

**Exercise 1.** 1. Let  $L'$  denote the field extension of  $K$  of degree 1. This means that  $L'$  is a field that contains  $K$ , and that has a  $K$ -vector space structure such that the dimension of  $L'$  as a  $K$ -vector space is 1. The  $K$ -subspace of  $L'$  generated by 1 is equal to  $K$ , and equal to  $L'$  as well, due to the dimension of  $L'$  over  $K$  being 1. Hence  $K$  and  $L'$  coincide.

2. We take any  $\alpha \in L \setminus K$ . Then we have the following field extensions,  $K \subseteq K(\alpha) \subseteq L$ . From this, it follows using Proposition 4.2.15 that

$$\underbrace{[L : K]}_{=2} = [L : K(\alpha)] \cdot [K(\alpha) : K].$$

Since we take  $\alpha \notin K$ , it holds that  $K \neq K(\alpha)$ , and hence by the first point,  $[K(\alpha) : K] \neq 1$ . From this, it follows using the equation above that  $[K(\alpha) : K] = 2$ . But that means that  $[L : K(\alpha)] = 1$ , from which it follows by the first point that  $L = K(\alpha)$ .

3. Since  $L = K(\alpha)$ , and  $[L : K] = 2$ , it holds that  $\{1, \alpha\}$  forms a  $K$ -linear basis of  $K(\alpha)$ . This means in particular that  $\alpha^2$  is a  $K$ -linear combination of 1 and  $\alpha$ . There exists  $a, b \in K$  such that  $\alpha^2 = b \cdot 1 + a \cdot \alpha \Leftrightarrow \alpha^2 - a\alpha - b = 0$ . We define  $d$  to be  $d = a^2 + 4b$ , the discriminant of the quadratic equation. We now show that  $d$  is a square in  $K(\alpha)$ . We do so by multiplying the quadratic equation by 4 (note that the characteristic of  $K$  is not equal to 2), and completing the square, to find:

$$4\alpha^2 - 4a\alpha - 4b = 0 \Leftrightarrow (2\alpha - a)^2 - a^2 - 4b = 0 \Leftrightarrow (2\alpha - a)^2 = a^2 + 4b = d.$$

Hence  $d$  is a square in  $K(\alpha)$ , and we let  $\delta = 2\alpha - a \in K(\alpha) \setminus K$ , with  $\delta^2 = d$ . By the second part of this exercise, it holds that  $L = K(\delta) = K(\sqrt{d})$ .

Let us give an alternative proof that illuminates the role of the discriminant. Since the characteristic of  $K$  is different from 2, the well-known theory of quadratic equations with coefficients in  $\mathbb{C}$  can be carried over verbatim to  $K$  to obtain the following: if  $p(x) = ax^2 + bx + c \in K[x]$  is a degree 2 polynomial, then the roots  $\xi_1, \xi_2$  of  $p(x)$  in any extension  $F$  of  $K$  can be written

$$\xi_1 = \frac{-2b + \sqrt{\Delta(p)}}{2a}, \quad \xi_2 = \frac{-2b - \sqrt{\Delta(p)}}{2a}$$

where  $\Delta(p) = b^2 - 4ac$  and  $\sqrt{\Delta(p)} \in F$  denotes a square root of  $\Delta(p)$ . Now observe that:

(a)  $K(\xi_i) = K(\xi_1, \xi_2)$  for any  $i = 1, 2$ . We can write in  $K(\xi_1)[x]$  that

$$p(x) = (x - \xi_1)q(x)$$

where necessarily  $\deg q(x) = 1$ . Thus  $q(x) = x - \xi_2$ , and so  $\xi_2 \in K(\xi_1)$ . Hence  $K(\xi_1) = K(\xi_1, \xi_2)$ , and by exchanging the roles of  $\xi_1$  and  $\xi_2$  we also obtain  $K(\xi_2) = K(\xi_1, \xi_2)$ .

(b)  $K(\xi_1, \xi_2) = K(\sqrt{\Delta(p)})$ . Indeed  $\sqrt{\Delta(p)} = 2a(\xi_1 - \xi_2)$  so the inclusion  $\supseteq$  holds. Also it follows from the formulae for  $\xi_1$  and  $\xi_2$  that  $\subseteq$  holds.

So we obtain that  $K(\xi_1) = K(\xi_2) = K(\xi_1, \xi_2) = K(\sqrt{\Delta(p)})$  as subfields of  $F$ . Taking  $F = L$  and  $p(x) = m_{\alpha, K}$ , we obtain an alternative proof of the exercise.

4. From the definition of  $\delta$ , it immediately follows that  $\{1, \delta\}$  forms a  $K$ -linear basis of  $K(\delta)$  as a  $K$ -vector space. By definition,  $[K(\delta) : K]$  is the dimension of  $K(\delta)$  as a  $K$ -vector space, which is 2.

**Exercise 2.** 1. There are two options for  $\mathbb{Q}(\sqrt{a})$ . If  $a$  is a square in  $\mathbb{Q}$ , then it holds that  $\sqrt{a}$  is contained in  $\mathbb{Q}$ , and hence  $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}$ , and so  $[\mathbb{Q}(\sqrt{a}) : \mathbb{Q}] = 1$ . If  $a$  is no square, then  $\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{a})$ , and the degree of this field extension is equal to 2, since the polynomial  $x^2 - a$  is zero for  $\sqrt{a}$ , and the polynomial is irreducible (since  $a$  is no square). The same holds for  $\mathbb{Q}(\sqrt{b})$ . We now use the fact (seen in Linear Algebra) that any two vector spaces over the same field are isomorphic if and only if they are of the same dimension. In our case, both  $\mathbb{Q}(\sqrt{a})$  and  $\mathbb{Q}(\sqrt{b})$  can be of dimension 1 or 2 over  $\mathbb{Q}$ , depending on whether or not  $a$  resp.  $b$  is a square. We conclude that  $\mathbb{Q}(\sqrt{a})$  is of the same dimension over  $\mathbb{Q}$  as  $\mathbb{Q}(\sqrt{b})$ , and hence isomorphic, if and only if both  $a$  and  $b$  are simultaneously squares in  $\mathbb{Q}$ , or both are simultaneously not squares.

2. We now assume that  $\mathbb{Q}(\sqrt{a})$  and  $\mathbb{Q}(\sqrt{b})$  are isomorphic as fields. We claim that this holds if and only if they are equal as subfields of  $\mathbb{C}$ . This means that there exists  $c \in \mathbb{Q}$  such that  $\sqrt{a} = c\sqrt{b}$ .

First, we assume that  $\sqrt{a} = c\sqrt{b}$ . Then,  $\sqrt{a}$  and  $\sqrt{b}$  generate the same field extension of  $\mathbb{Q}$ , and hence clearly the two fields are isomorphic.

Secondly, assume that the fields  $\mathbb{Q}(\sqrt{a})$  and  $\mathbb{Q}(\sqrt{b})$  are isomorphic. Denote the isomorphism  $\varphi : \mathbb{Q}(\sqrt{a}) \rightarrow \mathbb{Q}(\sqrt{b})$ . We note that from  $\varphi(1) = 1$ , it follows that  $\varphi$  acts as the identity on  $\mathbb{Z}$ , and furthermore on  $\mathbb{Q}$ . On one hand, we have that  $\varphi(\sqrt{a}) = u + \sqrt{b}v$  for some  $u, v \in \mathbb{Q}$ . On the other hand, with  $a \in \mathbb{Q}$ , it holds that

$$a = \varphi(a) = \varphi(\sqrt{a}^2) = \varphi(\sqrt{a})^2 = (u + \sqrt{b}v)^2 = (u^2 + bv^2) + \sqrt{b}(2uv).$$

We now distinguish between two cases.

- If  $\sqrt{b} \in \mathbb{Q}$ , then  $\varphi(\sqrt{a}) \in \mathbb{Q}$ , and hence  $\sqrt{a} \in \mathbb{Q}$ . (If  $\sqrt{a}$  was not contained in  $\mathbb{Q}$ , then  $\varphi$  would be an isomorphism from  $\mathbb{Q}(\sqrt{a}) \neq \mathbb{Q}$  to  $\mathbb{Q}$ . This is a contradiction to  $\varphi$  being injective.) Then,

$$\sqrt{a} = \frac{\sqrt{a}}{\sqrt{b}} \cdot \sqrt{b},$$

and  $\sqrt{a} = c\sqrt{b}$  with  $c := \frac{\sqrt{a}}{\sqrt{b}} \in \mathbb{Q}$ .

- If  $\sqrt{b} \notin \mathbb{Q}$ , then

$$a = (u^2 + bv^2) + \sqrt{b}(2uv),$$

with  $\sqrt{b} \notin \mathbb{Q}$ . Since  $a \in \mathbb{Q}$ , it follows that  $2uv = 0$ , and hence either  $u = 0$  or  $v = 0$ . If  $u = 0$ , then  $a = bv^2 \Rightarrow \sqrt{a} = \sqrt{b}v$ , and hence the property is satisfied. If  $v = 0$ , then  $\varphi(\sqrt{a}) = u \in \mathbb{Q}$ . It then follows that the image of  $\varphi$  is contained in  $\mathbb{Q}$ , which means that  $\varphi$  can not be an isomorphism. Hence this case does not occur.

**Exercise 3.** 1. We have the following field extensions,

$$K \subset K(\alpha^2) \subset K(\alpha) \subset L.$$

By proposition 4.2.15, it follows that

$$[L : K] = [L : K(\alpha)] \cdot [K(\alpha) : K(\alpha^2)] \cdot [K(\alpha^2) : K].$$

Since the degree of the field extension  $L$  over  $K$  is odd, it follows that the degrees on the right hand side of the equality above are odd as well. We now look at the extension  $K(\alpha)$  over  $K(\alpha^2)$ . The degree of this extension is at most 2, since the polynomial  $x^2 - \alpha^2 \in K(\alpha^2)[x]$  vanishes at  $\alpha$ . But since the degree needs to be odd, it follows that it is 1. Hence  $K(\alpha) = K(\alpha^2)$ .

2. We first show that  $\sqrt{p} \notin \mathbb{Q}(\sqrt{q})$ . If  $\sqrt{p}$  is contained in  $\mathbb{Q}(\sqrt{q})$ , then there are  $r, s \in \mathbb{Q}$  such that  $\sqrt{p} = r + s\sqrt{q}$ . From this, it follows that

$$p = (r + s\sqrt{q})^2 = (r^2 + s^2q) + (2rs)\sqrt{q}.$$

Using the fact that  $p \in \mathbb{Q}$ , we compare the right hand side and left hand side, and note that  $2rs = 0$ . If  $r = 0$ , then  $p = s^2q$  which is a contradiction with  $p, q$  prime and distinct.

If  $s = 0$ , then  $\sqrt{p} = r \Rightarrow p = r^2$ , which is a contradiction to  $p$  prime.

It follows that  $\sqrt{p} \notin \mathbb{Q}(\sqrt{q})$ . The same argument, with the roles of  $p$  and  $q$  reversed shows that  $\sqrt{q} \notin \mathbb{Q}(\sqrt{p})$ .

We now compute the degree of the field extension  $\mathbb{Q}(\sqrt{p}, \sqrt{q})$  over  $\mathbb{Q}$ . We have the following extensions of fields,

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\sqrt{p}, \sqrt{q}).$$

From proposition 4.2.15 it follows that

$$[\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}(\sqrt{p})] \cdot [\mathbb{Q}(\sqrt{p}) : \mathbb{Q}].$$

We calculate both degrees on the right hand side separately. Firstly,  $[\mathbb{Q}(\sqrt{p}) : \mathbb{Q}] = 2$ . This holds because  $\sqrt{p} \notin \mathbb{Q}$ . The polynomial  $x^2 - p \in \mathbb{Q}[x]$  vanishes at  $\sqrt{p}$ , and combining Gauss III with Eisenstein for the prime  $p$ , it follows that the polynomial is irreducible over  $\mathbb{Q}$ . Hence it is the minimal polynomial, and the degree is 2.

Secondly,  $[\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}(\sqrt{p})] = 2$ . This holds because  $\sqrt{q} \notin \mathbb{Q}(\sqrt{p})$ . Therefore, the degree of the extension is not equal to 1. Furthermore, the degree of the extension is at most 2, since  $\sqrt{q}^2 = q \in \mathbb{Q}$ , and hence  $\sqrt{q}^2 \in \mathbb{Q}(\sqrt{p})$ . Combining these restrictions, the degree of the extension is equal to 2, and hence the product of the two extensions is 4, meaning that  $[\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}] = 4$ .

3. We have the following extension of fields,  $K \subset K(\alpha) \subset K(\alpha, \beta)$ . Using proposition 4.2.15, it follows that

$$[K(\alpha, \beta) : K] = [K(\alpha, \beta) : K(\alpha)] \cdot [K(\alpha) : K].$$

From this, it follows that  $m = [K(\alpha) : K]$  divides  $[K(\alpha, \beta) : K]$ . The same argument for the extension of fields  $K \subset K(\beta) \subset K(\alpha, \beta)$  shows that  $n$  divides  $[K(\alpha, \beta) : K]$ . Using the fact that  $m$  and  $n$  are coprime, it follows that  $mn$  divides  $[K(\alpha, \beta) : K]$ . This means that the degree of the field extension is a multiple of  $mn$ . We show that it is equal to  $mn$  by considering the first field extension again,  $K \subset K(\alpha) \subset K(\alpha, \beta)$ . Since  $[K(\beta) : K] = n$ , it holds in particular that the degree of the field extension  $K(\alpha, \beta)$  over  $K(\alpha)$  is at most  $n$ . Hence  $[K(\alpha, \beta) : K]$  is at most  $nm$ . On the other hand, as we have seen above, it is at least  $mn$ , from which we conclude that it is exactly  $mn$ .

The two field extensions are illustrated below.

$$\begin{array}{ccc}
 & K & \\
 & \supseteq & \subseteq \\
 K(\alpha) & & K(\beta) \\
 & \subseteq & \supseteq \\
 & K(\alpha, \beta) & 
 \end{array}$$

#### Exercise 4.

It holds that  $\mathbb{Q}(\sqrt{3} + \sqrt{7}) \subseteq \mathbb{Q}(\sqrt{3}, \sqrt{7})$ . We show that indeed it holds that  $\mathbb{Q}(\sqrt{3} + \sqrt{7}) =$

$\mathbb{Q}(\sqrt{3}, \sqrt{7})$ . For this, it is enough to show that  $\sqrt{3} \in \mathbb{Q}(\sqrt{3} + \sqrt{7})$  and  $\sqrt{7} \in \mathbb{Q}(\sqrt{3} + \sqrt{7})$ . We denote  $K = \mathbb{Q}(\sqrt{3} + \sqrt{7})$ . It holds that  $(\sqrt{3} + \sqrt{7})^3 = 24\sqrt{3} + 16\sqrt{7} \in K$ . With this, and using that  $-16\sqrt{3} - 16\sqrt{7} \in K$ , it follows that their sum is contained in  $K$  as well,

$$(24\sqrt{3} + 16\sqrt{7}) + (-16\sqrt{3} - 16\sqrt{7}) = 8\sqrt{3}.$$

Now using that  $\frac{1}{8} \in K$ , and  $8\sqrt{3} \in K$  we deduce that their product  $\sqrt{3} \in K$ . From  $\sqrt{3} \in K$ , it immediately follows that  $\sqrt{7} \in K$  as well, since  $\sqrt{7} = (\sqrt{3} + \sqrt{7}) - \sqrt{3}$ . This shows that indeed  $K = \mathbb{Q}(\sqrt{3}, \sqrt{7})$ .

The degree of the field extension  $[\mathbb{Q}(\sqrt{3}, \sqrt{7}) : \mathbb{Q}]$  is by definition the dimension of  $\mathbb{Q}(\sqrt{3}, \sqrt{7})$  as a  $\mathbb{Q}$ -vector space. Using exercise 3.2, it follows that the degree is 4.  $\{1, \sqrt{3}, \sqrt{7}, \sqrt{3}\sqrt{7}\}$  forms a basis of this vector space.

**Exercise 5.** 1. If  $p = 2$ , then  $e^{2i\pi/2} = -1$ , which is contained in  $\mathbb{R}$ , and hence  $\mathbb{R}(e^{2i\pi/p}) = \mathbb{R}$ . From this, it follows that the degree of the extension is equal to 1.

For  $p \neq 2$ , it holds that  $e^{2i\pi/p}$  is a complex number, and not contained in  $\mathbb{R}$ . By example 4.2.14 (a), we know that  $[\mathbb{C} : \mathbb{R}] = 2$ . Using exercise 1.2, it follows that  $\mathbb{R}(e^{2i\pi/p}) = \mathbb{C}$ , and hence  $[\mathbb{R}(e^{2i\pi/p}) : \mathbb{R}] = [\mathbb{C} : \mathbb{R}] = 2$ .

- By definition,  $\alpha$  vanishes over  $t^{42} + t^{41} + \dots + t^2 + t + 1$ . Furthermore, using the fact that 43 is prime, and Example 3.9.4(b), it follows that  $t^{42} + t^{41} + \dots + t^2 + t + 1$  is irreducible over  $\mathbb{Q}$ . Hence we get that  $m_{\alpha, \mathbb{Q}} = t^{42} + t^{41} + \dots + t^2 + t + 1$ , and so  $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 42$ .
- We follow the same steps as example 4.2.16(a). First, we note that we have the following field extensions,  $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[5]{13}) \subseteq \mathbb{Q}(\sqrt[5]{13}, i)$ . We can calculate the degree of the extension  $\mathbb{Q}(\sqrt[5]{13}, i)$  over  $\mathbb{Q}$  using proposition 4.2.15. It holds that

$$[\mathbb{Q}(\sqrt[5]{13}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[5]{13}, i) : \mathbb{Q}(\sqrt[5]{13})] \cdot [\mathbb{Q}(\sqrt[5]{13}) : \mathbb{Q}].$$

First, we calculate  $[\mathbb{Q}(\sqrt[5]{13}) : \mathbb{Q}]$ . The polynomial  $x^5 - 13$  vanishes at  $\sqrt[5]{13}$ . Furthermore, the polynomial is irreducible over  $\mathbb{Q}$ : By Gauss III, it is equivalent to showing that the polynomial is irreducible over  $\mathbb{Z}$ . We can apply Eisenstein's criterion with  $p = 13$ , from which irreducibility over  $\mathbb{Z}$  follows. Therefore,  $m_{\sqrt[5]{13}, \mathbb{Q}} = x^5 - 13$ , and the degree of the field extension is 5.

Secondly, we calculate  $[\mathbb{Q}(\sqrt[5]{13}, i) : \mathbb{Q}(\sqrt[5]{13})]$ . Since  $\mathbb{Q} \subseteq \mathbb{R}$ , and  $\sqrt[5]{13} \in \mathbb{R}$ , it follows that  $\mathbb{Q}(\sqrt[5]{13}) \subseteq \mathbb{R}$ . Hence  $i \notin \mathbb{Q}(\sqrt[5]{13})$ . Using that  $i$  is a root of  $x^2 + 1$ , we get that the degree of  $i$  over  $\mathbb{Q}(\sqrt[5]{13})$  is 2, and hence  $[\mathbb{Q}(\sqrt[5]{13}, i) : \mathbb{Q}(\sqrt[5]{13})] = 2$ .

By the formula above, it follows that

$$[\mathbb{Q}(\sqrt[5]{13}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[5]{13}, i) : \mathbb{Q}(\sqrt[5]{13})] \cdot [\mathbb{Q}(\sqrt[5]{13}) : \mathbb{Q}] = 2 \cdot 5 = 10.$$

- There are two possibilities. The first possibility is that  $\alpha$  is the root  $\alpha = [1]_3$ . In that case,  $\mathbb{F}_3(\alpha) = \mathbb{F}_3$ , and hence  $[\mathbb{F}_3(\alpha) : \mathbb{F}_3] = 1$ . We can therefore write the polynomial  $t^4 - t^3 - t^2 - t - [1]_3 = (t - [1]_3)(t^3 - t + [1]_3)$ . If  $\alpha \neq [1]_3$ , then  $\alpha$  is a root of the polynomial  $t^3 - t + [1]_3$ . But this polynomial is irreducible over  $\mathbb{F}_3$ , since neither  $[0]_3$ ,  $[1]_3$  or  $[2]_3$  is a root of  $t^3 - t + [1]_3$ . We conclude with the fact that  $m_{\alpha, \mathbb{F}_3} = t^3 - t + [1]_3$ , and hence  $[\mathbb{F}_3(\alpha) : \mathbb{F}_3] = 3$ .
- We note that  $(3 + \sqrt{5})^2 = 14 + 6\sqrt{5} \Rightarrow 3 + \sqrt{5} = \sqrt{14 + 6\sqrt{5}}$ . Therefore,  $\mathbb{Q}(\sqrt{14 + 6\sqrt{5}}, \sqrt{3}) = \mathbb{Q}(3 + \sqrt{5}, \sqrt{3}) = \mathbb{Q}(\sqrt{5}, \sqrt{3})$ . It follows that  $[\mathbb{Q}(\sqrt{5}, \sqrt{3}) : \mathbb{Q}] = 4$ .  $\{1, \sqrt{3}, \sqrt{5}, \sqrt{3}\sqrt{5}\}$  forms a basis of  $\mathbb{Q}(\sqrt{5}, \sqrt{3})$  as a  $\mathbb{Q}$ -vector space.

6. We calculate the degree of the extension using proposition 4.2.15 for the extension  $\mathbb{Q} \subseteq \mathbb{Q}((\sqrt[6]{7})^2) \subseteq \mathbb{Q}(\sqrt[6]{7})$ , from which it follows that

$$[\mathbb{Q}(\sqrt[6]{7}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[6]{7}) : \mathbb{Q}((\sqrt[6]{7})^2)] \cdot [\mathbb{Q}((\sqrt[6]{7})^2) : \mathbb{Q}].$$

We first calculate  $[\mathbb{Q}(\sqrt[6]{7}) : \mathbb{Q}]$ . The polynomial  $x^6 - 7 \in \mathbb{Q}[x]$  is zero for  $\sqrt[6]{7}$ . Furthermore, by Gauss III, it is irreducible if it is irreducible over  $\mathbb{Z}$ . Applying Eisenstein with  $p = 7$ , this holds. Hence  $m_{\sqrt[6]{7}, \mathbb{Q}} = x^6 - 7$ , and the degree of the field extension is 6.

Secondly, we calculate  $[\mathbb{Q}((\sqrt[6]{7})^2) : \mathbb{Q}]$ . It holds that  $(\sqrt[6]{7})^2 = \sqrt[3]{7}$ . The polynomial  $x^3 - 7 \in \mathbb{Q}[x]$  is zero for  $\sqrt[3]{7}$ . Furthermore, by Gauss III, it is irreducible if it is irreducible over  $\mathbb{Z}$ . Applying Eisenstein with  $p = 7$ , this holds. Hence  $m_{\sqrt[3]{7}, \mathbb{Q}} = x^3 - 7$ , and the degree of the field extension is 3.

Using the formula above, we get that  $[\mathbb{Q}(\sqrt[6]{7}) : \mathbb{Q}((\sqrt[6]{7})^2)] = 2$ .

7. We apply the same technique as in the exercise above, noting that we have an extension as follows,  $\mathbb{F}_2 \subseteq \mathbb{F}_2(\alpha^2) \subseteq \mathbb{F}_2(\alpha)$ , and hence

$$[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = [\mathbb{F}_2(\alpha) : \mathbb{F}_2(\alpha^2)] \cdot [\mathbb{F}_2(\alpha^2) : \mathbb{F}_2].$$

On the left hand side, the degree is equal to 3, since  $m_{\alpha, \mathbb{F}_2} = t^3 + t + [1]_2$ . Hence on the right hand side, one of the factors is 1, and the other one is three. We note that  $[\mathbb{F}_2(\alpha^2) : \mathbb{F}_2]$  can not be 1, since  $\alpha^2 \notin \mathbb{F}_2$ . If  $\alpha^2$  was contained in  $\mathbb{F}_2$ , then the polynomial  $t^2 - \alpha^2 \in \mathbb{F}_2[t]$  vanishes at  $\alpha$ , which contradicts the fact that  $[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = 3$ . Therefore,  $[\mathbb{F}_2(\alpha^2) : \mathbb{F}_2] = 3$ , and so  $[\mathbb{F}_2(\alpha) : \mathbb{F}_2(\alpha^2)] = 1$ .

**Exercise 6.** 1. We show that the minimal polynomial  $m_{\beta, K} = x^7 - y \in K[x]$ . It holds that the polynomial vanishes at  $\beta$ , since

$$\beta^7 - y = \left(\frac{\alpha^3}{y^2}\right)^7 - y = \frac{(\alpha^7)^3}{y^{14}} - y \stackrel{*}{=} \frac{(y^5)^3}{y^{14}} - y = y - y = 0,$$

where in the equation  $*$ , we use the fact that  $\alpha$  is a root of  $f$  in  $L$ , and hence  $\alpha^7 = y^5$ . Furthermore, the polynomial is irreducible in  $K[x]$ : We use Gauss III to deduce that  $f$  is irreducible in  $K[x] = (\mathbb{C}(y))[x]$  if and only if  $f$  is irreducible in  $(\mathbb{C}[y])[x]$ . Since  $y$  is irreducible in  $\mathbb{C}[y]$ , we may use Eisenstein with  $p = y$  to deduce that  $x^7 - y$  is irreducible in  $(\mathbb{C}[y])[x]$ , and hence in  $K[x]$ . This proves that the minimal polynomial  $m_{\beta, K} = x^7 - y \in K[x]$ . We conclude that  $[K(\beta) : K] = 7$ .

2. To show that  $K(\alpha) = K(\beta)$ , we show that  $K(\alpha) \subseteq K(\beta)$  and  $K(\beta) \subseteq K(\alpha)$ .

We note that

$$\beta^5 = \left(\frac{\alpha^3}{y^2}\right)^5 = \frac{\alpha^{15}}{(y^5)^2} = \frac{\alpha^{15}}{(\alpha^7)^2} = \alpha.$$

From this, it follows that  $\alpha = \beta^5 \in K(\beta)$ , and hence  $K(\alpha) \subseteq K(\beta)$ . On the other hand,  $\beta = \frac{\alpha^3}{y^2} \in K(\alpha)$ , and hence  $K(\beta) \subseteq K(\alpha)$ .

3. We first remark that by Gauss III,  $f$  is irreducible in  $\mathbb{C}[x, y] = (\mathbb{C}[y])[y]$  if and only if  $f$  is irreducible in  $(\mathbb{C}(y))[x] = K[x]$ . By the first and second part of this exercise, it holds that  $[K(\alpha) : K] = 7$ . From this, it follows that the degree of the minimal polynomial  $m_{\alpha, K}$  is 7. Now since  $\alpha$  is a root of  $x^7 - y^5 \in K[x]$ , it follows that  $x^7 - y^5 \mid m_{\alpha, K}$ . Since both polynomials are of degree 7, it follows that  $m_{\alpha, K} \sim x^7 - y^5$ , and from  $m_{\alpha, K}$  being irreducible in  $K[x]$  it follows that  $x^7 - y^5$  is irreducible in  $K[x]$  as well. Applying Gauss III, with  $x^7 - y^5$  being primitive, it follows that  $x^7 - y^5$  is irreducible in  $\mathbb{C}[x, y]$ .