

Tutorial 10

1. Let $F(\alpha, \beta) : F$ be a field extension where α and β are algebraic over F . Suppose $[F(\alpha) : F] = m$ and $[F(\beta) : F] = n$ are relatively prime.
 - (i) Show $[F(\alpha, \beta) : F] = mn$.
 - (ii) Determine $[F(\alpha, \beta) : F(\alpha)]$ and $[F(\alpha, \beta) : F(\beta)]$.
 - (iii) Deduce that the minimal polynomial of α with respect to F is irreducible over $F(\beta)$, and, by symmetry, the minimal polynomial of β with respect to F is irreducible over $F(\alpha)$.

2. Let p be a prime, and $a(x) = 1 + x + x^2 + \dots + x^{p-1} \in \mathbb{Q}[x]$; it was shown in lectures that $a(x)$ is irreducible. Let $\omega = e^{2\pi i/p} \in \mathbb{C}$, and let k be any positive integer less than p .
 - (iv). Show that ω and ω^k are both roots of $a(x)$.
 - (v) Show that $\omega \in \mathbb{Q}(\omega^k)$, and deduce that $\mathbb{Q}(\omega^k) = \mathbb{Q}(\omega)$.
 - (vi) Let $E = \mathbb{Q}(\omega) = \mathbb{Q}(\omega^k)$. Use the First Isomorphism Theorem to find two different isomorphisms $\mathbb{Q}[x]/a(x)\mathbb{Q}[x] \rightarrow E$, and hence show that there is an isomorphism $\psi: E \rightarrow E$ such that $\psi(\omega) = \omega^k$.

2. Let $E = \mathbb{Q}(\omega)$, where $\omega \neq 1$ is a complex 7th root of 1.
 - (i) Show that there is a unique isomorphism $f: \mathbb{Q}(\omega) \rightarrow \mathbb{Q}(\omega)$ with the property that $f\omega = \omega^3$, and determine what f does to a general element of E .
 - (ii) Let $g: \mathbb{Q}(\omega) \rightarrow \mathbb{Q}(\omega)$ be an arbitrary isomorphism. Show that $g\omega$ is necessarily a root of the polynomial $a(x) = \sum_{i=0}^6 x^i$, and deduce that $g\omega = \omega^k$ for some $k \in \mathbb{Z}$.
 - (iii) Show that the identity, f , f^2 , f^3 , f^4 and f^5 are the only isomorphisms from E to E .
 - (iv) Show that $f^3 a$ is the complex conjugate of a (for all $a \in E$.)

3. Let E and ω be as in Exercise 3, and let $\alpha = \omega + \omega^6$. Determine all elements β of E such that $\beta = g\alpha$ for some isomorphism $g: E \rightarrow E$, and find a (cubic) polynomial $p(x) \in \mathbb{Q}[x]$ of which all these elements are roots. (Optional extra: use the method for solving cubics described on pages 1, 2 and 3 of the notes, or any other method for solving cubics, to find expressions, not involving ω , for the roots of this polynomial.)