Solution 19

Normality and separability

1. Let K/k be a field extension and $f \in k[X]$. Prove that f is separable as a polynomial in $k[X]$, then it is separable as a polynomial in $K[X]$. Does the converse hold?

   Solution: Write $f = \prod_i^r f_i$ with $f_i \in k[X]$ irreducible polynomials. By definition of separability, each f_i has no repeated roots in its splitting field E_i. Hence, by Lemma seen in class $\gcd_{k[X]}(f, f') = 1$, which by Assignment 16, Exercise 1a) is equivalent to saying that $\gcd_{K[X]}(f, f') = 1$, which implies that f_i, seen as a polynomial in $K[X]$, has no multiple roots. Since the decomposition $f = \prod_i^r f_i$ holds in $K[X]$ as well and $K[X]$ is a UFD, each irreducible factor g appearing in a decomposition of f in $K[X]$ divides one of the f_i and since f_i has no multiple roots in its splitting field, the same holds for g (the roots of g being roots of f_i with smaller multiplicity). Hence f is separable as a polynomial in $K[X]$ by definition.

   The converse does not true. For example, consider the field $k = \mathbb{F}_p(t^p)$ and its algebraic extension $K = \mathbb{F}_p(t) = k(t)$. The polynomial $f := X^p - t^p \in k[X]$ splits completely in $K[X]$ as $f = (X - t)^p$, so that it is separable as a polynomial in $K[X]$ by definition. On the other hand, it is not a separable polynomial in $k[X]$, because there it is irreducible and the root $t \in K$ of f is a multiple root. The fact that f is irreducible in $k[X]$ can be seen by noticing that a factor g of f must be of the form $(X - t)^r$ (up to multiplying by a constant) for some $0 \leqslant r \leqslant p$ and noticing that $(X-t)^r$ has constant term t^r which belongs to k if and only if $r = 0$ or $r = p$.

2. Let $f \in k[X]$ be a monic polynomial which splits and 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 $a_i \in k$ not necessarily distinct. The coefficients of f are then seen to be given by sums and products of the a_i's and since σ fixes the a_i's by assumption (as they are roots of f) and respects the field operations, then σ must fix all the coefficients of f.

   Alternatively, one can define $\tilde{\sigma} : k[X] \longrightarrow k[X]$ to be the unique ring homomorphism such that $\tilde{\sigma}|_k = \sigma$ and $\tilde{\sigma}(X) = X$. Write $f = \prod_{i=1}^r (X - a_i) = \sum_{j=0}^r b_j X^j$ with $b_n = 1$. Then we see that

$$\tilde{\sigma}(f) = \tilde{\sigma}(\prod_{i=1}^r (X - a_i)) = \prod_{i=1}^r \tilde{\sigma}(X - a_i) = \prod_{i=1}^r (X - \sigma a_i) = \prod_{i=1}^r (X - a_i) = f,$$

so that

$$f = \tilde{\sigma}(f) = \tilde{\sigma}(\sum_{j=0}^{r} b_j X^j) = \sum_{j=0}^{r} \tilde{\sigma}(b_j X^j) = \sum_{j=0}^{r} \sigma(b_j) X^j$$

so that a comparison by coefficients gives $\sigma(b_j) = b_j$.

3. 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 $\sigma \in \mathrm{Gal}(E'/k')$ satisfies $\sigma(E) = E$ and that the resulting homomorphism

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

is injective.

Solution: We know that $E = k(R(f)) \subset E' = k'(R(f))$. If $\sigma \in \mathrm{Gal}(E'/k')$, then σ fixes k. Moreover, σ sends roots of f to roots of f, hence $\sigma(E) = \sigma(k(R(f))) \subset k(R(f)) = E$. This means that the map φ in the assignment is defined. It is clear that it is a homomorphism since restriction and composition of morphisms commute.

Let $\sigma \in \ker(\varphi)$. Then $\sigma \in \mathrm{Gal}(E'/k')$ must fix the whole $E = k(R(f))$. Hence σ fixes k' and $R(f)$, resulting in σ fixing the whole $k'(R(f)) = E'$, so that $\sigma = \mathrm{id}_{E'}$. Hence φ is injective, as desired.

4. Let E/k be a finite field extension. Show that E/k is normal if and only if every irreducible polynomial $f \in k[X]$ which has a root in E splits completely over E.

Solution: Since E is a finite field extension, we know that it is finitely generated and we can write $E = k(\alpha_1, \ldots, \alpha_k)$ for some $\alpha_j \in E$.

Suppose that each polynomial $f \in k[X]$ which has a root in E splits completely over E. In particular, each polynomial $\mathrm{irr}(\alpha_j, k)$ splits completely over E and hence so does $g = \prod_{j=1}^{r} \mathrm{irr}(\alpha_j, k)$. This implies that E contains the splitting field $\mathrm{Sf}(g)$ of g. But $\mathrm{Sf}(g)$ must contain the roots $\alpha_1, \ldots, \alpha_k$ of f, so that it must contain $k(\alpha_1, \ldots, \alpha_k) = E$. This lets us conclude that $E = \mathrm{Sf}(g)$ so that E/k is a normal extension.

Conversely, suppose that $E = \mathrm{Sf}(g)$ for some polynomial g and let $f \in k[X]$ be an irreducible polynomial with a root $\alpha \in E$. Let $E' = \mathrm{Sf}(fg)$ and $\beta \in E'$ a root of f. Since α and β are roots of the irreducible polynomial $f \in k[X]$, there is an isomorphism $\psi : k(\alpha) \longrightarrow k(\beta)$ sending $\alpha \mapsto \beta$ and fixing elements of k. This can be extended to a field automorphism φ of the algebraic closure $\overline{k}$ of k, which must send E into E because E/k is normal and we can use the same argument used in the proof of Theorem II.26. Hence $\beta \in E$. By arbitrarity of β, we can conclude that E contains all roots of g as desired.

5. 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 $\mathrm{Aut}_{\mathbb{R}} = \{\mathrm{id}_{\mathbb{R}}\}$.