Solution 19

Normality and separability

1. Let $f \in k[X]$ be a monic polynomial which splits into linear factors over k. Suppose that $\sigma \in \mathrm{Aut}(k)$ fixes each root of f. Prove that σ fixes all the coefficients of f.

   Solution: Since f is monic and splits in $k[X]$, we can write $f = \prod_{i=1}^{r}(X - a_i)$ for $a_i \in k$ the not necessarily distinct roots of f. The coefficients of f are then given by sums and products of the roots a_i. Since σ fixes each a_i by assumption (as they are roots of f) and respects the field operations, σ must fix all the coefficients of f.

2. Let E/k be a splitting field of $f \in k[X]$ and consider an extension k' of k and the splitting field E' of f over k'. Show that each $\sigma \in \mathrm{Aut}(E'/k')$ satisfies $\sigma(E) = E$ and that the resulting homomorphism

$$\begin{aligned} \varphi\colon \mathrm{Aut}(E'/k') &\longrightarrow \mathrm{Aut}(E/k) \\ \sigma &\longmapsto \sigma|_E \end{aligned}$$

   is injective.

   Solution: Let $a_1, \dots, a_n \in E$ denote the roots of f. We know that $E = k(a_1, \dots, a_n)$ and $E' = k'(a_1, \dots, a_n)$, and since $k \subset k'$, we have $E \subset E'$ and any $\sigma \in \mathrm{Aut}(E'/k')$ fixes k. Moreover, σ sends roots of f to roots of f, hence $\sigma(E) \subset E$. This means that the map φ is well-defined. It is a homomorphism because restriction and composition commute.

   Let $\sigma \in \ker(\varphi) \subset \mathrm{Aut}(E'/k')$. Then $\sigma|_E = \mathrm{id}_E$, i.e. σ fixes E. Hence σ fixes both k' (by definition) and $a_1, \dots, a_n \in E$, resulting in σ fixing all of $k'(a_1, \dots, a_n) = E'$, so that $\sigma = \mathrm{id}_{E'}$. Hence φ is injective, as desired.

3. Let E/k be a finite field extension and let $\bar{E}$ be an algebraic closure of E (and thus of k).

   (a) Prove that the following are equivalent:

      (i) For every k-homomorphism $\varphi\colon E \to \bar{E}$ we have $\varphi(E) \subset E$.

      (ii) Every irreducible polynomial $f \in k[X]$ with a root in E splits into linear factors over E.

      (iii) E is the splitting field of some polynomial $f \in k[X]$.

Hint. Prove (ii)⇒(iii)⇒(i)⇒(ii) and use the fact that every k-homomorphism $K \to \bar{K}$ can be extended to a k-homomorphism $K(a) \to \bar{K}$ for any $a \in \bar{K}$.

(b) Suppose that the minimal polynomial over k of any element in E has distinct roots in $\bar{E}$. Prove that E/k is Galois if and only if every irreducible polynomial $f \in k[X]$ with a root in E splits into linear factors over E.

Solution: Since E is a finite field extension, we can write $E = k(a_1, \ldots, a_n)$ for some $a_1, \ldots, a_n \in E$. Let $f_1, \ldots, f_n \in k[X]$ denote their respective minimal polynomials.

(a) (ii)⇒(iii): Suppose (ii) is true. Then each f_j splits into linear factors over E and so E contains the splitting field E_f of $f := \prod_{i=1}^{n} f_i \in k[X]$. But E_f contains all roots of f, in particular $a_1, \ldots, a_n$. So E_f contains $k(a_1, \ldots, a_n) = E$, and thus $E = E_f$ is the splitting field of f.

(iii)⇒(i): Suppose E is the splitting field of $f \in k[X]$. Then $E = k(\alpha_1, \ldots, \alpha_d)$ where $\alpha_1, \ldots, \alpha_d$ are the distinct roots of f. Let $\varphi \in \mathrm{Hom}_k(E, \bar{E})$ and let $a \in \{\alpha_1, \ldots, \alpha_d\}$. Since f has coefficients in k, we have

$$f(\varphi(a)) = \varphi(f(a)) = \varphi(0) = 0$$

and so $\varphi(\{\alpha_1, \ldots, \alpha_d\}) \subset \{\alpha_1, \ldots, \alpha_d\}$; hence $\varphi(E) = \varphi(k(\alpha_1, \ldots, \alpha_d)) \subset E$.

(i)⇒(ii): Suppose (i) is true and let $f \in k[X]$ be irreducible with a root $a \in E$. Let $b \in \bar{E}$ be another root of f. Then there is a k-isomorphism $\psi \colon k(a) \to k(b) \subset \bar{k} = \bar{E}$ with $\psi(a) = b$, which can be extended to E according to the fact in the hint. By assumption, we have $\psi(E) \subset E$ and thus $b \in E$. Since b was arbitrary, all roots of f lie E.

(b) From the lecture we know that E/k is Galois if and only if E is the splitting field of a polynomial over k with distinct roots. Thus, using Part (a), the direction '⇒' is clear.

For the converse, note first that any two irreducible polynomials $f \neq g \in k[X]$ have no common roots in any extension k'/k: Indeed, suppose f and g have a common root in some extension k'/k. Then its minimal polynomial over k divides both f and g in $k[X]$. But f and g are irreducible and distinct, contradiction. By assumption, each of the minimal polynomials $f_1, \ldots, f_n$ of $a_1, \ldots, a_n$ has distinct roots in $\bar{E}$, and is irreducible over k with a root in E, thus by assumption splits into linear factors over E. By the preceding argument, any two of $f_1, \ldots, f_n$ are either equal or have no common zeros. Without loss of generality assume that $f_1, \ldots, f_d$ are all the distinct ones, for some $0 < d < n$. Then $f := \prod_{i=1}^{d} f_i$ is a polynomial over k with distinct roots $a_1, \ldots, a_n$, all of which lie in E. So for E_f the splitting field of f we have $E = k(a_1, \ldots, a_n) \subset E_f \subset E$, hence equality.

4. Show that $\mathrm{Aut}(\mathbb{R}) = \{\mathrm{id}_{\mathbb{R}}\}$.

Solution: Let $\sigma \in \mathrm{Aut}(\mathbb{R})$. Since σ respects the sum and $\sigma(1) = 1$, we notice that $\sigma|_{\mathbb{Z}} = \mathrm{id}_{\mathbb{Z}}$. Now let $f = 1/q$ with $q \in \mathbb{Z} \smallsetminus \{0\}$. We notice that $q \cdot \sigma(f) = \sigma(qf) = \sigma(1) = 1$, so that $\sigma(f) = 1/q = f$. This proves that σ must be the identity on $\mathbb{Q}$.

Next, we prove that σ is a strictly increasing function. Let $x, y \in \mathbb{R}$ with $x < y$ and write $y - x = z^2$ for $z \in \mathbb{R} \smallsetminus \{0\}$. Then

$$\sigma(y) - \sigma(x) = \sigma(y - x) = \sigma(z^2) = \sigma(z)^2 > 0,$$

where $\sigma(z) \neq 0$ because $z \neq 0$ and σ is injective. Hence $\sigma(y) > \sigma(x)$.

Now we check that σ is continuous by looking at the preimage of an open interval $I = (a, b)$ in $\mathbb{R}$. By bijectivity of σ we can write $a = \sigma(\alpha)$ and $b = \sigma(\beta)$ so that

$$\sigma^{-1}(I) = \{x \in \mathbb{R} : \sigma(\alpha) < \sigma(x) < \sigma(\beta)\} = (\alpha, \beta)$$

which implies, by arbitrarity of the open interval I, that σ is continuous.

Finally, the two maps σ and $\mathrm{id}_{\mathbb{R}}$ are continuous real functions coinciding on the dense subset $\mathbb{Q}$. This implies that they must coincide on the whole $\mathbb{R}$ and by arbitrarity of σ we conclude that $\mathrm{Aut}_{\mathbb{R}} = \{\mathrm{id}_{\mathbb{R}}\}$.