

1. Mark the following statements ‘T’ for True or ‘F’ for False. No justification is necessary.

(a) The extension $\mathbb{Q}(\pi^2) \subset \mathbb{Q}(\pi)$ is finite.

True: It is obtained by adjoining π , which is algebraic over $\mathbb{Q}(\pi^2)$, because it is a root of $x^2 - \pi^2$; therefore, the extension is finite.

(b) The extension $\mathbb{Q}(\pi^2) \subset \mathbb{Q}(\pi)$ is normal.

True: The roots of the polynomial $x^2 - \pi^2$ are π and $-\pi$, and both are contained in the extension.

(c) For any field F and any irreducible polynomial $P \in F[x]$, all roots of P in \overline{F} are simple.

False: This is only true if P is separable, which is not necessarily the case.

(d) The Galois group of a simple normal extension of fields is a simple group.

False: Any finite normal extension is simple (by the Primitive Element Theorem), but its Galois group need not be simple. For instance, one can check that $\mathbb{Q}(\sqrt{2} + \sqrt{-1}) = \mathbb{Q}(\sqrt{2}, \sqrt{-1})$; as we saw, its Galois group over \mathbb{Q} equals $\mathbb{Z}_2 \times \mathbb{Z}_2$, which is not a simple group.

(e) If A is a square matrix with real entries and $z = a + bi \in \mathbb{C}$ is an eigenvalue of A , then $\bar{z} = a - ib \in \mathbb{C}$ also is an eigenvalue of A .

True: if z is an eigenvalue, it is a root of the characteristic polynomial $p(x) = \det(xI - A) \in \mathbb{R}[x]$. But if z is a root of $p(x)$, then so is \bar{z} : roots of a polynomial with real coefficients come in conjugate pairs.

2. The equation $x^3 + x + 1 = 0$, $x \in \mathbb{R}$ has exactly one solution $\alpha \in \mathbb{R}$, which is irrational (you do not need to prove it). Consider $E = \mathbb{Q}(\alpha)$.

(a) Find $[E : \mathbb{Q}]$. (Some justification is required for full credit).

Clearly, the polynomial $x^3 + x + 1$ is irreducible over \mathbb{Q} . Indeed, if a cubic polynomial is reducible, one of its factors must be linear, so that it has a rational root. However, $x^3 + x + 1$ has no rational roots. Therefore, $x^3 + x + 1$ is the minimal polynomial of α over \mathbb{Q} . This implies $[E : \mathbb{Q}] = \deg(\alpha, \mathbb{Q}) = \deg(x^3 + x + 1) = 3$

(b) Write a basis for E over \mathbb{Q} in terms of α .
 $\{1, \alpha, \alpha^2\}$.

3. Give an example of a field extension $F \supset \mathbb{Z}_p$ that is algebraic, but not finite.

$\overline{\mathbb{Z}_p} \supset \mathbb{Z}_p$. Clearly, $\overline{\mathbb{Z}_p}$ is algebraic over \mathbb{Z}_p (this is part of the definition of an algebraic closure). To show that $\overline{\mathbb{Z}_p}$ is not finite, recall that the finite field $GF(p^n) = \{z \in \overline{\mathbb{Z}_p} : z^{p^n} = z\}$ is an extension of \mathbb{Z}_p of degree

n for any integer n . Therefore, $[\overline{\mathbb{Z}_p} : \mathbb{Z}_p] \geq n$ for any integer n , so $\overline{\mathbb{Z}_p}$ is an infinite extension.

4. A 3×3 matrix A has only two eigenvalues in \mathbb{R} : 0 and 1.

(a) What is the characteristic polynomial of A (two answers)?

The characteristic polynomial $p(x)$ is a monic polynomial of degree

3. The only roots of $p(x)$ in \mathbb{R} are 0 and 1. This means that $p(x) = x^2(x-1)$ or $p(x) = x(x-1)^2$.

(b) Compute $A^2(A-I)^2$.

From part (a), $p(x) | x^2(x-1)^2$; so the Cayley-Hamilton Theorem implies $A^2(A-I)^2 = 0$.

(c) Write the Jordan form of A (there are four significantly different answers).

There are two possibilities for $p(x)$; it is easy to see that the minimal polynomial is either $x(x-1)$ or $p(x)$. This leaves four possibilities for the Jordan form:

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

5. Let $E = \mathbb{Q}(\alpha)$ be the extension from Problem 2: so $\alpha \in \mathbb{R}$ is the unique real root of $x^3 + x + 1$ (you can use the fact that α is irrational).

(a) Is the extension $E \supset \mathbb{Q}$ normal?

No. As we saw, $x^3 + x + 1$ is the minimal polynomial of α over \mathbb{Q} , so E is normal if and only if all roots of $x^3 + x + 1$ are contained in E (since $E \supset \mathbb{Q}\alpha$ is separable, we only need to check it is a splitting field). However, α is the only real root of $x^3 + x + 1$; the other two roots are complex numbers that cannot belong to E .

(b) Let K be the splitting field of $x^3 + x + 1$ over \mathbb{Q} . Find $[K : \mathbb{Q}]$.

$[K : \mathbb{Q}] = 6$. Indeed, $K = \mathbb{Q}(\alpha, \beta, \gamma)$, where $\alpha, \beta, \gamma \in \mathbb{C}$ are the roots of $x^3 + x + 1$. As we saw, $E = \mathbb{Q}(\alpha)$ has degree 3 over \mathbb{Q} . Also, $\deg(\beta, E) = 2$: it cannot be more, because β is a root of $\frac{x^3+x+1}{x-\alpha} \in E[x]$, and it cannot be less, because $\beta \notin E$. Besides, $\gamma \in \mathbb{Q}(\alpha, \beta)$; actually, one easily sees from $(x-\alpha)(x-\beta)(x-\gamma) = x^3+x+1$ that $\alpha+\beta+\gamma = 0$. So we see that $K = \mathbb{Q}(\alpha, \beta)$ has degree $3 \cdot 2 = 6$.

6. Prove that the splitting fields of

$$(x^{p^2} - x)(x^{p^3} - x) \in \mathbb{Z}_p[x]$$

and

$$x^{p^6} - x \in \mathbb{Z}_p[x]$$

over \mathbb{Z}_p coincide. Here p is a prime number.

The roots of $x^{p^6} - x$ are exactly the elements of $GF(p^6)$, so this is the splitting field of $x^{p^6} - x$. Similarly, the roots of $(x^{p^2} - x)(x^{p^3} - x)$ are the elements of $GF(p^2)$ and the elements of $GF(p^3)$, so its splitting field is the smallest extension of \mathbb{Z}_p that contains both $GF(p^2)$ and $GF(p^3)$. However, all finite extensions of \mathbb{Z}_p are of the form $E = GF(p^k)$, and E contains $GF(p^2)$ if and only if k is even. Similarly, E contains $GF(p^3)$ if and only if k is divisible by 3. Thus the smallest such E is $GF(p^6)$.

7. Let $\mathbb{Q}(\alpha) \supset \mathbb{Q}$ be a normal extension whose Galois group $G(\mathbb{Q}(\alpha)/\mathbb{Q}) = \{id, \phi, \phi^2, \phi^3\}$ is the cyclic group of order 4 generated by $\phi : \mathbb{Q}(\alpha) \rightarrow \mathbb{Q}(\alpha)$.

(a) Prove that the minimal polynomial of α over \mathbb{Q} is $(x - \alpha)(x - \phi(\alpha))(x - \phi^2(\alpha))(x - \phi^3(\alpha))$.

As $\mathbb{Q}(\alpha) \supset \mathbb{Q}$ is normal, its degree is the order of its Galois group, i.e., 4. Therefore, the minimal polynomial of α must be quartic. Its roots are the conjugates of α , which are exactly the images of α under maps $\mathbb{Q}(\alpha) \rightarrow \mathbb{Q}(\alpha)$. This implies the formula.

(b) Show that there is exactly one subfield $E \subset \mathbb{Q}(\alpha)$ such that $E \neq \mathbb{Q}(\alpha)$, $E \neq \mathbb{Q}$.

By the Galois Theory, such E corresponds to a proper subgroup $H \subset G(\mathbb{Q}(\alpha)/\mathbb{Q})$. Such a subgroup cannot contain ϕ , because then it contains all powers of ϕ , and so coincides with $G(\mathbb{Q}(\alpha)/\mathbb{Q})$. For the same reason, it cannot contain $\phi^3 = \phi^{-1}$. The only proper subgroup is $H = \{id, \phi^2\}$; the field E is then the fixed field of this group, i.e., $E = \{x \in \mathbb{Q}(\alpha) : \phi^2(x) = x\}$.

(c) Show that $\beta = \alpha + \phi^2(\alpha)$ and $\gamma = \alpha \times \phi^2(\alpha)$ belong to E (in fact, $E = \mathbb{Q}(\beta, \gamma)$, but you do not need to prove it).

By part (b), we need to verify that $\phi^2(\beta) = \beta$ and $\phi^2(\gamma) = \gamma$. But this is obvious; for instance,

$$\phi^2(\beta) = \phi^2(\alpha + \phi^2(\alpha)) = \phi^2(\alpha) + \phi^4(\alpha) = \phi^2(\alpha) + \alpha = \beta.$$

Additional practice problems

8. Find the smallest normal extension of \mathbb{Q} that contains $\sqrt{1 + \sqrt{2}}$.

Clearly, this field must contain \mathbb{Q} and $\sqrt{1 + \sqrt{2}}$. Since it is normal over \mathbb{Q} , it must also contain all conjugates of $\sqrt{1 + \sqrt{2}}$. Thus, the field is $\mathbb{Q}(\sqrt{1 + \sqrt{2}}, \sqrt{1 - \sqrt{2}})$ (we do not have to adjoin the other two conjugates, $-\sqrt{1 + \sqrt{2}}$ and $-\sqrt{1 - \sqrt{2}}$, because they already belong to the field).

9. How many elements are there in the Galois group of $x^4 - 5x^2 + 6$ over \mathbb{Q} (the Galois group of $P \in F[x]$ over F is the Galois group of its splitting field)?

To find the splitting field, we need to find the roots of the polynomial. Since $x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3)$, the roots of the polynomial are $\pm\sqrt{2}$ and $\pm\sqrt{3}$, so the splitting field is $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Its degree over \mathbb{Q} equals 4 (because $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ and $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$), so the number of elements in the Galois group is also 4.

10. Let $E \supset F$ be a finite normal extension. Is it true that E is the splitting field of some polynomial $P \in F[x]$ over F ?

Yes. By the Primitive Element Theorem, $E = F(\alpha)$ for some $\alpha \in E$. Let $P = \text{irr}(\alpha, F)$ be the minimal polynomial of α over F . As E is normal, all roots of P belong to E , and so E is the splitting field of P . (The Primitive Element Theorem is necessary only if you want P to be irreducible; if this is not required, this is one of the homework problems).

11. Give an example of three fields $K \supset E \supset F$ such that K is a splitting field over E , E is a splitting field over F , but K is not a splitting field over F .

$$K = \mathbb{Q}(\sqrt{1 + \sqrt{2}}), E = \mathbb{Q}(\sqrt{2}), \text{ and } F = \mathbb{Q}.$$

12. Give an example of an irreducible polynomial $P \in \mathbb{Q}[x]$ whose Galois group is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ (hint: start with the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \supset \mathbb{Q}$).

Set $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. We know from the class that $G(E/\mathbb{Q}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ (see also Problem 4). So we only need to find a polynomial whose splitting field equals E . We saw that $E = \mathbb{Q}(\sqrt{2} + \sqrt{3})$, so E is the splitting field of the minimal polynomial of $\sqrt{2} + \sqrt{3}$, which equals $(x^2 - 5)^2 - 24$.

13. Is the Galois group of $x^4 - 2x^2 - 1$ over \mathbb{Q} abelian? How many elements does it have?

The roots of the polynomial $x^4 - 2x^2 - 1 = (x^2 - 1)^2 - 2$ are $\pm\sqrt{1 \pm \sqrt{2}}$; its splitting field is $K = \mathbb{Q}(\sqrt{1 + \sqrt{2}}, \sqrt{1 - \sqrt{2}})$ (see Problem 8). Thus, K is obtained from \mathbb{Q} by first adjoining $\sqrt{2}$, and then adjoining the square roots of $\alpha = 1 + \sqrt{2}$ and $\beta = 1 - \sqrt{2}$. It is clear from this description that $[K : \mathbb{Q}] = 8$, so the Galois group has 8 elements. Let us describe all elements in the Galois group.

First of all, $\phi : K \rightarrow K$ is determined by $a = \phi(\sqrt{\alpha})$ and $b = \phi(\sqrt{\beta})$. Since α and β are conjugate, there are two cases: either $\phi(\alpha) = \alpha$ and $\phi(\beta) = \beta$, or $\phi(\alpha) = \beta$ and $\phi(\beta) = \alpha$. In the former case, there are four possibilities: $a = \pm\sqrt{\alpha}$ and $b = \pm\sqrt{\beta}$, while in the latter, $a = \pm\sqrt{\beta}$ and

$b = \pm\sqrt{\alpha}$. Since we must have eight automorphisms, all of these possibilities correspond to actual homomorphisms. Now it is easy to see that $G(K/\mathbb{Q})$ is not abelian. For example, take $\phi, \psi \in G(K/E)$ such that ϕ satisfies $\phi(\sqrt{\alpha}) = -\sqrt{\alpha}$, $\phi(\sqrt{\beta}) = \beta$ and ψ satisfies $\psi(\sqrt{\alpha}) = \sqrt{\beta}$, $\psi(\sqrt{\beta}) = \sqrt{\alpha}$; then $\phi(\psi(\alpha)) = \beta$ and $\psi(\phi(\alpha)) = -\beta$.

14. Let E be the splitting field of a polynomial $P \in F[x]$ over F . Suppose that $[E : F] = (\deg(P))!$; show that P is irreducible.

Let $\alpha_1, \dots, \alpha_n$ be the roots of P , where $n = \deg(P)$. Then $E = F(\alpha_1, \dots, \alpha_n) = F(\alpha_1)(\alpha_2) \dots (\alpha_n)$. notice that $\deg(\alpha_1, F) \leq n$ with equality if and only if P is irreducible. Over $F(\alpha_1)$, P splits as $(x - \alpha_1)Q(x)$, where $Q \in (F(\alpha_1))[x]$ has degree $n - 1$. So $\deg(\alpha_2, F(\alpha_1)) \leq n - 1$ with equality iff Q is irreducible. Similarly, $\deg(\alpha_3, F(\alpha_1, \alpha_2)) \leq n - 2$, and so on. Finally, $[E : F] = [F(\alpha_1) : F][F(\alpha_1, \alpha_2) : F(\alpha_1)] \dots = \deg(\alpha_1, F) \deg(\alpha_2, F(\alpha_1)) \dots \leq n(n - 1) \dots = n!$. Notice that the equality only happens if all polynomials $P(x)$, $Q(x)$ (and so on) are irreducible.

Remark: There's another proof that uses the Galois Theory. It is a more elegant, but it only works for separable polynomials.

15. F is a field with algebraic closure \overline{F} . You are told that $F(\alpha)$ and $F(\beta)$ are splitting fields over F , where $\alpha, \beta \in \overline{F}$. Prove that $F(\alpha, \beta)$ is also a splitting field over F .

E is a splitting field over F if and only if any embedding $\phi : E \rightarrow \overline{F}$ with $\phi|_F = id$ satisfies $\phi(E) = E$. If we have a homomorphism $\phi : F(\alpha, \beta) \rightarrow \overline{F}$ that fixes F , we have $\phi(F(\alpha, \beta)) = F(\phi(\alpha), \phi(\beta))$. But $F(\phi(\alpha)) = F(\alpha)$ (because $F(\alpha)$ is a splitting field) and similarly $F(\phi(\beta)) = F(\beta)$, this implies $F(\phi(\alpha), \phi(\beta)) = F(\alpha, \beta)$.

Another way to prove it: set $P(x) = irr(\alpha, F)$, $Q(x) = irr(\beta, F)$. Then $F(\alpha)$ is the splitting field of P (it contains α and all its conjugates), $F(\beta)$ is the splitting field of Q , and $F(\alpha, \beta)$ is the splitting field of $\{P(x), Q(x)\}$ (or if you prefer, the splitting field of $P(x)Q(x) \in F[x]$).

16. Let $E \supset F$ be a finite extension with the property that $E_{G(E/F)} = F$ (that is, the only elements of E that satisfy $\phi(e) = e$ for all automorphisms of E over F are elements of F). Show that E is a splitting field over F . (Hint: for an element $a \in E$, use the polynomial

$$\prod_{\sigma \in G(E/F)} (x - \sigma(a))$$

to prove that all conjugates of a over F are in E . With a little more work, this approach also shows $E \supset F$ is separable.)

Let $P(x) \in E[x]$ be the product of linear polynomials defined above. Let us check that the coefficients of $P(x)$ actually belong to F . By the assumption, we need to check that the coefficients are fixed by all $\phi \in G(E/F)$. But this is almost clear: such ϕ permutes the linear term in the product (so that $(x - \sigma(a))$ becomes $(x - (\phi \circ \sigma)(a))$), and the product does not change. Thus, $P \in F[x]$. Now we notice that all conjugates of a must be roots of P ; since all roots of P belong to E , this implies the statement.