Solution 16

SEPARABILITY, COMPUTATION OF SOME GALOIS 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 to elements is unique up to association (i.e. multiplication by units). We prove that $\gcd_{F[X]}(f, g) = \gcd_{k[X]}(f, g)$ for all $f, g \in k[X]$ by checking that they divide each other in $F[X]$. The statement will immediately follow.

   First, we notice that $\gcd_{k[X]}(f, g)$ divides both f and g in $k[X]$, hence also in $F[X]$, implying that it must divide their greatest common divisor $\gcd_{F[X]}(f, g)$. On the other hand, we can write $\gcd_{k[X]}(f, g) = pf + qg$ for some $p, q \in k[X]$ by Bezout's identity. Since $\gcd_{F[X]}(f, g)$ divides both f and g, it must then divide $\gcd_{k[X]}(f, g)$.

   (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 an easy induction we can generalize this to

   $$\forall i \in \mathbb{Z}_{\geq 1}, \ \forall p_1, \ldots, p_r \in E[X], \ (p_1 \cdots p_r)' = \sum_{i=1}^{r} \left(p_i' \prod_{\substack{j \neq i \\ j=1,\ldots,r}} p_j \right).$$

Applying this formula with $f = \prod_{i=1}^{n}(X - \alpha_i)$ we obtain

$$f' = \sum_{i=1}^{n}\left(1 \cdot \prod_{\substack{j \neq i \\ j=1,\ldots,n}}(X - \alpha_j)\right).$$

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

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

which implies

$$\prod_{k=1}^{n} f'(\alpha_k) = \prod_{k=1}^{n}\prod_{\substack{j \neq k \\ j=1,\ldots,n}}(\alpha_k - \alpha_j) = \prod_{k=1}^{n}\left(\prod_{\substack{j>k \\ j=1,\ldots,n}}(\alpha_k - \alpha_j)\prod_{\substack{j<k \\ j=1,\ldots,n}}(-1)(\alpha_j - \alpha_k)\right)$$

$$= \prod_{j=1}^{n}\left(\prod_{\substack{k>j \\ k=1,\ldots,n}}(\alpha_j - \alpha_k)\right)\prod_{k=1}^{n}(-1)^{k-1}\left(\prod_{\substack{j<k \\ j=1,\ldots,n}}(\alpha_j - \alpha_k)\right)$$

$$= (-1)^{\binom{n}{2}}\left(\prod_{1\leqslant j<k\leqslant n}(\alpha_k - \alpha_j)\right)^2.$$

(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 $i = 1, \ldots, n$ the polynomial $X - \alpha_i$ does not divide f'. This is equivalent to saying that none of the α_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 α_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. Consider the polynomial $\varphi_p := \frac{X^p-1}{X-1} \in \mathbb{Q}[X]$ and let $\zeta := e^{\frac{2\pi i}{p}}$. Let $E := \mathrm{Sf}(\varphi_p)$.

   (a) Prove that φ_p is irreducible in $\mathbb{Q}[X]$ and deduce that $\varphi_p = \mathrm{irr}(\zeta; \mathbb{Q})$.

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

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

   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 $k \in \{0, 1, \ldots, p-1\}$. We see than 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 power of ζ, we can conclude that $E = \mathbb{Q}(\zeta)$.

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

We define the map

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

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, let $k_1, k_2 \in \mathbb{Z}$, $(k_1 + p\mathbb{Z}) \cdot (k_2 + p\mathbb{Z}) := k_1 k_2 + p\mathbb{Z}$. Then

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

while

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

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 $\xi(k_1 + p\mathbb{Z}) \circ \xi(k_2 + p\mathbb{Z}) = \xi(k_1 k_2 + p\mathbb{Z})((k_1 + p\mathbb{Z}) \cdot (k_2 + p\mathbb{Z}))$, so that ξ is a group homomorphism. It is surjective by the observations done in the beginning of this part. It is injective because

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

Hence we have proven that $\mathrm{Gal}(E/\mathbb{Q})$ 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 $\mathrm{Gal}(E/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Solution:

(a) First we check that $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Suppose that for $a, b \in \mathbb{Q}$ the equality $(a + b\sqrt{2})^2 = 3$ holds. 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 eventuality give 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) As E is the splitting field of the separable irreducible polynomial $X^2 - 3 \in \mathbb{Q}(\sqrt{2})[X]$, we know that $2 \mid \mathrm{Gal}(E/\mathbb{Q}(\sqrt{2}))$. Notice that an automorphism $\sigma \in \mathrm{Gal}(E/\mathbb{Q}(\sqrt{2}))$ is uniquely determined by the image of $\sqrt{3}$, which must be either $\sqrt{3}$ or $-\sqrt{3}$. Hence $\mathrm{Gal}(E/\mathbb{Q}(\sqrt{2}))$ 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 $\mathrm{Gal}(E/\mathbb{Q}(\sqrt{2}))$).

Similarly, one sees that $\mathrm{Gal}(E/\mathbb{Q}(\sqrt{3})) = \{\mathrm{id}, \sigma_2\}$ where σ_2 maps $\sqrt{2} \mapsto -\sqrt{2}$ (and $\sqrt{3} \mapsto \sqrt{3}$).

The automorphisms of E above mentioned are all elements of $\mathrm{Gal}(E/\mathbb{Q})$ as well, which contains the 4 distinct automorphisms $\mathrm{id}, \sigma_2, \sigma_3, \sigma_2 \circ \sigma_3$. On the other hand, $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ 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 $\mathrm{Gal}(E/\mathbb{Q}) = \{\mathrm{id}, \sigma_2, \sigma_3, \sigma_2 \circ \sigma_3\}$. The only two groups up to isomorphism containing 4 elements are $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Notice that σ_2 and σ_3 have order 2 (because if we perform σ_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

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

4. Show that the Galois group of $X^3 - 2 \in \mathbb{Q}[X]$ is isomorphic to S_3. [*Hint:* Let $E = \mathrm{Sf}(X^3 - 2)$. 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 $\mathrm{Gal}(E/\mathbb{Q})$ 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 $\mathrm{Gal}(E/\mathbb{Q}) \cong S_3$, it is enough to check that $|\mathrm{Gal}(E/\mathbb{Q})| \geqslant 6$. We see that the roots of $X^3 - 2$ in $\mathbb{C}$ are

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

4

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 polynomial 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, 2 and 3 are divisors of $[E : \mathbb{Q}]$. Moreover $[E : \mathbb{Q}(\sqrt[3]{2}] \leqslant 2$ because $\zeta^2 + \zeta + 1$. 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

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

By Corollary II.19 seen in class, 2 divides $|\operatorname{Gal}(E/\mathbb{Q}(\sqrt[3]{2}))|$ and 3 divides $|\operatorname{Gal}(E/\mathbb{Q}(\zeta))|$. Since those two Galois groups are subgroups of $\operatorname{Gal}(E/\mathbb{Q})$, we deduce that 6 divides $|\operatorname{Gal}(E/\mathbb{Q})|$. By the initial observation, we can conclude that $\operatorname{Gal}(E/\mathbb{Q}) \cong S_3$.