

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 $F(\alpha)$.

Solution.

(i) We have

$$[F(\alpha, \beta : F)] = [F(\alpha, \beta) : F(\alpha)][F(\alpha) : F], \quad (1)$$

Hence $m = [F(\alpha) : F]$ divides $[F(\alpha, \beta) : F]$. Similarly n divides $[F(\alpha, \beta) : F]$. Since m and n are relatively prime mn must divide $[F(\alpha, \beta) : F]$. Let $p(x) = m_{\alpha, F}$ be the minimum polynomial of α over F . Then $\deg p(x) = m$. The minimal polynomial of α over $F(\beta)$ is a divisor of $p(x)$. Recall the reason: The minimal of α with respect to $F(\alpha)$ divides every $f(x)$ with coefficients in $F(\alpha)$, and $p(x)$ is such a polynomial. Hence the degree $[F(\alpha, \beta) : F(\beta)]$ of the minimal polynomial of α over $F(\beta)$ is less than or equal to m . This gives

$$[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\beta)][F(\beta) : F] \leq mn. \quad (2)$$

Since the left-hand side is divisible by mn from above, $[F(\alpha, \beta) : F] = mn$.

(ii) Putting $[F(\alpha, \beta) : F] = mn$, $[F(\alpha) : F] = m$ in (1) gives $[F(\alpha, \beta) : F(\alpha)] = n$. By symmetry, $[F(\alpha, \beta) : F(\beta)] = m$.

(iii) From $[F(\alpha, \beta) : F(\beta)] = m$ we deduce $m_{\alpha, F(\beta)}$ has degree m . From above it is a divisor of $p(x)$ the minimal polynomial α over F , which is of degree m too. Hence $m_{\alpha, F(\beta)} = p(x)$. Since minimum polynomials over a field are irreducible over the field we deduce $p(x)$ is irreducible over $F(\beta)$. By symmetry, $m_{\beta, F(\alpha)} = m_{\beta, F}$.

- 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 $\psi(\omega) = \omega^k$.

Solution.

(i) Note that $\omega^k \neq 1$, since $0 < k < p$. By the formula for summing a geometric series, $a(\omega^k) = \sum_{i=0}^{p-1} (\omega^k)^i = \frac{\omega^{kp} - 1}{\omega^k - 1} = \frac{(\omega^p)^k - 1}{\omega^k - 1} = 0$, as $\omega^p = 1$. Hence ω^k is a root of $a(x)$. This calculation applies when $k = 1$; so, in particular, $a(\omega) = 0$.

(ii) Since p is prime, $\gcd(k, p) = 1$. Hence there exist integers r and s with $kr + ps = 1$, and it follows that $\omega = \omega^{kr+ps} = (\omega^k)^r (\omega^p)^s = (\omega^k)^r \in \mathbb{Q}[\omega^k]$. Hence $\mathbb{Q}[\omega] \subseteq \mathbb{Q}[\omega^k]$, and since obviously $\omega^k \in \mathbb{Q}[\omega]$ the reverse inclusion also holds. (Note that $\mathbb{Q}(\omega) = \mathbb{Q}[\omega]$ since ω is algebraic over \mathbb{Q} .)

(iii) Define $\theta: \mathbb{Q}[x] \rightarrow \mathbb{C}$ by $\theta(f(x)) = f(\omega)$ for all $f(x) \in \mathbb{Q}[x]$. From lectures we know that such ‘‘evaluation’’ maps are homomorphisms. Now $\ker \theta = p(x)\mathbb{Q}[x]$, where $p(x)$ is the minimal polynomial of ω over \mathbb{Q} , and since $\theta(a(x)) = a(\omega) = 0$ we see that $a(x) \in \ker \theta$; hence $p(x)|a(x)$. But $a(x)$ is irreducible, and so it follows that $a(x)$ and $p(x)$ are associates. Thus $\ker \theta = a(x)\mathbb{Q}[x]$. Now since $\text{im } \theta = \mathbb{Q}[\omega]$ the First Isomorphism Theorem yields an isomorphism $\bar{\theta}: \mathbb{Q}[x]/a(x)\mathbb{Q}[x] \rightarrow \mathbb{Q}[\omega]$ such that $\bar{\theta}(f(x) + a(x)\mathbb{Q}[x]) = f(\omega)$ for all $f(x) \in \mathbb{Q}[x]$.

Using the evaluation map φ given by $\varphi(f(x)) = f(\omega^k)$ and applying the same arguments as for θ yields an isomorphism $\bar{\varphi}: \mathbb{Q}[x]/a(x)\mathbb{Q}[x] \rightarrow \mathbb{Q}[\omega^k] = \mathbb{Q}[\omega]$ such that $\bar{\varphi}(f(x) + a(x)\mathbb{Q}[x]) = f(\omega^k)$ for all $f(x) \in \mathbb{Q}[x]$. Now $\psi = \bar{\varphi}(\bar{\theta})^{-1}$ is an isomorphism $\mathbb{Q}[\omega] \rightarrow \mathbb{Q}[\omega^k]$ which satisfies $\psi(f(\omega)) = f(\omega^k)$ for all $f(x) \in \mathbb{Q}[x]$. In particular, $\psi(\omega) = \omega^k$.

The above proof avoids using the Isomorphism Extension Theorem, by essentially just repeating the steps used in the proof of the theorem. Using the theorem gives a shorter proof, as follows: The identity isomorphism $\mathbb{Q} \rightarrow \mathbb{Q}$ takes the irreducible polynomial $a(x)$, of which ω is a root, to $a(x)$, of which ω^k is a root; so the Isomorphism Extension Theorem guarantees that the identity isomorphism $\mathbb{Q} \rightarrow \mathbb{Q}$ extends to an isomorphism $\mathbb{Q}[\omega] \rightarrow \mathbb{Q}[\omega^k]$ taking ω to ω^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 $a \in E$.)

Solution.

(i) By Exercise 2 there exists an isomorphism $f: \mathbb{Q}(\omega) \rightarrow \mathbb{Q}(\omega)$ with $f\omega = \omega^3$. By Question 3 of Tutorial 3 we know that a nonzero homomorphism of integral

domains must take the identity element to the identity element. So f takes 1 to 1, and an easy induction shows that $fn = n$ for all positive integers n . So $f(nm^{-1}) = (fn)(fm)^{-1} = nm^{-1}$ for all positive integers n, m . Thus $f q = q$ for all positive $q \in \mathbb{Q}$, and as $f(-q) = -(fq)$ it follows that f fixes all negative elements of \mathbb{Q} as well. Now as the minimal polynomial of ω over \mathbb{Q} is $a(x) = \sum_{j=0}^5 x^j$, which has degree 6, we know that $[\mathbb{Q}(\omega) : \mathbb{Q}] = 6$ and that every element of $\mathbb{Q}(\omega)$ is expressible in the form $\sum_{j=0}^5 q_j \omega^j$ with coefficients $q_j \in \mathbb{Q}$. Given that $f\omega = \omega^3$ we deduce that $f(\sum_{j=0}^5 q_j \omega^j) = \sum_{j=0}^5 (fq_j)(f\omega)^j = \sum_{j=0}^5 q_j (\omega^3)^j$. Thus we have determined a formula for the effect of f on an arbitrary element of $\mathbb{Q}(\omega)$, using only the information that $f\omega = \omega^3$.

(ii) Now let $g: \mathbb{Q}(\omega) \rightarrow \mathbb{Q}(\omega)$ be an arbitrary isomorphism. Since $g1 = 1$ and $g0 = 0$ we have $0 = g(\sum_{j=0}^5 \omega^j) = \sum_{j=0}^5 (g\omega)^j$, which shows that $g\omega$ is a root of $a(x)$. The roots of $a(x)$ are also roots of $x^7 - 1 = (x - 1)a(x)$, and thus $g\omega = e^{2\pi ik/7} = \omega^k$ for some $k \in \mathbb{Z}$.

(iii) The same arguments as used for f in Part (i) above show that once $g\omega$ is specified the isomorphism g is completely determined. Specifically, if $g\omega = \omega^k$ then $g(\sum_{j=0}^5 q_j \omega^j) = \sum_{j=0}^5 q_j (\omega^k)^j$ for all $q_j \in \mathbb{Q}$. There are six possible values for $g\omega$: namely, the six roots of $a(x)$. These are ω^k for $k \in \{1, 2, 3, 4, 5, 6\}$. Now the identity automorphism obviously satisfies $g\omega = \omega$, which accounts for the case $k = 1$, and f accounts for $k = 3$. We find, successively, that

$$\begin{aligned} f^2\omega &= f(f\omega) = f(\omega^3) = (f\omega)^3 = (\omega^3)^3 = \omega^9 = \omega^2 \\ f^3\omega &= f(f^2\omega) = f(\omega^2) = (f\omega)^2 = (\omega^3)^2 = \omega^6 \\ f^4\omega &= f(f^3\omega) = f(\omega^6) = (f\omega)^6 = (\omega^3)^6 = \omega^{18} = \omega^4 \\ f^5\omega &= f(f^4\omega) = f(\omega^4) = (f\omega)^4 = (\omega^3)^4 = \omega^{12} = \omega^5, \end{aligned}$$

and this accounts for all the other possibilities.

(iv) Recall that if a complex number $a+bi$ lies on the unit circle, so that $a^2+b^2 = 1$, then its conjugate $a-bi$ equals $\frac{1}{a+bi}$. So $\omega^6 = \omega^{-1} = \bar{\omega}$, and thus for an arbitrary $a = \sum_{j=0}^5 q_j \omega^j \in E$ we have

$$f^3 a = f^3 \left(\sum_{j=0}^5 q_j \omega^j \right) = \sum_{j=0}^5 q_j (\bar{\omega})^j = \overline{\sum_{j=0}^5 q_j \omega^j} = \bar{a},$$

as claimed.

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.)

Solution.

Observe that $\omega + \omega^6 = \omega + f^3\omega$, and so

$$\begin{aligned} f(\omega + \omega^6) &= f\omega + f(f^3\omega) = f\omega + f^4\omega = \omega^3 + \omega^4 \\ f^2(\omega + \omega^6) &= f^2\omega + f^2(f^3\omega) = f^2\omega + f^5\omega = \omega^2 + \omega^5. \end{aligned}$$

Furthermore, $f^3(\omega + \omega^6) = f(\omega^2 + \omega^5) = (\omega^3)^2 + (\omega^3)^5 = \omega^6 + \omega$, and so $f^4(\omega + \omega^6)$ and $f^5(\omega + \omega^6)$ will equal (respectively) $f(\omega + \omega^6)$ and $f^2(\omega + \omega^6)$. So the six possibilities for the isomorphism g yield three possibilities (occurring twice each) for $g(\omega + \omega^6)$, namely, $\omega + \omega^6$, $\omega^3 + \omega^4$ and $\omega^2 + \omega^5$. (Note that these are all real, since ω^6 , ω^4 and ω^5 are the complex conjugates of ω , ω^3 and ω^2 . Indeed, the three real numbers we get are $2 \cos(2\pi k/7)$, for $k \in \{1, 3, 2\}$.)

The cubic with these three roots is $(x - (\omega + \omega^6))(x - (\omega^3 + \omega^4))(x - (\omega^2 + \omega^5))$. To find the coefficients of this polynomial, observe that

$$\begin{aligned} (\omega + \omega^6)(\omega^3 + \omega^4)(\omega^2 + \omega^5) &= \omega^6 + \omega^9 + \omega^7 + \omega^{10} + \omega^{11} + \omega^{14} + \omega^{12} + \omega^{15} \\ &= 2 + \sum_{j=1}^6 \omega^j = 1 \end{aligned}$$

and

$$\begin{aligned} (\omega + \omega^6)(\omega^3 + \omega^4) + (\omega + \omega^6)(\omega^2 + \omega^5) + (\omega^3 + \omega^4)(\omega^2 + \omega^5) \\ &= (\omega^4 + \omega^5 + \omega^9 + \omega^{10}) + (\omega^3 + \omega^6 + \omega^8 + \omega^{11}) + (\omega^5 + \omega^{10} + \omega^6 + \omega^9) \\ &= 2 \sum_{j=1}^6 \omega^j = -2, \end{aligned}$$

while

$$(\omega + \omega^6) + (\omega^3 + \omega^4) + (\omega^2 + \omega^5) = -1.$$

Thus the polynomial $p(x)$ is $x^3 + x^2 - 2x - 1$.

In the notation of pp.1,2,3 of the notes, we have $S_1 = -1$, $S_2 = -2$ and $S_3 = 1$, so that $A = 2S_1^3 - 9S_1S_2 + 27S_3 = 7$ and $B = (S_1^2 - 3S_2)^3 = 7^3$, giving

$$\theta = \sqrt[3]{\frac{7}{2} + \frac{1}{2}\sqrt{7^2 - 4 \times 7^3}} = \sqrt[3]{\frac{7}{2}(7 + 7\sqrt{-27})} = \sqrt[3]{\frac{7}{2}(1 + 3\sqrt{-3})}$$

and therefore

$$\psi = (S_1^2 - 3S_2)\theta^{-1} = 7\theta^{-1}.$$

Note that $\sqrt[3]{\frac{7}{2}(1 + 3\sqrt{-3})}$ is a six-valued expression, though all the values have the same modulus, which is $\sqrt[3]{\frac{7}{2}\sqrt{28}} = \sqrt{7}$. So $\psi = 7|\theta|^{-2}\bar{\theta} = \bar{\theta}$. If we let θ_1 denote one of the values of θ then the others are $\theta_2 = \omega\theta_1$, $\theta_3 = \omega^2\theta_1$ and the complex conjugates of θ_1 , θ_2 and θ_3 . So $\theta + 7\theta^{-1} = \theta + \bar{\theta}$ is three-valued. By the

formula on p.3 of the notes, the three roots of the equation are the three values of $\frac{1}{3}S_1 + \theta + 7\theta^{-1}$. That is, the roots are given by

$$\frac{1}{3} \left(-1 + \sqrt[3]{\frac{7}{2}(1 + 3\sqrt{-3})} + \frac{7}{\sqrt[3]{\frac{7}{2}(1 + 3\sqrt{-3})}} \right),$$

where implicitly the same value of the cube root must be used in both places it occurs within the formula.

This does qualify as a “solution by radicals” of $x^3 + x^2 - 2x - 1 = 0$, although the answer may seem unsatisfactory, since it seems at first sight to be six valued, and involves cube roots of quantities which are not in the field of coefficients of the original polynomial, nor even in the field generated by the roots, since the roots are all real while the formula involves cube roots of complex numbers. However, if one wants to claim that cubics are soluble by radicals, this sort of thing has to be allowed. If you want actual numbers, you are better off forgetting about solution by radicals, since we know after all that the roots are $2 \cos(2\pi k/7)$ for $k \in \{1, 2, 3\}$.