Math 535
Solutions to Midterm 1

Thursday, March 7, 2024

1. Let r_1, r_2, r_3, r_4 be the four roots of a quartic polynomial with rational coefficients. Suppose that $r_1+r_2 \in \mathbb{Q}$ and that $r_1+r_2 \neq r_3+r_4$. Prove that $r_1 r_2 \in \mathbb{Q}$.

   Solution: Let $E = \mathbb{Q}(r_1, r_2, r_3, r_4)$ be the splitting field of the polynomial. This is a Galois extension, and we let $G = \mathrm{Gal}(E/\mathbb{Q})$ be the Galois group. Since $E^G = \mathbb{Q}$, it is enough to show that $g(r_1 r_2) = r_1 r_2$ for every $g \in G$. Take any $g \in G$. We observe that if $g(r_1) = r_1$, then also $g(r_2) = r_2$ (and vice versa), because

   $$g(r_1) + g(r_2) = g(r_1 + r_2) = r_1 + r_2,$$

   due to the fact that $r_1 + r_2 \in \mathbb{Q}$. Moreover, there is no $g \in G$ with $g(r_1) = r_3$ (or r_4): indeed, if $g(r_1) = r_3$, then necessarily $g(r_2) = r_4$, and therefore

   $$r_1 + r_2 = g(r_1 + r_2) = g(r_1) + g(r_2) = r_3 + r_4,$$

   contradicting the information we have about the roots. So we either have $g(r_1) = r_1$ and $g(r_2) = r_2$; or $g(r_1) = r_2$ and $g(r_2) = r_1$. In both cases, $g(r_1 r_2) = r_1 r_2$, and therefore $r_1 r_2 \in \mathbb{Q}$.

   Alternatively, one can prove this without Galois theory as follows. The coefficients of the quartic are in $\mathbb{Q}$, and this gives

   $$\begin{aligned} r_1 + r_2 + r_3 + r_4 &\in \mathbb{Q} \\ r_1 r_2 + r_1 r_3 + r_1 r_4 + r_2 r_3 + r_2 r_4 + r_3 r_4 &\in \mathbb{Q} \\ r_1 r_2 r_3 + r_1 r_2 r_4 + r_1 r_3 r_4 + r_2 r_3 r_4 &\in \mathbb{Q} \\ r_1 r_2 r_3 r_4 &\in \mathbb{Q}. \end{aligned}$$

   From $r_1 + r_2 \in \mathbb{Q}$ and the first line, we deduce that $r_3 + r_4 \in \mathbb{Q}$. Therefore $r_1 r_3 + r_1 r_4 + r_2 r_3 + r_2 r_4 = (r_1 + r_2)(r_3 + r_4) \in \mathbb{Q}$. After subtracting this from the second line, we obtain $r_1 r_2 + r_3 r_4 \in \mathbb{Q}$. Now rewrite the third line as

   $$r_1 r_2 \big((r_3 + r_4) - (r_1 + r_2)\big) + (r_1 r_2 + r_3 r_4)(r_1 + r_2) \in \mathbb{Q}.$$

   Since $(r_3+r_4)-(r_1+r_2) \neq 0$, we can divide and conclude that $r_1 r_2 \in \mathbb{Q}$.

2. Let $f(x) \in k[x]$ be an irreducible polynomial of degree n. Let $k \subseteq E$ be a field extension such that $(E : k)$ is relatively prime to n. Show that $f(x)$ remains irreducible in $E[x]$.

   Solution: We argue by contradiction. Suppose that $g(x) \in E[x]$ is an irreducible polynomial of degree $1 \leq d \leq n-1$ such that $g(x) \mid f(x)$. Let $E \subseteq F$ be a field extension in which $g(x)$ has a root $\alpha \in F$. Being irreducible, $g(x)$ is the minimal polynomial of α over E, and so

   $$\big(E(\alpha) : E\big) = d.$$

   We also have $f(\alpha) = 0$, and for the same reason, $f(x)$ must be the minimal polynomial of α over k, and $\big(k(\alpha) : k\big) = n$. Since the degree is multiplicative in field extensions, we get

   $$d \cdot (E : k) = \big(E(\alpha) : k\big) = \big(E(\alpha) : k(\alpha)\big) \cdot \big(k(\alpha) : k\big).$$

   This is a contradiction because the right-hand side is divisible by n, but the left-hand side is not.

3. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial with splitting field E. Suppose that $\mathrm{Gal}(E/\mathbb{Q})$ is abelian. Show that $E = \mathbb{Q}(\alpha)$, where $\alpha \in E$ is an arbitrary root of $f(x)$.

   Solution: Let $\alpha \in E$ be any root of the polynomial $f(x)$. By the Galois correspondence, the subfield $\mathbb{Q}(\alpha)$ is the fixed field of a subgroup $H \subseteq \mathrm{Gal}(E/\mathbb{Q})$. Because the Galois group is abelian, H is a normal subgroup, and therefore $\mathbb{Q}(\alpha) = E^H$ is itself a Galois extension of $\mathbb{Q}$. In particular, it is normal, and therefore contains all the roots of $f(x)$. This gives $E = \mathbb{Q}(\alpha)$, as desired.

4. Consider the real number $\alpha = 2\cos(2\pi/7)$. Determine the minimal polynomial of α over $\mathbb{Q}$.

   Solution: Let $\zeta = e^{2\pi i/7} \in \mathbb{C}$ be a primitive 7-th root of unity. Then

   $$\zeta = \cos(2\pi/7) + i\sin(2\pi/7)$$

   and therefore $\alpha = \zeta + \zeta^{-1} = \zeta + \zeta^6$. We know from class that $\mathbb{Q}(\zeta)$ is a Galois extension of degree $\varphi(7) = 6$ over $\mathbb{Q}$. Consider the extensions

   $$\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\zeta).$$

From $\alpha = \zeta + \zeta^{-1}$, we get $\zeta^2 - \alpha\zeta + 1 = 0$; also, $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$, but ζ is obviously not real. It follows that $\big(\mathbb{Q}(\zeta) : \mathbb{Q}(\alpha)\big) = 2$; consequently,

$$\big(\mathbb{Q}(\alpha) : \mathbb{Q}\big) = \frac{\big(\mathbb{Q}(\zeta) : \mathbb{Q}\big)}{\big(\mathbb{Q}(\zeta) : \mathbb{Q}(\alpha)\big)} = \frac{6}{2} = 3.$$

The minimal polynomial of α must therefore be a cubic polynomial. Recall that the minimal polynomial of ζ is

$$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1.$$

To find the cubic equation satisfied by α, we compute

$$\begin{aligned}
\alpha &= \zeta + \zeta^{-1} = \zeta^6 + \zeta \\
\alpha^2 &= (\zeta + \zeta^{-1})^2 = \zeta^2 + 2 + \zeta^{-2} = \zeta^5 + \zeta^2 + 2 \\
\alpha^3 &= (\zeta + \zeta^{-1})^3 = \zeta^3 + 3\zeta + 3\zeta^{-1} + \zeta^{-3} = 3\zeta^6 + \zeta^4 + \zeta^3 + 3\zeta.
\end{aligned}$$

Taking a suitable linear combination, we get

$$\alpha^3 + \alpha^2 - 2\alpha - 1 = \zeta^6 + \zeta^5 + \cdots + 1 = 0.$$

Therefore the minimal polynomial is $f(x) = x^3 + x^2 - 2x - 1$.