

Tutorial 11

- Let α be the real 7th root of 2. Using Eisenstein's Criterion, show that $F = \mathbb{Q}(\alpha)$ is a degree 7 extension of \mathbb{Q} . Show also that F is not a splitting field for the polynomial $x^7 - 2$.

Solution.

Writing $x^7 - 2$ as $\sum_{n=0}^7 a_n x^n$, the leading coefficient is $a_7 = 1$, which is not divisible by 2, the coefficients a_n for n from 2 to 6 are all zero and hence divisible by 2, and the constant coefficient $a_0 = -2$ is divisible by 2 but not by 2^2 . So Eisenstein's Criterion applies and says that $x^7 - 2$ is irreducible over \mathbb{Q} . Hence $x^7 - 2$ is the minimal polynomial of α over \mathbb{Q} (since α is a root of it and it is irreducible over \mathbb{Q}), and the degree over \mathbb{Q} of the simple algebraic extension $\mathbb{Q}(\alpha)$ must be 7, the degree of $x^7 - 2$ (by a result proved in lectures).

Since α is real, $\mathbb{Q}(\alpha)$ is a subfield of \mathbb{R} . But if $\omega = \cos(2\pi/7) + i\sin(2\pi/7)$ then $\omega\alpha \notin \mathbb{R}$ and so $\omega\alpha \notin \mathbb{Q}(\alpha)$, and since $\omega\alpha$ is one of the complex roots of $x^7 - 2$ it follows that $\mathbb{Q}(\alpha)$ does not contain all the roots of $x^7 - 2$. Hence it is not a splitting field.

- Let $\omega = e^{2\pi i/7}$, a complex 7th root of 1. Determine the minimal polynomial $p(x)$ of ω over \mathbb{Q} , and thus show that $E = \mathbb{Q}(\omega)$ is a degree 6 extension of \mathbb{Q} . Show also that E is a splitting field for $x^7 - 1$, and that there are exactly six \mathbb{Q} -automorphisms of E . (See questions in Tutorials 9 and 10.)

Solution.

Since $\sum_{n=0}^6 \omega^n = (\omega^7 - 1)/(\omega - 1) = 0$ we see that ω is a root of the polynomial $p(x) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6$. Observe that

$$p(x+1) = 7 + 21x + 35x^2 + 35x^3 + 21x^4 + 7x^5 + x^6,$$

and by Eisenstein's Criterion applied with $p = 7$ this is irreducible over \mathbb{Q} (since the leading coefficient is not divisible by 7, all the other coefficients are divisible by 7, and the constant coefficient is not divisible by 49). It follows that $p(x)$ is irreducible, since a factorization $p(x) = a(x)b(x)$ with $a(x), b(x)$ both of degree less than 7 would yield a factorization $p(x+1) = a(x+1)b(x+1)$, contradicting irreducibility of $p(x+1)$. As ω is a root of $p(x)$ and $p(x)$ is irreducible over \mathbb{Q} , it follows that $p(x)$ is the minimal polynomial over \mathbb{Q} of ω . Since $p(x)$ has degree 6, the degree of $\mathbb{Q}(\omega)$ over \mathbb{Q} is 6.

The seven complex numbers ω^n , for n from 0 to 6, are all roots of $x^7 - 1$ (since $(\omega^n)^7 = (\omega^7)^n = 1^n = 1$), and are all distinct. So $x^7 - 1 = \prod_{n=0}^6 (x - \omega^n)$, and $p(x) = \prod_{n=1}^6 (x - \omega^n)$. Since all the factors have coefficients in $E = \mathbb{Q}(\omega)$ it follows that $p(x)$ splits into linear factors in E . Furthermore, no proper subfield of E contains ω (since $E = \mathbb{Q}(\omega)$), and so no proper subfield of E splits $p(x)$. Hence E is a splitting field for $p(x)$ over \mathbb{Q} .

If $1 \leq j \leq 6$ then ω^j has the same minimal polynomial over \mathbb{Q} as ω (namely, $p(x)$), and so the Isomorphism Extension Theorem guarantees that there exists an isomorphism $\mathbb{Q}(\omega) \rightarrow \mathbb{Q}(\omega^j)$ such that $\omega \mapsto \omega^j$. This isomorphism is unique: it is given by $\sum_{k=0}^5 a_k \omega^k \mapsto \sum_{k=0}^5 a_k (\omega^j)^k$ for all $a_k \in \mathbb{Q}$. Since $\omega^j \in \mathbb{Q}(\omega)$ we know that $\mathbb{Q}(\omega^j) \subseteq \mathbb{Q}(\omega)$, and since both $\mathbb{Q}(\omega^j)$ and $\mathbb{Q}(\omega)$ are six-dimensional vector spaces over \mathbb{Q} it follows that they must be equal. So this gives us six isomorphisms from $\mathbb{Q}(\omega)$ to itself. There can be no others since every isomorphism from $\mathbb{Q}(\omega)$ to a subfield of \mathbb{C} must take ω to a root of $p(x)$, and hence must be one of the six above.

- Let E and F be as in Questions 1 and 2, and let $K = E(\alpha)$. Show that the minimal polynomial of α over E is a divisor of $x^7 - 2$, and hence show that if $d = [K : E]$ then $d \leq 7$. Show that F is a subfield of K , and hence that $[K : \mathbb{Q}]$ is a multiple of 7. Use this to prove that $d = 7$, hence that $x^7 - 2$ is irreducible over E and is the minimal polynomial of α over E . Is K a splitting field for $x^7 - 2$ over E ?

Solution.

Observe that $x^7 - 2 \in \{f(x) \in E[x] \mid f(\alpha) = 0\}$, and by the definition the minimal polynomial of α over E is a generator of this ideal of $E[x]$. So $x^7 - 2$ is a multiple of the minimal polynomial. In particular, the degree of the minimal polynomial is at most 7. Now $d = [K : E]$ equals the degree of the minimal polynomial, and so $d \leq 7$.

By definition $F = \mathbb{Q}(\alpha)$. Now $\mathbb{Q} \subseteq E \subseteq K$, and $\alpha \in K$; so $F \subseteq K$. (In more detail, $F = \{\sum_{n=0}^7 q_n \alpha^n \mid q_n \in \mathbb{Q}\}$, and by closure of K under multiplication and addition we see that all elements of F are in K). Now by the multiplicative property of extension degrees,

$$[K : \mathbb{Q}] = [K : F][F : \mathbb{Q}] = 7[K : F]$$

is a multiple of 7. But similarly

$$[K : \mathbb{Q}] = [K : E][E : \mathbb{Q}] = 6d,$$

and for this to be a multiple of 7 it is necessary that d be a multiple of 7 (since $\gcd(6, 7) = 1$). Since $1 \leq d \leq 7$ it follows that $d = 7$. Recalling that d is the degree of the minimal polynomial of α over E , it follows that this minimal polynomial is $x^7 - 2$ itself (rather than a proper divisor of $x^7 - 2$). Since it is the minimal polynomial of α over E , it must be irreducible over E (since minimal polynomials are always irreducible). Because the seven complex numbers $\omega^n \alpha$ (for n from 0 to 6) are all distinct and are all roots of $x^7 - 2$ (since $(\omega^n \alpha)^7 = (\omega^7)^n \alpha^7 = 2$) we

deduce that $x^7 - 2 = \prod_{n=0}^6 (x - \omega^n \alpha)$. As all the factors lie in $K[x]$ it follows that $x^7 - 2$ splits over K . But any extension of E which contains the root α must also contain $E(\alpha) = K$; hence K is a minimal extension of E that splits $x^7 - 2$. So K is a splitting field for $x^7 - 2$ over E . (Note also that K is a minimal extension of \mathbb{Q} which contains the roots α and $\omega\alpha$ of $x^7 - 2$; hence K is a splitting field for $x^7 - 2$ over \mathbb{Q} .)

4. Continuing with the notation as in Questions 1, 2 and 3, show that $p(x)$ is irreducible as an element of $F[x]$ (by considering the degree $[F(\omega) : F]$, noting that $F(\omega) = K$). Show that the identity map $F \rightarrow F$ extends to an automorphism $g: K \rightarrow K$ such that $\omega \mapsto \omega^3$. Show that the identity map $E \rightarrow E$ extends to an automorphism $f: K \rightarrow K$ such that $\alpha \mapsto \omega\alpha$.

Solution.

Since $F \subseteq K$ and $\omega \in K$, certainly $F(\omega) \subseteq K$. But similar arguments yield the reverse inclusion: $E = \mathbb{Q}(\omega) \subset F(\omega)$ (as $\mathbb{Q} \subseteq F$), and since $\alpha \in F \subseteq F(\omega)$ it follows that $K = E(\alpha) \subseteq F(\omega)$. But we saw above that $[K : \mathbb{Q}] = 6d = 42$, and since $K = F(\omega)$ it follows that

$$42 = [F(\omega) : \mathbb{Q}] = [F(\omega) : F][F : \mathbb{Q}] = 7[F(\omega) : F].$$

So $[F(\omega) : F] = 6$, whence the minimal polynomial of ω over F has degree 6. But $p(x)$ is an element of $F[x]$ which has degree 6 and has ω as a root (and is monic). So $p(x)$ is the minimal polynomial of ω over F , and hence it is irreducible as an element of $F[x]$.

Note that $K = F(\omega) = F(\omega^3)$, since $\omega = (\omega^3)^5 \in F(\omega^3)$, and $\omega^3 \in F(\omega)$ (obviously). Furthermore, ω^3 is also a root of $p(x)$. Now, since the identity isomorphism $F \rightarrow F$ takes $p(x)$, which is the minimal polynomial of ω , to $p(x)$, which is the minimal polynomial of ω^3 , the Isomorphism Extension Theorem says that there is an isomorphism g from $F(\omega) = K$ to $F(\omega^3) = K$ extending the identity map on F and taking ω to ω^3 . Note that $g(\alpha) = \alpha$ and $g(\omega) = \omega^3$.

Since $x^7 - 2$ is irreducible in $E[x]$ and since α and $\omega\alpha$ are both roots of $x^7 - 2$, it follows that $E(\alpha)$ and $E(\omega\alpha)$ are isomorphic degree 7 extensions of E . Since $\omega\alpha \in E(\alpha)$ it follows that $E(\omega\alpha) = E(\alpha)$. (Alternatively, simply observe that $\alpha \in E(\omega\alpha)$ and $\omega\alpha \in E(\alpha)$.) The Isomorphism Extension Theorem again shows that the identity map $E \rightarrow E$ extends to an isomorphism f from $E(\alpha) = K$ to $E(\omega\alpha) = K$ taking α to $\omega\alpha$, since the identity $E \rightarrow E$ takes the minimal polynomial of α to the minimal polynomial of $\omega\alpha$. Note that $f(\omega) = \omega$ and $f(\alpha) = \omega\alpha$.

5. Let $f, g \in \text{Aut}_{\mathbb{Q}}(K)$ be as in Q4 above. Show that g^6 is the identity automorphism of K , and that the order of g is 6. Show also that the order of f is 7. Show that if $0 \leq j \leq 6$ and $0 \leq k \leq 5$ then $(f^j g^k)\omega = \omega^{3^k}$ and $(f^j g^k)\alpha = \alpha\omega^j$, and that these 42 automorphisms $f^j g^k$ are the only automorphisms of K . Show that $(gfg^{-1})(\alpha) = f^3(\alpha)$.

Solution.

If h is any automorphism of K then $0 = h0 = h(\alpha^7 - 2) = (h\alpha)^7 - 2$ (since $h(= 1$ gives $h2 = 2$). So $h\alpha$ must be one of the seven roots of $x^7 - 2$. Similarly $h\omega$ must be one of the six roots of $p(x)$. Since α and ω together generate K as an extension of \mathbb{Q} it follows that h is determined by $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\omega)$. So there are at most $7 \times 6 = 42$ automorphisms of K .

An easy induction shows that $g^k \alpha = \alpha^{3^k}$ for all integers $k \geq 0$: it is true for $k = 0$ (trivially) and for $k = 1$ by the definition of g , and if $g^{k-1} \omega = \omega^{3^{k-1}}$ then

$$g^k \omega = g(g^{k-1} \omega) = g(\omega^{3^{k-1}}) = (g\omega)^{3^{k-1}} = (\omega^3)^{3^{k-1}} = \omega^{3^k}.$$

Since f acts as the identity on E we know that $f\omega^l = \omega^l$ for all integers l , and hence $f^j(\omega^l) = f(f(\dots f(\omega^l)\dots)) = \omega^l$ for all $j \geq 0$ and all l . So

$$(f^j g^k)\omega = f^j(g^k \omega) = f^j(\omega^{3^k}) = \omega^{3^k}.$$

Similarly, since g acts as the identity on F we have $g^k \alpha = \alpha$ for all k , and now we can use induction on j to prove that $(f^j g^k)\alpha = \alpha\omega^j$ for all $j \geq 0$: the case $j = 0$ is trivial, and if $(f^{j-1} g^k)\alpha = \alpha\omega^{j-1}$ then

$$(f^j g^k)\alpha = f((f^{j-1} g^k)\alpha) = f(\alpha\omega^{j-1}) = (f\alpha)(f\omega^{j-1}) = (\alpha\omega)\omega^{j-1} = \alpha\omega^j.$$

Note that these formulas readily show that the 42 maps $f^j g^k$ obtained as j varies from 0 to 6 and k from 0 to 5 are all distinct (since $\alpha\omega^j = \alpha\omega^{j'}$ implies $j \equiv j' \pmod{7}$), and $\omega^{3^k} = \omega^{3^{k'}}$ implies that $3^k \equiv 3^{k'} \pmod{7}$, which implies that $k \equiv k' \pmod{6}$). So these are all the automorphisms of K .

Since $g(\alpha) = \alpha$, we have $g^{-1}(\alpha) = \alpha$, and so

$$(gfg^{-1})(\alpha) = g(f(g^{-1}(\alpha))) = g(f(\alpha)) = g(\omega\alpha) = g(\omega)g(\alpha) = \omega^3\alpha.$$

Similarly,

$$\begin{aligned} f^3(\alpha) &= f(f(f(\alpha))) = f(f(\omega\alpha)) = f(f(\omega)f(\alpha)) \\ &= f(\omega^2\alpha) = f(\omega)^2 f(\alpha) = \omega^3\alpha. \end{aligned}$$

So $g^{-1}fg = f^3$, as claimed.

6. Let $K:F$ and $E:K$ be field extensions that are both algebraic. Assume that the overall extension $E:F$ is separable. Show that $K:F$ and $E:K$ are both separable. (Recall that $E:F$ separable means that for every $t \in E$ the minimal polynomial of t over F is a separable polynomial, which in turn means that there is no extension of F over which this polynomial has a repeated factor.)

Solution.

Let $t \in K$ and let $p(x) \in F[x]$ be the minimal polynomial of t over K . Then $p(x)$ is separable since it is the minimal polynomial of $t \in E$, and $E:F$ is separable. Hence $K:F$ is separable.

Now let $t \in E$ and let $f(x) \in K[x]$ be the minimal polynomial of t over K , and suppose that there exists an extension $L:K$ such that $f(x)$ has a repeated factor in $L[x]$. Let $p(x) \in F[x]$ be the minimal polynomial of t over F , and observe that $f(x)|p(x)$ in $K[x]$, since $p(t) = 0$ and $f(x)$ is the minimal polynomial of t over K . Since $f(x)|p(x)$ is still true in $L[x]$, the fact that $f(x)$ has a repeated factor in $L[x]$ means that $p(x)$ does too. This contradicts separability of $E:F$, because $p(x)$ is the minimal polynomial over F of an element of E . So no such L can exist, and it follows that $E:K$ is separable.