Solution 18

Radical extensions, Transitive group actions

1. Let $f = X^3 + pX + q \in \mathbb{Q}[X]$ be an irreducible polynomial. Let $z_1, z_2, z_3 \in \mathbb{C}$ be the roots of f and E its splitting field.

   (a) Define the *discriminant* of f as
   $$D(f) := \prod_{i<j}(z_i - z_j)^2.$$
   Prove that $D(f) = -4p^3 - 27q^2 \neq 0$.
   Hint: $f = (X - z_1)(X - z_2)(X - z_3)$

   (b) Check that E contains the square roots of $D(f)$.

   (c) Suppose that $D(f)$ is not a square in $\mathbb{Q}$. Show that $\mathrm{Gal}(E/\mathbb{Q}) = S_3$.

   (d) Suppose that $D(f)$ is a square in $\mathbb{Q}$. Show that there exists no automorphism $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ switching z_1 and z_2 and deduce that $\mathrm{Gal}(E/\mathbb{Q}) = A_3$.

   (e) Prove that the roots of f are all real if and only if $D(f) > 0$. Else, f has one real root and two non-real conjugated roots.

Solution:

(a) Since $\mathbb{Q}$ has characteristic zero and f is irreducible, we know that f is separable. Hence $z_1 \neq z_2 \neq z_3 \neq z_1$, so that $D(f) \neq 0$ by definition.
Following the hint, we notice that $z_1z_2z_3 = -q$, $z_1z_2 + z_1z_3 + z_2z_3 = p$ and $z_1 + z_2 + z_3 = 0$. Hence

$$\begin{aligned}
D(f) &= (z_1 - z_2)^2(z_1 - z_3)^2(z_2 - z_3)^2 \\
&= (z_1^2 + z_2^2 - 2z_1z_2)(z_1^2 + z_3^2 - 2z_1z_3)(z_2^2 + z_3^2 - 2z_2z_3) \\
&= \sum_{i\neq j} z_i^4 z_j^2 + 2z_1^2z_2^2z_3^2 - 2\sum_{i<j} z_i^3 z_j^3 - 2z_1z_2z_3(\sum_{i\neq j} z_i^2 z_j + \sum_{i=1}^{3} z_i^3) \\
&+ 4z_1z_2z_3 \sum_{i\neq j} z_i^2 z_j - 8z_1^2z_2^2z_3^2 \\
&= \sum_{i\neq j} z_i^4 z_j^2 - 2\sum_{i<j} z_i^3 z_j^3 - 2q(\sum_{i\neq j} z_i^2 z_j - \sum_{i=1}^{3} z_i^3) - 6q^2.
\end{aligned}$$

We now construct symmetric expressions of z_1, z_2, z_3 out of $z_1 + z_2 + z_3$, $z_1z_2 + z_1z_3 + z_2z_3$ and $z_1z_2z_3$ in order to rewrite the above expression in terms of p and q. First, notice that $z_1 + z_2 + z_3 = 0$ implies that

$$0 = \sum_{i=1}^{3} z_i^2 \sum_{j=1}^{3} z_j = \sum_{i \neq j} z_i^2 z_j + \sum z_i^3$$

$$0 = (\sum_{i=1}^{3} z_i)^3 = \sum_{i=1}^{3} z_i^3 + 3 \sum_{i \neq j} z_i^2 z_j + 6z_1z_2z_3$$

from which we obtain, using $z_1z_2z_3 = -q$,

$$\sum_{i \neq j} z_i^2 z_j = 3q \text{ and } \sum_{i=1}^{3} z_i^3 = -3q.$$

Moreover, we compute

$$\sum_{i=1}^{3} z_i^2 + 2p = (\sum_{i=1}^{3} z_i)^2 = 0 \implies \sum_{i=1}^{3} z_i^2 = -2p,$$

$$p^2 = (\sum_{i<j} z_i z_j)^2 = \sum_{i<j} z_i^2 z_j^2 + 2z_1z_2z_3 \sum_{i=1}^{3} z_i = \sum_{i<j} z_i^2 z_j^2.$$

Then

$$-2p^3 = \sum_{k=1}^{3} z_k^2 \cdot \sum_{i<j} z_i^2 z_j^2 = 3z_1^2 z_2^2 z_3^2 + \sum_{i \neq j} z_i^4 z_j^2 \implies \sum_{i \neq j} z_i^4 z_j^2 = -2p^3 - 3q^2$$

Also,

$$4p^2 = \sum_{i=1}^{3} z_i^2 \cdot \sum_{j=1}^{3} z_j^2 = \sum_{i=1}^{3} z_i^4 + 2 \sum_{i<j} z_i^2 z_j^2 \implies \sum_{i=1}^{3} z_i^4 = 2p^2,$$

which lets us compute

$$-4p^3 = \sum_{i=1}^{3} z_i^2 \cdot \sum_{j=1}^{3} z_j^4 = \sum_{i=1}^{3} z_i^6 + \sum_{i<j} z_i^2 z_j^4 \implies \sum_{i=1}^{3} z_i^6 = -2p^3 + 3q^2$$

from which we obtain the remaining expression appearing $D(f)$ via

$$9q^2 = \sum_{i=1}^{3} z_i^3 \sum_{j=1}^{3} z_j^3 = \sum_{i=1}^{3} z_i^6 + 2 \sum_{i<j} z_i^3 z_j^3 \implies \sum_{i<j} z_i^3 z_j^3 = 3q^2 + p^3.$$

Substituting all the above expression in the initial formula for $D(f)$, we get

$$D(f) = -2p^3 - 3q^2 - 2(3q^2 + p^3) - 2q \cdot 6q - 6q^2 = -4p^3 - 27q^2.$$

(b) Recall that E is taken to be the splitting field of f in $\mathbb{C}$. The roots of $D(f)$ in $\mathbb{C}$ are then given by $\pm(z_1 - z_2)(z_1 - z_3)(z_2 - z_3)$ which are elements of E since $z_1, z_2, z_3 \in E$.

(c) By the previous point, $E \supset \mathbb{Q}(z_1, \Delta(f))$, where $\Delta(f) = (z_1 - z_2)(z_1 - z_3)(z_2 - z_3)$ is a square root of $D(f)$. Hence $[E : \mathbb{Q}]$ is divisible by both $[\mathbb{Q}(z_1) : \mathbb{Q}]$ and $[\mathbb{Q}(\Delta(f)) : \mathbb{Q}]$. We know that $[\mathbb{Q}(z_1) : \mathbb{Q}] = \deg(f) = 3$, while $[\mathbb{Q}(\Delta(f)) : \mathbb{Q}] = 2$ because $\Delta(f)^2 = D(f) \in \mathbb{Q}$ and $\Delta(f) \notin \mathbb{Q}$ by assumption. Hence $6|[E : \mathbb{Q}]$. Since $[E : \mathbb{Q}]$ is also the cardinality of $\mathrm{Gal}(E/\mathbb{Q})$ which is a subgroup of S_3 (by looking at its action on the roots of f), we can conclude that $\mathrm{Gal}(E/\mathbb{Q}) \cong S_3$.

(d) Suppose $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ switches z_1 and z_2. Then it must fix z_3. We obtain

$$\sigma(\Delta(f)) = \sigma((z_1 - z_2)(z_1 - z_3)(z_2 - z_3)) = (z_2 - z_1)(z_2 - z_3)(z_1 - z_3) = -\Delta(f),$$

so that $\Delta(f) \notin \mathbb{Q}$ by definition of $\mathrm{Gal}(E/\mathbb{Q})$. Hence no such a σ can exist if $D(f)$ is a square in $\mathbb{Q}$ (because then we know that $\Delta(f) \in \mathbb{Q}$). Still $3 = [\mathbb{Q}(z_1) : \mathbb{Q}]$ divides $[E : \mathbb{Q}] = |\mathrm{Gal}(E/\mathbb{Q})|$ and since $\mathrm{Gal}(E/\mathbb{Q})$ can be seen as a proper subgroup of S_3 (not containing transpositions), the only possibility is that $\mathrm{Gal}(E/\mathbb{Q}) \cong A_3$.

(e) By the mean value theorem we know that f has a root in $\mathbb{R}$. If it has a non-real root, then the complex conjugate of this root must also be a root, since the coefficients of f are in $\mathbb{Q}$ and hence real, so that they are fixed by complex conjugation. Moreover, we know that f has three distinct roots as proved in a), so that the only two possibilities are that f has three real roots or a real root and two conjugated non-real roots. Without loss of generality, assume that $z_1 \in \mathbb{R}$. We distinguished the cases treated in parts c) and d) above to check the given statement.

- Suppose that $D(f)$ is a square in $\mathbb{Q}$ (so that in particular, $D(f) > 0$). Then $E = \mathbb{Q}(z_1)$ because $[E : \mathbb{Q}] = 3$ by part d). Hence $E \subset \mathbb{R}$, so that all roots of f are real.
- Suppose that $D(f)$ is not a square in $\mathbb{Q}$. The argument used in c) shows that $\mathbb{Q}(z_1, \Delta(f))$ has degree 6 over $\mathbb{Q}$, so that $E = \mathbb{Q}(z_1, \Delta(f))$. The roots of f are all real if and only if $E \subset \mathbb{R}$, which is then equivalent to $\Delta(f) \in \mathbb{R}$, which happens if and only if $D(f) > 0$.

2. *(Artin-Schreier extension)* Let k be a field of characteristic 2 and K/k a quadratic extension such that $|\mathrm{Gal}(K/k)| = 2$. Show that there exist $\beta \in K$ and $a \in k$ such that β is a root of $X^2 - X + a \in k[X]$ and $K = k(\beta)$.

Solution: Let $b_0 \in K \setminus k$ and consider its minimal polynomial $f = X^2 + sX + t$ over k. Then $K = k(b_0)$.

Suppose that $s = 0$. Then $b_0^2 = t$ so that $(X - b_0)^2 = X^2 + b_0^2 = X^2 + t$ and the Galois group can map b_0 only to itself, so that $|\mathrm{Gal}(K/k)| = 1$, contradicting our assumptions. Hence $s \neq 0$.

We look for $b = \lambda b_0 + \mu \in K \setminus k$ with $\lambda, \mu \in k$ such that $b^2 - b + a = 0$ for some $a \in k$, that is, such that $b^2 - b \in k$. We compute

$$b^2 - b = (\lambda b_0 + \mu)^2 - (\lambda b_0 + \mu) = \lambda^2 b_0^2 + \lambda b_0 + \mu^2 - \mu = \lambda^2(sb_0 + t) + \lambda b_0 + \mu^2 - \mu$$

and notice that the last quantity belongs to k if and only if $\lambda(\lambda s + 1) = 0$. Since $b \notin k$, we necessarily have $\lambda \neq 0$, so that we need $\lambda = 1/s$. This implies that $b := b_0/s$ has minimal polynomial $X^2 - X + t/s^2$ and generated K/k, as desired.

3. Let G be a group acting on a set X with at least two elements. We say that the action is *doubly transitive* if for each $x_1, x_2, y_1, y_2 \in X$ with $x_1 \neq x_2$ and $y_1 \neq y_2$ there exists $g \in G$ such that $g \cdot x_i = y_i$ for $i = 1, 2$. Show that the following statements are true:

   (a) S_n acts doubly transitively on $\{1, \ldots, n\}$ for each $n \geqslant 2$.

   (b) A_n acts doubly transitively on $\{1, \ldots, n\}$ for each $n \geqslant 4$.

   (c) For each $n \geqslant 4$ the group D_n does *not* act doubly transitively on the vertices of an n-gon (see Assignment 8, Exercise 7).

   Solution:

   (a) As proved in Assignment 9, Exercise 8, the action of S_n on $\{1, \ldots, n\} \times \{1, \ldots, n\}$ has only two orbits: $\{(i, i)\}$ and $\{(i, j) : i \neq j\}$. This means that each (i, j) can be mapped to each (i', j') for $i \neq j$ and $i' \neq j'$ by a permutation in S_n, that is, the action of S_n on $\{1, \ldots, n\}$ is doubly transitive.

   (b) Let $x_1, x_2, y_1, y_2 \in \{1, \ldots, n\}$ with $x_1 \neq x_2$ and $y_1 \neq y_2$. We reason on different cases distinguished by the cardinality of $\{x_1, x_2, y_1, y_2\}$, which ranges from 2 to 4 and find $\sigma \in A_n$ sending $x_i \mapsto y_i$. Recall that a 3-cycle is a product of two 2-cycles and as such it belongs to A_n.

   - Suppose that $|\{x_1, x_2, y_1, y_2\}| = 2$, so that $\{x_1, x_2\} = \{y_1, y_2\}$. If both $x_i = y_i$, then $\sigma = \mathrm{id} \in A_n$ does the job. Else, $x_1 = y_2$ and $x_2 = y_1$. In this second subcase $n \geqslant 4$, we can take $u, v \in \{1, \ldots, n\} \setminus \{x_1, x_2, y_1, y_2\}$ with $u \neq v$ and choose $\sigma = (u\ v)(x_1\ y_1) = (u\ v)(x_2\ y_2)$.
   - Suppose that $|\{x_1, x_2, y_1, y_2\}| = 3$. Without loss of generality, we can assume that either $x_1 = y_1$ or $x_1 = y_2$. In the first subcase, we want to map $x_1 \mapsto x_1$ and $x_2 \mapsto y_2$ and we know that $x_2 \neq y_2$. This can be done by taking $u \in \{1, \ldots, n\} \setminus \{x_1, x_2, y_2\}$ and choosing $\sigma = (x_2\ y_2\ u) \in A_n$. In the second subcase, we want to map $x_1 \mapsto y_1$ and $x_2 \mapsto x_1$, which can be done via $\sigma = (x_2\ x_1\ y_1) \in A_n$.
   - Suppose that $|\{x_1, x_2, y_1, y_2\}| = 4$. Then $\sigma = (x_1\ y_1)(x_2\ y_2) \in A_n$ does the job.

(c) Recall that D_n consists of n rotations (including the identity) and n axial symmetries (*reflections*). Suppose that $\sigma \in D_n$ fixes one vertex P. Then σ is either the identity or the reflection through the axis passing through P. Hence, for a given $P' \neq P$, $\sigma(P')$ has only two possible images, one of which is P' itself, the other is another vertex P''. Since $n \geqslant 4$, we can take P''', a vertex different from P, P' and P'' and see that there exist no $\sigma \in D_n$ mapping $P \mapsto P$ and $P' \mapsto P'''$, so that the action is not doubly transitive.