Problem Set 9 solutions

Problem 1. Let $K \subseteq L$ be a finite extension of fields and assume $f(x)$ is a polynomial with coefficients in K that is irreducible in the ring $K[x]$.

a) Prove $f(x)$ remains irreducible when regarded as an element of the ring $L[x]$ provided $[L : K]$ is relatively prime to the degree of $f(x)$.

Proof. Let $\overline{F}$ be an algebraic closure of F and let $L = K(\alpha)$ where α is a root of $f(x)$ in L. Then $[L : F] = [L : K][K : F] = [L : K] \cdot n = e \cdot n$, where e is the degree of $m_{\alpha,K}(x)$. We also have $[L : F] = [L : F(\alpha)][F(\alpha) : F] = [L : F(\alpha)] \cdot d$. Since $\gcd(d, n) = 1$, it follows that $d \mid e$. But since α is a root of $f(x)$, $m_{\alpha,K}$ must divide $f(x)$ in $K[x]$. Since they have the same degree, it must be that $m_{\alpha,K}(x) = cf(x)$ for some nonzero constant c. Since $m_{\alpha,K}(x)$ is irreducible in $K[x]$, then $f(x)$ is irreducible in $K[x]$. □

b) Give an explicit example with justification showing that the statement in part a) would become false if we ommitted the assumption that $[L : K]$ is relatively prime to the degree of $f(x)$.

Proof. Take $F = \mathbb{R}$, $K = \mathbb{C}$ and $f(x) = x^2 + 1$. The polynomial f is irreducible over $\mathbb{R}$, since it has no roots over $\mathbb{R}$ and it has degree 2, while f factors as $f = (x + i)(x - i)$ over $\mathbb{C}$. On the other hand, $[\mathbb{C} : \mathbb{R}] = 2 < \infty$. □

Problem 2. Let p be a prime integer and let $F = \mathbb{Q}(i)$. Use the theory of field extensions to show that the polynomial $x^3 - p$ is irreducible in $F[x]$.

Proof. Let $q(x) = x^3 - p \in \mathbb{Q}[x] \subseteq F[x]$. Note that q is also a polynomial in $\mathbb{Z}[x]$. Since p is a prime integer, Eisenstein's Criterion applies to q with the prime ideal (p): p divides all the coefficients of q of degree up to 2, p does not divide the coefficient of degree 3, and $p^2 \nmid -p$. Therefore, q is irreducible over $\mathbb{Z}$, and thus by Gauss' Criterion we conclude that q is irreducible over $\mathbb{Q}$.

On the other hand, $i \notin \mathbb{Q}$, since i is not even a real number. Thus the polynomial $x^2 + 1$, which has degree 2 and roots i and $-i$ over $\mathbb{C}$, must be irreducible over $\mathbb{Q}$. We conclude that $x^2 + 1$ is the minimal polynomial of i over $\mathbb{Q}$, so $[\mathbb{Q}(i) : \mathbb{Q}] = 2$.

Since $(2, 3) = 1$, by Problem 1 we conclude that q is irreducible over $\mathbb{Q}(i)$. □

Problem 3. Let E be the field extension of $\mathbb{Q}$ obtained by adjoining to $\mathbb{Q}$ all four complex roots of the polynomial $x^4 + 5$. That is, $E = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ where

$$\alpha_1 = e^{\pi i/4}\sqrt[4]{5}, \quad \alpha_2 = e^{3\pi i/4}\sqrt[4]{5}, \quad \alpha_3 = e^{5\pi i/4}\sqrt[4]{5}, \quad \alpha_4 = e^{7\pi i/4}\sqrt[4]{5}.$$

a) Prove that there exist a field extension $\mathbb{Q} \subseteq F$ such that $F \subseteq E$, $F \subseteq \mathbb{R}$, and $[F : \mathbb{Q}] = 4$.

Hint: Note that $\alpha_1 + \alpha_4$ is a real number; find it explicitly.

Proof. Note that

$$\alpha_1 = \sqrt[4]{5} \cdot \frac{\sqrt{2}}{2}(1 + i) = \frac{\sqrt[4]{20}}{2}(1 + i) \quad \text{and} \quad \alpha_4 = \frac{\sqrt[4]{20}}{2}(1 - i)$$

so $\alpha_1 + \alpha_4 = \sqrt[4]{20}$.

Moreover, $\alpha_1 + \alpha_4$ is thus a root of $x^4 - 20$, which is irreducible: using Gauss' Lemma, we just need to show it is irreducible over $\mathbb{Z}$, and Eisenstein's Criterion applies with $p = 5$ to show that $x^4 - 20$ is irreducible over $\mathbb{Z}$. Hence, $m_{\alpha_1+\alpha_2,\mathbb{Q}}(x) = x^4 - 20$. Set $F = \mathbb{Q}(\alpha_1 + \alpha_4)$. Then $F \subseteq E$ and $[F : \mathbb{Q}] = 4$, as desired. Moreover, $F \subseteq \mathbb{R}$ since $\alpha_1 + \alpha_4 \in \mathbb{R}$ and $\mathbb{Q} \subseteq \mathbb{R}$. □

b) Determine $[E : \mathbb{Q}]$ with justification.

Proof. By the Degree Formula, $[E : \mathbb{Q}] = [E : F][F : \mathbb{Q}] = [E : F] \cdot 4$. We claim that $E = F(i)$. First note that $\frac{\alpha_1}{\alpha_4} = \frac{1+i}{1-i} = i$ so that $i \in E$ and hence $F(i) \subseteq E$.

Since each α_j has the form $\frac{\sqrt[4]{20}}{2}(\pm 1 \pm i)$ and both $\sqrt[4]{20}$ and i belong to $F(i)$, we have $\alpha_j \in F(i)$ for all j and thus $E \subseteq F(i)$. We conclude that $E = F(i)$.

Since i is a root of $x^2 + 1 \in F[x]$ we have $[F(i) : F] \leqslant 2$. Since $F \subseteq \mathbb{R}$, we have $F \neq F(i)$ and thus $[E : F] = 2$. By the Degree Formula, $[E : \mathbb{Q}] = [E : F][F : \mathbb{Q}] = 2 \cdot 4 = 8$. □

Problem 4. Let

$$F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots$$

be fields such that $F_i \subseteq F_{i+1}$ is an algebraic extension for all $i \geqslant 0$, and let

$$E = \bigcup_i F_i.$$

a) Show that E is a field.

b) Show that $F_0 \subseteq E$ is an algebraic extension.

Problem 5. Let F be a field and $f, g \in F[x]$ be nonzero polynomials. Show that $\gcd(f, g) = 1$ in $F[x]$ if any only if f and g have no common roots in an algebraic closure $\overline{F}$ of F.

Proof. We prove the contrapositive: 1 is not a gcd for f and g in $F[x]$ if any only if f and g have a common root in an algebraic closure $\overline{F}$ of F.

($\Rightarrow$) If 1 is not a gcd for f and g in $F[x]$, then $\gcd(f, g) = h \in F[x]$ for some polynomial h with $\deg(h) \geqslant 1$. Then since h is nonconstant polynomial, we know h has a root $\alpha \in \overline{F}$. Since $h \mid f$ and $h \mid g$, it follows that α is also a root for both f and g.

($\Leftarrow$) Suppose that f and g have a common root $\alpha \in \overline{F}$, that is $f(\alpha) = g(\alpha) = 0$. Then α is algebraic over F and hence it has a minimal polynomial $m_{\alpha,F} \in F[x]$. Furthermore, by properties of the minimal polynomial it follows that since $f(\alpha) = 0$ then $m_{\alpha,F} \mid f$ and since $g(\alpha) = 0$ then $m_{\alpha,F} \mid g$. Thus $m_{\alpha,F}$ is a common divisor for f, g in $F[x]$ and therefore by properties of the gcd $m_{\alpha,F} \mid \gcd(f, g)$. This shows that, since $\deg(m_{\alpha,F}) \geqslant 1$, $\deg(\gcd(f, g)) \neq 0$, therefore no unit of F can be a gcd for f, g in $F[x]$. □