Honors Algebra 4, MATH 371 Winter 2010

Solutions 7

Due Friday, April 9 at 08:35

1. Let p be a prime and let K be a splitting field of $X^p-2 \in \mathbf{Q}[X]$, so $K/\mathbf{Q}$ is a Galois extension. Show that $K = \mathbf{Q}(a,\zeta)$ for $a \in K$ satisfying $a^p = 2$ and $\zeta \in K$ a primitive p th root of unity. Describe generators of $G := \mathrm{Gal}(K/\mathbf{Q})$ in terms of their actions on a and ζ, and describe G as an abstract group (in terms of generators and relations, say). Write out the diagrams of intermediate fields and groups, indicating clearly the various containments. Also indicate which subfields of K are Galois over $\mathbf{Q}$.

   Solution: We treat the case that $p > 2$ as $p = 2$ is a bit different and should be analyzed separately (it's not at all hard). Let $a = a_1, \ldots, a_p \in K$ be the p distinct roots of the separable polynomial $X^p - 2$ in K. Since $(a/a_i)^p = 1$ we see that $\zeta_i := a/a_i$ is a p-th root of unity in K for all i. Moreover, for $i \neq j$ we have $\zeta_i \neq \zeta_j$ as the a_i are distinct. This gives p distinct roots of unity in K so since $\mu_p(\overline{K})$ has size p, we conclude that K contains all the p-th roots of unity. Let $\zeta \in K$ be any primitive p-th root of unity. Then up to relabeling, we have $a_i = \zeta^i a$ and it follows that $K \subseteq \mathbf{Q}(a,\zeta)$. The reverse containment has already been noted, we have equality. Any automorphism of K over $\mathbf{Q}$ is therefore uniquely determined by its action on a and ζ.

   For $u \in (\mathbf{Z}/p\mathbf{Z})^\times$ and $v \in \mathbf{Z}/p\mathbf{Z}$, it is not hard to check that the map

$$\sigma_{u,v} : \begin{cases} a \mapsto \zeta^v a \\ \zeta \mapsto \zeta^u \end{cases}$$

   is a well-defined automorphism of K that fixes $\mathbf{Q}$. Furthermore, every automorphism of K fixing $\mathbf{Q}$ must have this form, as the roots of the minimal polynomials of ζ and of a are permuted among themselves.

   Via the canonical isomorphism of groups $(\mathbf{Z}/p\mathbf{Z})^\times \simeq \mathrm{Aut}(\mathbf{Z}/p\mathbf{Z})$, we have a natural action of $(\mathbf{Z}/p\mathbf{Z})^\times$ on $\mathbf{Z}/p\mathbf{Z}$, and one checks that the map

$$(\mathbf{Z}/p\mathbf{Z})^\times \ltimes \mathbf{Z}/p\mathbf{Z} \to G \qquad (u,v) \mapsto \sigma_{u,v}$$

   is an isomorphism of groups. This group is also isomorphic with the group

$$\{x \mapsto ux + v \ : u \in \mathbf{F}_p^\times,\ v \in \mathbf{F}_p\}$$

   of affine transformations of the $\mathbf{F}_p$-line. Classifying the subgroups of this group is a good exercise in group theory, and is left to the reader.

2. Let F be a finite field of size $\#F$, with K/F a finite extension of degree d. Prove that K/F is Galois and that $\mathrm{Gal}(K/F)$ is a cyclic group of order d with generator the automorphism of K given by

$$\alpha \mapsto \alpha^{\#F}.$$

   (This automorphism is called the *arithmetic Frobenius* map of F).

   Solution: Set $q := \#F$ and let p be the characteristic of F, so $q = p^r$ for some r. We have seen that $K^\times$ is cyclic of order $q^d - 1$, and hence every α in K is a root of $X^{q^d} - X$, which

is a separable polynomial with F (even $\mathbf{F}_p$) coefficients. Thus, K/F is the splitting field of a separable polynomial and hence Galois. Consider the map $\varphi_F : K \to K$ given by $\varphi_F(\alpha) = \alpha^q$. It is straightforward to check that this is an automorphism of K which fixes F pointwise as every $x \in F$ is a root of $X^q - X$. The iterates $\{\varphi_F^i\}$ for $i = 0, 1, \ldots, d-1$ are all distinct, since otherwise we would have $\varphi^j = 1$ for some $1 \leq j \leq d-1$, whence every element of K would be a root of $X^{q^j} - X$ which is impossible as this polynomial has at most q^j roots and K has q^d elements. On the other hand, the Galois group of K/F has order d as $[K : F] = d$ and we conclude by size considerations that $\mathrm{Gal}(K/F)$ is cyclic of order d, generated by φ_F.

3. This exercise gives Artin's proof of the fundamental theorem of Algebra. Let F be a field not of characteristic 2 and assume that all odd degree polynomials in $F[X]$ have a root in F. Let K be a quadratic extension of F with the property that every element of K has a square root in K.

   (a) Prove that any finite extension of K has degree a power of 2. (Hint: Reduce to the Galois case and then consider the fixed field of the 2-Sylow subgroup of the Galois group).

   (b) Prove that K has no non-trivial finite extensions which are Galois over F, and conclude that K is algebraically closed. (Hint: Use the fact that a non-trivial 2-group has an index 2 normal subgroup).

   (c) Let $F = \mathbf{R}$ and $K = \mathbf{R}[X]/(X^2+1)$. Explain (using the intermediate value theorem) why F satisfies the hypotheses above, and using explicit formulae, show that K also satisfies the hypotheses. Conclude that $\mathbf{C} := K$ is algebraically closed (this is the Fundamental Theorem of Algebra).

   Solution:

   (a) Let L be any finite extension of K. To show that L/K has degree a power of 2 it suffices to show that this holds for any finite extension L' of F which contains L and is Galois over F (using that $[K : F]$ has degree 2). Such an extension exists, as we could take the Galois closure of L over F. Thus, we may assume that L is Galois over F with group G. Let H be the Sylow 2-subgroup of G and $E = L^H$ the corresponding fixed field, so $[E : F] = [G : H]$ has odd degree. If $\alpha \in E$ then $m_{\alpha,F}$ must have odd degree, as this degree divides $[E : F]$ and our hypothesis on F ensures that $m_{\alpha,F}$ has a root in F and hence that $\alpha \in F$. Thus, $E = F$ and $H = G$ by Galois theory (as $F = L^G$). We conclude that G is a 2-group, whence $[L : F]$ is a power of 2. It follows that $[L : K]$ is also a power of 2.

   (b) Suppose L/K is a finite extension which is Galois over F. Then L is Galois over K, with Galois group G, say, which must be a 2-group by part (3a). If G is nontrivial, then there exists a normal index 2 subgroup H of G, or what is the same thing, a nontrivial degree 2 (Galois) extension of K. Such an extension is obtained by adjoining a square-root of an element of K (as the characteristic of K is not 2). But every element of K has a square root in K, so any such extension must be trivial and G is the trivial group. Hence $L = K$. This implies that K is an algebraic closure of F, since any polynomial with F coefficients has splitting field over K that is finite Galois over F and hence must be trivial as an extension of K; that is, any polynomial over F has all root in K.

(c) Any odd degree polynomial f with real coeffecients has a real root by the intermediate value theorem since

$$\lim_{x\to\pm\infty} f(x) = \pm\infty.$$

On the other hand, let $a + bX \in K := \mathbf{R}[X]/(X^2+1)$ be arbitrary (so $a, b \in \mathbf{R}$). Let $D := \sqrt{a^2+b^2}$ be the unique positive (real) square root of the positive real number a^2+b^2, and note that $D \pm a > 0$. We set

$$s := \sqrt{\frac{1}{2}(D+a)} \qquad t := \sqrt{\frac{1}{2}(D-a)}.$$

It is straightforward to check that for $u := \operatorname{sgn}(b) = \pm 1$

$$(s + utX)^2 = (s^2 - t^2) + 2stuX = a + bX,$$

so every element of K has a square root in K. Thus K is algebraically closed by part (3b).

4. Determine the Galois group of the splitting field (over $\mathbf{Q}$) of $X^4 - 14X^2 + 9$, and write down the lattice of subgroups and corresponding subfields. Which subfields are Galois over $\mathbf{Q}$?

Solution: Observe first that $f := X^4 - 14X^2 + 9$ is irreducible: the rational root test shows it has no rational roots, and if f were to factor as a product of two quadratics, then since the X^3 and X coeffieicnts are zero, it is not hare to see that such a factorization must take the form

$$(X^2 + aX + b)(X^2 - aX + b) = X^4 + (2b - a^2)X^2 + b^2.$$

This would force $b = \pm 3$ whence we must have $\pm 6 - a^2 = -14$. But neither 8 nor 20 are perfect rational squares, so this last equation has no rational solutuons.

Using the quadratic formula, one sees that the roots of $f := X^4 - 14X^2 + 9$ in $\mathbf{C}$ are

$$\alpha := \sqrt{7 + 2\sqrt{10}}, \quad \beta := -\alpha, \quad \gamma := \sqrt{7 - 2\sqrt{10}}, \quad \delta := -\gamma.$$

Observe that $\alpha\gamma = \sqrt{49 - 40} = 3$, whence $\gamma \in \mathbf{Q}(\alpha)$ so $K := \mathbf{Q}(\alpha)$ contains all 4 roots of f and is hence a splitting field. By the irreducibility of f, we have $[K : \mathbf{Q}] = 4$ so $G := \operatorname{Gal}(K/\mathbf{Q})$ has order 4.

Since $\alpha(\alpha^3 - 14\alpha) = -9$, we deduce that

$$\gamma = \frac{3}{\alpha} = \alpha\frac{14 - \alpha^2}{3}$$

Since $K = \mathbf{Q}(\alpha)$, and $\sigma \in G$ is completely determined by its action on α, and since f is irreducible, for any root α' of f there exists $\sigma \in G$ taking α to α'. Thus, the elements of G are:

$$1, \quad \sigma_1 : \alpha \mapsto \gamma, \quad \sigma_2 : \alpha \mapsto -\alpha, \quad \sigma_3 : \alpha \mapsto -\gamma.$$

We compute

$$\sigma_1^2(\alpha) = \sigma_1(\gamma) = \sigma_1\left(\frac{3}{\alpha}\right) = \frac{3}{\gamma} = \alpha$$

so σ_1 has order 2. Since σ_1 obviously has order 2, we deduce that G contains at least 3 elements of order dividing 2 and hence $G \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ is the Klein 4-group.

Thus, G has 3 nontrivial subgroups given by $H_i := \langle 1, \sigma_i \rangle$ for $i = 1, 2, 3$. Note that $\eta_i := \alpha\sigma_i(\alpha)$ and $\tau_i = \alpha + \sigma_i(\alpha)$ are fixed by H_i for $i = 1, 2, 3$. We easily compute that

$$\eta_1 = 3, \quad \tau_1 = 2\sqrt{5}, \qquad \eta_2 = -7 - 2\sqrt{10}, \quad \tau_2 = 0, \qquad \eta_3 = -3, \quad \tau_3 = 2\sqrt{2}.$$

From this, we conclude that

$$K^{H_1} = \mathbf{Q}(\sqrt{5}), \qquad K^{H_2} = \mathbf{Q}(\sqrt{10}), \qquad K^{H_3} = \mathbf{Q}(\sqrt{2})$$

since in each case K^{H_i} is degree 2 over $\mathbf{Q}$ and contains the given quadratic field. Each of these is Galois over $\mathbf{Q}$ since G is abelian so every subgroup is normal.

5. Fix a positive integer n and let $K := \mathbf{Q}(\zeta_n)$ for a primitive n th root of unity $\zeta_n \in \mathbf{C}$. Prove that complex conjugation $\tau \in \mathrm{Aut}(\mathbf{C})$ restricts to an automorphism of K fixing $\mathbf{Q}$, and show that the corresponding element of $\mathrm{Gal}(K/\mathbf{Q})$ corresponds to -1 under the isomorphism $\mathrm{Gal}(K/\mathbf{Q}) \simeq (\mathbf{Z}/n\mathbf{Z})^\times$. Prove that the fixed field K^+ of the subgroup generated by complex conjugation is equal to the intersection $K \cap \mathbf{R}$ taken inside $\mathbf{C}$. We call K^+ the *maximal real subfield* of K.

Solution: We suppose $n \geq 3$ as the cases $n = 1, 2$ are trivial. The primitive n th roots of unity in $\mathbf{C}$ are given by

$$e^{2\pi ik/n} = \cos(2\pi k/n) + i\sin(2\pi k/n)$$

for $k \in (\mathbf{Z}/n\mathbf{Z})^\times$. Thus, if $\tau \in \mathrm{Aut}(\mathbf{C})$ denotes complex conjugation, we have

$$\tau(e^{2\pi ik/n}) = \cos(2\pi k/n) - i\sin(2\pi k/n) = e^{2\pi ik/n}$$

so $\tau(\zeta_n) = \zeta_n^{-1}$. In particular, τ preserves K and so restricts to an automorphism of K which obviously fixes $\mathbf{Q}$ (any field automorphism automatically fixes the prime subfield). We also see from this that under the isomorphism $\mathrm{Gal}(K/Q) \simeq (\mathbf{Z}/n\mathbf{Z})^\times$ which associates $\sigma \in \mathrm{Gal}(K/\mathbf{Q})$ to the unique $a_\sigma \in (\mathbf{Z}/n\mathbf{Z})^\times$ satisfying $\sigma\zeta_n = \zeta_n^{a_\sigma}$ (independent of ζ_n), complex conjugation corresponds to $-1 \in (\mathbf{Z}/n\mathbf{Z})^\times$. Now it is clear that K^+ contains $K \cap \mathbf{R}$ since $\mathbf{R}$ is fixed by complex conjugation. On the other hand, $b := \zeta_n + \tau\zeta_n$ and $c := \zeta_n\tau\zeta_n$ lie in $K \cap \mathbf{R}$ so ζ_n and $\tau\zeta_n$ are the roots of the degree 2 polynomial

$$X^2 - bX + c \in K \cap \mathbf{R}[X].$$

In particular, $[K : K \cap \mathbf{R}] \leq 2$. But $[K : K^+] = 2$ since complex conjugation generates an order 2 subgroup of $\mathrm{Gal}(K/\mathbf{Q})$ (here I'm using that $n \geq 3$), whence

$$2 = [K : K^+] \leq [K : K^+] \cdot [K^+ : K \cap \mathbf{R}] = [K : K \cap \mathbf{R}] \leq 2$$

so we must have equality throughout, forcing $[K^+ : K \cap \mathbf{R}] = 1$ so $K^+ = K \cap \mathbf{R}$.

6. This problem works out a formula for $\cos(2\pi/17)$ in terms of square-root extractions. Let $\zeta := e^{2\pi i/17}$; it is a primitive 17 th root of unity. Let $\alpha := \zeta + \zeta^{-1} = 2\cos(2\pi/17)$. Let $\sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$ be the element determined by

$$\sigma\zeta = \zeta^3.$$

(a) Show that σ generates $\mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$

(b) Define the *periods* of α to be

$$\eta_1 := \alpha + \sigma^2\alpha + \sigma^4\alpha + \sigma^8\alpha \qquad \eta_1' := \sigma\eta_1$$
$$\eta_2 := \alpha + \sigma^4\alpha \qquad \eta_2' := \sigma^2\eta_2$$
$$\eta_3 := \sigma\eta_2 \qquad \eta_3' := \sigma\eta_2'$$

Prove that η_1, η_1' are the roots of $X^2 + X - 4$, that η_2, η_2' are the roots of $X^2 - \eta_1 X - 1$, that η_3, η_3' are the roots of $X^2 - \eta_1' - 1$ and that α and $\sigma^4\alpha$ are the roots of $X^2 - \eta_2 X + \eta_3$.

(c) Conclude that $\cos(2\pi/17)$ is equal to

$$\frac{1}{16}\left(-1 + \sqrt{17} + \sqrt{2(17 - \sqrt{17})} + 2\sqrt{17 + 3\sqrt{17} - \sqrt{2(17 - \sqrt{17})} - 2\sqrt{2(17 + \sqrt{17})}}\right)$$

Solution: This is all straightforward and we refer the reader to Dummit and Foote, pg.

7. Let F be a field and $f \in F[X]$ a monic separable polynomial of degree n. Fix a splitting field K of f and write $G := \mathrm{Gal}(K/F)$.

(a) Prove that G is a subgroup of S_n, the symmetric group on n letters. If f is irreducible, prove that G is a *transitive* subgroup of S_n with $\#G$ divisible by n. (Viewing S_n as the permutations of an n-element set T, a transitive subgroup G is one which acts transitively on these n elements, i.e. for any $x, y \in T$ there exists $g \in G$ such that $gx = y$).

(b) Prove that if n is prime and f is irreducible, then G contains an n-cycle. (Hint: use Sylow's theorem.)

(c) Suppose that f is irreducible of degree 5 and has exactly 3 real roots. Prove that G is isomorphic to S_5. (Hint: View K as a subfield of $\mathbf{C}$ and consider complex conjugation acting on K. Now use (7b) and some group theory.)

Solution:

(a) We have seen that for any $g \in G$ and any root α of f in K, we must have $g\alpha$ a root of f; in particular, G acts on the set of n distinct roots of f (using separability here) by permutations, and in this way we get a map $G \to S_n$ which is obviously a homomorphism since the group law in each case is composition. This map is injective since any $g \in G$ is determined by its action on the roots of f, as K is generated over F by these roots. Thus, we may view G as a subgroup of S_n.

If f is irreducible, then we use the following theorem from class:

Theorem 1. *Let F be any field and K, K' extensions of F. Suppose that $f \in F[X]$ is irreducible over F and has roots $\alpha \in K$ and $\beta \in K'$. Then there exists an isomorphism of fields $F(\alpha) \simeq F(\beta)$ restricting to the identity on F and mapping α to β.*

Proof. By the universal mapping property of polynomial rings, we have a surjective map $F[X] \twoheadrightarrow F(\alpha)$ mapping X to α. This map kills (f) so yields a surjective mapping $F[X]/(f) \twoheadrightarrow F(\alpha)$ which must be injective since the source is a field (since f is

irreducible, (f) is prime and hence maximal as $F[X]$ is a PID so the quotient ring is a field). Thus, $F(\alpha) \simeq F[X]/(f)$. By the same token, $F[X]/(f) \simeq F(\beta)$. Composing these isomorphisms yields the desired isomorphism. $\square$

Applying this theorem, we see that in our situation (with f irreducible) for *any* roots α, β of f in K, there exists an automorphism of K over F mapping α to β; in other words, G acts transitively on the roots of f so via our embedding of G into S_n we see that G is a transitive subgroup of S_n. Moreover, since f is irreducible, we have $[F(\alpha) : F] = n$ for any root α of f in K. Since $\#G = [K : F] = [K : F(\alpha)][F(\alpha) : F]$, we see that $n|\#G$.

(b) If $n = p$ is prime and f is irreducible, then by the previous part we know that $\#G$ is divisible by p. By Sylow's theorem, G then contains an element of order p, which under the embedding of G into S_p must be a p-cycle.

(c) If f is an irreducible quintic with exactly 3 real roots, then f has exactly 2 complex non-real roots. The action of complex conjugation on the roots of f therefore swaps these two roots, so under the embedding of G in S_5 corresponds to a 2-cycle. By the previous part, the image of G in S_5 also contains a 5-cycle. But S_5 is generated (as a group) by any 5-cycle and any 2-cycle, so the image of G is all of S_5 whence $G \simeq S_5$.

8. Keep the notation of the previous problem.

(a) Let $r_1, \ldots, r_n$ be the n distinct roots of f in K, and define the *discriminant of* f to be

$$\Delta(f) := \prod_{i \neq j} (r_i - r_j),$$

where the product runs over all pairs $(i, j) \in \mathbf{Z}^2$ with $1 \leq i, j \leq n$. Prove that $\Delta(f) \in F$.

(b) Prove that G is a subgroup of A_n (the alternating group) if and only if $\Delta(f)$ is a square in F. Hint: use the formula for $\Delta(f)$ above and the definition of A_n as the group of even permutations.

Soultion:

(a) For an arbitrary element $\sigma \in S_n$, we have

$$\prod_{i,j} (r_{\sigma i} - r_{\sigma j}) = \prod_{i,j} (r_i - r_j)$$

which shows that *any* permutation of the r_i's leaves $\Delta(f)$ unchanged. In particular, G acts trivially on $\Delta(f)$ so $\Delta(f) \in F$ by Galois theory.

(b) Observe that $\Delta(f)$ is the square of

$$P(r_1, \ldots, r_n) := \prod_{i<j} (r_i - r_j) \in K$$

so that $\Delta(f)$ is a square if and only if $P(r_1, \ldots, r_n) \in F$. If $\sigma \in S_n$, then by definition we have

$$\operatorname{sgn}(\sigma) = \frac{P(r_{\sigma 1}, r_{\sigma 2}, \ldots, r_{\sigma_n})}{P(r_1, r_2, \ldots, r_n)},$$

which shows that $\sigma \in S_n$ fixes $P(r_1, \ldots, r_n)$ if and only if σ is an even permutation. Putting these together, we see that G is a subgroup of A_n if and only if G fixes $P(r_1, \ldots, r_n)$, i.e. if and only if $\Delta(f)$ is a square in F.