# Galois theory - Problem Set 2 solutions

Solved on Thursday 15.02

## Chapter 15.3

**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 have no root in $\mathbb{Q}$ and so they are irreducible by Lemma 3.4(3). 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 $\alpha$ such that

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

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

**Solution.** We first show the more general claim that if $a, b \in \mathbb{C}$ satisfy $a - b \in \mathbb{Q}$, 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

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

and so

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

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 $2 - 5 = -3 \in \mathbb{Q}$. Hence by our general statement above we can pick $\alpha = \sqrt{2} + \sqrt{5}$.

(b) In this exercise we have $a = 3$ and $b = -1$ and $3 - (-1) = 4 \in \mathbb{Q}$. Hence by our general statement above we can pick $\alpha = \sqrt{3} + i$.

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

(a) Let $\alpha$ 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 $\alpha$ is a root of $f(x)$ and so $[F(\alpha) : F(\alpha^2)] \leq 2$. 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 $1$, $\omega$ and $\omega^2$, 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 $\omega$ and $\omega^2$ are not real. Hence

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

which is not odd.

**Problem 4.** (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 $\alpha$ in $F[x]$ has degree $n$.

(b) Let $E = F(\alpha, \beta)$, where $\alpha$ has minimal polynomial in $F[x]$ of degree $d_1$, and $\beta$ 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 $\alpha$ and $\beta$ 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 $\beta$ 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 $\alpha$ is algebraic over $F$. Hence the minimal polynomial $p(x)$ of $\alpha$ 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 $\alpha$ and $\beta$ 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 $f_\alpha(x)$ has $\alpha$ 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

$$n = [E : F] = [F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\beta)][F(\beta) : F] = md_2.$$

Similarly, we obtain $n = kd_1$. Hence $md_2 = kd_1$. Since $d_2 \mid kd_1$ 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 $\alpha$ 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 $\beta$ 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 $\beta$ 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 5.** (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 $f(x)$, 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 $f(x) \in F[x]$ is irreducible, monic, and has $b$ as a root, it follows that $f(x)$ 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 $\frac{n}{m}$.

## Chapter 15.4

**Problem 6.** (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 $\deg(f) \leq \deg(g)$. 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 $\deg(f) \leq \deg(g)$.

**Solution.**

(a) Assume to a contradiction that $f(x)$ is reducible over $F$. Then $f(x) = g(x)h(x)$ with $\deg(g) \geq 1$ and $\deg(h) \geq 1$. 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 $\deg(f) \leq \deg(g)$. But

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

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

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

**Problem 7.** (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 $\alpha$ 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 $\beta$ be a root of $f(x)$ 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 $\alpha$ 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 $\beta$ 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 $\beta$ as a root, and we also have that $[F(\alpha, \beta) : F(\beta)] = d' \leq q$ since $g(x) \in F(\beta)[x]$ has $\alpha$ 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 $p \mid (dq)$ and so $p \mid d$ or $p \mid q$ since $p$ is prime. But $d < p$ and so we have that $p \mid q$. Since $p$ and $q$ are both prime numbers, we conclude that $p = q$.

## Chapter 16.1

**Problem 8.** (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 $\omega$, $\omega^2$ and $\omega^3$ 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 $\omega$ 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 $\omega$ 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

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

which we can rearrange to

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

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

$$a^3 + 6ab^2 - 3 = 0,$$
$$3a^2 b + 2b^3 = 0.$$

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

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

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

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

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

**Problem 9.** (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 $\alpha$ 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 $\alpha^2$ 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 10.** (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, $\alpha_1$ 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.

## Chapter 16.2

**Problem 11.** (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 12.** (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 13.** (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 14.** (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 $f(x)$, say $\alpha_1, \alpha_2, \dots, \alpha_n$, belong to $E_i$. We conclude that $\alpha_1, \alpha_2, \dots, \alpha_n \in \bigcap_{i\in\Lambda} E_i = E$, as required.

**Problem 15.** (Exam June 2014, Problem 5.)

(a) Let $\alpha = \sqrt{2+\sqrt{2}} \in \mathbb{R}^+$. Find the minimal polynomial of $\alpha$ 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 $\alpha$ 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 $f(x)$ is the minimal polynomial of $\alpha$ 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 $f(x)$ are in $\mathbb{Q}(\alpha)$. To find the roots of $f(x)$ 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

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

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.

## Extra problems

**Problem 16. (Chapter 16.1)** Let $f(x) = x^3 + ax + b \in \mathbb{Q}[x]$. Let $E$ be the splitting field of $f(x)$. Let $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$ be the roots of $f(x)$ (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 $[E : \mathbb{Q}] = 6$.

(e) (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.**

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

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

from which we get

$$\alpha_1 + \alpha_2 + \alpha_3 = 0, \tag{5}$$
$$\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = a, \tag{6}$$
$$-\alpha_1\alpha_2\alpha_3 = b. \tag{7}$$

Using (5) we may eliminate $\alpha_3$ from (6) and (7) to obtain

$$-(\alpha_1^2 + \alpha_1\alpha_2 + \alpha_2^2) = a, \tag{8}$$
$$\alpha_1\alpha_2(\alpha_1 + \alpha_2) = b. \tag{9}$$

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 $\alpha_1$. Then $f(x) = (x - \alpha_1)g(x)$ where $g(x)$ has degree 2 and has $\alpha_2, \alpha_3$ 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 $\alpha_2$. Then $g(x) = (x - \alpha_2)h(x)$ where $h(x)$ has degree 1 and has $\alpha_3$ 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 $\alpha_2$ and $\alpha_3$ are not 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 $\alpha_3$ 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 $f(x)$ is irreducible and $\alpha_1$ is a root of $f(x)$, 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 $f(x)$ is irreducible and $\alpha_i$ is a root of $f(x)$. 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 $f(x)$ are in $\mathbb{Q}(\sqrt{D})$, and since $f(x)$ has degree 3, it follows that $f(x)$ 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.

(e) Let $f(x)=x^3-3x+1$. By Theorem 3.7 we have that any root of $f(x)$ is an integer dividing 1. Since $f(1)=-1$ and $f(-1)=3$, we conclude that $f(x)$ has no roots in $\mathbb{Q}$. Since $\deg(f)=3$ we conclude that $f(x)$ is irreducible over $\mathbb{Q}$. Let $\alpha_1,\alpha_2,\alpha_3\in\mathbb{C}$ be the roots of $f(x)$ and let $E$ be the splitting field of $f(x)$ over $\mathbb{Q}$. Using part (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 part (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 $f(x)$ is irreducible with $\alpha_i$ 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 $f(x)$ is not irreducible over a field $K\supseteq\mathbb{Q}$ and we show that $f(x)$ splits into linear factors in $K$. Since $f(x)$ is not irreducible over $K$ and since $\deg(f)=3$, it follows that $K$ contains a root $\alpha_i$ of $f(x)$. Hence $E=\mathbb{Q}(\alpha_i)\subseteq K$. Since $K$ contains the splitting field of $f(x)$, we conclude that $f(x)$ splits into linear factors in $K$, as required.

**Problem 17. (Chapter 16.1)** Let $E$ be the splitting field of a polynomial $f(x)$ of degree $n$ over a field $F$. Show that $[E : F]$ divides $n!$.

**Solution.** We use induction on $[E : F]$. If $[E : F] = 1$ then we trivially have $[E : F] = 1 \mid n!$. Now assume that $[E : F] > 1$ and that for all $k < [E : F]$ we have that $k \mid n!$ and we show that $[E : F] \mid n!$ as well.

First assume that $f(x)$ is irreducible. In particular, we have that $n > 1$. Indeed, assume instead that $n = 1$. Then $E = F$ and $[E : F] = 1$, which contradicts our assumption $[E : F] > 1$. Let $\alpha$ be a root of $f(x)$ in $E$. Then $[F(\alpha) : F] = \deg(f) = n$ by Theorem 4.6. Since both $f(x)$ and $(x - \alpha)$ are in $F(\alpha)[x]$ and $F(\alpha)$ is a field, we may divide $f(x)$ by $(x - \alpha)$ to obtain that

$$g(x) = \frac{f(x)}{(x - \alpha)} \in F(\alpha).$$

Clearly $g(x)$ splits in $E$ since $f(x)$ does. Assume that $g(x)$ splits in some intermediate field $F(\alpha) \subseteq L \subseteq E$. Then $f(x)$ splits in that field as well and since $F \subseteq L \subseteq E$, we conclude that $L = E$. Therefore $E$ is the splitting field of $g(x)$ over $F(\alpha)$. Since

$$[E : F] = [E : F(\alpha)][F(\alpha) : F] = kn,$$

and since $n > 1$, we obtain that $[E : F(\alpha)] < [E : F]$. Hence by induction hypothesis we obtain that $[E : F(\alpha)]$ divides $\deg(g)! = (n - 1)!$. Write $(n - 1)! = s \cdot [E : F(\alpha)]$. Then

$$n! = ((n - 1)!) \cdot n = s \cdot [E : F(\alpha)] \cdot [F(\alpha) : F] = s \cdot [E : F],$$

and so $[E : F]$ divides $n!$ as required.

Now assume that $f(x)$ is not irreducible. We claim that $f(x)$ has an irreducible factor of degree at least 2. Indeed, assume instead that all irreducible factors of $f(x)$ are of degree 1. Then $f(x)$ is of the form

$$f(x) = \beta(x - \alpha_1) \cdots (x - \alpha_n)$$

for some $\beta, \alpha_1, \ldots, \alpha_n \in F$. Then $f(x)$ splits in $F[x]$ and so $E = F$, giving $[E : F] = 1$, which contradicts our assumption $[E : F] > 1$. Therefore there exists an irreducible factor $h(x) \in F[x]$ of $f(x)$ with $\deg(h) \geq 2$. Hence there exists a polynomial $g(x) \in F[x]$ such that

$$f(x) = h(x)g(x).$$

Since we have assumed that $f(x)$ is not irreducible, it follows that $g(x)$ cannot be a constant polynomial, and so $\deg(g) \geq 1$. Let $d = \deg(h)$. Since

$$n = \deg(f) = \deg(h) + \deg(g) \geq d + 1,$$

we have that $d < n$. Now if $E$ is the splitting field of $h(x)$ over $F$, then by the previous case we have that $[E : F]$ divides $d!$. Since $d! < n!$, it follows that in this case $[E : F]$ divides $n!$ as well. Hence we may assume that $E$ is not the splitting field of $h(x)$ over $F$. Let $K$ be the splitting field of $h(x)$ over $F$. Then $F \subseteq K \subsetneq E$ and so $[E : K] > 1$. We claim that we also have that $[K : F] > 1$. Indeed, assume instead that $[K : F] = 1$ so that $K = F$. Then $h(x)$ splits in $F$ and in particular it has a root in $F$. Since $\deg(h) \geq 2$, Lemma 3.4(2) gives that $h(x)$ is reducible, which contradicts our assumption. Therefore we also have that $[K : F] > 1$. Now in $K[x]$ we still have that $f(x) = h(x)g(x)$, and so $E$ is the splitting field of $g(x)$ over $K$. Then

$$[E : F] = [E : K][K : F],$$

where both $[E : K]$ and $[K : F]$ are greater than 1. It follows that both $[E : K]$ and $[K : F]$ are strictly smaller than $[E : F]$. By induction hypothesis we obtain that $[K : F]$ divides $\deg(h)! = d!$ and that $[E : K]$ divides $\deg(g)! = (n - d)!$. Then $[E : F] = [E : K][K : F]$ divides $d!(n - d)!$ which itself divides $n!$ since

$$\binom{n}{d} = \frac{n!}{n!(n - d)!} \in \mathbb{Z}.$$