

ALGEBRA HW 10

CLAY SHONKWILER

1

Let p be a prime number.

(a): Use Eisenstein's Irreducibility Criterion to show that the polynomial

$$f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$$

is irreducible over \mathbb{Q} .

Proof. We consider $f(x+1)$:

$$\begin{aligned} f(x+1) &= (x+1)^{p-1} + (x+1)^{p-2} + \cdots + (x+1) + 1 \\ &= \sum_{k=0}^{p-1} \sum_{j=0}^k \binom{k}{j} y^{k-j} \end{aligned}$$

Now, for each $0 \leq n \leq p-1$, the coefficient on y^n is

$$\sum_{k=n}^{p-1} \binom{k}{k-n} = \sum_{k=n}^{p-1} \binom{k}{n} = \binom{p}{n+1}.$$

Hence, we see that

$$f(x+1) = x^{p-1} + px^{p-2} + \cdots + \frac{p(p-1)}{2}x + p,$$

which is monic, has all coefficients divisible by p and constant term not divisible by p^2 . Hence, by Eisenstein, this polynomial is irreducible. Now, suppose $f(x) = g(x)h(x)$ for some non-constant $g, h \in \mathbb{Q}[x]$. Then $f(x+1) = g(x+1)h(x+1)$; however, this is impossible, since we just saw that $f(x+1)$ is irreducible over \mathbb{Q} . Therefore, we conclude that $f(x)$ is irreducible as well. \square

(b): Give another proof of the same assertion, by first showing that $f(x) = \Phi_p(x)$.

Proof. Note that

1

Using this result, we see that

$$\text{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \simeq (\mathbb{Z}/5\mathbb{Z})^\times \simeq C_4$$

$$\text{Gal}(\mathbb{Q}(\zeta_6)/\mathbb{Q}) \simeq (\mathbb{Z}/6\mathbb{Z})^\times = \{1, 5\} \simeq C_2$$

$$\text{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q}) \simeq (\mathbb{Z}/7\mathbb{Z})^\times \simeq C_6$$

$$\text{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}) \simeq (\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\} \simeq C_2 \times C_2$$

$$\text{Gal}(\mathbb{Q}(\zeta_{12})/\mathbb{Q}) \simeq (\mathbb{Z}/12\mathbb{Z})^\times = \{1, 5, 7, 11\} \simeq C_2 \times C_2$$

These last two are due to the fact that $3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}$ and $5^2 \equiv 7^2 \equiv 11^2 \equiv 1 \pmod{12}$.



(b): For which n is this extension abelian? cyclic? of order 2? of order 3? For which n does it have a cyclic quotient of order 3?

Answer: $(\mathbb{Z}/n\mathbb{Z})^\times$ is certainly abelian for all n , so we see that $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is abelian for all n . Furthermore, $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic only if $n = p^2$ for odd prime p , $n = 2$ or 4 , or $n = 2p^2$ for some odd prime p , so these are the cases where $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is cyclic.

Now, $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ has order 2 only if $\phi(n) = 2$. This is the case for $n = 3, 4, 6$ and for no other values of n , so these are the cases where the Galois group has order 2. Now, $\phi(n)$ cannot be odd for any value of $n \geq 3$ (and $\phi(2) = 1$), so we see that there is no n such that the extension $\mathbb{Q}(\zeta_n)$ is odd. Finally, $(\mathbb{Z}/n\mathbb{Z})^\times$ has a cyclic quotient of order 3 whenever $\phi(n)$ is a multiple of 3, meaning that some factor $m|n$ has $\phi(m)$ a multiple of 6 (remember, we cannot have $\phi(m) = 3$). Since ϕ is multiplicative and $\phi(p) = p - 1$ for all primes p , we see that this implies that n must be a multiple of a prime of the form $6a + 1$ for some $a \in \mathbb{N}$.



(c): Let $K_7^+ = \mathbb{Q}(\zeta_7 + \zeta_7^{-1})$. Find $[K_7 : \mathbb{Q}]$, $[K_7 : K_7^+]$, and $[K_7^+ : \mathbb{Q}]$. Also find $\text{Gal}(K_7/K_7^+)$ and $\text{Gal}(K_7^+/\mathbb{Q})$.

Answer: As we showed in PS9#2, $[K_n : \mathbb{Q}] = \phi(n)$; in particular, $[K_7 : \mathbb{Q}] = \phi(7) = 6$. Now, note that

$$\zeta_7^2 - \zeta_7(\zeta_7 + \zeta_7^{-1}) + 1 = \zeta_7^2 - (\zeta_7^2 + 1) + 1 = 0,$$

so ζ_7 satisfies the polynomial $g(x) = x^2 - (\zeta_7 + \zeta_7^{-1})x + 1 \in K_7^+[x]$. On the other hand,

$$x^2 - (\zeta_7 + \zeta_7^{-1})x + 1 = (x - \zeta_7)(x - \zeta_7^{-1})$$

in K_7 ; since $\zeta_7, \zeta_7^{-1} \notin K_7^+$, this implies that $g(x)$ is irreducible over K_7^+ , and so $g(x)$ is the minimal polynomial for ζ_7 over K_7^+ . Hence, $[K_7 : K_7^+] = 2$. In turn,

$$6 = [K_7 : \mathbb{Q}] = [K_7 : K_7^+][K_7^+ : \mathbb{Q}] = 2[K_7^+ : \mathbb{Q}],$$

so $[K_7^+ : \mathbb{Q}] = 3$. Since the only group of order 2 is C_2 , we see that $\text{Gal}(K_7/K_7^+) = C_2 = \langle h \rangle$, where $h(\zeta_7) = \zeta_7^{-1}$. In turn, if we can show that K_7^+ is Galois over \mathbb{Q} , then this will imply that $\text{Gal}(K_7^+/\mathbb{Q}) = C_3$, since this is the only group of order 3. Note that

$$\begin{aligned} (\zeta_7 + \zeta_7^{-1})^3 + (\zeta_7 + \zeta_7^{-1})^2 - 2(\zeta_7 + \zeta_7^{-1}) - 1 &= (\zeta_7^3 + 3\zeta_7 + 3\zeta_7^{-1} + \zeta_7^{-3}) + (\zeta_7^2 + 2 + \zeta_7^{-2}) - (2\zeta_7 + 2\zeta_7^{-1}) - 1 \\ &= \zeta_7 + \zeta_7^2 + \zeta_7^3 + \zeta_7^{-3} + \zeta_7^{-2} + \zeta_7^{-1} + 1 \\ &= f(\zeta_7) \\ &= 0 \end{aligned}$$

where $f(x)$ is as in problem 1 above. Hence, we see that $\zeta_7 + \zeta_7^{-1}$ satisfies the polynomial $x^3 + x^2 - 2x - 1 \in \mathbb{Q}[x]$. Since $[K_7^+ : \mathbb{Q}] = 3$, the minimal polynomial of $\zeta_7 + \zeta_7^{-1}$ over \mathbb{Q} must be of degree at least 3, so we see that $h(x) = x^3 + x^2 - 2x - 1$ is the minimal polynomial of $\zeta_7 + \zeta_7^{-1}$ over \mathbb{Q} . Now, the other roots of $h(x)$ are $\zeta_7^2 + \zeta_7^{-2}$ and $\zeta_7^3 + \zeta_7^{-3}$, which are both in K_7^+ , since

$$\zeta_7^2 + \zeta_7^{-2} = \zeta_7^2 + 2 + \zeta_7^{-2} - 2 = (\zeta_7 + \zeta_7^{-1})^2 - 2$$

and

$$\zeta_7^3 + \zeta_7^{-3} = \zeta_7^3 + 3\zeta_7 + 3\zeta_7^{-1} + \zeta_7^{-3} - 3(\zeta_7 + \zeta_7^{-1}) = (\zeta_7 + \zeta_7^{-1})^3 - 3(\zeta_7 + \zeta_7^{-1}).$$

Therefore, K_7^+ is normal and, hence, Galois over \mathbb{Q} , so $\text{Gal}(K_7^+/\mathbb{Q}) = C_3$.



(d): Find a Galois extension of \mathbb{Q} having degree 5. Find another of degree 7.

Answer: Consider $K_{11}^+ = \mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1})$. Now,

$$[K_{11} : \mathbb{Q}] = \phi(11) = 10.$$

Also,

$$\zeta_{11}^2 - \zeta_{11}(\zeta_{11} + \zeta_{11}^{-1}) + 1 = \zeta_{11}^2 - (\zeta_{11}^2 + 1) + 1 = 0,$$

so ζ_{11} satisfies $x^2 - (\zeta_{11} + \zeta_{11}^{-1})x + 1 \in K_{11}^+[x]$, which is irreducible (and hence the minimal polynomial of ζ_{11} over K_{11}^+) since neither of its roots, ζ_{11} and ζ_{11}^{-1} , is in K_{11}^+ . Hence, $[K_{11} : K_{11}^+] = 2$, which in turn implies that $[K_{11}^+ : \mathbb{Q}] = 5$. Now, $\text{Gal}(K_{11}/\mathbb{Q}) = C_2 \times C_5 = C_{10}$; since

$$\text{Gal}(K_{11}/K_{11}^+) = C_2 \triangleleft C_{10} = \text{Gal}(K_{11}/\mathbb{Q}),$$

we see, by the Fundamental Theorem of Galois Theory, that K_{11}^+ is Galois over \mathbb{Q} with Galois group

$$\text{Gal}(K_{11}^+/\mathbb{Q}) = \text{Gal}(K_{11}/\mathbb{Q})/\text{Gal}(K_{11}/K_{11}^+) \simeq C_{10}/C_2 = C_5.$$

To find a Galois extension of degree 7, consider K_{29} . $\text{Gal}(K_{29}/\mathbb{Q}) = C_4 \times C_7 = C_{28}$; hence, if we can find K such that $\text{Gal}(K_{29}/K) = C_4$,

then K will be a Galois extension of \mathbb{Q} with Galois group C_7 . Now, note that $h(\zeta_{29}) = \zeta_{29}^{12}$ induces an automorphism of K_{29} , which is to say an element of the Galois group. Now,

$$\begin{aligned} h(\zeta_{29}) &= \zeta_{29}^{12} \\ h^2(\zeta_{29}) &= h(\zeta_{29}^{12}) = (\zeta_{29}^{12})^{12} = \zeta_{29}^{144} = \zeta_{29}^{-1} \\ h^3(\zeta_{29}) &= h(h^2(\zeta_{29})) = h(\zeta_{29}^{-1}) = (\zeta_{29}^{-1})^{12} = \zeta_{29}^{-12} \\ h^4(\zeta_{29}) &= h(h^3(\zeta_{29})) = h(\zeta_{29}^{-12}) = (\zeta_{29}^{-12})^{12} = 1 \end{aligned}$$

so we see that h has order 4 in $\text{Gal}(K_{29}/\mathbb{Q})$. Hence, $\langle h \rangle \simeq C_4 \triangleleft C_{28}$, so we see that the fixed field K of $\langle h \rangle$ must be Galois over \mathbb{Q} with Galois group

$$\text{Gal}(K/\mathbb{Q}) = \text{Gal}(K_{29}/K)/\langle h \rangle = C_{28}/C_4 = C_7.$$

However, the fixed field of $\langle h \rangle$ is simply

$$\mathbb{Q}(\zeta_{29} + h(\zeta_{29}) + h^2(\zeta_{29}) + h^3(\zeta_{29})) = \mathbb{Q}(\zeta_{29} + \zeta_{29}^{12} + \zeta_{29}^{-1} + \zeta_{29}^{-12}),$$

so this is a Galois extension of \mathbb{Q} having degree 7. ♣

3

Find the Galois group of (the splitting field of) each of the following polynomials.

(a): $x^3 - 10$ over \mathbb{Q} .

Answer: The three roots of this polynomial are $\sqrt[3]{10}$, $\zeta_3 \sqrt[3]{10}$ and $\zeta_3^2 \sqrt[3]{10}$, so we see that the splitting field of this polynomial is

$$\mathbb{Q}[\zeta_3, \sqrt[3]{10}].$$

Now, if ϕ is a \mathbb{Q} -automorphism of $\mathbb{Q}[\zeta_3, \sqrt[3]{10}]$, then ϕ is completely determined by what it does to ζ_3 and $\sqrt[3]{10}$. Also,

$$1 = \phi(1) = \phi(\zeta_3^3) = \phi(\zeta_3)^3,$$

so $\phi(\zeta_3) = \zeta_3$ or ζ_3^2 (since $\phi(\zeta_3) \neq 1$). Similarly,

$$10 = \phi(10) = \phi(\sqrt[3]{10}^3) = \phi(\sqrt[3]{10})^3,$$

so $\phi(\sqrt[3]{10})$ is a third root of 10. Hence, $\phi(\sqrt[3]{10}) = \sqrt[3]{10}$, $\zeta_3 \sqrt[3]{10}$ or $\zeta_3^2 \sqrt[3]{10}$. Since there are two possibilities for $\phi(\zeta_3)$ and 3 possibilities for $\phi(\sqrt[3]{10})$, we see there are 6 elements of $\text{Gal}(\mathbb{Q}[\zeta_3, \sqrt[3]{10}]/\mathbb{Q})$. Now, if

$$\begin{aligned} \phi : \zeta_3 &\mapsto \zeta_3, & \phi : \sqrt[3]{10} &\mapsto \zeta_3 \sqrt[3]{10} \\ \psi : \zeta_3 &\mapsto \zeta_3^2, & \psi : \sqrt[3]{10} &\mapsto \zeta_3 \sqrt[3]{10}, \end{aligned}$$

then

$$\begin{aligned}(\phi \circ \psi)(\sqrt[3]{10}) &= \phi(\zeta_3 \sqrt[3]{10}) = \zeta_3^2 \sqrt[3]{10} \\ (\psi \circ \phi)(\sqrt[3]{10}) &= \psi(\zeta_3 \sqrt[3]{10}) = \zeta_3^3 \sqrt[3]{10} = \sqrt[3]{10}\end{aligned}$$

so we see that $\text{Gal}(\mathbb{Q}[\zeta_3, \sqrt[3]{10}]/\mathbb{Q})$ is not abelian. Since the only non-abelian group of order 6 is S_3 , we see that $\text{Gal}(\mathbb{Q}[\zeta_3, \sqrt[3]{10}]/\mathbb{Q}) \simeq S_3$. \clubsuit

(b): $x^3 - 10$ over $\mathbb{Q}(\sqrt{2})$.

Answer: Again, note that the roots of this polynomial are $\sqrt[3]{10}$, $\zeta_3 \sqrt[3]{10}$ and $\zeta_3^2 \sqrt[3]{10}$. Since neither $\sqrt[3]{10}$ nor ζ_3 lie in $\mathbb{Q}(\sqrt{2})$, we see that $x^3 - 10$ is irreducible over $\mathbb{Q}(\sqrt{2})$ and that the splitting field is given by

$$K = \mathbb{Q}(\sqrt{2})[\zeta_3, \sqrt[3]{10}].$$

All of the automorphisms described in (a) above can be extended to automorphisms of $K = \mathbb{Q}[\sqrt{2}, \zeta_3, \sqrt[3]{10}]$ simply by requiring $\sqrt{2} \mapsto \sqrt{2}$, so we see that

$$\text{Gal}(K/\mathbb{Q}(\sqrt{2})) \simeq S_3. \quad \clubsuit$$

(c): $x^3 - 10$ over $\mathbb{Q}(\sqrt{-3})$.

Answer: Note that

$$\zeta_3 = e^{i2\pi/3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i,$$

so $\zeta_3 \in \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\sqrt{3}i)$. Hence, all three roots of $x^3 - 10$ are already in $\mathbb{Q}(\sqrt{-3})[\sqrt[3]{10}]$. Since $x^3 - 10$ is still irreducible over $\mathbb{Q}(\sqrt{-3})$, we see that

$$\#\text{Gal}(\mathbb{Q}(\sqrt{-3})[\sqrt[3]{10}]/\mathbb{Q}(\sqrt{-3})) = [\mathbb{Q}(\sqrt{-3})[\sqrt[3]{10}] : \mathbb{Q}(\sqrt{-3})] = 3,$$

so the Galois group is C_3 , the only group of order 3. \clubsuit

(d): $x^4 - 5$ over \mathbb{Q} , $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{-5})$, $\mathbb{Q}(i)$.

Answer: Note that the roots of $x^4 - 5$ are $\pm\sqrt[4]{5}$, $\pm i\sqrt[4]{5}$. Hence, the splitting field over \mathbb{Q} of this polynomial is

$$\mathbb{Q}[i, \sqrt[4]{5}].$$

This extension is certainly normal and, hence, Galois. Now, if $\phi \in \text{Gal}(\mathbb{Q}[i, \sqrt[4]{5}]/\mathbb{Q})$, then

$$-1 = \phi(-1) = \phi(i^2) = \phi(i)^2,$$

so $\phi(i) = \pm i$. Also,

$$5 = \phi(5) = \phi\left(\sqrt[4]{5^4}\right) = \phi\left(\sqrt[4]{5}\right)^4,$$

so $\phi(\sqrt[4]{5}) = \pm\sqrt[4]{5}, \pm i\sqrt[4]{5}$. Hence, there are a total of 8 elements of $\text{Gal}(\mathbb{Q}[i, \sqrt[4]{5}]/\mathbb{Q})$. Now, suppose

$$\begin{aligned}\phi : i &\mapsto i & \phi : \sqrt[4]{5} &\mapsto i\sqrt[4]{5} \\ \psi : i &\mapsto -i & \psi : \sqrt[4]{5} &\mapsto i\sqrt[4]{5}\end{aligned}$$

Then

$$\begin{aligned}(\phi \circ \psi)(\sqrt[4]{5}) &= \phi(i\sqrt[4]{5}) = i^2\sqrt[4]{5} = -\sqrt[4]{5} \\ (\psi \circ \phi)(\sqrt[4]{5}) &= \psi(i\sqrt[4]{5}) = -i^2\sqrt[4]{5} = \sqrt[4]{5},\end{aligned}$$

so we see that $\text{Gal}(\mathbb{Q}[i, \sqrt[4]{5}]/\mathbb{Q})$ is not abelian; hence, it is either D_4 or Q_8 . Now, if ϕ and ψ are given by:

$$\begin{aligned}\phi : i &\mapsto -i & \phi : \sqrt[4]{5} &\mapsto \sqrt[4]{5} \\ \psi : i &\mapsto -i & \psi : \sqrt[4]{5} &\mapsto -\sqrt[4]{5}\end{aligned}$$

then both ϕ and ψ have order 2. Since there is only one element of Q_8 of order 2 (namely -1), this implies that the Galois group is D_4 .

Over $\mathbb{Q}(\sqrt{5})$,

$$x^4 - 5 = (x^2 - \sqrt{5})(x^2 + \sqrt{5}).$$

Hence, the minimal polynomial of $\sqrt[4]{5}$ over $\mathbb{Q}(\sqrt{5})$ is $x^2 - \sqrt{5}$, so if ϕ is an element of the Galois group of the splitting field, $\phi(\sqrt[4]{5}) = \pm\sqrt[4]{5}$. On the other hand, the minimal polynomial of i is still $x^2 + 1$, so $\phi(i) = \pm i$. This leaves only 4 possibilities for ϕ , so we see that the Galois group of the splitting field $\mathbb{Q}(\sqrt{5})[i, \sqrt[4]{5}] = \mathbb{Q}[i, \sqrt[4]{5}]$ over $\mathbb{Q}(\sqrt{5})$ has only four elements. Now, if

$$\begin{aligned}\phi : i &\mapsto i & \sqrt[4]{5} &\mapsto -\sqrt[4]{5} \\ \psi : i &\mapsto -i & \sqrt[4]{5} &\mapsto \sqrt[4]{5},\end{aligned}$$

then it's clear that both ϕ and ψ are of order 2; the only group of order 4 with at least 2 elements of order 2 is $C_2 \times C_2$, so we see that

$$\text{Gal}(\mathbb{Q}[i, \sqrt[4]{5}]/\mathbb{Q}(\sqrt{5})) \simeq C_2 \times C_2.$$

Since $[\mathbb{Q}(\sqrt{-5}) : \mathbb{Q}] = 2$ and $[\mathbb{Q}(i, \sqrt[4]{5}) : \mathbb{Q}] = 8$ and $\mathbb{Q}(\sqrt{-5}) \subset \mathbb{Q}(i, \sqrt[4]{5})$, we see that $[\mathbb{Q}(i, \sqrt[4]{5}) : \mathbb{Q}(\sqrt{-5})] = 4$. This extension is certainly Galois, so the order of the Galois group is 4. Now, if ϕ is in the Galois group, then

$$-1 = \phi(-1) = \phi(i^2) = \phi(i)^2,$$

so $\phi(i) = \pm i$. However, if $\phi(i) = -i$, then $\phi(i\sqrt{5}) = \phi(i)\phi(\sqrt{5}) = -i\phi(\sqrt{5})$; since $\sqrt{-5} = i\sqrt{5}$ must be fixed by ϕ , this implies that $\phi(\sqrt{5}) = -\sqrt{5}$. Similarly, if $\phi(i) = i$, then $\phi(\sqrt{5}) = \sqrt{5}$. Now,

$$5 = \phi(5) = \phi(\sqrt[4]{5^4}) = \phi(\sqrt[4]{5})^5,$$

so $\phi(\sqrt[4]{5}) = \pm\sqrt[4]{5}, \pm i\sqrt[4]{5}$. If $\phi(i) = i$, then

$$\sqrt{5} = \phi(i\sqrt{5}) = \phi(\sqrt[4]{5}^2) = \phi(\sqrt[4]{5})^2,$$

so $\phi(\sqrt[4]{5}) = \pm\sqrt[4]{5}$. A similar argument shows that if $\phi(i) = -i$, then $\phi(\sqrt[4]{5}) = \pm i\sqrt[4]{5}$. Hence, we see that there are a total of 4 elements of the Galois group. Since each of the elements described here has order 2, we see that the Galois group is isomorphic to $C_2 \times C_2$.

Finally, over $\mathbb{Q}(i)$, $\mathbb{Q}(i, \sqrt[4]{5}) = \mathbb{Q}(i)(\sqrt[4]{5})$. The elements of the Galois group will be the same as over \mathbb{Q} , except i must be fixed. Hence, there are four elements of the Galois group, namely those mapping $\sqrt[4]{5}$ to $\pm\sqrt[4]{5}, \pm i\sqrt[4]{5}$. If $\phi(\sqrt[4]{5}) = i\sqrt[4]{5}$, then

$$\phi^2(\sqrt[4]{5}) = \phi(i\sqrt[4]{5}) = i^2\sqrt[4]{5} = -\sqrt[4]{5},$$

so $\phi^2 \neq id$, meaning that ϕ must have order greater than two. Since the order of the group is 4, we see that ϕ has order 4 and that, therefore, the Galois group is $\langle \phi \rangle = C_4$.



(e): $x^4 - t$ over $\mathbb{R}(t), \mathbb{C}(t)$.

Answer: Note that the roots of $x^4 - t$ are $\pm\sqrt[4]{t}, \pm i\sqrt[4]{t}$. Hence, the splitting field over $\mathbb{R}(t)$ of this polynomial is

$$\mathbb{R}(t)[i, \sqrt[4]{t}].$$

This extension is certainly normal and, hence, Galois. Now, if $\phi \in \text{Gal}(\mathbb{R}(t)[i, \sqrt[4]{t}]/\mathbb{R}(t))$, then

$$-1 = \phi(-1) = \phi(i^2) = \phi(i)^2,$$

so $\phi(i) = \pm i$. Also,

$$t = \phi(t) = \phi\left(\sqrt[4]{t}^4\right) = \phi\left(\sqrt[4]{t}\right)^4,$$

so $\phi(\sqrt[4]{t}) = \pm\sqrt[4]{t}, \pm i\sqrt[4]{t}$. Hence, there are a total of 8 elements of $\text{Gal}(\mathbb{R}(t)[i, \sqrt[4]{t}]/\mathbb{R}(t))$. Now, suppose

$$\begin{aligned} \phi : i &\mapsto i & \phi : \sqrt[4]{t} &\mapsto i\sqrt[4]{t} \\ \psi : i &\mapsto -i & \psi : \sqrt[4]{t} &\mapsto i\sqrt[4]{t} \end{aligned}$$

Then

$$\begin{aligned} (\phi \circ \psi)(\sqrt[4]{t}) &= \phi(i\sqrt[4]{t}) = i^2\sqrt[4]{t} = -\sqrt[4]{t} \\ (\psi \circ \phi)(\sqrt[4]{t}) &= \psi(i\sqrt[4]{t}) = -i^2\sqrt[4]{t} = \sqrt[4]{t}, \end{aligned}$$

so we see that $\text{Gal}(\mathbb{R}(t)[i, \sqrt[4]{t}]/\mathbb{R}(t))$ is not abelian; hence, it is either D_4 or Q_8 . Now, if ϕ and ψ are given by:

$$\begin{aligned} \phi : i &\mapsto -i & \phi : \sqrt[4]{t} &\mapsto \sqrt[4]{t} \\ \psi : i &\mapsto -i & \psi : \sqrt[4]{t} &\mapsto -\sqrt[4]{t} \end{aligned}$$

then both ϕ and ψ have order 2. Since there is only one element of Q_8 of order 2 (namely -1), this implies that the Galois group is D_4 .

Over $\mathbb{C}(t)$, the roots of $x^4 - t$ are still $\pm\sqrt[4]{t}$, $\pm i\sqrt[4]{t}$; now, of course, $i \in \mathbb{C}(t)$, so the splitting field of this polynomial is given by

$$\mathbb{C}(t)[\sqrt[4]{t}].$$

This extension is clearly normal and, hence, Galois, and the Galois group consists of the four possible maps $\sqrt[4]{t} \mapsto \pm\sqrt[4]{t}, \pm i\sqrt[4]{t}$. Now, if $\phi(\sqrt[4]{t}) = i\sqrt[4]{t}$, then

$$\phi^2(\sqrt[4]{t}) = \phi(i\sqrt[4]{t}) = i^2\sqrt[4]{t} = -\sqrt[4]{t},$$

so $\phi^2 \neq id$ and so ϕ has order 4. Hence, the Galois group is given by $\langle \phi \rangle = C_4$.



4

Show that for every finite group G , there are field extensions $\mathbb{Q} \subset K \subset L$ such that L is a finite Galois extension of K with $\text{Gal}(L/K) = G$.

Proof. Let G be a finite group and let $n = \#G$. Let $L = \mathbb{Q}(x_1, \dots, x_n)$ and let $K_0 = \mathbb{Q}(s_1, \dots, s_n)$ where s_i is the i th symmetric polynomial in the x_j . Then, by PS9#3, L is Galois over K_0 and $\text{Gal}(L/K_0) = S_n$. Now, by Cayley's Theorem, G can be embedded into S_n ; let $\phi : G \hookrightarrow S_n$ be this embedding and let $H = \phi(G)$. Let $K = L^H$. Then

$$\text{Gal}(L/K) = \text{Gal}(L/L^H) = H = \phi(G) \simeq G,$$

so L and K are the desired extensions of \mathbb{Q} . \square

5

(a): Find a Galois extension of \mathbb{Q} with Galois group $C_6 \times C_{15}$.

Answer: Note, first, that $\text{Gal}(K_7/\mathbb{Q}) = C_6$. Now, let $K = \mathbb{Q}(\zeta_{31} + \zeta_{31}^{-1})$. Now, $\text{Gal}(K_{31}/\mathbb{Q}) = C_2 \times C_{15} = C_{30}$. Furthermore,

$$(\zeta_{31})^2 - \zeta_{31}(\zeta_{31} + \zeta_{31}^{-1}) + 1 = \zeta_{31}^2 - (\zeta_{31}^2 + 1) + 1 = 0,$$

so ζ_{31} satisfies $x^2 - (\zeta_{31} + \zeta_{31}^{-1})x + 1 \in K[x]$. Since the roots of this polynomial are ζ_{31} and ζ_{31}^{-1} , neither of which is in K , we see that this polynomial is irreducible and, hence, the minimal polynomial of ζ_{31} over K , so $[K_{31} : K] = 2$. Hence, $\text{Gal}(K_{31}/K) = C_2 = \langle h \rangle$ where $h(\zeta_{31}) = \zeta_{31}^{-1}$. Since $K = K_{31}^{\langle h \rangle}$ and $C_2 \triangleleft C_{30}$, we see that K is Galois over \mathbb{Q} with

$$\text{Gal}(K/\mathbb{Q}) = \text{Gal}(K_{31}/K)/\langle h \rangle \simeq C_{30}/C_2 = C_{15}.$$

Hence, since $K_7 \cap K = \mathbb{Q}$, the compositum K_7K is be Galois over \mathbb{Q} with Galois group $C_6 \times C_{15}$.



(b): Do the same over the field $\overline{\mathbb{F}_5}(t)$.

Answer: Note that

$$4^6 = (2^2)^6 = 2^{12} = 4096 \equiv 1 \pmod{5},$$

so 4 is a 6th root of unity in $\overline{\mathbb{F}_5}(t)$. Hence, by Kummer's Theorem, $K = \overline{\mathbb{F}_5}(t) [\sqrt[6]{t+1}]$ is a cyclic extension of $\overline{\mathbb{F}_5}(t)$ with Galois group C_6 .

Now, suppose there exists $h(t) \in \overline{\mathbb{F}_5}(t)$ such that $h(t)^5 - h(t) = t$. Then $h(t)^5 = t + h(t)$. $h(t)$ cannot be a constant polynomial. Furthermore, if a is the leading coefficient of $h(t)$, then the leading coefficient in $h(t)^5$ must be a^5 . However,

$$1^5 = 1$$

$$2^5 = 32 \equiv 2 \pmod{5}$$

$$3^5 = 243 \equiv 3 \pmod{5}$$

$$4^5 = 2^{10} = 1024 \equiv 4 \pmod{5},$$

so we see that, since $a \neq 0$, $a^5 \neq 0$ in $\overline{\mathbb{F}_5}(t)$. Hence,

$$\deg h(t)^5 = 5(\deg h(t)) \geq 5(\deg(t + h(t))) > \deg(t + h(t))$$

which is impossible, since $h(t)^5 = t + h(t)$. Therefore, we conclude that there is no such $h(t)$. Therefore, we have the Artin-Schreier extension $L_1 = \overline{\mathbb{F}_5}(t)[x]/(x^5 - x - t)$, which is Galois over $\overline{\mathbb{F}_5}(t)$ with Galois group C_5 . On the other hand, since $3^3 = 81 \equiv 1 \pmod{5}$, 3 is a 3rd root of unity in $\overline{\mathbb{F}_5}(t)$, so, by Kummer, since t has no 3rd root in $\overline{\mathbb{F}_5}(t)$, $L_2 = \overline{\mathbb{F}_5}(t) [\sqrt[3]{t}]$ is a cyclic extension with Galois group C_3 .

Now, since $L_1 \cap L_2 = \overline{\mathbb{F}_5}(t)$, the compositum $L = L_1 L_2$ is Galois over $\overline{\mathbb{F}_5}(t)$ with Galois group

$$C_3 \times C_5 \simeq C_{15}.$$

Finally, since $K \cap L = \overline{\mathbb{F}_5}(t)$, their compositum KL is Galois with Galois group

$$C_6 \times C_{15}.$$



(c): Let $L = \mathbb{C}(x, y)$, $M = \mathbb{C}(x^2, xy, y^2) \subset L$, and $K = \mathbb{C}(x^2, y^2) \subset M$. Find $[L : M]$, $[M : K]$, $[L : K]$. Is L Galois over M ? Is M Galois over K ? Is L Galois over K ? For those extensions that are Galois, find the Galois group.

Answer: Note that $\frac{1}{xy} = \frac{xy}{x^2y^2}$ and $\frac{1}{x^2y^2} \in K$, so $M = K[xy]$. Similarly, $\frac{1}{x^2} \in M$ and $\frac{1}{x} = \frac{x}{x^2}$; also $\frac{1}{y} = \frac{y}{y^2}$ and

$$\frac{1}{x}xy = \frac{xy}{x} = y,$$

so $L = M[x]$. Now, $x^2 - x^2 = 0$, so x satisfies $t^2 - x^2 \in M[t]$. Since $x, -x$ are the two roots of $t^2 - x^2$ in L and $x, -x \notin M$, we see that x has minimal polynomial $t^2 - x^2$ over M , so $[L : M] = 2$.

On the other hand, $(xy)^2 - x^2y^2 = x^2y^2 - x^2y^2 = 0$, so xy satisfies the polynomial $t^2 - x^2y^2 \in K[t]$. Since $xy, -xy \notin K$ and these are the two roots of $t^2 - x^2y^2$, we see that this polynomial is irreducible and, hence, the minimal polynomial of xy over K . Thus, $[M : K] = 2$ as well. In turn,

$$[L : K] = [L : M][M : K] = 2 \cdot 2 = 4.$$

Now, since any degree two extension is normal and, since we're in characteristic zero, all these extensions are separable, we immediately see that L is Galois over M and M is Galois over K , each with Galois group C_2 . Now, considering L over K , since $L = K[x, y]$, any automorphism of L is completely determined by where it sends x and y ; there are four possibilities, given by the possible combinations of:

$$\begin{aligned} x &\mapsto \pm x \\ y &\mapsto \pm y. \end{aligned}$$

Each of these four possibilities yields a distinct automorphism of L fixing K , since $x^2 = (-x)^2$ and $y^2 = (-y)^2$, so $\#\text{Gal}(L/K) \geq 4$. On the other hand, $\#\text{Gal}(L/K) \leq [L : K] = 4$, so we conclude that $\#\text{Gal}(L/K) = [L : K]$, meaning L is Galois over K . Note that each element of the Galois group is of order 2, meaning that $\text{Gal}(L/K) \simeq C_2 \times C_2$.



6

Let K and L be finite extensions of a field k , and let KL be their compositum (inside some fixed algebraic closure).

(a): Find a surjective k -algebra homomorphism $\pi : K \otimes_k L \twoheadrightarrow KL$.

Answer: Define $\phi : K \times L \rightarrow KL$ by

$$(a, b) \mapsto ab.$$

Now, if $a_1, a_2 \in K$, $b_1, b_2 \in L$ and $r_1, r_2 \in k$, then

$$\begin{aligned} \phi((r_1a_1, b_1) + (r_2a_2, b_2)) &= \phi((r_1a_1 + r_2a_2, b_1)) = (r_1a_1 + r_2a_2)b_1 \\ &= r_1(a_1b_1) + r_2(a_2b_1) \\ &= r_1\phi((a_1, b_1)) + r_2\phi((a_2, b_1)) \end{aligned}$$

and

$$\begin{aligned} \phi((a_1, r_1b_1) + (a_1, r_2b_2)) &= \phi((a_1, r_1b_1 + r_2b_2)) = a_1(r_1b_1 + r_2b_2) \\ &= r_1(a_1b_1) + r_2(a_1b_2) \\ &= r_1\phi((a_1, b_1)) + r_2\phi((a_1, b_2)), \end{aligned}$$

so ϕ is k -bilinear. Therefore, by the universal property of the tensor product, ϕ induces a unique k -algebra homomorphism $\pi : K \otimes_k L \rightarrow KL$ where

$$\pi(a \otimes b) = \phi(a, b).$$

Now, $L = k[\alpha_1, \dots, \alpha_n]$ for some $\alpha_1, \dots, \alpha_n \in K$. Hence,

$$KL = K[\alpha_1, \dots, \alpha_n],$$

so if $\gamma \in KL$,

$$\gamma = f_\gamma(\alpha_1, \dots, \alpha_n)$$

for some $f_\gamma \in K[x_1, \dots, x_n]$. In turn, this means that

$$\gamma = f_\gamma(\alpha_1, \dots, \alpha_n) = \sum_{i_1=0}^{m_1} \cdots \sum_{i_n=0}^{m_n} a_{i_1 \dots i_n} \alpha_1^{i_1} \cdots \alpha_n^{i_n}.$$

for some $m_1, \dots, m_n \in \mathbb{N}$ and $a_{i_1 \dots i_n} \in K$ for all $0 \leq i_j \leq m_j$ and all $j = 1, \dots, n$. Now, $a_{i_1 \dots i_n} \otimes (\alpha_1^{i_1} \cdots \alpha_n^{i_n}) \in K \otimes_k L$ for all $0 \leq i_j \leq m_j$ and all $j = 1, \dots, n$ and $\pi(a_{i_1 \dots i_n} \otimes (\alpha_1^{i_1} \cdots \alpha_n^{i_n})) = a_{i_1 \dots i_n} \alpha_1^{i_1} \cdots \alpha_n^{i_n}$. Therefore, since π is linear,

$$\begin{aligned} \pi \left(\sum_{i_1=0}^{m_1} \cdots \sum_{i_n=0}^{m_n} a_{i_1 \dots i_n} \otimes (\alpha_1^{i_1} \cdots \alpha_n^{i_n}) \right) &= \sum_{i_1=0}^{m_1} \cdots \sum_{i_n=0}^{m_n} \pi(a_{i_1 \dots i_n} \otimes (\alpha_1^{i_1} \cdots \alpha_n^{i_n})) \\ &= \sum_{i_1=0}^{m_1} \cdots \sum_{i_n=0}^{m_n} a_{i_1 \dots i_n} \alpha_1^{i_1} \cdots \alpha_n^{i_n} \\ &= \gamma. \end{aligned}$$

Since our choice of γ was arbitrary, we conclude that π is a surjective k -algebra homomorphism. ♣

(b): Suppose that K is Galois over k . Show that π is an isomorphism if and only if $K \cap L = k$.

Proof. Note, first, that $\dim_k K \otimes_k L = (\dim_k K) \cdot (\dim_k L) = [K : k][L : k]$. Now, since K is Galois over k ,

$$\dim_k(KL) = [KL : k] = [K : k][L : k]$$

if and only if $K \cap L = k$. If π is an isomorphism, then certainly we must have that

$$[K : k][L : k] = \dim_k K \otimes_k L = \dim_k(KL),$$

so $K \cap L = k$.

On the other hand, if $K \cap L = k$, then

$$\dim_k(KL) = [K : k][L : k] = \dim_k K \otimes_k L;$$

since π is a surjective k -algebra homomorphism between vector spaces of the same dimension, π must also be injective and, therefore, an isomorphism. □

(c): Does (b) still hold if K is no longer assumed Galois over k ?

Answer: No. Let $k = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2})$ and $L = \mathbb{Q}(\zeta_3\sqrt[3]{2})$. Then, as we've seen in class, $[K : k] = [L : k] = 3$, $K \cap L = k$ and $[KL : k] = 6$. However, since

$$\dim_k K \otimes_k L = [K : k][L : k] = 3 \cdot 3 = 9 \neq 6 = \dim_k(KL),$$

we see that $\pi : K \otimes_k L \rightarrow KL$ cannot be an isomorphism.

