# Solution 16

SEPARABILITY, COMPUTATION OF AUTOMORPHISM GROUPS

1. Let $f \in k[X]$ and let $E \supset k$ be a splitting field of $f$. We want to prove that $f$ has no multiple root in $E$ if and only if $\gcd_{k[X]}(f, f') = 1$.

   (a) Let $F/k$ be a field extension and $f, g \in k[X]$. Prove that $\gcd_{k[X]}(f, g) = 1$ if and only if $\gcd_{F[X]}(f, g) = 1$.

   (b) Write $f = \prod_{i=1}^{n}(X - \alpha_i)$ in $E[X]$. Establish the formula
   $$\prod_{i=1}^{n} f'(\alpha_i) = \pm \left( \prod_{i<j} (\alpha_i - \alpha_j) \right)^2.$$

   (c) Use the above steps in order to conclude.

   *Solution*:

   (a) Recall that the gcd of two elements is unique up to association (i.e. multiplication by units). Hence, there is a unique monic gcd of two given polynomials with coefficients in a field. By Bezout's identity, a monic polynomial $t \in k[X]$ (or $F[X]$) is the gcd of $f$ and $g$ in $k[X]$ (or $F[X]$) if and only if there exist $p, q \in k[X]$ (or $F[X]$) such that $t = pf + qg$. Since $k[X] \subset F[X]$, we notice that $\gcd_{k[X]}(f, g) = \gcd_{E[X]}(f, g)$, from which it follows immediately that $f, g$ are coprime in $k[X]$ if and only if they are coprime in $E[X]$.

   (b) We can write $f = \prod_{i=1}^{n}(X - \alpha_i)$ in $E[X]$ by definition of splitting field. Recall the Leibniz rule of the derivation (Assignment 3, Exercise 5c):
   $$\forall p, q \in E[X],\ (pq)' = pq' + p'q.$$
   Via induction we can generalize this to
   $$\forall i \in \mathbb{Z}_{\geqslant 1} \colon \forall p_1, \ldots, p_r \in E[X] \colon (p_1 \cdots p_r)' = \sum_{i=1}^{r} \Big( p_i' \prod_{\substack{j \neq i \\ j=1,\ldots,r}} p_j \Big).$$
   Applying this formula with $f = \prod_{i=1}^{n}(X - \alpha_i)$ we obtain
   $$f' = \sum_{i=1}^{n} \Big( 1 \cdot \prod_{\substack{j \neq i \\ j=1,\ldots,n}} (X - \alpha_j) \Big).$$

Evaluating this derivative at $\alpha_k$, all summands with $i \neq k$ vanish, because for $i \neq k$ the product contains the factor $(\alpha_k - \alpha_k) = 0$. Hence

$$f'(\alpha_k) = \prod_{\substack{j \neq k \\ j=1,\dots,n}} (\alpha_k - \alpha_j)$$

which implies

$$\begin{aligned}
\prod_{k=1}^{n} f'(\alpha_k) &= \prod_{k=1}^{n} \prod_{\substack{j \neq k \\ j=1,\dots,n}} (\alpha_k - \alpha_j) = \prod_{k=1}^{n} \Big( \prod_{\substack{j > k \\ j=1,\dots,n}} (\alpha_k - \alpha_j) \prod_{\substack{j < k \\ j=1,\dots,n}} (-1)(\alpha_j - \alpha_k) \Big) \\
&= \prod_{j=1}^{n} \Big( \prod_{\substack{k > j \\ k=1,\dots,n}} (\alpha_j - \alpha_k) \Big) \prod_{k=1}^{n} (-1)^{k-1} \Big( \prod_{\substack{j < k \\ j=1,\dots,n}} (\alpha_j - \alpha_k) \Big) \\
&= (-1)^{\binom{n}{2}} \Big( \prod_{1 \leqslant j < k \leqslant n}^{n} (\alpha_k - \alpha_j) \Big)^2.
\end{aligned}$$

(c) By part (a), $f$ and $f'$ are coprime in $k[X]$ if and only if they are coprime in $E[X]$. Since $E[X]$ is a UFD and $f$ factors into irreducible polynomials as $f = \prod_{i=1}^{n} (X - \alpha_i)$, it is coprime to $f'$ in $E[X]$ if and only if for each $i = 1, \dots, n$ the polynomial $X - \alpha_i$ does not divide $f'$. This is equivalent to saying that none of the $\alpha_i$ is a root of $f'$, which in turns means that $\prod_{i=1}^{n} f'(\alpha_i) \neq 0$. This last property is equivalent to the $\alpha_i$ being all distinct. Hence $f$ and $f'$ are coprime if and only if $f$ has no multiple roots.

2. Let $p$ be a prime number and $\zeta := e^{\frac{2\pi i}{p}}$ a primitive $p$-th root of unity. Consider the polynomial $\varphi_p := \frac{X^p - 1}{X - 1} \in \mathbb{Q}[X]$ with splitting field $E$.

   (a) Prove that $\varphi_p$ is irreducible in $\mathbb{Q}[X]$ and deduce that $\varphi_p$ is the minimal polynomial of $\zeta$ over $\mathbb{Q}$.

   (b) Show that $E = \mathbb{Q}(\zeta)$.

   (c) Prove that $\mathrm{Aut}(E/\mathbb{Q}) = (\mathbb{Z}/p\mathbb{Z})^\times$.

*Solution*:

(a) See Assignment 11, Exercise 4.

(b) A complex root $x$ of $X^p - 1$ must have absolute value equal to 1 (because $|x|^p = |x^p| = |1| = 1$), hence it should be of the form $x = e^{\alpha i}$ for $\alpha \in \mathbb{R}$. Imposing $x^p = 1$ we obtain $\alpha = 2\pi i \frac{k}{p}$ for some $k \in \mathbb{Z}$. Since $e^{2\pi i} = 1$, we can consider $k \in \{0, 1, \dots, p-1\}$. We see then that

$$X^p - 1 = \prod_{k=0}^{p-1} (X - \zeta^k),$$

so that

$$\varphi_p = \prod_{k=1}^{p-1}(X - \zeta^k).$$

Since $\mathbb{Q}(\zeta)$ contains all powers of $\zeta$, we conclude that $E = \mathbb{Q}(\zeta)$.

(c) By part (b), an automorphism $\sigma$ of $E$ over $\mathbb{Q}$ is uniquely determined by the image of $\zeta$. Since $\mathrm{Aut}(E/\mathbb{Q})$ maps roots of $\varphi_p$ to roots of $\varphi_p$, we know that $\sigma(\zeta) \in \{\zeta^k,\ k \in \{1, 2, \ldots, p-1\}\}$ for all $\sigma \in \mathrm{Aut}(E/\mathbb{Q})$.
We define the map

$$\begin{aligned} \xi : (\mathbb{Z}/p\mathbb{Z})^\times &\longrightarrow \mathrm{Aut}(E/\mathbb{Q}) \\ k + p\mathbb{Z} &\longmapsto (\zeta \mapsto \zeta^k). \end{aligned}$$

This map is well-defined because $\zeta^{\ell p} = 1$ for each $\ell \in \mathbb{Z}$. In order to prove that it is a group homomorphism, recall that the multiplicative structure on $(\mathbb{Z}/p\mathbb{Z})$ is defined by $(k_1 + p\mathbb{Z}) \cdot (k_2 + p\mathbb{Z}) := k_1k_2 + p\mathbb{Z}$ for $k_1, k_2 \in \mathbb{Z}$. Then

$$\xi(k_1k_2 + p\mathbb{Z})(\zeta) = \zeta^{k_1k_2},$$

while

$$(\xi(k_1 + p\mathbb{Z}) \circ \xi(k_2 + p\mathbb{Z}))(\zeta) = (\xi(k_1 + p\mathbb{Z}))(\zeta^{k_2}) \overset{(*)}{=} (\zeta^{k_1})^{k_2} = \zeta^{k_1k_2},$$

where in the step $(*)$ we used the fact that $\xi(k_1+p\mathbb{Z})$ is a field homomorphism sending $\zeta \mapsto \zeta^{k_1}$. This means that

$$\xi(k_1 + p\mathbb{Z}) \circ \xi(k_2 + p\mathbb{Z}) = \xi(k_1k_2 + p\mathbb{Z}) = \xi((k_1 + p\mathbb{Z}) \cdot (k_2 + p\mathbb{Z})),$$

so $\xi$ is a group homomorphism. It is surjective by the observations made at the beginning of this part. It is injective because $\forall k \in \{1, \ldots, p-1\}$:

$$k + p\mathbb{Z} \in \ker \xi \iff \xi(k + p\mathbb{Z}) = \mathrm{id}_E \iff \zeta^k = \zeta \iff k = 1$$

Hence we have proven that $\mathrm{Aut}(E/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times$.

3. Let $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

   (a) Prove that $[E : \mathbb{Q}] = 4$.

   (b) Show that $\mathrm{Aut}(E/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

*Solution*:

(a) First we check that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Suppose that for $a, b \in \mathbb{Q}$ we have the equality $(a + b\sqrt{2})^2 = 3$. Then $a^2 + 2b^2 + 2ab\sqrt{2} = 3$, which by $\mathbb{Q}$-linear independence of 1 and $\sqrt{2}$ implies that $ab = 0$. If $a = 0$, then $2b^2 = 3$, while if $b = 0$, then $a^2 = 3$. Both possibilities yield a contradiction. Hence $E/\mathbb{Q}(\sqrt{2})$ is not a trivial extension. Since it is generated by the element $\sqrt{3}$, which is a root of $X^2 - 3 \in \mathbb{Q}(\sqrt{2})[X]$, we see that $[E : \mathbb{Q}(\sqrt{2})] = 2$. Then by multiplicativity of the degree in towers, we obtain

$$[E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

(b) Since $E$ is the splitting field of the separable irreducible polynomial $X^2 - 3$ in $\mathbb{Q}(\sqrt{2})[X]$, we know that $2 \mid \mathrm{Aut}(E/\mathbb{Q}(\sqrt{2}))$. Note that an automorphism $\sigma \in \mathrm{Aut}(E/\mathbb{Q}(\sqrt{2}))$ is uniquely determined by the image of $\sqrt{3}$, which must be either $\sqrt{3}$ or $-\sqrt{3}$. Hence $\mathrm{Aut}(E/\mathbb{Q}(\sqrt{2}))$ contains precisely 2 elements: the identity id and $\sigma_3 : \sqrt{3} \mapsto -\sqrt{3}$ (which sends $\sqrt{2} \mapsto \sqrt{2}$ by definition of $\mathrm{Aut}(E/\mathbb{Q}(\sqrt{2}))$).
Similarly, one sees that $\mathrm{Aut}(E/\mathbb{Q}(\sqrt{3})) = \{\mathrm{id}, \sigma_2\}$ where $\sigma_2$ maps $\sqrt{2} \mapsto -\sqrt{2}$ (and $\sqrt{3} \mapsto \sqrt{3}$).
The automorphisms of $E$ mentioned above are all also elements of $\mathrm{Aut}(E/\mathbb{Q})$, which contains the 4 distinct automorphisms $\mathrm{id}, \sigma_2, \sigma_3, \sigma_2 \circ \sigma_3$. On the other hand, $\sigma \in \mathrm{Aut}(E/\mathbb{Q})$ is uniquely determined by the images of $\sqrt{2}$ and $\sqrt{3}$, and since both can be mapped to precisely two values, we have at most 4 possibilities. Hence $\mathrm{Aut}(E/\mathbb{Q}) = \{\mathrm{id}, \sigma_2, \sigma_3, \sigma_2 \circ \sigma_3\}$. The only two groups up to isomorphism containing 4 elements are $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Note that $\sigma_2$ and $\sigma_3$ have order 2 (because if we perform $\sigma_j$ twice, both $\sqrt{2}$ and $\sqrt{3}$ are mapped to themselves), while $\mathbb{Z}/4\mathbb{Z}$ contains only one element of order 2. Hence

$$\mathrm{Aut}(E/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

4. Show that the Galois group of $X^3 - 2 \in \mathbb{Q}[X]$ is isomorphic to $S_3$.

*Hint:* Let $E$ be the splitting field of $X^3 - 2$. Find the roots of $X^3 - 2$ in $\mathbb{C}$. Consider the intermediate extension $\mathbb{Q}(\exp(2\pi i/3))/\mathbb{Q}$ of $E$ and show that $[E : \mathbb{Q}] > 3$.

*Solution*: Recall that $\mathrm{Aut}(E/\mathbb{Q})$ can be seen as a subgroup of $S_3$ by considering its actions on the roots of $X^3 - 2$. Hence, in order to prove that $\mathrm{Aut}(E/\mathbb{Q}) \cong S_3$, it is enough to check that $|\mathrm{Aut}(E/\mathbb{Q})| \geqslant 6$. The roots of $X^3 - 2$ in $\mathbb{C}$ are

$$\sqrt[3]{2},\ \sqrt[3]{2}\zeta,\ \sqrt[3]{2}\zeta^2,$$

where $\zeta = e^{\frac{2\pi i}{3}}$. Hence $E = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\zeta, \sqrt[3]{2}\zeta^2) = \mathbb{Q}(\sqrt[3]{2}, \zeta)$. It contains the intermediate extensions $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ and $\mathbb{Q}(\zeta)/\mathbb{Q}$ which have degree 3 and 2 respectively since $X^3 - 2$ and $X^2 + X + 1$ are their respective minimal polynomials over $\mathbb{Q}$ ($X^3 - 2 \in \mathbb{Q}[X]$ is irreducible by Eisenstein's criterion, $X^2 + X + 1 \in \mathbb{Q}[X]$ is irreducible by Exercise 2). Hence, by multiplicativity of the degree, both 2 and 3 are divisors of $[E : \mathbb{Q}]$. Moreover $[E : \mathbb{Q}(\sqrt[3]{2})] \leqslant 2$ because $\zeta^2 + \zeta + 1 = 0$. Then

$$6 \leqslant [E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] \leqslant 2 \cdot 3 = 6,$$

so that $[E : \mathbb{Q}] = 6$. Then, again by multiplicativity of the degree, we see that

$$[E : \mathbb{Q}(\sqrt[3]{2})] = 2 \text{ and } [E : \mathbb{Q}(\zeta)] = 3.$$

From the lecture we thus know that 2 divides $|\mathrm{Aut}(E/\mathbb{Q}(\sqrt[3]{2}))|$ and 3 divides $|\mathrm{Aut}(E/\mathbb{Q}(\zeta))|$. Since these two automorphism groups are subgroups of $\mathrm{Aut}(E/\mathbb{Q})$, we deduce that 6 divides $|\mathrm{Aut}(E/\mathbb{Q})|$. By the initial observation, we can conclude that $\mathrm{Aut}(E/\mathbb{Q}) \cong S_3$.