitting field of $x^9 - 2$ over $\mathbb{F}_7$. Each root has multiplicative order 27 in E, since none of them has order 9 (as $\alpha^9 = 2$, not 1, for any root α of $x^9 - 2$). Therefore, if $d = [E : \mathbb{F}_7]$, then it must be the case that $|E^\times| = 7^d - 1$ is divisible by 27. Reducing mod 9 gives $(-2)^d = -1$ mod 9, so $d \equiv 3$ mod 6. We also see that $d = 3$ does not work since $7^3 - 1 = 342$ is not divisible by 27, so it must be true that $d \geq 9$. However, obviously $d = 9$ does work because every root of $x^9 - 2$ lives in an extension of degree at most 9: thus we see that the splitting field of $x^9 - 2$ over $\mathbb{F}_7$ is degree 9, hence the polynomial is irreducible.

   Remark Using an analysis like the above, one can show that the full factorization of $x^{27} - 1$ into irreducibles over $\mathbb{F}_7$ is $(x-1)(x-2)(x-4)(x^3-2)(x^3-4)(x^9-2)(x^9-4)$.

---

5. (Aug-08.3): Let $E \subseteq \mathbb{C}$ be the splitting field of $x^3 - 2$ over $\mathbb{Q}$.

   (a) Show that $[E : \mathbb{Q}] = 6$.

   (b) If $\alpha \in E$ and $\alpha^5 \in \mathbb{Q}$ show that $\alpha \in \mathbb{Q}$.

   (c) Show that there exists $\beta \in E$ with $\beta^2 \in \mathbb{Q}$ but $\beta \notin \mathbb{Q}$.

Solution:

a) Clearly, $E = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ where ζ_3 is a nonreal cube root of unity. $x^3 - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion or the fact that it has no roots, so $\left[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}\right] = 3$. Similarly, $[\mathbb{Q}(\zeta_3) : \mathbb{Q}] = 2$ since $x^2 + x + 1$ has no roots. Then $[E : \mathbb{Q}] \leq 6$ since $[EF : \mathbb{Q}] \leq [E : \mathbb{Q}] \cdot [F : \mathbb{Q}]$ but it is also divisible by 2 and 3, hence must be 6.

b) First observe that $x^5 - \alpha^5 \in \mathbb{Q}[x]$ cannot be irreducible, since otherwise $\mathbb{Q}[\alpha]$ would have degree 5 over $\mathbb{Q}$ – so it must have a linear or quadratic factor. If it has a quadratic factor, the constant term must be $\alpha^2 \zeta_5^d$ for some d: then $\alpha \zeta_5^{-2d} = \alpha^5 (\alpha^2 \zeta_5^d)^{-2}$ is in $\mathbb{Q}$, but this is one of the roots of $x^5 - \alpha^5$. Thus, $x^5 - \alpha^5$ has a linear factor over $\mathbb{Q}$, so $\alpha \zeta_5^d \in \mathbb{Q}$ for some $0 \leq d \leq 4$. If $d \neq 0$ then $\mathbb{Q}[\alpha] = \mathbb{Q}[\zeta_5]$ has degree 4 over $\mathbb{Q}$, which is impossible since $\mathbb{Q}[\alpha]$ is a subfield of E. We conclude $\alpha \in \mathbb{Q}$.

Remark The result of (b) has very little to do with the field E chosen here: the argument given above actually shows that $\alpha^p \in \mathbb{Q}$ and $\alpha \in E$ implies $\alpha \in \mathbb{Q}$ for any prime p such that neither p nor $p-1$ divides $[E : \mathbb{Q}]$. To see this, consider the minimal polynomial of α over $\mathbb{Q}$: by hypothesis it must divide $x^p - \alpha^p$, so its constant term is some product of Galois conjugates of α hence is of the form $\alpha^d \cdot \zeta_p^r$ for some d and r. If $d < p$ then d is invertible mod p: then for a, b with $ad - bp = 1$, we have $(\alpha^d \zeta_p^r)^a \cdot (\alpha^p)^{-b} = \alpha \cdot \zeta_p^{ra}$ is in $\mathbb{Q}$. Hence $[\mathbb{Q}[\alpha] : \mathbb{Q}]$ is either 1 or $p - 1$ (depending on whether ra is divisible by p or not). Otherwise, if $d = p$, we see $x^p - \alpha^p$ is irreducible over $\mathbb{Q}$, so $[\mathbb{Q}[\alpha] : \mathbb{Q}] = p$. Thus, since $\alpha \in E$, we require one of $p - 1$ or p to divide $[E : \mathbb{Q}]$.

c) $\beta = \sqrt{-3}$ is in E, since $\sqrt{-3} = 1 + 2\zeta_3$, and $\zeta_3 \in E$.

---

6. (Aug-96.3): Let $f(x) = x^6 + 3 \in \mathbb{Q}[x]$, let α be a root of f over $\mathbb{C}$, and set $E = \mathbb{Q}[\alpha]$.

   (a) Show that E contains a primitive 6th root of unity.

   (b) Show that E is Galois over $\mathbb{Q}$.

   (c) Find the number of intermediate fields F with $\mathbb{Q} \subset F \subset E$ with $[F : \mathbb{Q}] = 3$.

Solution:

a) If $\alpha^6 = -3$, then$\alpha^3 = \pm\sqrt{-3}$, so (in either case) $\sqrt{-3} \in E$. Then $\dfrac{1}{2} + \dfrac{\sqrt{-3}}{2} \in E$, and this is a primitive sixth root of unity.

b) The other roots of f are $\alpha \zeta_6^k$ where $k = 1, \cdots, 5$ and $\zeta_6 = e^{i\pi/3}$ is a primitive sixth root of unity. Since α and ζ_6 are both in E we see that E is the splitting field of $f(x)$, hence it is Galois.

c) The Galois group has order 6 so the question is whether it is abelian or not. Complex conjugation and multiplication by -1 are both elements of the Galois group (since $\bar{\alpha}^6 + 3 = (-\alpha)^6 + 3 = 0$) and have order 2, so the Galois group must be nonabelian, hence S_3. Then the extensions of degree 3 correspond to subgroup of index 3 = order 2 in S_3, of which there are 3 (generated by the 3 transpositions).

c-alt) If the extension $E/\mathbb{Q}$ were abelian then by the Kronecker-Weber theorem E would be contained in some cyclotomic extension of $\mathbb{Q}$. By adjoining additional roots of unity we then see that $(-3)^{1/6}$ hence $3^{1/6}$ hence $3^{1/3}$ would also be contained in a cyclotomic extension. But because $x^3 - 3$ has Galois group S_3, not A_3 (complex conjugation is an element of order 2, or because its discriminant is not a square), we see that $3^{1/3}$ is not contained in any cyclotomic extension (since cyclotomic extensions are abelian, and S_3 is not).

---

7. (Aug-09.3): Let F be a field and $f(x) \in F[x]$ irreducible with splitting field E. Choose $\alpha \in E$ with $f(\alpha) = 0$ and a positive integer n and let $g(x) \in F[x]$ irreducible with $g(\alpha^n) = 0$.

   (a) Show that $\deg(g)$ divides $\deg(f)$ and $\deg(f)/\deg(g) \leq n$.

   (b) If $\deg(f)/\deg(g) = n$ and the characteristic of F does not divide n, show E contains a primitive nth root of unity.

Solution:

a) Let $E' = F[\alpha^n]$. By the assumptions, $g(x)$ is the minimal polynomial of α^n, so $[E' : F] = \deg(g)$ and $[E : F] = \deg(f)$. Then $\deg(g) \cdot [E' : E] = \deg(f)$ and $[E' : E] \leq n$ since α satisfies the polynomial $x^n - \alpha^n \in E'[x]$.

b) If equality holds, the polynomial $x^n - \alpha^n$ must be irreducible over E'. Now since E is Galois over F (it is a splitting field), it is also Galois over any intermediate extension hence in particular it is Galois over E'. Therefore, E is the splitting field of $x^n - \alpha^n$ over E', and so since the polynomial is separable (its derivative is nx^{n-1} which is relatively prime to $x^n - \alpha^n$ by the assumption on the characteristic) all of its roots lie in E. In particular, since its roots are $\alpha \cdot \zeta_n^k$ for $0 \leq k \leq n-1$ where ζ_n is a primitive nth root of unity, E contains α and $\alpha\zeta_n$ hence contains ζ_n.