HOMEWORK 2
SOLUTIONS

Problem 1 [13.2.14] Prove that if $[F(\alpha) : F]$ is odd then $F(\alpha) = F(\alpha^2)$.

Proof. If $\alpha \notin F(\alpha^2)$ then $F(\alpha^2)$ is a proper subfield of $F(\alpha)$. Moreover α satisfies $x^2 - \alpha^2 \in F(\alpha^2)$, so $[F(\alpha) : F(\alpha^2)] = 2$. However,

$$[F(\alpha) : F] = [F(\alpha) : F(\alpha^2)][F(\alpha^2) : F] = 2 \cdot [F(\alpha^2) : F],$$

which contradicts the fact that $[F(\alpha) : F]$ is odd. Thus $\alpha \in F(\alpha^2)$, and therefore $F(\alpha) = F(\alpha^2)$. $\square$

Problem 2. Let F be a field and let $f \in F[X]$ with a splitting field E over F.

(a) Show that for any element α of some extension of F, $E(\alpha)$ is a splitting field of f over $F(\alpha)$.

(b) Show that every irreducible polynomial $g \in F[X]$ with a root in E has all roots in E.

Proof. (a) Since E is the splitting field of f over F, it is generated over F by the roots of f. Consequently, $E(\alpha)$ is generated by the roots as an extension of $F(\alpha)$, so $E(\alpha)$ is the splitting field of f over $F(\alpha)$.

(b) Assume that β is a root of g in E, and let γ be any other root of g in an algebraic closure of E. Since β and γ are roots of the same irreducible polynomial g, it follows from Theorem 8, Sec. 13.1, that $F(\beta) \cong F(\gamma)$. Since E is a splitting field of f over F, it follows (by (a)) that $E(\beta)$ is a splitting field of f over $F(\beta)$, and $F(\gamma)$ is a splitting field of f over $F(\gamma)$. Hence, by Theorem 27, Sec. 13.4, the F-isomorphism from $F(\beta)$ onto $F(\gamma)$ can be extended to an isomorphism from $E(\beta)$ onto $E(\gamma)$. By assumption, $\beta \in E$, thus $E \cong E(\beta) \cong E(\gamma)$, showing that $\gamma \in E$. $\square$

Remark. *The converse of part (b) also holds, namely: If any irreducible polynomial $g \in F[X]$ with a root in a finite extension E of F has all of its roots in E then E is a splitting field over F. Indeed, set $E = F(\alpha_1, \ldots, \alpha_n)$ and let f_i be the minimal polynomial of α_i. Since each f_i has a root in E, the hypothesis implies that each f_i splits completely in $E[X]$. Hence, it is easy to see that E is the splitting field of $f = \prod_{i=1}^n f_i$ over F.*

Problem 3 [13.4.6] Let K_1 and K_2 be finite extensions of F contained in the field K, and assume both are splitting fields over F.

(a) Prove that their composite K_1K_2 is a splitting field over F.

(b) Prove that $K_1 \cap K_2$ is a splitting field over F.

Proof. (a) Let K_1 be the splitting field of $f \in F[x]$, and K_2 the splitting field of $g \in F[x]$. Then K_1K_2 contains the roots of both f and g. Therefore K_1K_2 is the splitting field of the polynomial $h = fg$ over F.

(b) Let $g(x) \in F[x]$ be an irreducible polynomial with a root in $K_1 \cap K_2$. This means that g has a root in K_1 and also a root in K_2. Since both K_1 and K_2 are splitting fields, we can use the previous remark to conclude that g splits completely in K_1 and in K_2. Hence g splits completely in $K_1 \cap K_2$, showing that $K_1 \cap K_2$ is a splitting field over F. $\square$

Problem 4. Let α and β be two algebraic elements over a field F. Assume that the degree of the minimal polynomial of α over F is relatively prime to the degree of the minimal polynomial of β over F. Prove that the minimal polynomial of β over F is irreducible over $F(\alpha)$.

Proof. We know that $\deg m_{\alpha,F}(x) = [F(\alpha) : F]$ and $\deg m_{\beta,F}(x) = [F(\beta) : F]$. Also

$$\begin{aligned} [F(\alpha,\beta) : F] &= [F(\alpha,\beta) : F(\alpha)][F(\alpha) : F] \\ &= [F(\alpha,\beta) : F(\beta)][F(\beta) : F]. \end{aligned}$$

Since $gcd\big(\deg m_{\alpha,F}(x), \deg m_{\beta,F}(x)\big) = 1$ it follows that $[F(\beta) : F]$ divides $[F(\alpha,\beta) : F(\alpha)]$. Equivalently, the degree of the minimal polynomial of β over $F(\alpha)$ is divisible by the degree of the minimal polynomial of β over F. Considering that the former polynomial divides the latter polynomial (by Proposition 9, Sec 13.2) we infer that the two polynomials are in fact equal. In other words, $m_{\beta,F}(x)$ remains irreducible over $F(\alpha)$, as desired.

$\square$

Problem 5. Let E and K be finite field extensions of F such that $[EK : F] = [E : F][K : F]$. Show that $K \cap E = F$.

Solution 1. Let $L = K \cap E$, then

$$\begin{aligned} [EK : F] = [E : F][K : F] &= [E : L][L : F][K : L][L : F] \\ &= [E : L][K : L][L : F]^2 \\ &\geq [EK : L][L : F]^2 \text{ by Proposition 21, Sec 13.2} \\ &= [EK : F][L : F]. \end{aligned}$$

In conclusion $[L : F] = 1$ and hence $L = F$, as desired.

$\square$

Solution 2. Let $\alpha_1, \ldots, \alpha_n$ be an F-basis for E and let $\beta_1, \ldots, \beta_m$ be an F-basis for K. By the proof of Proposition 21, Sec. 13.2, we conclude that the equality $[EK : F] = [E : F][K : F]$ implies that the set $\mathcal{B} = \{\alpha_i\beta_j\}$ is a basis for EK over F. Clearly we can choose the above bases such that $\alpha_1 = \beta_1 = 1 \in F$. Then $\mathcal{S} := \{1, \alpha_2, \ldots, \alpha_n, \beta_2, \ldots, \beta_m\} \subset \mathcal{B}$ so the elements of this set are linearly independent over F.

Now if $\gamma \in E \cap K$ then we can write $\gamma = \sum_{i=1}^n a_i\alpha_i = \sum_{j=1}^m b_j\beta_j$ for $a_i, b_j \in F$. It yields that $0 = (a_1 - b_1) \cdot 1 + \sum_{i=2}^n a_i\alpha_i - \sum_{j=2}^m b_j\beta_j$. By the above, the elements of $\mathcal{S}$ are linearly independent over F. Therefore $a_1 = b_1$ and $a_i = b_j = 0$ for $i, j \geq 2$. Consequently $\gamma = a_1 = b_1 \in F$ implying that $E \cap K \subseteq F$ and thus $E \cap K = F$.

$\square$