School of Mathematics and Statistics

MT5836 Galois Theory

Problem Sheet III: Splitting Fields and Normal Extensions (Solutions)

1. **For each of the following polynomials $f(X)$ and given base field F, determine the splitting field K of $f(X)$ over F and calculate the degree $|K : F|$ of the extension:**

   (a) $X^2 + 1$ **over** $\mathbb{Q}$;
   (b) $X^2 + 1$ **over** $\mathbb{R}$;
   (c) $X^2 - 4$ **over** $\mathbb{Q}$;
   (d) $X^4 + 4$ **over** $\mathbb{Q}$;
   (e) $X^4 - 1$ **over** $\mathbb{Q}$;
   (f) $X^4 + 1$ **over** $\mathbb{Q}$;
   (g) $X^6 - 1$ **over** $\mathbb{Q}$;
   (h) $X^6 + 1$ **over** $\mathbb{Q}$;
   (i) $X^6 - 27$ **over** $\mathbb{Q}$.

Solution: (a) The roots of X^2+1 in $\mathbb{C}$ are $\pm i$. Since $-i \in \mathbb{Q}(i)$, we conclude the splitting field of $X^2 + 1$ over $\mathbb{Q}$ is $\mathbb{Q}(i)$.

The minimum polynomial of i over $\mathbb{Q}$ is $X^2 + 1$, since this polynomial cannot factorize over $\mathbb{Q}$ as it has no roots in $\mathbb{Q}$. Hence the degree is

$$|\mathbb{Q}(i) : \mathbb{Q}| = 2.$$

(b) Again the roots of $X^2 + 1$ in $\mathbb{C}$ are $\pm i$ and we conclude the splitting field of $X^2 + 1$ over $\mathbb{R}$ is $\mathbb{R}(i)$; that is, $\mathbb{C}$ (as every element in $\mathbb{C}$ is an $\mathbb{R}$-linear combination of 1 and i). Hence the degree of the extension is

$$|\mathbb{C} : \mathbb{R}| = 2,$$

as we already know (or using the fact that the minimum polynomial of i over $\mathbb{R}$ is X^2+1).

(c) The roots of $X^2 - 4$ are ± 2, both of which belong to $\mathbb{Q}$. Hence the splitting field of $X^2 - 4$ over $\mathbb{Q}$ is $\mathbb{Q}$ and the degree of the extension is

$$|\mathbb{Q} : \mathbb{Q}| = 1.$$

(d) Note that

$$\left(\sqrt{2}\,\mathrm{e}^{\pi i/4}\right)^4 = 2^2\,\mathrm{e}^{\pi i} = -4,$$

so $\left(\sqrt{2}\,\mathrm{e}^{\pi i/4}\right)^4 + 4 = 0$. We conclude that the roots of $X^4 + 4$ over $\mathbb{Q}$ are

$$\sqrt{2}\,\mathrm{e}^{\pi i/4}, \quad \sqrt{2}\,\mathrm{e}^{3\pi i/4}, \quad \sqrt{2}\,\mathrm{e}^{5\pi i/4}, \quad \sqrt{2}\,\mathrm{e}^{7\pi i/4}.$$

Moreover

$$\sqrt{2}\,\mathrm{e}^{\pi i/4} = \sqrt{2}\left(\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}\,i\right) = 1 + i$$

and similarly for the other roots, so we conclude the four roots of $X^4 + 4$ in $\mathbb{C}$ are

$$\pm 1 \pm i.$$

From this we conclude that the splitting field of $X^4 + 4$ over $\mathbb{Q}$ is $\mathbb{Q}(i)$, since $i = (1 + i) - 1$ belongs to the field obtained by adjoining $\pm 1 \pm i$ to $\mathbb{Q}$. The degree of the extension is

$$|\mathbb{Q}(i) : \mathbb{Q}| = 2,$$

as the minimum polynomial of i over $\mathbb{Q}$ is $X^2 + 1$.

(e)

$$X^4 - 1 = (X^2 - 1)(X^2 + 1) = (X - 1)(X + 1)(X^2 + 1),$$

and the roots of $X^2 + 1$ are $\pm i$. Hence the splitting field of $X^4 - 1$ over $\mathbb{Q}$ is $\mathbb{Q}(i)$ and the degree is

$$|\mathbb{Q}(i) : \mathbb{Q}| = 2.$$

(f) The roots of $f(X) = X^4 + 1$ in $\mathbb{C}$ are $\mathrm{e}^{\pi i/4}$, $\mathrm{e}^{3\pi i/4}$, $\mathrm{e}^{5\pi i/4}$ and $\mathrm{e}^{7\pi i/4}$. Note that the second, third and fourth roots are powers of $\mathrm{e}^{\pi i/4}$, so the splitting field of $X^4 + 1$ over $\mathbb{Q}$ is $\mathbb{Q}(\mathrm{e}^{\pi i/4})$.

Observe

$$\begin{aligned} f(X + 1) &= (X + 1)^4 + 1 \\ &= X^4 + 4X^3 + 6X^2 + 4X + 2, \end{aligned}$$

which is irreducible over $\mathbb{Q}$ by Eisenstein's Criterion (with $p = 2$). Hence $f(X) = X^4 + 1$ is irreducible over $\mathbb{Q}$ and this is therefore the minimum polynomial of $\mathrm{e}^{\pi i/4}$ over $\mathbb{Q}$. Thus the degree of the extension is

$$|\mathbb{Q}(\mathrm{e}^{\pi i/4}) : \mathbb{Q}| = 4.$$

(g) The roots of $X^6 - 1$ in $\mathbb{C}$ are

$$\mathrm{e}^{\pi i/3}, \quad \mathrm{e}^{2\pi i/3}, \quad \mathrm{e}^{\pi i} = -1, \quad \mathrm{e}^{4\pi i/3}, \quad \mathrm{e}^{5\pi i/3}, \quad \mathrm{e}^{\pi i} = 1,$$

each of which is a power of $\mathrm{e}^{\pi i/3}$, so the splitting field of $X^6 - 1$ over $\mathbb{Q}$ is $\mathbb{Q}(\mathrm{e}^{\pi i/3})$. Note that $X^6 - 1$ factorizes as

$$\begin{aligned} X^6 - 1 &= (X^3 - 1)(X^3 + 1) \\ &= (X - 1)(X^2 + X + 1)(X + 1)(X^2 - X + 1). \end{aligned}$$

Also $(\mathrm{e}^{\pi i/3})^3 = \mathrm{e}^{\pi i} = -1$, so $\mathrm{e}^{\pi i/3}$ is a root of $X^3 + 1 = (X + 1)(X^2 - X + 1)$ and hence $\mathrm{e}^{\pi i/3}$ is a root of $X^2 - X + 1$. This quadratic polynomial is irreducible over $\mathbb{Q}$, since its roots are complex (non-real) and so it has no linear factors in $\mathbb{Q}[X]$. Thus $X^2 - X + 1$ is the minimum polynomial of $\mathrm{e}^{\pi i/3}$ over $\mathbb{Q}$ and the degree of the extension is

$$|\mathbb{Q}(\mathrm{e}^{\pi i/3}) : \mathbb{Q}| = 2.$$

(h) The roots of $X^6 + 1$ in $\mathbb{C}$ are

$$\mathrm{e}^{\pi i/6}, \quad \mathrm{e}^{\pi i/2} = i, \quad \mathrm{e}^{5\pi i/6}, \quad \mathrm{e}^{7\pi i/6}, \quad \mathrm{e}^{3\pi i/2} = -i, \quad \mathrm{e}^{11\pi i/6},$$

each of which is a power of $\mathrm{e}^{\pi i/6}$, so the splitting field of $X^6 + 1$ over $\mathbb{Q}$ is $\mathbb{Q}(\mathrm{e}^{\pi i/6})$. Note that $X^6 + 1$ factorizes as

$$X^6 + 1 = (X^2 + 1)(X^4 - X^2 + 1).$$

The roots of the first factor are $\pm i$, so $e^{\pi i/6}$ is a root of $f(X) = X^4 - X^2 + 1$. The roots of $f(X)$ are all complex (non-real) numbers, so $f(X)$ has no linear factors over $\mathbb{Q}$. Hence if $f(X)$ were reducible over $\mathbb{Q}$, then it would be reducible over $\mathbb{Z}$, by Gauss's Lemma, so would factorize as a product of two quadratic polynomials

$$X^4 - X^2 + 1 = (X^2 + \alpha X + \beta)(X^2 + \gamma X + \delta)$$

where $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$. Then

$$\alpha + \gamma = 0, \qquad \alpha\gamma + \beta + \delta = -1,$$
$$\alpha\delta + \beta\gamma = 0, \qquad \beta\delta = 1.$$

The fourth equation tells us $\beta = \delta = \pm 1$, while the first tells us $\gamma = -\alpha$. Hence the second equation gives $-\alpha^2 + 2\beta = -1$; that is,

$$\alpha^2 = 2\beta + 1 = -1 \text{ or } 3.$$

This is impossible for $\alpha \in \mathbb{Z}$. In conclusion, $X^4 - X^2 + 1$ is irreducible over $\mathbb{Q}$, so is the minimum polynomial of $e^{\pi i/6}$ over $\mathbb{Q}$. Hence the degree of the extension is

$$|\mathbb{Q}(e^{\pi i/6}) : \mathbb{Q}| = 4.$$

(i) Note $(\sqrt{3})^6 = 3^3 = 27$, so multiplying the roots from part (g) by $\sqrt{3}$ we conclude the roots of $X^6 - 27$ in $\mathbb{C}$ are

$$\sqrt{3}, \quad \sqrt{3}\,e^{\pi i/3}, \quad \sqrt{3}\,e^{2\pi i/3}, \quad -\sqrt{3}, \quad \sqrt{3}\,e^{4\pi i/3}, \quad \sqrt{3}\,e^{5\pi i/3}.$$

Since $e^{\pi i/3}$ is the quotient of the second by the first, we conclude the splitting field of $X^6 - 27$ over $\mathbb{Q}$ is

$$\mathbb{Q}(\sqrt{3}, e^{\pi i/3}).$$

Now $|\mathbb{Q}(\sqrt{3}) : \mathbb{Q}| = 2$ because $X^2 - 3$ is irreducible over $\mathbb{Q}$ by Eisenstein's Criterion and hence is the minimum polynomial of $\sqrt{3}$ over $\mathbb{Q}$. Furthermore, $e^{\pi i/3}$ is a root of $X^2 - X + 1$, as observed in part (g), and this does not factorize into linear factors over $\mathbb{Q}(\sqrt{3})$ as its roots are complex (non-real). Hence $X^2 - X + 1$ is irreducible over $\mathbb{Q}(\sqrt{3})$ and is the minimum polynomial of $e^{\pi i/3}$ over $\mathbb{Q}(\sqrt{3})$. Thus

$$|\mathbb{Q}(\sqrt{3}, e^{\pi i/3}) : \mathbb{Q}(\sqrt{3})| = 2$$

and, by an application of the Tower Law, the degree of our splitting field is

$$|\mathbb{Q}(\sqrt{3}, e^{\pi i/3}) : \mathbb{Q}| = 4.$$

2. **For each of the following polynomials $f(X)$ and given base field F, determine the degree of the splitting field of $f(X)$ over F:**

   (a) $X^3 - 2$ over $\mathbb{F}_5$;

   (b) $X^3 - 3$ over $\mathbb{F}_{13}$.

Solution: (a) We first check for roots of $f(X) = X^3 - 2$ in $\mathbb{F}_5$. Observe

$$f(0) = -2 = 3, \qquad f(1) = -1 = 4$$
$$f(2) = 1 \qquad f(3) = 0$$
$$f(4) = 2.$$

Hence $f(X)$ has a root, namely 3, in $\mathbb{F}_5$ and therefore has a linear factor. By dividing, we then obtain a factorization

$$f(X) = X^3 - 2 = (X - 3)(X^2 + 3X - 1).$$

Let $g(X) = X^2 + 3X - 1$. Observe

$$g(3) = 2$$

while $g(a) \neq 0$ for $a = 0$, 1, 2 and 4, as we know $f(a) \neq 0$ for such a. Hence $g(X)$ has no roots in $\mathbb{F}_5$ and therefore this quadratic polynomial is irreducible over $\mathbb{F}_5$.

Let α be a root of $g(X)$ in some extension field. Then $g(X)$ has a root in $\mathbb{F}_5(\alpha)$ and therefore factorizes as a product of two linear polynomials over $\mathbb{F}_5(\alpha)$. Hence the splitting field of $f(X)$ over $\mathbb{F}_5$ is $\mathbb{F}_5(\alpha)$ and

$$|\mathbb{F}_5(\alpha) : \mathbb{F}_5| = \deg g(X) = 2,$$

as $g(X)$ is the minimum polynomial of α over $\mathbb{F}_5$.

(b) We first calculate all cubes in $\mathbb{F}_{13}$:

$$0^3 = 0, \qquad 1^3 = 1,$$
$$2^3 = 8, \qquad 3^3 = 1,$$
$$4^3 = 12, \qquad 5^3 = 8,$$
$$6^3 = 8, \qquad 7^3 = 5,$$
$$8^3 = 5, \qquad 9^3 = 1,$$
$$10^3 = 12, \qquad 11^3 = 5,$$
$$12^3 = 12.$$

Since $a^3 \neq 3$ for all $a \in \mathbb{F}_{13}$, we conclude that $X^3 - 3$ has no roots in $\mathbb{F}_{13}$, hence no linear factors over $\mathbb{F}_{13}$, and therefore $X^3 - 3$ is irreducible over $\mathbb{F}_{13}$.

Let α be a root of $X^3 - 3$ in some extension. Thus $\alpha^3 = 3$. Now using the above calculation of cubes,

$$(3\alpha)^3 = 3^3\alpha^3 = \alpha^3 = 3$$

and

$$(9\alpha)^3 = 9^3\alpha^3 = \alpha^3 = 3.$$

Hence $X^3 - 3$ has three roots in the extension $\mathbb{F}_{13}(\alpha)$, namely α, 3α and 9α. Note these are distinct since $\alpha \neq 0$ and 1, 3 and 9 are distinct in $\mathbb{F}_{13}$. Thus $X^3 - 3$ splits over $\mathbb{F}_{13}(\alpha)$ as

$$X^3 - 3 = (X - \alpha)(X - 3\alpha)(X - 9\alpha).$$

Thus $\mathbb{F}_{13}(\alpha)$ is the splitting field of $X^3 - 3$ over $\mathbb{F}_{13}$ and the degree is

$$|\mathbb{F}_{13}(\alpha) : \mathbb{F}_{13}| = 3,$$

since $X^3 - 3$ is the minimum polynomial of α over $\mathbb{F}_{13}$.

3. **Let p be a prime and $f(X) = X^p - 2$. Find the splitting field of $f(X)$ over $\mathbb{Q}$ and show that the degree of this extension is $p(p-1)$.**

Solution: The roots of $X^p - 2$ in $\mathbb{C}$ are the complex pth roots of 2:

$$\sqrt[p]{2}, \quad \sqrt[p]{2}\,\omega, \quad \sqrt[p]{2}\,\omega^2, \quad \dots, \quad \sqrt[p]{2}\,\omega^{p-1}$$

where $\omega = \mathrm{e}^{2\pi i/p}$. Since ω is the quotient of the second root by the first, we conclude that splitting field of $X^p - 2$ over $\mathbb{Q}$ is

$$\mathbb{Q}(\sqrt[p]{2}, \omega)$$

where $\omega = \mathrm{e}^{2\pi i/p}$.

Now $X^p - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein's Criterion. Hence this is the minimum polynomial of $\sqrt[p]{2}$ over $\mathbb{Q}$ and therefore

$$|\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}| = p.$$

Since $X^p - 1 = (X-1)(X^{p-1} + X^{p-2} + \dots + X + 1)$, we see ω is a root of $X^{p-1} + X^{p-2} + \dots + X + 1$ and we know this polynomial is irreducible over $\mathbb{Q}$. Hence this is the minimum polynomial of ω over $\mathbb{Q}$ and

$$|\mathbb{Q}(\omega) : \mathbb{Q}| = p - 1.$$

Since $\mathbb{Q}(\sqrt[p]{2}, \omega)$ contains both $\mathbb{Q}(\sqrt[p]{2})$ and $\mathbb{Q}(\omega)$, by two applications of the Tower Law,

$$|\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}| = p \qquad \text{and} \qquad |\mathbb{Q}(\omega) : \mathbb{Q}| = p - 1$$

both divide $|\mathbb{Q}(\sqrt[p]{2}, \omega) : \mathbb{Q}|$. Since these are coprime, we conclude $|\mathbb{Q}(\sqrt[p]{2}, \omega) : \mathbb{Q}|$ is divisible by $p(p-1)$, so

$$|\mathbb{Q}(\sqrt[p]{2}, \omega) : \mathbb{Q}| \geqslant p(p-1).$$

On the other hand, certainly ω is a root of $X^{p-1} + X^{p-2} + \dots + X + 1$, so the minimum polynomial of ω over $\mathbb{Q}(\sqrt[p]{2})$ has degree at most $p - 1$. Thus, by the Tower Law,

$$\begin{aligned} |\mathbb{Q}(\sqrt[p]{2}, \omega) : \mathbb{Q}| &= |\mathbb{Q}(\sqrt[p]{2}, \omega) : \mathbb{Q}(\sqrt[p]{2})| \cdot |\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}| \\ &\leqslant (p-1)p. \end{aligned}$$

Putting this together, we now conclude the degree of the splitting field $\mathbb{Q}(\sqrt[p]{2}, \omega)$ over $\mathbb{Q}$ is indeed

$$|\mathbb{Q}(\sqrt[p]{2}, \omega) : \mathbb{Q}| = p(p-1).$$

4. **Let $f(X)$ be a polynomial over a field F and let K be the splitting field of $f(X)$ over F. If L is an intermediate field (that is, $F \subseteq L \subseteq K$), show that K is the splitting field of $f(X)$ over L.**

Solution: Let α_1, α_2, …, α_n be the roots of $f(X)$ in the splitting field K. Then necessarily

$$K = F(\alpha_1, \alpha_2, \dots, \alpha_n).$$

Now the splitting field of $f(X)$ over L is obtained by adjoining the roots α_1, α_2, …, α_n to L; that is, it is

$$L(\alpha_1, \alpha_2, \dots, \alpha_n).$$

Note $L \subseteq K$ and $\alpha_1, \alpha_2, \dots, \alpha_n \in K$. Hence

$$\begin{aligned} K &= F(\alpha_1, \alpha_2, \dots, \alpha_n) \\ &\subseteq L(\alpha_1, \alpha_2, \dots, \alpha_n) \\ &\subseteq K \end{aligned}$$

and we conclude $K = L(\alpha_1, \alpha_2, \dots, \alpha_n)$; that is, K is the splitting field of $f(X)$ over L.

5. **Let ϕ be an automorphism of a field F. Show that the set of fixed-points of ϕ,**

$$\mathbf{Fix}_F(\phi) = \{\, a \in F \mid a\phi = a \,\},$$

is a subfield of F. Hence deduce that ϕ is a P-isomorphism where P is the prime subfield of F.

Solution: Since ϕ is, in particular, a homomorphism $(F,+) \to (F,+)$ of the additive group of F, it must map the additive identity to itself:

$$0\phi = 0.$$

Similarly, ϕ induces a homomorphism $F^* \to F^*$ of the multiplicative group, so it maps the multiplicative identity to itself:

$$1\phi = 1.$$

Hence $0, 1 \in \mathrm{Fix}_F(\phi)$.

Now let $a, b \in \mathrm{Fix}_F(\phi)$. Then, as ϕ is a homomorphism $F \to F$ of the field,

$$\begin{aligned}(a+b)\phi &= a\phi + b\phi = a + b,\\ (ab)\phi &= (a\phi)(b\phi) = ab,\\ (-a)\phi &= -a\phi = -a,\end{aligned}$$

and, if $a \neq 0$,

$$(1/a)\phi = 1/(a\phi) = 1/a.$$

Hence $\mathrm{Fix}_F(\phi)$ is closed under addition, multiplication, subtraction and under division by non-zero elements.

In conclusion, $\mathrm{Fix}_F(\phi)$ is a subfield of F.

Now consider the prime subfield P of F. Since P is contained in all subfields of F,

$$P \subseteq \mathrm{Fix}_F(\phi);$$

that is,

$$a\phi = a \qquad \text{for all } a \in P.$$

Hence ϕ is a P-automorphism of F.

6. **(a) Determine all automorphisms of $\mathbb{Q}$.**
   (b) Determine all automorphisms of $\mathbb{Q}(\sqrt{2})$.
   (c) Determine all $\mathbb{Q}$-automorphisms of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.
   (d) Show that the only automorphism of $\mathbb{R}$ is the identity.

Solution: (a) By Question 5, if ϕ is an automorphism of $\mathbb{Q}$, then it must fix all elements in the prime subfield; that is,

$$a\phi = a \qquad \text{for all } a \in \mathbb{Q}.$$

Hence the identity map is the only automorphism of $\mathbb{Q}$.

(b) Consider any automorphism ψ of $\mathbb{Q}(\sqrt{2})$. It must first fix all points in the prime subfield $\mathbb{Q}$, by Question 5:

$$a\psi = a \qquad \text{for all } a \in \mathbb{Q}.$$

Also $\sqrt{2}$ is a root of $X^2 - 2$:

$$(\sqrt{2})^2 - 2 = 0.$$

Applying ψ, we conclude

$$(\sqrt{2}\psi)^2 - 2 = 0;$$

that is,

$$\sqrt{2}\psi = \pm\sqrt{2}.$$

The effect of ψ is now determined: Since $\{1, \sqrt{2}\}$ is a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$, every element of $\mathbb{Q}(\sqrt{2})$ can be uniquely expressed as $a + b\sqrt{2}$ with $a, b \in \mathbb{Q}$ and, for such an element,

$$(a + b\sqrt{2})\psi = a + b(\sqrt{2}\psi).$$

Thus any automorphism ψ of $\mathbb{Q}$ is determined by whether $\sqrt{2}\psi = \sqrt{2}$ or $\sqrt{2}\psi = -\sqrt{2}$. We conclude that there are at most two automorphisms of $\mathbb{Q}(\sqrt{2})$.

On the other hand, if $\beta = \pm\sqrt{2}$, then we can extend the identity map $\mathbb{Q} \to \mathbb{Q}$ to an isomorphism $\psi\colon \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\beta)$ that maps $\sqrt{2}$ to β (by Lemma 3.5 applied to the irreducible polynomial $X^2 - 2$). Note $\mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{2})$ irrespective of whether $\beta = \pm\sqrt{2}$. Hence ψ is an automorphism of $\mathbb{Q}(\sqrt{2})$ and we conclude there are precisely two automorphisms of $\mathbb{Q}(\sqrt{2})$, namely the identity map and the automorphism

$$a + b\sqrt{2} \mapsto a - b\sqrt{2}$$

induced by $\sqrt{2} \mapsto -\sqrt{2}$.

(c) Any automorphism ψ of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ must fix all points in the prime subfield $\mathbb{Q}$ (by Question 5) and, applying ψ to the equations

$$(\sqrt{2})^2 - 2 = 0 \qquad \text{and} \qquad (\sqrt{3})^2 - 3 = 0,$$

it must satisfy $\sqrt{2}\psi = \pm\sqrt{2}$ and $\sqrt{3}\psi = \pm\sqrt{3}$. By use of the Tower Law,

$$|\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}| = 4$$

and $\{1, \sqrt{2}, \sqrt{3}, \sqrt{2}\cdot\sqrt{3}\}$ is a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$. The effect of ψ is now determined:

$$(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\cdot\sqrt{3})\psi = a + b(\sqrt{2}\psi) + c(\sqrt{3}\psi) + d(\sqrt{2}\psi)(\sqrt{3}\psi).$$

We conclude there are at most four automorphisms of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Since $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, the polynomial $f(X) = X^2 - 3$ is irreducible over $\mathbb{Q}(\sqrt{2})$. Consider one of the two automorphisms ϕ of $\mathbb{Q}(\sqrt{2})$ determined in part (b). Note $f^\phi(X) = X^2 - 3 = f(X)$ in the notation of Lemma 3.5. Hence if $\gamma = \pm\sqrt{3}$, we can, by that Lemma, extend ϕ to an isomorphism $\psi\colon \mathbb{Q}(\sqrt{2}, \sqrt{3}) \to \mathbb{Q}(\sqrt{2}, \gamma)$ that maps $\sqrt{3}$ to γ. Note $\mathbb{Q}(\sqrt{2}, \gamma) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, so we conclude that we can construct an automorphism ψ of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ mapping $\sqrt{2}$ to either $\sqrt{2}$ or $-\sqrt{2}$ and mapping $\sqrt{3}$ to either $\sqrt{3}$ or $-\sqrt{3}$.

In conclusion, there are precisely four automorphisms ψ of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ determined by the choices

$$\sqrt{2}\psi = \pm\sqrt{2}, \quad \sqrt{3}\psi = \pm\sqrt{3}.$$

(d) Let ϕ be an automorphism of $\mathbb{R}$. If x is a positive real number, then $x = z^2$ for some non-zero $z \in \mathbb{R}$, so

$$x\phi = (z\phi)^2 > 0.$$

Hence $x > 0$ implies $x\phi > 0$.

Now if $x, y \in \mathbb{R}$ with $x < y$, then by the previous step $y\phi - x\phi = (y - x)\phi > 0$, so $x\phi < y\phi$; that is, ϕ is an increasing function.

Furthermore, by Question 5, $q\phi = q$ for all $q \in \mathbb{Q}$. Let $x \in \mathbb{R}$. If $x\phi \neq x$, then either $x < x\phi$ or $x > x\phi$.

If $x < x\phi$, choose a rational number $q \in \mathbb{Q}$ with $x < q < x\phi$. Then, as ϕ is increasing,

$$x\phi < q\phi = q < x\phi,$$

which is a contradiction. Similarly if $x\phi < x$, choose $q \in \mathbb{Q}$ with $x\phi < q < x$ and then

$$x\phi < q = q\phi < x\phi,$$

which is also a contradiction.

In conclusion, $x\phi = x$ for all $x \in \mathbb{R}$, so ϕ is the identity map.

7. **Suppose that $f(X)$ is an arbitrary polynomial over a field F, K is the splitting field for $f(X)$ over F, and α and β are roots of $f(X)$ in K. Does there exist an automorphism of K that maps α to β?**

Solution: Consider the polynomial $f(X) = X(X-1)$ over $\mathbb{Q}$. It is already a product of linear factors over $\mathbb{Q}$, so the splitting field for $f(X)$ over $\mathbb{Q}$ is $\mathbb{Q}$ itself. The only automorphism of $\mathbb{Q}$ is the identity (by Question 6(a)) and this does not map 0 to 1.

Hence, in general, if $f(X)$ is a polynomial over a field F, with splitting field K, and $\alpha, \beta \in K$ are roots of $f(X)$, there does not necessarily exist an automorphism of K mapping α to β.

8. **Which of the following fields are normal extensions of $\mathbb{Q}$? [As always, justify your answers.]**
   - **(a)** $\mathbb{Q}(\sqrt{2})$;
   - **(b)** $\mathbb{Q}(\sqrt[4]{2})$;
   - **(c)** $\mathbb{Q}(\sqrt{2}, \sqrt{3})$;
   - **(d)** $\mathbb{Q}(\theta)$, **where** $\theta^4 - 10\theta^2 + 1 = 0$.

Solution: (a) The field $\mathbb{Q}(\sqrt{2})$ is the splitting field of $X^2 - 2$ over $\mathbb{Q}$ (as it is obtained by adjoining the roots to $\mathbb{Q}$). Hence $\mathbb{Q}(\sqrt{2})$ is a normal extension of $\mathbb{Q}$.

(b) Consider the polynomial $X^4 - 2$ over $\mathbb{Q}$. It is irreducible over $\mathbb{Q}$, by Eisenstein's Criterion. It also has a root in $\mathbb{Q}(\sqrt[4]{2})$, namely $\sqrt[4]{2}$, but it does not split over $\mathbb{Q}(\sqrt[4]{2})$, since two of the roots of $X^4 - 2$ are complex (non-real) so do not belong to $\mathbb{Q}(\sqrt[4]{2})$.

Hence, by definition, $\mathbb{Q}(\sqrt[4]{2})$ is *not* a normal extension of $\mathbb{Q}$.

(c) The field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is the splitting field of $(X^2 - 2)(X^2 - 3)$ over $\mathbb{Q}$, and hence $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a normal extension of $\mathbb{Q}$.

(d) Let $\varepsilon, \eta \in \{\pm 1\}$. Then

$$\begin{aligned}(\varepsilon\sqrt{2} + \eta\sqrt{3})^2 &= 2 + 2\varepsilon\eta\sqrt{6} + 3 \\ &= 5 + 2\varepsilon\eta\sqrt{6}\end{aligned}$$

and

$$\begin{aligned}(\varepsilon\sqrt{2} + \eta\sqrt{3})^4 &= (5 + 2\varepsilon\eta\sqrt{6})^2 \\ &= 25 + 20\varepsilon\eta\sqrt{6} + 24 \\ &= 49 + 20\varepsilon\eta\sqrt{6}.\end{aligned}$$

Hence

$$\begin{aligned}(\varepsilon\sqrt{2} + \eta\sqrt{3})^4 - 10(\varepsilon\sqrt{2} + \eta\sqrt{3})^2 + 1 &= 49 + 20\varepsilon\eta\sqrt{6} - 50 - 20\varepsilon\eta\sqrt{6} + 1 \\ &= 0.\end{aligned}$$

We conclude that the four roots of $X^4 - 10X^2 + 1$ are $\pm\sqrt{2} \pm \sqrt{3}$. We observed (in Example 2.18 in the lecture notes) that

$$\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

and hence $|\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}| = 4$. Thus the minimum polynomial of $\sqrt{2}+\sqrt{3}$ over $\mathbb{Q}$ is of degree 4 and consequently it must be $X^4 - 10X^2 + 1$. This shows that this polynomial is irreducible over $\mathbb{Q}$. Now if θ is a root of the polynomial, then $|\mathbb{Q}(\theta) : \mathbb{Q}| = 4$ and $\mathbb{Q}(\theta) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ since $\theta = \pm\sqrt{2} \pm \sqrt{3}$. Hence $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, which is a normal extension of $\mathbb{Q}$ by part (c).

9. **Let $F \subseteq K \subseteq L$ be field extensions where L is a finite extension of F. Prove, or give a counterexample, to each of the following assertions:**

   (a) If L is a normal extension of K, then L is a normal extension of F.

   (b) If L is a normal extension of F, then L is a normal extension of K.

   (c) If L is a normal extension of F, then K is a normal extension of F.

Solution: (a) Take $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2})$ and $L = \mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$. Then L is the splitting field of $\sqrt{3}$ over K, so is a normal extension of K. However, L is not a normal extension of F, since $X^3 - 2$ is an irreducible polynomial over $F = \mathbb{Q}$ which has a root $\sqrt[3]{2}$ in L, but does not split over L (as two of the roots of $X^3 - 2$ are complex (non-real)).

[One could, for example, also obtain a counterexample by taking $F = \mathbb{Q}$ and $K = L = \mathbb{Q}(\sqrt[3]{2})$.]

(b) Suppose L is a normal extension of F. Then L is the splitting field of some polynomial $f(X)$ over F. Now the coefficients of $f(X)$ belong to F, so we can view $f(X)$ as a polynomial over K. We obtain L from F by adjoining the roots of $f(X)$ to F, so we also obtain L *from* K by adjoining the roots of $f(X)$ to K; that is, L is also the splitting field for $f(X)$ *over* K. (See also the solution to Question 4.) Hence L is a normal extension of K.

(c) Take $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2})$ and $L = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$. Then L is the splitting field of $X^3 - 2$ over $\mathbb{Q}$, so is a normal extension of $\mathbb{Q}$. On the other hand, K is not a normal extension of $\mathbb{Q}$, since $X^3 - 2$ is an irreducible polynomial over $\mathbb{Q}$ that has a root (namely $\sqrt[3]{2}$) in K, but does not split as its other two roots are complex (non-real).