Galois theory - Problem Set 2

To be solved on Friday 10.02

Problem 1. (Exercise 15.3.2 in the book.) Prove that $\sqrt{2}$ and $\sqrt{3}$ are algebraic over $\mathbb{Q}$. Find the degree of

(a) $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$.

(b) $\mathbb{Q}(\sqrt{3})$ over $\mathbb{Q}$.

(c) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$.

(d) $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ over $\mathbb{Q}$.

Solution. Since $\sqrt{2}$ is a root of $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ and $\sqrt{3}$ is a root of $g(x) = x^2 - 3 \in \mathbb{Q}[x]$, we have that $\sqrt{2}$ and $\sqrt{3}$ are algebraic over $\mathbb{Q}$. Moreover, both of these polynomials are have no root in $\mathbb{Q}$ and so they are irreducible by Lemma 3.4(e). Hence by Theorem 4.6 we have

$$[\mathbb{Q}(\sqrt{2} : \mathbb{Q}] = \deg(f) = 2 \text{ and } [\mathbb{Q}(\sqrt{3} : \mathbb{Q}] = \deg(g) = 2.$$

This solves (a) and (b). For $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$, notice that we have by Example 5.5 that

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

Finally

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

since $\sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$. On the other hand, we have

$$(\sqrt{2}+\sqrt{3})(\sqrt{2}-\sqrt{3}) = 4 - 3 = 1,$$

and so $\sqrt{2}-\sqrt{3} = (\sqrt{2}+\sqrt{3})^{-1} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Then

$$\sqrt{2} = \frac{1}{2}\left(\underbrace{\sqrt{2}+\sqrt{3}}_{\in\mathbb{Q}(\sqrt{2}+\sqrt{3})} + \underbrace{\sqrt{2}-\sqrt{3}}_{\in\mathbb{Q}(\sqrt{2}+\sqrt{3})}\right)$$

and hence $\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Then

$$\sqrt{3} = \underbrace{\sqrt{2}+\sqrt{3}}_{\in\mathbb{Q}(\sqrt{2}+\sqrt{3})} - \underbrace{\sqrt{2}}_{\in\mathbb{Q}(\sqrt{2}+\sqrt{3})}$$

and so $\sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$ as well. Thus $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}+\sqrt{3})$ and we conclude that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$ and so

$$[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4.$$

Problem 2. (Exercise 15.3.4 in the book) Find a suitable number α such that

(a) $\mathbb{Q}(\sqrt{2}, \sqrt{5}) = \mathbb{Q}(\alpha)$.

(b) $\mathbb{Q}(\sqrt{3}, i) = \mathbb{Q}(\alpha)$.

Solution. We first the more general claim if $a, b \in \mathbb{C}$ satisfy $a^2 - b^2 \in \mathbb{Q}$, then $\mathbb{Q}(\sqrt{a}, \sqrt{b}) = \mathbb{Q}(\sqrt{a} + \sqrt{b})$. Since $\sqrt{a} + \sqrt{b} \in \mathbb{Q}(\sqrt{a}, \sqrt{b})$, we have that $\mathbb{Q}(\sqrt{a} + \sqrt{b}) \subseteq \mathbb{Q}(\sqrt{a}, \sqrt{b})$. For the other direction we have

$$(\sqrt{a} + \sqrt{b})(\sqrt{a} - \sqrt{b}) = a^2 - b^2 \in \mathbb{Q}(\alpha)$$

and so

$$(\sqrt{a} - \sqrt{b}) = \frac{a^2 - b^2}{\sqrt{a} - \sqrt{b}} \in \mathbb{Q}(\sqrt{a} + \sqrt{b}).$$

Then

$$\sqrt{a} = \frac{1}{2}\left(\underbrace{\sqrt{a} + \sqrt{b}}_{\in \mathbb{Q}(\sqrt{a}+\sqrt{b})} + \underbrace{\sqrt{a} - \sqrt{b}}_{\in \mathbb{Q}(\sqrt{a}+\sqrt{b})}\right)$$

and hence $\sqrt{a} \in \mathbb{Q}(\sqrt{a} + \sqrt{b})$. Then

$$\sqrt{b} = \underbrace{\sqrt{a} + \sqrt{b}}_{\in \mathbb{Q}(\sqrt{a}+\sqrt{b})} - \underbrace{\sqrt{a}}_{\in \mathbb{Q}(\sqrt{a}+\sqrt{b})}$$

and so $\sqrt{b} \in \mathbb{Q}(\sqrt{a} + \sqrt{b})$ as well. Since $\sqrt{a}, \sqrt{b} \in \mathbb{Q}(\sqrt{a} + \sqrt{b})$, we have that $\mathbb{Q}(\sqrt{a}, \sqrt{b}) \subseteq \mathbb{Q}(\sqrt{a} + \sqrt{b})$, which shows the claim.

(a) In this exercise we have $a = 2$ and $b = 5$ and $2^2 - 5^2 = -21 \in \mathbb{Q}$. Hence by our general statement above we can pick $\alpha = \sqrt{2} + \sqrt{5}$.

(b) In this exercise we have $a = 3$ and $b = i = \sqrt{-1}$ and $3^2 - \sqrt{-1}^2 = 10 \in \mathbb{Q}$. Hence by our general statement above we can pick $\alpha = \sqrt{3} + i$.

Problem 3. (Exam June 2014, Problem 1.)

(a) Write down the irreducible polynomials over $\mathbb{Z}_2$ of degrees two and three, respectively.

(b) How many irreducible polynomials of degree four are there over $\mathbb{Z}_2$?

Solution.

(a) Let $f(x) = a + bx + cx^2 + dx^3 \in \mathbb{Z}_2[x]$ be irreducible and of degree 2 or 3. Equivalently, by Lemma 3.4(c), we have that f has no roots if $\mathbb{Z}_2$. Since $f(x) \in \mathbb{Z}_2[x]$, we have that $a, b, c, d \in \{0, 1\}$. If $a = 0$, then $f(0) = 0$ and so we have $a = 1$. If an odd number of b, c and d are equal to 1, then $f(1) = 0$. Hence we have that an even number of b, c and d are equal to 1. Since $f(x)$ has degree at least 2, at least one of c and d is equal to 1. Since at least one of c and d is equal to 1 and since an even number of b, c and d is equal to 1, we conclude that two of b, c and d must be equal to 1. Hence the irreducible polynomials of degree 2 or 3 in $\mathbb{Z}_2[x]$ are

$$1 + x + x^2, 1 + x + x^3, 1 + x^2 + x^3.$$

(b) Now let $f(x) = a + bx + cx^2 + dx^3 + x^4 \in \mathbb{Z}_2[x]$ be irreducible. By Lemma 3.4(b), this implies that f has no roots if $\mathbb{Z}_2$. Since $f(x) \in \mathbb{Z}_2[x]$, we have that $a, b, c, d \in \{0, 1\}$. If $a = 0$, then $f(0) = 0$ and so we have $a = 1$. Moreover, if an even number of b, c and d are equal to 1, then $f(1) = 0$. Hence either one of b, c and d is equal to 1, or all three of them are equal to 1. We conclude that

$$f(x) \in \{1 + x + x^4, 1 + x^2 + x^4, 1 + x^3 + x^4, 1 + x + x^2 + x^3 + x^4\} =: \mathcal{P},$$

and it remains to check which of these four polynomials in $\mathcal{P}$ are irreducible. Hence we want to check which of these four polynomials in $\mathcal{P}$ can be written as a product $g(x)h(x)$ with $\deg(g) \geq 1$ and $\deg(h) \geq 1$. The polynomials of degree 1 in $\mathbb{Z}_2[x]$ are x and $1 + x$ and both have a root in $\mathbb{Z}_2$. Hence $g(x)$ and $h(x)$ cannot be of degree 1 since none of the polynomials in $\mathcal{P}$ have roots in $\mathbb{Z}_2$. Therefore $\deg(g) \geq 2$ and $\deg(h) \geq 2$. Since polynomials in $\mathcal{P}$ have degree 4, we conclude that

$\deg(g) = \deg(h) = 2$. By part (a) we know that the only polynomial of degree 2 with no roots in $\mathbb{Z}_2$ is $1 + x + x^2$. Hence $g(x) = h(x) = 1 + x + x^2$ which gives

$$(1 + x + x^2)(1 + x + x^2) = 1 + x + x^2 + x + x^2 + x^3 + x^2 + x^3 + x^4 = 1 + x^2 + x^4 \in \mathcal{P}.$$

We conclude that the rest of the polynomials in $\mathcal{P}$ are irreducible, and so the irreducible polynomials of degree four in $\mathbb{Z}_2$ are

$$1 + x + x^4, 1 + x^3 + x^4, 1 + x + x^2 + x^3 + x^4.$$

Problem 4. (Exam June 2014, Problem 3.) Let $f(x) \in F[x]$ be a nonzero polynomial over the field F with various properties as described below. Let $\alpha \in \overline{F}$, where $\overline{F}$ denotes the algebraic closure of F.

(a) Let $f(\alpha) = 0$. Assume that whenever $g(\alpha) = 0$ for some nonzero $g(x) \in F[x]$, then $\deg(f) \le \deg(g)$. Show that $f(x)$ is irreducible over F.

(b) Show the converse of (a), that is: Assume $f(x)$ is irreducible over F and $f(\alpha) = 0$. Let $g(\alpha) = 0$ for some nonzero $g(x) \in F[x]$. Show that $\deg(f) \le \deg(g)$.

Solution.

(a) Assume to a contradiction that $f(x)$ is reducible over F. Then $f(x) = g(x)h(x)$ with $\deg(g) \ge 1$ and $\deg(h) \ge 1$. Since $f(\alpha) = 0$, we have that $g(\alpha) = 0$ or $h(\alpha) = 0$. Without loss of generality assume that $g(\alpha) = 0$. Then by assumption we have $\deg(f) \le \deg(g)$. But

$$\deg(g) = \deg(f) - \deg(h) \le \deg(f) - 1,$$

gives a contradiction. Hence $f(x)$ is irreducible over F.

(b) Let $p(x)$ be the minimal polynomial of α over F. Then $\deg(p) \le \deg(f)$ and so by division algorithm there exist polynomials $q(x), r(x) \in F[x]$ with $f(x) = q(x)p(x) + r(x)$ and $\deg(r) < \deg(p)$. Since

$$0 = f(\alpha) = q(\alpha)p(\alpha) + r(\alpha) = q(\alpha) \cdot 0 + r(\alpha) = r(\alpha),$$

we conclude that α is a root of $r(x)$. Since $\deg(r) < \deg(p)$ and $p(x)$ is the minimal polynomial of α over F, we conclude that $r(x) = 0$. Then $f(x) = q(x)p(x)$ and f irreducible implies that $q(x) \in F$ or $p(x) \in F$. Since $p(x)$ is irreducible, we conclude that $p(x) \in F$. Hence $\deg(f) = \deg(p)$. Now let $g(\alpha) = 0$ for some nonzero $g(x) \in F[x]$. Then $\deg(p) \le \deg(g)$ since $p(x)$ is the minimal polynomial of α over F. Since $\deg(f) = \deg(p)$, the claim follows.

Problem 5. (Exam May 2013, Problem 3.)

(a) Let α be an algebraic number over the field F such that $[F(\alpha) : F]$ is an odd number. Show that this implies that $F(\alpha^2) = F(\alpha)$.

(b) Give an example to show that the converse implication is not true (Hint: Cyclotomic extensions.)

Solution.

(a) Notice that $F(\alpha^2) \subseteq F(\alpha)$. Consider the polynomial $f(x) = x^2 - \alpha^2 \in F(\alpha^2)[x]$. Then α is a root of $f(x)$ and so $[F(\alpha) : F(\alpha^2)] \le 2$. Assume to a contradiction that $[F(\alpha) : F(\alpha^2)] = 2$. Then the field extensions $F \subseteq F(\alpha^2) \subseteq F(\alpha)$ give

$$[F(\alpha) : F] = [F(\alpha) : F(\alpha^2)][F(\alpha^2) : F] = 2[F(\alpha^2) : F],$$

contradicting $[F(\alpha) : F]$ being odd. Hence $[F(\alpha) : F(\alpha^2)] < 2$ from which it follows that $[F(\alpha) : F(\alpha^2)] = 1$ or $F(\alpha) = F(\alpha^2)$.

(b) The roots of $x^3 - 1 = (x-1)(x^2+x+1) \in \mathbb{R}[x]$ are 1, ω and ω^2, where $\omega = e^{\frac{2\pi i}{3}}$. Since $(\omega^2)^2 = \omega^4 = \omega$, we have that $\mathbb{R}(\omega) = \mathbb{R}(\omega^2)$. But the polynomial $x^2 + x + 1$ is irreducible over $\mathbb{R}$ since its roots ω and ω^2 are not real. Hence

$$[\mathbb{R}(\omega) : \mathbb{R}] = \deg(x^2 + x + 1) = 2,$$

which is not odd.

Problem 6. (Exam June 2015, Problem 3.) Let $F \subseteq E$ be a field extension of degree $[E : F] = n$.

(a) Show that if n is a prime number, then there is no proper intermediate field between E and F (that is, no field K with $F \subseteq K \subseteq E$ and $E \neq K \neq F$). Deduce that if $\alpha \in E \setminus F$, then the minimal polynomial of α in $F[x]$ has degree n.

(b) Let $E = F(\alpha, \beta)$, where α has minimal polynomial in $F[x]$ of degree d_1, and β has minimal polynomial in $F[x]$ of degree d_2. Show that if d_1 and d_2 are coprime (i.e. $\gcd(d_1, d_2) = 1$), then $[E : F] = d_1 d_2$.

(c) Give an example where α and β are as in (b), and such that $\alpha\beta$ has minimal polynomial in $F[x]$ of degree d_1 or d_2. (Hint: consider $F = \mathbb{Q}$ with $\alpha = \sqrt[3]{2}$ and β a suitable root of unity.)

Solution.

(a) Let K be a field with $F \subseteq K \subseteq E$. Then

$$n = [E : F] = [E : K][K : F].$$

If n is a prime number, then either $[E : K] = 1$ and so $K = E$ or $[K : F] = 1$ and so $K = F$. Now let $\alpha \in E \setminus F$. Since $F \subseteq E$ is a finite extension, it is also algebraic and so α is algebraic over F. Hence the minimal polynomial $p(x)$ of α over F exists. Then $F \subseteq F(\alpha) \subseteq E$ implies that $F(\alpha) = F$ or $F(\alpha) = E$. Since $\alpha \notin F$, we have $F(\alpha) = E$. Then

$$\deg(p) = [F(\alpha) : F] = [E : F] = n,$$

as claimed.

(b) Let $f_\alpha(x), f_\beta(x) \in F[x]$ be the minimal polynomials of α and β over F. Then $\deg(f_\alpha) = d_1$ and $\deg(f_\beta) = d_2$. Moreover, we have

$$[F(\alpha) : F] = \deg(f_\alpha) = d_1 \text{ and } [F(\beta) : F] = \deg(f_\beta) = d_2.$$

Notice that $f_\alpha(x) \in F(\beta)[x]$ and f_α has α as a root. Let $m := [F(\alpha, \beta) : F(\beta)]$. Then

$$m = [F(\alpha, \beta) : F(\beta)] \leq \deg(f_\alpha) = d_1,$$

and similarly we obtain $k := [F(\alpha, \beta) : F(\alpha)] \leq d_2$. Then we have

$$n = [E : F] = [F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\beta)][F(\beta) : F] = m d_2.$$

Similarly, we obtain $n = k d_1$. Hence $m d_2 = k d_1$. Since $d_2 \mid k d_1$ and $\gcd(d_1, d_2) = 1$, we obtain $d_2 \mid k$. Since $k \leq d_2$, we obtain $k = d_2$ and so $[E : F] = n = d_1 d_2$ as required.

(c) Let $\alpha = \sqrt[3]{2}$ and let $\beta = e^{\frac{2\pi i}{3}}$. Then the minimal polynomial of α over $\mathbb{Q}$ is $x^3 - 2$ (is irreducible by Eisenstein criterion for $p = 2$, is monic, and has $\sqrt[3]{2}$ as a root), and the minimal polynomial of β over $\mathbb{Q}$ is $x^2 + x + 1$ (is irreducible since its roots $\beta, \beta^2 \notin \mathbb{Q}$ and has degree 2, is monic, and has β as a root). Then the degree of $x^3 - 2$ is 3 and the degree of $x^2 + x + 1$ is 2 and $\gcd(2, 3) = 1$. On the other hand the minimal polynomial of $\alpha\beta = e^{\frac{2\pi i}{3}} \sqrt[3]{2}$ over $\mathbb{Q}$ is again $x^3 - 2$ (is irreducible and monic and has $e^{\frac{2\pi i}{3}} \sqrt[3]{2}$ as a root).

Problem 7. (Exercise 15.4.8 in the book.) Let F be a field and let $n \geq 1$. Let $f(x) = x^n - \alpha \in F[x]$ be an irreducible polynomial over F and let $b \in K$ be a root of f, where $F \subseteq K$ is a field extension. If m is a positive integer such that $m \mid n$, find the degree of the minimal polynomial of b^m over F.

Solution. Since f is irreducible and monic, f is the minimal polynomial of b over F. It follows that

$$[F(b) : F] = \deg(f) = n.$$

Consider the sequence of field extensions

$$F \subseteq F(b^m) \subseteq F(b).$$

Let $n = mk$. Let $g(x) = x^k - a \in F[x]$ and $h(x) = x^m - b^m \in F(b^m)[x]$. Then b^m is a root of $g(x)$ and b is a root of $h(x)$. Hence

$$[F(b^m) : F] \leq \deg(g) = k \text{ and } [F(b) : F(b^m)] \leq \deg(h) = m.$$

Using Theorem 4.3 we obtain

$$mk = n = [F(b) : F] = [F(b) : F(b^m)][F(b^m) : F] \leq mk$$

which implies that $[F(b^m) : F] = k$. Hence the degree of the minimal polynomial of b^m over F is $\frac{n}{m}$.

Problem 8. (Exam August 2013, Problem 4.) Let $f(x) \in F[x]$ be an irreducible polynomial of prime degree p over the field F, with $\text{char}(F) = 0$ (**Warning: I don't think the characteristic of F plays a role.**). Let $K = F(\alpha)$, where α is a root of an irreducible polynomial $g(x) \in F[x]$ of prime degree q over the field F. Assume $f(x)$ is reducible in $K[x]$. Show that $p = q$.

Solution. Let β be a root of f in the algebraic closure $\overline{F}$ of F. Consider the field extension $F \subseteq F(\alpha, \beta)$. Using

$$F \subseteq F(\alpha) \subseteq F(\alpha, \beta),$$

we first have that $[F(\alpha) : F] = \deg(g) = q$ since $g(x)$ is irreducible over F and has α as a root, and we also have that $[F(\alpha, \beta) : F(\alpha)] = d < p$ since $f(x)$ is reducible in $F(\alpha)[x] = K[x]$, and so the minimal polynomial of β over $F(\alpha)$ has degree strictly less than $\deg(f) = p$. Hence

$$[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\alpha)][F(\alpha) : F] = dq.$$

Using

$$F \subseteq F(\beta) \subseteq F(\alpha, \beta),$$

we first have that $[F(\beta) : F] = \deg(f) = p$, since $f(x)$ is irreducible over F and has β as a root, and we also have that $[F(\alpha, \beta) : F(\beta)] = d' \leq q$ since $g(x) \in F(\beta)[x]$ has α as a root and $\deg(g) = q$. Hence

$$[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\beta)][F(\beta) : F] = d'p.$$

We conclude that $dq = d'p$. Then $p \bigm| (dq)$ and so $p \bigm| d$ or $p \bigm| q$ since p is prime. But $d < p$ and so we have that $p \bigm| q$. Since p and q are both prime numbers, we conclude that $p = q$.

Problem 9. (**Warning: Needs field of fractions.**) (Exercise 15.4.10 in the book.) Give an example of a field E containing a proper subfield K such that E is embeddable in K and $[E : K]$ is finite.

Solution. Consider the field

$$E \coloneqq \mathbb{Q}(x) = \left\{ \frac{p(x)}{q(x)} \mid p(x), q(x) \in \mathbb{Q}[x], q(x) \neq 0 \right\},$$

with standard addition and multiplication. Similarly, define

$$K \coloneqq \mathbb{Q}(x^2) = \left\{ \frac{p(x^2)}{q(x^2)} \mid p(x), q(x) \in \mathbb{Q}[x], q(x) \neq 0 \right\}.$$

We claim that $K \subsetneq E$. In particular, it is enough to show that $x \notin K$. Indeed, assume to a contradiction that $x \in \mathbb{Q}(x^2)$. Then there exist polynomials $p(x), q(x) \in \mathbb{Q}[x]$ such that

$$x = \frac{p(x^2)}{q(x^2)}$$

or that $xq(x^2) = p(x^2)$. But the right hand side is a polynomial of even degree, while the left hand side is a polynomial of odd degree and so we reach a contradiction. On the other hand, we have the field embedding

$$\phi : \mathbb{Q}(x) \to \mathbb{Q}(x^2), \quad \phi\left(\frac{p(x)}{q(x)}\right) = \frac{p(x^2)}{q(x^2)}.$$

Now notice that $\mathbb{Q} \subseteq \mathbb{Q}(x^2) \subseteq \mathbb{Q}(x)$ gives

$$E = \mathbb{Q}(x) \subseteq \mathbb{Q}(x^2)(x) \subseteq \mathbb{Q}(x)(x) = E,$$

and so $E = \mathbb{Q}(x^2)(x) = K(x)$. Hence

$$[E : K] = [K(x) : K] \geq 2,$$

where the last inequality follows since $x \notin K$. Since $f(y) = y^2 - x^2 \in K[y](= \mathbb{Q}(x^2)[y])$ and since x is a root of $f(y)$, we have that the $[K(x) : K] \leq 2$. We conclude that $[E : K] = 2$ is finite.

Problem 10. (Exercise 16.1.1 in the book.) Construct splitting fields K over $\mathbb{Q}$ for the polynomial $f(x)$ and find the degree $[K : \mathbb{Q}]$ where $f(x)$ is

(a) $x^3 - 1$.

(b) $x^4 + 1$.

(c) $x^6 - 1$.

(d) $(x^2 - 2)(x^3 - 3)$.

Solution.

(a) Let $\omega = e^{\frac{2\pi i}{3}}$ be a primitive third root of unity. Then the roots of $x^3 - 1$ are ω, ω^2 and ω^3 and so $K = \mathbb{Q}(\omega)$. We have $x^3 - 1 = (x - 1)(x^2 + x + 1)$, and $x^2 + x + 1$ is irreducible over $\mathbb{Q}$ since its roots are $\omega, \omega^2 \notin \mathbb{Q}$. Hence the splitting field of $x^3 - 1$ over $\mathbb{Q}$ is $K = \mathbb{Q}(\omega)$. Since $x^2 + x + 1$ is irreducible and monic, it is the minimal polynomial of ω over $\mathbb{Q}$ and so $[K : \mathbb{Q}] = \deg(x^2 + x + 1) = 2$.

(b) To find the roots of $x^4 + 1$ in $\mathbb{C}$ we may write

$$x^4 + 1 = x^4 + 2x^2 + 1 - 2x^2 = (x^2 + 1)^2 - (\sqrt{2}x)^2 = (x^2 + 1 + \sqrt{2}x)(x^2 + 1 - \sqrt{2}x)$$

and so finding the roots of each second degree polynomial we obtain the roots

$$x_1 = \frac{1+i}{\sqrt{2}}, \quad x_2 = \frac{-1+i}{\sqrt{2}}, \quad x_3 = \frac{-1-i}{\sqrt{2}}, \quad x_4 = \frac{1-i}{\sqrt{2}}.$$

We claim that $x^4 + 1$ is irreducible. Here are three ways to see this.

(i) Since all roots of $x^4 + 1$ are complex, there is only one possible factorization of $x^4 + 1$ into a product of polynomials, namely

$$x^4 + 1 = (ax^2 + bx + c)(dx^2 + ex + f)$$

for some $a, b, c, d, e, f \in \mathbb{Q}$. By computing the right hand side and equating the same degree terms we obtain an impossible system of equations.

(ii) Since all roots of $x^4 + 1$ are complex, there is only one possible factorization of $x^4 + 1$ into a product of polynomials, namely

$$x^4 + 1 = (ax^2 + bx + c)(dx^2 + ex + f)$$

for some $a, b, c, d, e, f \in \mathbb{Q}$. We have shown that

$$x^4 + 1 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1)$$

over $\mathbb{R}$. Moreover, the polynomials $x^2 + \sqrt{2}x + 1$ and $x^2 - \sqrt{2}x + 1$ are irreducible over $\mathbb{R}$ since they have no roots in $\mathbb{R}$. Therefore, any possible factorization of $x^4 + 1$ in $\mathbb{Q}[x]$ as a product of two irreducible polynomials of degree 2 would differ up to a unit at most from the factorization in $\mathbb{R}$. This is impossible since $\sqrt{2} \notin \mathbb{Q}$.

(iii) Let $p(x) = x^4+1$ and compute $p(x+1) = x^4+4x^3+6x^2+4x+2$. This is irreducible by Eisenstein criterion for $p = 2$ and so $p(x)$ is irreducible as well.

Therefore x^4+1 is irreducible over $\mathbb{Q}$. Moreover, notice that $x_1^3 = x_2$, that $x_1^5 = x_3$, and that $x_1^7 = x_5$. Hence the splitting field of x^4+1 over $\mathbb{Q}$ is $K = \mathbb{Q}(x_1)$. Since x^4+1 is irreducible and monic, it is the minimal polynomial of x_1 over $\mathbb{Q}$ and so $[K : \mathbb{Q}] = 4$.

(c) We have $x^6 - 1 = (x-1)(x^5+x^4+x^3+x^2+x+1)$ and -1 is a root of the second factor. So we factorize further to obtain $x^6 - 1 = (x-1)(x+1)(x^4+x^2+1)$. We have

$$x^4+x^2+1 = x^4+2x^2+1-x^2 = (x^2+1)^2 - x^2 = (x^2+x+1)(x^2-x+1)$$

and so finding the roots of each second degree polynomial we obtain that the roots of $x^6 - 1$ are

$$x_1 = -1,\ \ x_2 = 1,\ \ x_3 = \frac{1+i\sqrt{3}}{2},\ \ x_4 = \frac{-1+i\sqrt{3}}{2},\ \ x_5 = \frac{-1-i\sqrt{3}}{2},\ \ x_6 = \frac{1-i\sqrt{3}}{2}.$$

Hence the splitting field of x^6-1 over $\mathbb{Q}$ is $K = \mathbb{Q}(i\sqrt{3})$. Since x^2+3 is irreducible, monic, and has $i\sqrt{3}$ as a root, it is the minimal polynomial of $i\sqrt{3}$ over $\mathbb{Q}$ and so $[K : \mathbb{Q}] = 2$.

(d) The roots of $(x^2-2)(x^3-3)$ are

$$x_1 = \sqrt{2}, x_2 = -\sqrt{2}, x_3 = \omega\sqrt[3]{3}, x_4 = \omega^2\sqrt[3]{3}, x_5 = \sqrt[3]{3},$$

where ω is a primitive third root of unity. Hence the splitting field of $(x^2-2)(x^3-3)$ over $\mathbb{Q}$ is $K = \mathbb{Q}(\sqrt{2}, \sqrt[3]{3}, \omega)$. Consider the field extensions

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt[3]{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt[3]{3}, \omega) = K. \tag{1}$$

We have

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = \deg(x^2-2) = 2. \tag{2}$$

We claim that the polynomial $x^3 - 3 \in \mathbb{Q}(\sqrt{2})[x]$ is irreducible over $\mathbb{Q}(\sqrt{2})$. By Lemma 3.4(3) it is enough to show that x^3-3 has no roots in $\mathbb{Q}(\sqrt{2})$. The roots of x^3-3 are x_3, x_4 and x_5. Since x_3 and x_4 are not real, it is enough to show that $x_4 = \sqrt[3]{3} \notin \mathbb{Q}(\sqrt{2})$. Assume to a contradiction that $\sqrt[3]{3} \in \mathbb{Q}(\sqrt{2})$. Since $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, there exist $a, b \in \mathbb{Q}$ such that

$$\sqrt[3]{3} = a + b\sqrt{2}.$$

Raising both sides to the third power we obtain

$$3 = a^3 + 3a^2b\sqrt{2} + 6ab^2 + 2b^3\sqrt{2},$$

which we can rearrange to

$$(a^3+6ab^2-3) + (3a^2b+2b^3)\sqrt{2} = 0.$$

Since $1, \sqrt{2}$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(\sqrt{2})$, we have that

$$\begin{aligned} a^3+6ab^2-3 &= 0,\\ 3a^2b+2b^3 &= 0. \end{aligned}$$

If $b = 0$, the first equation gives $a^3 - 3 = 0$ which is impossible since $a \in \mathbb{Q}$. Hence $b \neq 0$ and the second equation gives $3a^2 + 2b^2 = 0$, which is impossible in $\mathbb{Q}$ (since $b \neq 0$). Hence we reach a contradiction. We conclude that $x^3 - 3 \in \mathbb{Q}(\sqrt{2})[x]$ is irreducible over $\mathbb{Q}(\sqrt{2})$ and so

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = \deg(x^3-3) = 3. \tag{3}$$

Finally, recall from part (a) that the polynomial $x^2+x+1 \in \mathbb{Q}(\sqrt{2}, \sqrt{3})[x]$ has only the nonreal roots ω, ω^2, and so none of them is in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Hence x^2+x+1 is irreducible over $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ and so

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \omega) : \mathbb{Q}(\sqrt{2}, \sqrt{3})] = 2. \tag{4}$$

Using (1), (2), (3), (4) we conclude that $[K : \mathbb{Q}] = 2 \cdot 3 \cdot 2 = 12$.

Problem 11. (Exam June 2014, Problem 7.) Show that $\sqrt{2}+\sqrt[3]{3} \notin \mathbb{Q}$. (Hint: Consider an appropriate field extension of $\mathbb{Q}$.)

Solution. Assume to a contradiction that $\sqrt{2}+\sqrt[3]{3} \in \mathbb{Q}$. Then $\sqrt{2}+\sqrt[3]{3} \in \mathbb{Q}(\sqrt{2})$. In particular, we have

$$\sqrt[3]{3} = \underbrace{\sqrt{2}+\sqrt[3]{3}}_{\in\mathbb{Q}(\sqrt{2})} - \underbrace{\sqrt{2}}_{\in\mathbb{Q}(\sqrt{2})},$$

and so $\sqrt[3]{3} \in \mathbb{Q}(\sqrt{2})$. But this is not true, see the solution of Problem 10(d).

Problem 12. (Exercise 16.1.2 in the book.) Construct a splitting field for $x^3+x+1 \in \mathbb{Z}_2[x]$ and list all its elements.

Solution. By evaluating the polynomial x^3+x+1 at 0 and 1, we see that it has no roots in $\mathbb{Z}_2$ and hence it is irreducible (since its degree is 3). Let $\mathbb{Z}_2(\alpha)$ be a field extension of $\mathbb{Z}_2$ where α is a root of x^3+x+1, that is $\alpha^3+\alpha+1=0$. Then $[\mathbb{Z}_2(\alpha):\mathbb{Z}_2] = \deg(x^3+x+1) = 3$, and $\{1,\alpha,\alpha^2\}$ is a $\mathbb{Z}_2$-basis of $\mathbb{Z}_2(\alpha)$. By checking we see that α^2 is also a root of x^3+x+1 since

$$(\alpha^2)^3+\alpha^2+1 = \alpha^6+\alpha^2+1 = (1+\alpha^2)+\alpha^2+1 = 0$$

where using $\alpha^3+\alpha+1=0$, we computed $\alpha^3 = -1-\alpha = 1+\alpha$ and so $\alpha^6 = 1+\alpha^2$. Therefore x^3+x+1 has two roots in $\mathbb{Z}_2(\alpha)$ and hence it has all its roots in $\mathbb{Z}_2(\alpha)$ since its degree is 3. We conclude that $\mathbb{Z}_2(\alpha) = \{0,1,\alpha,1+\alpha,\alpha^2,1+\alpha^2,\alpha+\alpha^2,1+\alpha+\alpha^2\}$ is the splitting field of x^3+x+1 over $\mathbb{Z}_2$.

Problem 13. (Exercise 16.1.5 in the book.) Let E be the spliting field of a polynomial of degree n over a field F. Show that $[E:F] \leq n!$.

Solution. We use induction on $n \geq 1$. For the base case $n=1$ we have that $E=F$ and so $[E:F]=1\leq 1!$. Assume now that the claim is true for all polynomials of degree at most $n-1$ and we show that the claim holds for polynomials of degree n. Let $f(x) \in F[x]$ be a polynomial of degree n and E its splitting field. Let $\alpha_1,\ldots,\alpha_n$ be the roots of f in E (possibly with duplicates). Then $E = F(\alpha_1,\ldots,\alpha_n)$. Since $x-\alpha_1 \in F(\alpha_1)[x]$ divides $f(x)$, the polynomial $g(x) = \frac{f(x)}{x-\alpha_1}$ is a well-defined polynomial in $F(\alpha_1)[x]$. Moreover, its degree is $n-1$ and its roots are $\alpha_2,\ldots,\alpha_n$ and so its splitting field over $F(\alpha_1)$ is $F(\alpha_1)(\alpha_2,\ldots,\alpha_n) = E$. Hence by induction hypothesis we have $[E:F(\alpha_1)] \leq (n-1)!$. On the other hand, α_1 is a root of $f(x)\in F[x]$ and so $[F(\alpha_1):F] \leq \deg(f) = n$. Then from the field extensions $F \subseteq F(\alpha_1) \subseteq E$ we obtain

$$[E:F] = [E:F(\alpha_1)][F(\alpha_1):F] \leq n(n-1)! = n!$$

as required.

Problem 14. Let $f(x) = x^3+ax+b \in \mathbb{Q}[x]$. Let E be the splitting field of f. Let $\alpha_1,\alpha_2,\alpha_3 \in \mathbb{C}$ be the roots of f (not necessarily distinct).

(a) Define $D = (\alpha_2-\alpha_1)^2(\alpha_3-\alpha_1)^2(\alpha_3-\alpha_2)^2$. Show that $D = -(4a^3+27b^2)$.

(b) Show that if $f(x)$ is reducible, then $[E:\mathbb{Q}]=1$ or $[E:\mathbb{Q}]=2$.

(c) (Exercise 16.1.3 in the book.) Show that if $f(x)$ is irreducible and $\sqrt{D}\in\mathbb{Q}$, then $[E:\mathbb{Q}]=3$.

(d) (Exercise 16.1.4 in the book.) Show that if $f(x)$ is irreducible and $\sqrt{D}\notin\mathbb{Q}$, then $[E:\mathbb{Q}]=6$.

Solution.

(a) We have $f(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$. Then

$$\begin{aligned} x^3+ax+b &= (x-\alpha_1)(x-\alpha_2)(x-\alpha_3) \\ &= x^3-\alpha_3x^2-\alpha_2x^2-\alpha_1x^2+\alpha_1\alpha_2x+\alpha_1\alpha_3x+\alpha_2\alpha_3x-\alpha_1\alpha_2\alpha_3 \\ &= x^3-(\alpha_1+\alpha_2+\alpha_3)x^2+(\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3)x-\alpha_1\alpha_2\alpha_3, \end{aligned}$$

from which we get

$$\begin{aligned} \alpha_1 + \alpha_2 + \alpha_3 &= 0, && (5)\\ \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 &= a, && (6)\\ -\alpha_1\alpha_2\alpha_3 &= b. && (7) \end{aligned}$$

Using (5) we may eliminate α_3 from (6) and (7) to obtain

$$\begin{aligned} -(\alpha_1^2 + \alpha_1\alpha_2 + \alpha_2^2) &= a, && (8)\\ \alpha_1\alpha_2(\alpha_1 + \alpha_2) &= b. && (9) \end{aligned}$$

Now we compute D:

$$\begin{aligned}
(\alpha_2 - \alpha_1)^2(\alpha_3 - \alpha_1)^2(\alpha_3 - \alpha_2)^2 &\overset{(5)}{=} (\alpha_2 - \alpha_1)^2(\alpha_2 + 2\alpha_1)^2(\alpha_1 + 2\alpha_2)^2\\
&= (\alpha_1^2 - 2\alpha_1\alpha_2 + \alpha_2^2)(4\alpha_1^2 + 4\alpha_1\alpha_2 + \alpha_2^2)(\alpha_1^2 + 4\alpha_1\alpha_2 + 4\alpha_2^2)\\
&\overset{(8)}{=} (-3\alpha_1\alpha_2 - a)(3\alpha_1^2 + 3\alpha_1\alpha_2 - a)(3\alpha_2^2 + 3\alpha_1\alpha_2 - a)\\
&= (-9\alpha_1^3\alpha_2 - 9\alpha_1^2\alpha_2^2 + 3a\alpha_1\alpha_2 - 3a\alpha_1^2 - 3a\alpha_1\alpha_2 + a^2)(3\alpha_2^2 + 3\alpha_1\alpha_2 - a)\\
&= (-9\alpha_1^2\alpha_2(\alpha_1 + \alpha_2) - 3a\alpha_1^2 + a^2)(3\alpha_2^2 + 3\alpha_1\alpha_2 - a)\\
&\overset{(9)}{=} (-9b\alpha_1 - 3a\alpha_1^2 + a^2)(3\alpha_2^2 + 3\alpha_1\alpha_2 - a)\\
&= -27b\alpha_1\alpha_2^2 - 27b\alpha_1^2\alpha_2 + 9ab\alpha_1 - 9a\alpha_1^2\alpha_2^2 - 9a\alpha_1^3\alpha_2 + 3a^2\alpha_1^2 + 3a^2\alpha_2^2 + 3a^2\alpha_1\alpha_2 - a^3\\
&= -27b\alpha_1\alpha_2(\alpha_1 + \alpha_2) + 9ab\alpha_1 - 9a\alpha_1^2\alpha_2(\alpha_1 + \alpha_2) + 3a^2(\alpha_1^2 + \alpha_1\alpha_2 + \alpha_2^2) - a^3\\
&\overset{(9)}{=} -27b^2 + 9ab\alpha_1 - 9ab\alpha_1 + 3a^2(\alpha_1^2 + \alpha_1\alpha_2 + \alpha_2^2) - a^3\\
&\overset{(8)}{=} -27b^2 - 3a^3 - a^3\\
&= -(4a^3 + 27b^2)
\end{aligned}$$

as required.

(b) If $f(x)$ is reducible, then it has a root in $\mathbb{Q}$, say α_1. Then $f(x) = (x - \alpha_1)g(x)$ where $g(x)$ has degree 2 and has α_2, α_3 as roots. We consider the cases $g(x)$ reducible and $g(x)$ irreducible separately.

If $g(x)$ is reducible, it has a root in $\mathbb{Q}$, say α_2. Then $g(x) = (x - \alpha_2)h(x)$ where $h(x)$ has degree 1 and has α_3 as a root. It follows that $\alpha_3 \in \mathbb{Q}$ and so in this case $E = \mathbb{Q}$ and $[E : \mathbb{Q}] = [\mathbb{Q} : \mathbb{Q}] = 1$.

If $g(x)$ is irreducible, then α_2 and α_3 do not belong in $\mathbb{Q}$. Then $\alpha_2 \in \mathbb{Q}(\alpha_2)$ and so $g(x) = (x - \alpha_2)h(x)$ in $\mathbb{Q}(\alpha_2)$ where $h(x)$ has degree 1 and has α_3 as a root. It follows that $\alpha_3 \in \mathbb{Q}(\alpha_2)$ and so $E = \mathbb{Q}(\alpha_2, \alpha_3) = \mathbb{Q}(\alpha_2)$. Since $g(x)$ is irreducible and $\alpha_2 \notin \mathbb{Q}$ is a root of g, it follows that $[E : \mathbb{Q}] = [\mathbb{Q}(\alpha_2) : \mathbb{Q}] = \deg(g) = 2$.

(c) By part (a) we have that $\sqrt{D} = (\alpha_2 - \alpha_1)(\alpha_3 - \alpha_1)(\alpha_3 - \alpha_2) \in \mathbb{Q}$. Now consider $\mathbb{Q}(\alpha_1)$. By (5) we have $\alpha_2 + \alpha_3 = -\alpha_1 \in \mathbb{Q}(\alpha_1)$. By (7) we have $\alpha_2\alpha_3 = -b\alpha_1^{-1} \in \mathbb{Q}(\alpha_1)$. Hence

$$(\alpha_2 - \alpha_1)(\alpha_3 - \alpha_1) = \underbrace{\alpha_2\alpha_3}_{\in\mathbb{Q}(\alpha_1)} - \alpha_1 \underbrace{(\alpha_2 + \alpha_3)}_{\in\mathbb{Q}(\alpha_1)} + \alpha_1^2 \in \mathbb{Q}(\alpha_1).$$

Then

$$\alpha_3 - \alpha_2 = \underbrace{(\alpha_2 - \alpha_1)(\alpha_3 - \alpha_1)(\alpha_3 - \alpha_2)}_{\in\mathbb{Q}} \underbrace{(\alpha_2 - \alpha_1)(\alpha_3 - \alpha_1)^{-1}}_{\in\mathbb{Q}(\alpha_1)} \in \mathbb{Q}(\alpha_1).$$

Then

$$\alpha_3 = \frac{1}{2}(\underbrace{\alpha_2 + \alpha_3}_{\in\mathbb{Q}(\alpha_1)} + \underbrace{\alpha_3 - \alpha_2}_{\in\mathbb{Q}(\alpha_1)}) \in \mathbb{Q}(\alpha_1),$$

and so $\alpha_2 = \alpha_3 + \alpha_2 - \alpha_3 \in \mathbb{Q}(\alpha_1)$. Hence all roots of $f(x)$ are in $\mathbb{Q}(\alpha_1)$ and so $E = \mathbb{Q}(\alpha_1)$. Since f is irreducible and α_1 is a root of f, we conclude that

$$[E : \mathbb{Q}] = [\mathbb{Q}(\alpha_1) : \mathbb{Q}] = \deg(f) = 3.$$

(d) If $\sqrt{D} \notin \mathbb{Q}$, then the minimal polynomial of $\sqrt{D}$ over $\mathbb{Q}$ is $x^2 - D$ and so $[\mathbb{Q}(\sqrt{D}) : \mathbb{Q}] = \deg(x^2 - D) = 2$. Assume to a contradiction that $\alpha_i \in \mathbb{Q}(\sqrt{D})$ for some $i \in \{1, 2, 3\}$. Then $\mathbb{Q} \subseteq \mathbb{Q}(\alpha_i) \subseteq \mathbb{Q}(\sqrt{D})$. But $[\mathbb{Q}(\alpha_i) : \mathbb{Q}] = \deg(f) = 3$, since f is irreducible and α_i is a root of f. Hence

$$2 = [\mathbb{Q}(\sqrt{D}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{D}) : \mathbb{Q}(\alpha_1)][\mathbb{Q}(\alpha_1) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{D}) : \mathbb{Q}(\alpha_1)] \cdot 3,$$

which is a contradiction. Following the proof of the case $\sqrt{D} \in \mathbb{Q}$, we can show that $\alpha_2, \alpha_3 \in \mathbb{Q}(\sqrt{D}, \alpha_1)$. Hence $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) \subseteq \mathbb{Q}(\sqrt{D}, \alpha_1)$. On the other hand, we have

$$\sqrt{D} = (\alpha_2 - \alpha_1)(\alpha_3 - \alpha_1)(\alpha_3 - \alpha_2) \in \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$$

and so $\mathbb{Q}(\sqrt{D}, \alpha_1) \subseteq \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$. It follows that

$$E = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) = \mathbb{Q}(\sqrt{D}, \alpha_1).$$

Hence $[E : \mathbb{Q}] = [\mathbb{Q}(\sqrt{D}, \alpha_1) : \mathbb{Q}]$. Since none of the roots of f are in $\mathbb{Q}(\sqrt{D})$, and since f has degree 3, it follows that f is irreducible over $\mathbb{Q}(\sqrt{D})$. Hence

$$[\mathbb{Q}(\sqrt{D}, \alpha_1) : \mathbb{Q}(\sqrt{D})] \deg(f) = 3.$$

Therefore, we have

$$[E : \mathbb{Q}] = [\mathbb{Q}(\sqrt{D}, \alpha_1) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{D}, \alpha_1) : \mathbb{Q}(\sqrt{D})][\mathbb{Q}(\sqrt{D}) : \mathbb{Q}] = 3 \cdot 2 = 6,$$

as required.

Problem 15. (Exercise 16.1.8 in the book.) Show that over any field $K \supseteq \mathbb{Q}$ the polynomial $x^3 - 3x + 1$ is either irreducible or splits into linear factors.

Solution. Let $f(x) = x^3 - 3x + 1$. By Theorem 3.7 we have that any root of f is an integer dividing 1. Since $f(1) = -1$ and $f(-1) = 3$, we conclude that f has no roots in $\mathbb{Q}$. Since $\deg(f) = 3$ we conclude that f is irreducible over $\mathbb{Q}$. Let $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$ be the roots of f and let E be the splitting field of f over $\mathbb{Q}$. Using Problem 14(a), we compute

$$D = -(4(-3)^3 + 27) = -(4(-27) + 27) = 81,$$

and we have that $\sqrt{D} = \sqrt{81} = 9 \in \mathbb{Q}$. Hence by Problem 14(c) we have that $[E : \mathbb{Q}] = 3$. Moreover, for every $i \in \{1, 2, 3\}$ we have $[\mathbb{Q}(\alpha_i) : \mathbb{Q}] = \deg(f) = 3$ since f is irreducible with α_i as a root. Hence

$$3 = [E : \mathbb{Q}] = [E : \mathbb{Q}(\alpha_i)][\mathbb{Q}(\alpha_i) : \mathbb{Q}] = [E : \mathbb{Q}(\alpha_i)] \cdot 3,$$

and so $\mathbb{Q}(\alpha_i) = E$.

Now assume that f is not irreducible over a field $K \supseteq \mathbb{Q}$ and we show that f splits into linear factors in K. Since f is not irreducible over K and since $\deg(f) = 3$, it follows that K contains a root α_i of f. Hence $E = \mathbb{Q}(\alpha_i) \subseteq K$. Since K contains the splitting field of f, we conclude that f splits into linear factors in K, as required.

Problem 16. (Exercise 16.2.2 in the book.) Is $\mathbb{R} \subseteq \mathbb{R}(\sqrt{-5})$ a normal field extension?

Solution. We have that $\sqrt{-5}$ is the root of $x^2 + 5 \in \mathbb{R}[x]$ and that $x^2 + 5 = (x - \sqrt{-5})(x + \sqrt{-5})$ in $\mathbb{R}[x]$. Hence $\mathbb{R}(\sqrt{-5})$ is the splitting field of $x^2 + 5$ and so $\mathbb{R} \subseteq \mathbb{R}(\sqrt{-5})$ is normal.

Problem 17. (Exercise 16.2.3 in the book.) Let E be a normal extension of F and let K be a subfield of E containing F. Show that E is a normal extension over K. Give an example to show that K need not be a normal extension of F.

Solution. We have field extensions $F \subseteq K \subseteq E$ with $F \subseteq E$ being normal. Therefore, E is the splitting field of a collection of polynomials $\{f_i(x) \in F[x] \mid i \in I\}$. But the polynomials $f_i(x)$ belong to $K[x]$ as well and so E is also the splitting field of $\{f_i(x) \in K[x] \mid i \in I\}$. Hence $K \subseteq E$ is normal.

Now consider the field extensions $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$, that is $F = \mathbb{Q}$, $K = \mathbb{R}$ and $E = \mathbb{C}$. The field extensions $\mathbb{Q} \subseteq \mathbb{C}$ and $\mathbb{R} \subseteq \mathbb{C}$ are normal by Theorem 8.5. On the other hand, $\mathbb{Q} \subseteq \mathbb{R}$ is not normal by Example 8.6(2).

Problem 18. (Exercise 16.2.4 in the book.) Let $F = \mathbb{Q}(\sqrt{2})$ and $E = \mathbb{Q}(\sqrt[4]{2})$. Show that E is a normal extension of F, F is a normal extension of $\mathbb{Q}$, but E is not a normal extension of $\mathbb{Q}$.

Solution. The field extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ is normal, as it is the splitting field of $x^2 - 2 \in \mathbb{Q}[x]$ (the roots of $x^2 - 2$ are $\sqrt{2}, -\sqrt{2} \in \mathbb{Q}(\sqrt{2})$.)

The field extension $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$ is normal, as it is the splitting field of $x^2 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})[x]$ (the roots of $x^2 - \sqrt{2}$ are $\sqrt[4]{2}, -\sqrt[4]{2} \in \mathbb{Q}(\sqrt[4]{2})$.)

Regarding the field extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2})$, note that the irreducible polynomial $x^4 - 2 \in \mathbb{Q}[x]$ (Eisenstein criterion for $p = 2$) has two root in $\mathbb{Q}(\sqrt[4]{2})$, namely $\sqrt[4]{2}$ and $-\sqrt[4]{2}$, but it does not have all of its roots in $\mathbb{Q}(\sqrt[4]{2})$ since its other two roots, $i\sqrt[4]{2}$ and $-i\sqrt[4]{2}$ are not real. By Theorem 8.5 we conclude that the extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2})$ is not normal.

Problem 19. (Exercise 16.2.6 in the book.) Let E_i, $i \in \Lambda$ be a family of normal extensions of a field F in some extension K of F. Show that $E \coloneqq \bigcap_{i\in\Lambda} E_i$ is also a normal extension of F.

Solution. Let $f(x) \in F[x]$ be an irreducible polynomial that has a root $\alpha_1 \in E$. By Theorem 8.5 we need to show that it has all of its roots in E. Since $\alpha_1 \in E = \bigcap_{i\in\Lambda} E_i$, we have that $\alpha_1 \in E_i$ for all $i \in \Lambda$. Hence $f(x)$ has a root in E_i. Since $F \subseteq E_i$ is normal for all $i \in \Lambda$, we have that $f(x)$ has all of its roots in E_i for all $i \in \Lambda$ by Theorem 8.5. Hence for every $i \in \Lambda$, the roots of f, say $\alpha_1, \alpha_2, \ldots, \alpha_n$, belong to E_i. We conclude that $\alpha_1, \alpha_2, \ldots, \alpha_n \in \bigcap_{i\in\Lambda} E_i = E$, as required.

Problem 20. (Exam June 2014, Problem 5.)

(a) Let $\alpha = \sqrt{2 + \sqrt{2}} \in \mathbb{R}^+$. Find the minimal polynomial of α over $\mathbb{Q}$.

(b) Show that $\mathbb{Q}(\alpha)$ is a normal extension of $\mathbb{Q}$. (Hint: Consider $\alpha\sqrt{2 - \sqrt{2}}$.)

Solution.

(a) We have

$$\begin{aligned} \alpha^2 = 2 + \sqrt{2} &\implies \alpha^2 - 2 = \sqrt{2} \\ &\implies (\alpha^2 - 2)^2 = (\sqrt{2})^2 \\ &\implies \alpha^4 - 4\alpha^2 + 4 = 2 \\ &\implies \alpha^4 - 4\alpha^2 + 2 = 0. \end{aligned}$$

Hence α is a root of $f(x) = x^4 - 4x^2 + 2 \in \mathbb{Q}[x]$. This is irreducible over $\mathbb{Q}$ by Eisenstein criterion for $p = 2$ and is a monic polynomial. Hence f is the minimal polynomial of α over $\mathbb{Q}$.

(b) It is enough to show that $\mathbb{Q}(\alpha)$ is the splitting field of $f(x) = x^4 - 4x^2 + 2$ over $\mathbb{Q}$. To show this we need to show that all the roots of f are in $\mathbb{Q}(\alpha)$. To find the roots of f in $\mathbb{C}$ we have

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

Hence the roots of f in $\mathbb{C}$ are

$$\alpha = \sqrt{2 + \sqrt{2}}, \quad -\alpha = -\sqrt{2 + \sqrt{2}}, \quad \beta \coloneqq \sqrt{2 - \sqrt{2}}, \quad -\beta = -\sqrt{2 - \sqrt{2}}.$$

Hence it is enough to show that $\beta = \sqrt{2-\sqrt{2}} \in \mathbb{Q}(\alpha)$. We compute

$$\alpha\beta = \sqrt{2+\sqrt{2}}\sqrt{2-\sqrt{2}} = \sqrt{(2+\sqrt{2})(2-\sqrt{2})} = \sqrt{4-(\sqrt{2})^2} = \sqrt{4-2} = \sqrt{2}.$$

Hence $\beta = \frac{\alpha}{\sqrt{2}}$ and it is enough to show that $\sqrt{2} \in \mathbb{Q}(\alpha)$. We have $\alpha^2 = 2+\sqrt{2}$ and so $\sqrt{2} = \alpha^2 - 2 \in \mathbb{Q}(\alpha)$, which completes the proof.