Algebra Homework 3

Solutions

1 Let $F \subseteq K \subseteq E$ and suppose $\alpha \in E$ is algebraic over F. Let $f = m_{K,\alpha}$. Show that all the coefficients of f are algebraic over F.

Solution

Let $L \supseteq E$ be a splitting field for f over E. If we rename L, calling it E from now on, it does not have any effect on the coefficients of f – they are still either algebraic or not.

Now in E we can write $f = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_k)$ with each α_i evidently algebraic. The coefficients of f are then algebraic combinations of the α_i, and since $K = \{\alpha \in E \,|\, \alpha \text{ is algebraic over } F\}$ is a field, each of the coefficients is algebraic over F.

2 Let F have characteristic $p \neq 0$, and let $f(X) = X^p - X - a$ where a is some element of F.

(a) Show that f splits over any extension field of F in which it has a root.

Solution

Suppose $F \subseteq E$ and $\alpha \in E$ is a root of f. Then

$$\begin{aligned} f(\alpha + 1) &= (\alpha + 1)^p - (\alpha + 1) - a \\ &= \alpha^p + 1 - \alpha - 1 - a \\ &= \alpha^p - \alpha - a = 0, \end{aligned}$$

so $\alpha + 1$ is also a root of f. Continuing, we see that the elements $\alpha, \alpha + 1, \alpha + 2, \ldots, \alpha + (p - 1)$ form a complete list of roots of f. Since each root evidently lies in E, f splits over E.

(b) If f is not irreducible in $F[X]$, show that it splits over F.

Solution

From part (a) we see that if $\alpha \in E$ is a root of f then $F[\alpha]$ is the (unique) splitting field for f in E over F. Let $f = g_1 g_2 \cdots g_k$ be a factorization of f into irreducible factors. Let $\alpha \in E$ be a root of g_i and $\beta \in E$ be a root of g_j. Then $F[\alpha] = F[\beta]$, so $\deg(g_i) = |F[\alpha] : F| = |F[\beta] : F| = \deg(g_j)$. Since all the irreducible factors of f have the same degree, call it d, it follows that d divides p. Therefore $d = p$ or $d = 1$, and since we are given that $d < p$, we see that f splits into linear factors.

(c) If f is irreducible over F and E is a splitting field for f over F, show that $\mathrm{Gal}(E/F)$ contains an element of order p.

Solution

We know that the identity map for F can be extended to an F-isomorphism $\phi : F[\alpha] \longrightarrow F[\beta]$ with $\phi(\alpha) = \beta$ for any two roots α and β of f. By the uniqueness of splitting fields, ϕ can be extended to an F-automorphism of E.

Now let $\alpha \in E$ be a root of f, and notice that it follows from part (a) that $E = F[\alpha]$. Therefore an automorphism $\sigma \in \mathrm{Gal}(E/F)$ is determined by its value on α. Let $\phi \in \mathrm{Gal}(E/F)$ be the unique element such that $\phi(\alpha) = \alpha + 1$. It is easy to check that ϕ has order p.

3 Let E be a splitting field for $f \in F[X]$ over F. Let $g \in F[X]$ be irreducible and suppose g has a root $\alpha \in E$. Show that g splits over E.

Solution

Let L be a splitting field for g over E. Then L is a splitting field for fg over f. To see this, let $F \subseteq K \subseteq L$ and suppose fg splits over K. Then clearly f splits over K, so K must contain E. Since $E \subseteq K \subseteq L$ and g splits over K, K must be L because L is a splitting field for g over E.

Next we'll show that if $\sigma \in G = \mathrm{Gal}(L/F)$ then $\sigma(E) = E$. Let $\alpha_1, \ldots, \alpha_k$ be a complete list of the roots of f (each of which is in E). Then $E = F[\alpha_1, \ldots, \alpha_k]$, and the action of σ is to simply permute these roots, and so $\sigma(E) = E$.

Now since L is a splitting field over F and $g \in F[X]$ is irreducible, the action of G on the roots of g is transitive. So every root of g can be written as $\sigma(\alpha)$ for some $\sigma \in G$. But since $\alpha \in E$, it must be that $\sigma(\alpha) \in E$, so all the roots of g are in E.

4 Let $E = F[\epsilon]$, where $\epsilon \in E$ satisfies $\epsilon^n = 1$ for some positive integer n.

a Show that E is normal over F.

Solution

By 3, it suffices to show that E is a splitting field for some polynomial over F. Let n be the smallest positive integer such that $\epsilon^n = 1$. Then $\epsilon, \epsilon^1, \ldots, \epsilon^{n-1}$ is a complete list of roots of $X^n - 1$, so E is a splitting field for $X^n - 1$ over F.

b Show that $\mathrm{Gal}(E/F)$ is abelian.

Solution

An element $\sigma \in \mathrm{Gal}(E/F)$ is determined by its value on ϵ. Also, $\sigma(\epsilon)$ must be a root of $X^n - 1$. Write σ_i for the unique element of $\mathrm{Gal}(E/F)$ which satisfies $\sigma_i(\epsilon) = \epsilon^i$. Then you can easily check that $\sigma_i \sigma_j = \sigma_{i+j} = \sigma_j \sigma_i$.