2014 Algebra SEP $\sim$ Fields Day 1 Solutions, by E. Dummit

1. (Aug-13.2): Let K be the splitting field of $x^4 - 2$ over $\mathbb{Q}$.

   (a) Find $[K : \mathbb{Q}]$.

   (b) Give an example of an ideal I of $\mathbb{Q}[x, y]$ such that K is isomorphic to $\mathbb{Q}[x, y]/I$.

   (c) Find $\mathrm{Gal}(K/\mathbb{Q})$.

   Solution:

   a) Since the roots of x^4-2 are $2^{1/4}i^k$ for $k = 0, 1, 2, 3$, we see that $K = \mathbb{Q}(2^{1/4}, i)$, which has degree 8 over $\mathbb{Q}$: $x^4 - 2$ is irreducible by Eisenstein, so $\left[\mathbb{Q}(2^{1/4}) : \mathbb{Q}\right] = 4$, and furthermore K contains i but $L = \mathbb{Q}(2^{1/4})$, being a subfield of $\mathbb{R}$, does not, so $\left[K : \mathbb{Q}(2^{1/4})\right] = 2$.

   b) By the above, we could take $I = (x^4 - 2, y^2 + 1)$, since then $\mathbb{Q}[x, y]/I \cong L[y]/(y^2 + 1) \cong K$.

   c) If $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, then the action of σ on K is determined by $\sigma(2^{1/4}) \in \{\pm 2^{1/4}, \pm 2^{1/4}i\}$ and $\sigma(i) \in \{\pm i\}$. Since there are only 8 such possibilities, all 8 must actually be automorphisms. Then it is straightforward to see that the two maps $r : (2^{1/4}, i) \mapsto (2^{1/4}i, i)$ and $s : (2^{1/4}, i) \mapsto (2^{1/4}, -i)$, generate a group isomorphic to the dihedral group of order 8. (It is nonabelian and has more than one element of order 2, for example.)

   c-alt) Since $\mathrm{Gal}(K/\mathbb{Q})$ has order 8, it must be the dihedral group, the quaternion group, or one of the three abelian groups. We can see K has several subfields of degree 2: $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-2})$, and several others of degree 4: $\mathbb{Q}(2^{1/4})$, $\mathbb{Q}(2^{1/4}i)$, $\mathbb{Q}(\sqrt{2}, i)$. If we draw all of the appropriate subfield containments and then convert to the subgroup containments for G, we see that the only possibility that is consistent with this information is the dihedral group.

   c-alt) Since K is a splitting field of a polynomial of degree 4, $\mathrm{Gal}(K/\mathbb{Q})$ is a subgroup of S_4 of order 8. Since it has order 8, it is a Sylow 2-subgroup of S_4. But the dihedral group of order 8 is also a Sylow 2-subgroup of S_4, and any two 2-Sylows of any group are isomorphic.

   Remark Of course, K actually has a primitive element α by the primitive element theorem, so in part (b) we could write $K = \mathbb{Q}[\alpha] \cong K[x]/p(x) \cong K[x, y]/(p(x), y)$, where $p(x)$ is the minimal polynomial of α, so we could get away with just one variable. As motivated by Aug-04.3(c) below, we see that $\alpha = 2^{1/4} + i$ is a generator of K since all its conjugates under G are different, and it is not so hard to compute its minimal polynomial $p(x) = \prod_{g \in G}(x - g\alpha) = x^8 + 4x^6 + 2x^4 + 28x^2 + 1$.

---

2. (Aug-04.3):

   (a) Show that $x^4 - 2$ is irreducible over $\mathbb{Q}[i]$.

   (b) If $\sqrt[4]{2} + i$ is a root of a polynomial $f(x) \in \mathbb{Q}[x]$, show that $i\sqrt[4]{2} + i$ is also a root of $f(x)$.

   (c) Find the degree of the minimal polynomial of $\sqrt[4]{2} + i$ over $\mathbb{Q}$.

   Solution: We continue with the notation from Aug-13.2 above.

   a) Let $K = \mathbb{Q}(2^{1/4}, i)$ with $L = \mathbb{Q}(2^{1/4})$, and $E = \mathbb{Q}(i)$. From Aug-13.2(a) we know that $|K : \mathbb{Q}| = 8$. Since $x^4 - 2$ splits completely over $K = E[2^{1/4}]$, we see that $x^4 - 2$ must be irreducible over E, because $|K : E| = \dfrac{|K : \mathbb{Q}|}{|E : \mathbb{Q}|} = 4$.

   Remark One could try to use Eisenstein's criterion in the ring $\mathbb{Z}[i]$ with the prime ideal $P = (1 + i)$, but, unfortunately, here it is true that $2 \in P^2$ – though Eisenstein does show $x^4 - p$ is irreducible over $\mathbb{Q}[i]$ for any odd prime p.

   b) We use the explicit description of the elements of $G = \mathrm{Gal}(K/\mathbb{Q})$ from Aug-13.2(c). If $f(x) \in \mathbb{Q}[x]$ is such that $f(2^{1/4} + i) = 0$, applying the element $\sigma \in G$ which fixes i and sends $2^{1/4} \mapsto 2^{1/4}i$ shows that $0 = \sigma(f(2^{1/4} + i)) = f(\sigma(2^{1/4} + i)) = f(2^{1/4}i + i)$, as desired.

   c) By the same argument as in part (b), the minimal polynomial of $\beta = 2^{1/4} + i$ over $\mathbb{Q}$ has all the Galois conjugates of this element as roots. But it is easy to see that no elements of the Galois group fix this element, so it has 8 distinct conjugates. Hence its minimal polynomial has degree 8, hence in fact α is a generator for $K/\mathbb{Q}$.

---

3. (Aug-12.3):

   (a) Suppose $K, L \subseteq \mathbb{C}$ are Galois over $\mathbb{Q}$. Show that $E = KL$ is Galois over $\mathbb{Q}$.

   (b) If additionally $[K : \mathbb{Q}]$ and $[L : \mathbb{Q}]$ are coprime, show that $\mathrm{Gal}(E/\mathbb{Q}) \cong \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q})$, and deduce $|E : \mathbb{Q}| = |K : \mathbb{Q}| \cdot |L : \mathbb{Q}|$.

   (c) Prove there is a subfield F of $\mathbb{C}$, Galois over $\mathbb{Q}$, with $[F : \mathbb{Q}] = 55$.

Solution:

a) If K is the splitting field of $f(x)$ and L is the splitting field of $g(x)$, then KL is the splitting field of the polynomial $f(x)g(x)$.

b) We show a more general version. First, observe that $K \cap L$ is Galois over $\mathbb{Q}$, since if $p(x) \in \mathbb{Q}[x]$ is irreducible with a root in $K \cap L$, then since $K/\mathbb{Q}$ is Galois all its roots lie in K; similarly all its roots lie in L, so all its roots lie in $K \cap L$. Now we claim that $\mathrm{Gal}(KL/\mathbb{Q})$ is the subgroup H of $\mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q})$ where the actions in both components agree on $K \cap L$ – to prove this, observe that the map $\mathrm{Gal}(KL/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(L/\mathbb{Q})$ via $\sigma \mapsto (\sigma|_{K_1}, \sigma|_{K_2})$ is well-defined, and the kernel is the set of maps which are trivial on K_1 and K_2 hence on the composite. The image lies in H, so we need only verify that its order agrees with that of H. We have $|H| = |\mathrm{Gal}(K/\mathbb{Q})| \cdot |\mathrm{Gal}(L/K \cap L)|$ since for every $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ there are $|\mathrm{Gal}(L/K \cap L)|$ elements whose restrictions to $K \cap L$ agree with σ. We then see that $|H| = |\mathrm{Gal}(K/\mathbb{Q})| \cdot |\mathrm{Gal}(L/K \cap L)| = |\mathrm{Gal}(K/\mathbb{Q})| \cdot \dfrac{|\mathrm{Gal}(L/\mathbb{Q})|}{|\mathrm{Gal}(K \cap L/\mathbb{Q})|} = |\mathrm{Gal}(KL/\mathbb{Q})|$.
Then for the deduction in the problem, we just need to observe that given our assumptions, $K \cap L = \mathbb{Q}$: its degree over $\mathbb{Q}$ divides both $[K : \mathbb{Q}]$ and $[L : \mathbb{Q}]$, so it must be 1 since these degrees are coprime. (We could of course shorten the original proof by incorporating this assumption.)

c) We know that $\mathbb{Q}(\zeta_{23})$ is cyclic Galois of degree $\phi(23) = 22$ over $\mathbb{Q}$, and $\mathbb{Q}(\zeta_{11})$ is cyclic Galois of degree $\phi(11) = 10$ over $\mathbb{Q}$. Then we can take fixed subfields of degrees 11 and 5, which are also Galois and abelian. By part (b) their compositum is abelian Galois over $\mathbb{Q}$ of degree 55.

c-alt) Since 331 is prime and 1 mod 55, $\mathbb{Q}(\zeta_{331})$ is abelian Galois of order 330, and hence has a subfield of degree 55 that is Galois over $\mathbb{Q}$.

---

4. (Jan-00.3): Let L/K be a finite-degree Galois extension with Galois group G, and $K \subseteq E \subseteq L$. E is said to be a "2-tower" over K if there exists a chain of fields $K = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_n = E$ with each extension of degree 2.

   (a) If G is abelian, show that E is a 2-tower over K iff $|E : K|$ is a power of 2.

   (b) Show by example that (a) is false if G is not abelian.

Solution:

a) Clearly $|E : K|$ must be a power of 2 if E is a 2-tower. For the other direction, since G is abelian, E/K is Galois. So by the Galois correspondence, if we look at the subgroup of G fixing each field in the chain, we see the claim is equivalent to showing: every abelian 2-group has a chain of (normal) subgroups $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{1\}$ such that the quotient G_i/G_{i+1} has order 2. The existence of such a composition series is a standard property of (not necessarily abelian) p-groups, which can be proven by induction: take any element of order p in the center of G, and pull back the identity under the quotient of $G/\langle g \rangle$ to get a subgroup of index p, and repeat.

b) The proof in (a) fails because E/K is not necessarily Galois anymore, so instead of needing a chain of subgroups in a 2-group, we need a chain of subgroups from $\mathrm{Fix}(E)$ to G, which may not exist: if we take $G = A_4$ and E to be the fixed field of an element of order 3, then $[E : K] = 4$, but E has no subfield of degree 2 over K (because it would correspond to a subgroup of A_4 of order 6).

Remark Here is a 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 $|L : F| \le n!$, 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 $\mathrm{Gal}(L/K) \cong G$.

---

5. (Aug-07.3): Let F be a field of characteristic 0 and E a finite Galois extension of F.

   (a) If $0 \neq \alpha \in E$ with $E = F[\alpha]$, show that $F[\alpha^2] \neq E$ iff there exists $\sigma \in \mathrm{Gal}(E/F)$ with $\alpha^\sigma = -\alpha$.

   (b) Prove there exists an element $\alpha \in E$ with $E = F[\alpha^2]$.

Solution: We show that both conditions in (a) are equivalent to the statement: the minimal polynomial of α over F contains only terms of even degree.

a1) If the minimal polynomial has a term of odd degree, then we can write it as $m(x) = p(x^2) + xq(x^2)$, so $\alpha = -\dfrac{p(\alpha^2)}{q(\alpha^2)} \in F[\alpha^2]$, and this makes sense because $q(x)$ is a nonzero polynomial and $q(\alpha^2) \neq 0$ since the degree of $q(x^2)$ is less than the degree of $m(x)$ hence cannot divide $m(x)$ since $m(x)$ is irreducible. Conversely, if $\alpha \in F[\alpha^2]$ then we can write $-\alpha = p(\alpha^2)$ for some nonzero polynomial p; then we obtain $\alpha + p(\alpha^2) = 0$, so the polynomial $f(x) = x + p(x^2)$ is nonzero and has α as a root, hence is a multiple of $m(x)$, so we see that $m(x)$ must have an odd-degree term.

a2) If there exists $\sigma \in \mathrm{Gal}(E/F)$ with $\alpha^\sigma = -\alpha$ then this means $-\alpha$ is also a root of the minimal polynomial $m(x)$ of α, or equivalently, that α is a root of $m(-x)$. But then since $m(x)$ is irreducible, we see that this implies $m(x)$ divides $m(-x)$, which is only possible if they are equal (since they have the same degree and same nonzero constant term). But since the characteristic is not 2, this means that $m(x)$ has only even-degree terms. Conversely, if $m(x)$ has only even-degree terms, then $m(x) = m(-x)$ so if β is any root then $-\beta$ is also a root. Then the map $\sigma : \beta \to -\beta$ is a well-defined permutation of the roots of the polynomial $m(x)$ whose splitting field is E, so σ extends linearly to the desired field automorphism.

b) From the criterion above we need only show there is a generator of E/F whose minimal polynomial has an odd-degree term. By the primitive element theorem, E has a generator α: if its minimal polynomial has an odd-degree term, we are done. If its minimal polynomial is $m(x) = x^{2n} + o(x^{2n-2})$ has only even-degree terms, then the minimal polynomial of $\alpha + k$ is $m(x-1) = x^{2n} - 2knx^{2n-1} + o(x^{2n-2})$, which has an odd-degree term for any $k \neq 0$ (and for some k, $\alpha + k$ must be also be a generator).

---

6. (Jan-03.3): Let $F/\mathbb{Q}$ be a finite abelian Galois extension of $\mathbb{Q}$, embedded in $\mathbb{C}$. Let $\alpha \in F$ and $f(x) \in \mathbb{Q}[x]$ be its minimal monic polynomial. Assume that $|\alpha| = 1$.

   (a) Show F is closed under complex conjugation.

   (b) Show that $|\beta| = 1$ for every root β of f.

   (c) For $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, show that $|a_i| \leq 2^n$ for each i.

   (d) Show that F contains only finitely many algebraic integers having absolute value 1, and that each of these is a root of unity.

Solution:

a) This is true for any Galois extension: suppose $\gamma \in F$ has minimal polynomial $p(x) \in \mathbb{Q}[x]$. Then $p(\bar{\gamma}) = \overline{p(\gamma)} = 0$, and since F is a splitting field, $\bar{\gamma} \in F$.

b) Since f is irreducible, the Galois group acts transitively on its roots, so there exists σ with $\sigma(\alpha) = \beta$. Then since $\alpha \cdot \bar{\alpha} = 1$, applying σ yields $\sigma(\alpha) \cdot \sigma(\bar{\alpha}) = 1$, and since the Galois group is abelian we obtain $\sigma(\alpha) \cdot \overline{\sigma(\alpha)} = 1$ so $\beta \cdot \bar{\beta} = 1$.

c) Each coefficient of f is an elementary symmetric function in the roots of the polynomial. Applying the triangle inequality and the fact that the absolute value of each root is 1 (from part (b)) shows that $|a_i| \leq \binom{n}{i} \leq 2^n$.

d) By part (c), there are only finitely many possibilities for the minimal polynomial of an algebraic integer $\alpha \in F$ of absolute value 1, since its degree is bounded by $[F : \mathbb{Q}]$ and all its coefficients are integers that are bounded above and below. Hence there are only finitely many such algebraic integers. Since taking powers of any of them must therefore eventually repeat, we see that they are all roots of unity.

---

7. (Aug-10.3): We say a polynomial $f \in \mathbb{Q}[x]$ is "special" if f is irreducible in $\mathbb{Q}[x]$, its degree is at least 2, and f splits over $\mathbb{Q}[\alpha]$ where α is some root of f in some extension of $\mathbb{Q}$.

   (a) If $f \in \mathbb{Q}[x]$ is irreducible with degree at least 2, with splitting field $L/\mathbb{Q}$ whose Galois group is abelian. Show that f is special.

   (b) If $L/\mathbb{Q}$ is finite and Galois (and not trivial), show that there exists a special polynomial f with a root in L.

   (c) Show that $x^n - 2$ is not special for any $n \geq 3$.

Solution:

a) Let $\deg(f) = n$ and let α be a root of f. Since $\mathrm{Gal}(L/\mathbb{Q})$ is abelian, $\mathbb{Q}[\alpha]$ is also Galois over $\mathbb{Q}$: say its Galois group is H and let $h \in H$. Now consider the polynomial $p(x) = \prod_{\sigma \in H}(x - \sigma(\alpha))$ of degree $|H| = [\mathbb{Q}[\alpha] : \mathbb{Q}] = \deg(f) = n$. Now observe that for any $h \in H$, $h\,p(x) = \prod_{\sigma \in G}(x - h\sigma(\alpha)) = \prod_{\tau \in G}(x - \tau(\alpha)) = p(x)$ by reindexing with $\tau = h\sigma$: thus all of the coefficients of $p(x)$ are fixed by all elements of the Galois group hence they all lie in $\mathbb{Q}$. We conclude that $p(x)$ is a monic polynomial of degree n in $\mathbb{Q}[x]$ with α as a root, hence it must equal f since f divides it as f is the minimal polynomial of α. We therefore see that all n roots of f lie in E (since they are the n values $\sigma(\alpha)$ as σ runs over H), so $\mathbb{Q}[\alpha]$ is a splitting field for f.

b) Let $G = \mathrm{Gal}(L/\mathbb{Q})$ and take any primitive element $\alpha \in L$ – note that in particular, it is not fixed by any element of the Galois group (as otherwise it would necessarily lie in the subfield of L fixed by the cyclic subgroup generated by that element, hence could not generate L). Now, as in part (a), consider the polynomial $f(x) = \prod_{\sigma \in G}(x - \sigma(\alpha))$ which has α as a root; as in part (a) we see $f(x) \in \mathbb{Q}[x]$. Now since α generates L we see that $[L : \mathbb{Q}] = |G| = \deg(f)$, so the minimal polynomial of α also has degree n hence must be $f(x)$ – thus, $f(x)$ is irreducible. And finally, obviously f splits over $\mathbb{Q}[\alpha] = L$.

c) Eisenstein's criterion says $f(x) = x^n - 2$ is irreducible, so $[\mathbb{Q}[\alpha] : \mathbb{Q}] = n$ for any root α of $\mathbb{Q}$. Since $\mathbb{Q}(2^{1/n})$ is a subfield of $\mathbb{R}$ but $\zeta_n = e^{2\pi i/n}$ is not a real number (since $n > 2$), we conclude $\zeta_n \notin \mathbb{Q}[2^{1/n}]$, so the splitting field $L = \mathbb{Q}(2^{1/n}, \zeta_n)$ of f is a proper extension of $\mathbb{Q}[2^{1/n}]$. We conclude that $[L : \mathbb{Q}] = [L : \mathbb{Q}(2^{1/n})] \cdot [\mathbb{Q}(2^{1/n}) : \mathbb{Q}] \geq 2 \cdot n$, so it cannot be $\mathbb{Q}[\alpha]$.

Remark With some additional work, one can in fact show in (c) that $[\mathbb{Q}(2^{1/n}, \zeta_n) : \mathbb{Q}(2^{1/n})]$ is $\phi(n)$ if $8 \nmid n$ and is $\phi(n/2)$ otherwise.