Algebra II: Tutorial 5

March 16, 2022

Problem 1. Suppose that p and q are distinct primes. Show that $\mathbb{Q}(\sqrt{p}, \sqrt{q}) = \mathbb{Q}(\sqrt{p} + \sqrt{q})$.

Solution. The inclusion $\mathbb{Q}(\sqrt{p} + \sqrt{q}) \subset \mathbb{Q}(\sqrt{p}, \sqrt{q})$ is clear. It remains to show that $\sqrt{p}$ and $\sqrt{q}$ lie in $\mathbb{Q}(\sqrt{p}+\sqrt{q})$. This will follow once we show that $\sqrt{p}-\sqrt{q}$ lies in $\mathbb{Q}(\sqrt{p}+\sqrt{q})$. Since p and q are distinct primes, $\sqrt{p} - \sqrt{q}$ is non-zero, and $(\sqrt{p} + \sqrt{q})(\sqrt{p} - \sqrt{q}) = p - q$. Then, $\sqrt{p} - \sqrt{q} = \frac{p-q}{\sqrt{p}+\sqrt{q}}$, where the right-hand side is in $\mathbb{Q}(\sqrt{p} + \sqrt{q})$ (since $\mathbb{Q}(\sqrt{p} + \sqrt{q})$ is a field). ■

Problem 2. Let L be a finite field extension of K, and consider $\alpha, \beta \in L$. If α and β have the same minimal polynomial in $K[x]$, then $K(\alpha)$ and $K(\beta)$ are isomorphic. Is the converse true?

Solution. The converse is not true. Take $\alpha = \sqrt{2}$, $\beta = \sqrt{2} + 1$. The element α is algebraic over $\mathbb{Q}$ since $m_1(x) = x^2 - 2$ has root α. Furthermore, this polynomial is monic irreducible over $\mathbb{Q}$, so $m_1(x)$ is the minimal polynomial of α. Note that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$, and $\mathbb{Q}(\alpha) = \mathbb{Q}[\alpha] = \{a + \sqrt{2}b \mid a, b \in \mathbb{Q}\}$. Similarly, the element β is algebraic over $\mathbb{Q}$ since $m_2(x) = x^2 - 2x - 1$ has root β. This polynomial is monic irreducible over $\mathbb{Q}$, so $m_2(x)$ is the minimal polynomial of β. Note that $[\mathbb{Q}(\beta) : \mathbb{Q}] = 2$, and $\mathbb{Q}(\beta) = \mathbb{Q}[\beta] = \{c+(\sqrt{2}+1)d \mid c, d \in \mathbb{Q}\}$. It is obvious that $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ are isomorphic, yet $m_1(x) \neq m_2(x)$. ■

Problem 3. Let L be a field generated over $K \subset L$ by two elements α, β. Let $p = [K(\alpha) \colon K]$ and $q = [K(\beta) \colon K]$ and assume that p and q are relatively prime.

1. Prove that $[L \colon K] = pq$.
2. If α is a fifth root of 2 and β a seventh root of 3, deduce that $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = 35$.

Solution. 1. Note that $K(\alpha, \beta)$ contains $K(\alpha)$ and $K(\beta)$ as subfields. By the tower theorem, $[K(\alpha, \beta) : K]$ is divisible by both $p = [K(\alpha) : K]$ and $q = [K(\beta) : K]$; hence divisible by their lowest common multiple $lcm(p, q)$. Since p and q are coprime, $lcm(p, q) = pq$, i.e. $[K(\alpha, \beta) : K]$ is divisible by pq; in particular $[K(\alpha, \beta) : K] \geq pq$. It remains to show that $[K(\alpha, \beta) : K] \leq pq$. To do so, we claim that $[K(\alpha, \beta) : K(\beta)] \leq [K(\alpha) : K]$.

Indeed, any monic polynomial with root α over K is a monic polynomial with root α over $K(\beta)$, so the degree of the minimal polynomial of α over $K(\beta)$ is smaller than or equal to that over K, implying that $[K(\alpha,\beta) : K(\beta)] \leq [K(\alpha) : K]$. By the tower theorem, $[K(\alpha,\beta) : K] = [K(\alpha,\beta) : K(\beta)][K(\beta) : K] \leq [K(\alpha) : K][K(\beta) : K]$, and we are done.
2. Since α is a root of the irreducible polynomial $x^5 - 2$ and β is a root of the irreducible polynomial $x^7 - 3$, one has $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$ and $[\mathbb{Q}(\beta) : \mathbb{Q}] = 7$. Since 5 and 7 are coprime, the result follows from part 1.

■

Problem 4. Let L/K be a field extension and let $f(x), g(x) \in K[x]$. Show that the greatest common divisor (with leading coefficient 1) of $f(x)$ and $g(x)$ in $L[x]$ is the same as the greatest common divisor of $f(x)$ and $g(x)$ in $K[x]$.

Solution. Let $p(x)$ denote the gcd of $f(x)$ and $g(x)$ in $K[x]$, and $q(x)$ the gcd of $f(x)$ and $g(x)$ in $L[x]$. It is clear that $\deg(q(x)) \geq \deg(p(x))$. On the other hand, $q(x)$ divides $f(x)$ and $g(x)$ in $L[x]$. By Bézout's identity, $q(x)$ must also divide $p(x)$ in $L[x]$. This implies that $\deg(q(x)) \leq \deg(p(x))$, and so $p(x)$ and $q(x)$ have same degree. Since they are both monic, this implies $p(x) = q(x)$, which proves our claim. ■