Dummit & Foote Chapter 14 Selected Exercises

Igor van Loo
LinkedIn

January 31, 2024

Contents

1 Chapter 14.1 **2**
1.1 2
1.2 2
1.3 2
1.4 3
1.5 3
1.6 3
1.7 4

2 Chapter 14.2 **4**
2.1 4
2.2 5
2.3 5
2.4 5
2.5 6
2.6 6
2.7 - Unfinished 6
2.8 - Unfinished 6
2.9 7
2.10 7
2.11 - Unfinished 7
2.12 7
2.13 8
2.14 8
2.15 8
2.16 9
2.17 10

3 Chapter 14.3 **11**
3.1 11
3.2 11
3.3 12
3.4 12
3.5 12
3.6 - Unfinished 13
3.7 13

1 Chapter 14.1

Question 1.1

1. Show that if the field K is generated over F by the elements $a_1, \cdots, a_n$ then an automorphism σ of K fixing F is uniquely determined by $\sigma(a_1), \cdots, \sigma(a_n)$. In particular, show that an automorphism fixes K if and only if it fixes a set of generators for K

2. Let $G \leq \mathrm{Gal}(K/F)$ be a subgroup of the Galois group of the extension K/F and suppose $\sigma_1, \cdots, \sigma_k$ are generators for G. Show that the subfield E/F is fixed by G if and only if it is fixed by the generators $\sigma_1, \cdots, \sigma_k$

Solution.

(a) Let $x \in K = F(\alpha_1, \cdots, \alpha_n)$, then we have that $x = a_1\theta_1 + \cdots + a_m\theta_m$ where $\theta_i = \alpha_1^{j_{i,1}} \cdots \alpha_n^{j_{i,n}}$. (This is basically saying that each element in K is expressed as a linear combination of all possible products of the α_i's, which is obviously true, for example, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}$)

Then, we have that

$$\sigma(x) = \sigma(a_1\theta_1 + \cdots + a_m\theta_m) = a_1\sigma(\theta_1) + \cdots + a_m\sigma(\theta_m)$$

since σ is a homomorphism that fixes F. Furthermore,

$$\sigma(\theta_i) = \sigma(\alpha_1^{j_{i,1}} \cdots \alpha_n^{j_{i,n}}) = \sigma(\alpha_1^{j_{i,1}}) \cdots \sigma(\alpha_n^{j_{i,n}})$$

and therefore $\sigma(x)$ is determined by $\sigma(a_1), \cdots, \sigma(a_n)$.

In particular, $\sigma(x) = x \in K \iff \sigma(\alpha_i) = \alpha_i$ for $1 \leq i \leq n$

(b) Let $G = \langle \sigma_1, \ldots, \sigma_k \rangle$. That is, any element $\sigma \in G$ can be written in the form

$$\sigma = \prod_{j=1}^{m} \gamma_j^{n_j}$$

where each $\gamma_j \in \{\sigma_i \mid 1 \leq i \leq k\}$ (note that γ_j are not necessarily distinct, in fact there are likely to be repeats), and $n_j \in \mathbb{Z}$.

By assumption, each $\sigma_i \restriction_E = \mathbb{1}$, that is $\sigma_i^{n_i}(x) = x$ for any $x \in E$ and $n_i \in \mathbb{Z}$. It follows immediately that

$$\sigma(x) = (\prod_{j=1}^{m} \gamma_j^{n_j})(x) = x.$$

□

Question 1.2

Let τ be the map $\tau : \mathbb{C} \to \mathbb{C}$ defined by $\tau(a + bi) = a - bi$. Prove that τ is an automorphism of $\mathbb{C}$

Solution. It is easily shown that τ is a homomorphism and that it is bijective and hence τ is an isomorphism □

Question 1.3

Determine the fixed field of complex conjugation on $\mathbb{C}$

Solution. The fixed field of complex conjugation is $F = \{a + bi \in \mathbb{C} \mid \tau(a + bi) = a + bi\}$, therefore we need $\tau(a + bi) = a - bi = a + bi \implies 2bi = 0 \implies b = 0$ therefore $a + bi \in F \iff b = 0$. In this case we have $a + bi = a \in \mathbb{R}$ and therefore $F = \mathbb{R}$ □

Question 1.4

Prove that $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are not isomorphic

Solution. An important note is that these 2 fields are isomorphic as vector spaces over $\mathbb{Q}$, however, they are not field isomorphic. We have previously shown in Chapter 13 that $\sqrt{2} \notin \mathbb{Q}(\sqrt{3})$ and therefore if there was an isomorphism $\varphi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$ then we can notice that $\varphi(\sqrt{2})^2 = \varphi(2) = 2$ because $\mathbb{Q}$ is fixed (Alternatively you can use the simpler fact that $\sigma(1) = 1$) which implies $\varphi(\sqrt{2}) = \pm\sqrt{2} \notin \mathbb{Q}(\sqrt{3})$ and therefore this isomorphism cannot exist. □

Question 1.5

Determine the automorphisms of the extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ explicitly

Solution. First we note that $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})] = 2$ and we have minimal polynomial $x^2 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})$ with roots $\pm\sqrt[4]{2}$ and therefore we can only have 2 automorphisms

$$\begin{aligned} \mathbb{1} &: \sqrt[4]{2} \mapsto \sqrt[4]{2} \quad (Identity) \\ \sigma &: \sqrt[4]{2} \mapsto -\sqrt[4]{2} \end{aligned}$$

□

Question 1.6

Let k be a field

(a) Show that the mapping $\varphi : k[t] \to k[t]$ defined by $\varphi(f(t)) = f(at+b)$ for fixed $a, b \in k, a \neq 0$ is an automorphism of $k[t]$ which is the identity on k

(b) Conversely, let φ be an automorphism of $k[t]$ which is the identity on k. Prove that there exist $a, b \in k$ with $a \neq 0$ such $\varphi(f(t)) = f(at+b)$ as in (a)

Solution.

(a) Let $f(t), g(t) \in k[t]$, then we show that φ is an isomorphism.

$$\varphi((f+g)(t)) = (f+g)(at+b) = f(at+b) + g(at+b) = \varphi(f(t)) + \varphi(g(t))$$

and

$$\varphi((fg)(t)) = (fg)(at+b) = f(at+b)g(at+b) = \varphi(f(t))\varphi(g(t))$$

Therefore φ is a homomorphism. Now, suppose $\varphi(f(t)) = \varphi(g(t))$. Then $f(at+b) = g(at+b)$ and because $k[at+b] = k[t]$ we have that $f(t) = g(t)$. Lastly let $g(t) \in k[t]$ then take $f(t) = g(\frac{t}{a} - \frac{b}{a}) \in k[t]$ and we have $\varphi(f(t)) = \varphi(f(at+b)) = g(a(\frac{t}{a} - \frac{b}{a}) + b) = g(t)$ and therefore φ is bijective, finally we conclude φ is an isomorphism.

Lastly, if $f(t) = c \in k \subset k[t]$ then $\varphi(f(t)) = f(at+b) = c$ and therefore φ is the identity on k

(b) Suppose $\varphi(f(t)) = h(t)f(t) + g(t)$ where $g(t), h(t) \in k[t]$ then because φ is identity on k we would have $\varphi(c) = h(t)c + g(t) = c \implies g(t) = 0, h(t) = 1$ therefore we must have that $\varphi(f(t)) = f(g(t))$ for some $g(t) \in k[t]$.

We want $g(t) = at + b$ therefore we must show that if $\deg(g(t)) \geq 2$ there is a contradiction.

Suppose $\deg(g(t)) \geq 2$ this implies that the $\deg(f(g(t)) \geq 2$ and therefore this map is not surjective, therefore we conclude $\deg(g(t)) \leq 1$.

If $\deg(g(t)) = 0$ then $g(t) = b \in k$ and this map is not injective.

Finally, we conclude that $\deg(g(t)) = 1$ and therefore $g(t) = at + b$ where $a, b \in k$ and $\varphi(f(t)) = f(g(t)) = f(at+b)$

□

Question 1.7

This exercise determines $\mathrm{Aut}(\mathbb{R}/\mathbb{Q})$

(a) Prove that any $\sigma \in \mathrm{Aut}(\mathbb{R}/\mathbb{Q})$ takes squares to squares and takes positive reals to positive reals. Conclude that $a < b$ implies $\sigma(a) < \sigma(b)$ for every $a, b \in \mathbb{R}$

(b) Prove that any $-\frac{1}{m} < a - b < \frac{1}{m}$ implies $-\frac{1}{m} < \sigma(a) - \sigma(b) < \frac{1}{m}$ for every positive integer m. Conclude that σ is a continuous map on $\mathbb{R}$

(c) Prove that any continuous map on $\mathbb{R}$ which is the identity on $\mathbb{Q}$ is the identity map, hence $\mathrm{Aut}(\mathbb{R}/\mathbb{Q}) = 1$

Solution.

(a) Let $a \in \mathbb{R}$ be a square. That is, $\exists b \in \mathbb{R}$ s.t. $b^2 = a$. Then $\sigma(a) = \sigma(b^2) = (\sigma(b))^2$. That is, σ takes squares to squares. Since the only squares in $\mathbb{R}$ are the non-negative reals, but $\sigma(a) = 0 \implies a = 0$, so it must be that σ takes positive reals to positive reals.

Suppose now that $b - a > 0$, then $\sigma(b - a) > 0$, giving that $\sigma(b) - \sigma(a) > 0$.

(b) Since $\forall \sigma \in \mathrm{Aut}(\mathbb{R}/\mathbb{Q})$, σ fixes $\mathbb{Q}$, then

$$\begin{aligned} -\frac{1}{m} &< a - b < \frac{1}{m} \\ \sigma\left(-\frac{1}{m}\right) &< \sigma(a-b) < \sigma\left(\frac{1}{m}\right), \quad \sigma \text{ preserves order by part (a)} \\ -\frac{1}{m} &< \sigma(a) - \sigma(b) < \frac{1}{m}, \quad \sigma \restriction_{\mathbb{Q}} = \mathbb{1} \end{aligned}$$

Now we prove continuity. Let $\varepsilon > 0$ and take $|a - b| < \delta = \frac{1}{m} < \varepsilon$ then we have that $|\sigma(a) - \sigma(b)| < \frac{1}{m} < \varepsilon$

(c) (Method 1) Let $x \in \mathbb{R}$, suppose $x < \sigma(x)$ then $\exists q \in \mathbb{Q}$ such that $x < q < \sigma(x)$ and then using $x < q$ we have from part (a) $\sigma(x) < \sigma(q) = q$ and therefore $x = \sigma(x)$ which is a contradiction. Similarly if $x > \sigma(x)$ we get a contradiction, therefore we conclude $x = \sigma(x), \forall x \in \mathbb{R}$

(Method 2) Let $x \in \mathbb{R}, \varepsilon > 0$. Since σ is continuous we know $\exists \delta_1 > |x - y|$ such that $|\sigma(x) - \sigma(y)| < \frac{\varepsilon}{2}$. Take $a \in \mathbb{Q}$ such that $|a - x| < \min\{\frac{\varepsilon}{2}, \delta_1\}$ then we have that

$$|\sigma(x) - x| = |\sigma(x) - a + a - x| = |\sigma(x) - a| + |a - x| = |\sigma(x) - \sigma(a)| + |a - x| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$$

which shows that $|\sigma(x) - x| < \varepsilon, \forall x \in \mathbb{R}$

□

2 Chapter 14.2

Question 2.1

Determine the minimal polynomial over $\mathbb{Q}$ for the element $\sqrt{2} + \sqrt{5}$

Solution. $\mathbb{Q}(\sqrt{2} + \sqrt{5}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{5})$ which is Galois over $\mathbb{Q}$ and therefore the roots of the minimal polynomial are $\pm\sqrt{2} \pm \sqrt{5}$ which are all distinct. Hence the minimal polynomial is $(x - (\sqrt{2} + \sqrt{5})(x + (\sqrt{2} + \sqrt{5}))(x - (\sqrt{2} - \sqrt{5}))(x + (\sqrt{2} - \sqrt{5})) = x^4 - 14x^2 + 9$ □

Question 2.2

Determine the minimal polynomial over $\mathbb{Q}$ for the element $1 + \sqrt[3]{2} + \sqrt[3]{4}$

Solution. We have shown in chapter 13 that $\mathbb{Q}(1 + \sqrt[3]{2} + \sqrt[3]{4}) \subset \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[3]{2}, \zeta)$ where $\zeta = e^{\frac{2\pi i}{3}}$ which is a Galois extension, therefore $\sqrt[3]{2}$ must be sent to $\sqrt[3]{2}, \sqrt[3]{2}\zeta, \sqrt[3]{2}\zeta^2$ and notice that we only care about where $\sqrt[3]{2}$ is sent as $\sqrt[3]{2}^2 = \sqrt[3]{4}, \sqrt[3]{2}^3 = 1$.

Knowing this we know that the 3 roots of our minimal polynomial are

$$r_1 = 1 + \sqrt[3]{2} + \sqrt[3]{4}$$
$$r_2 = 1 + \sqrt[3]{2}\zeta + \sqrt[3]{4}\zeta^2$$
$$r_3 = 1 + \sqrt[3]{2}\zeta^2 + \sqrt[3]{4}\zeta$$

Painfully expanding $(x-r_1)(x-r_2)(x-r_3)$ gives you $x^3 - 3x^2 - 3x - 1$. Alternatively $(r_1 - 1)^3 = (\sqrt[3]{2} + \sqrt[3]{4})^3 = 2 + 3\sqrt[3]{16} + 3\sqrt[3]{32} + 4 = 6 + 6(\sqrt[3]{2} + \sqrt[3]{4}) = 6 + 6(r_1 - 1) = 6r_1$ □

Question 2.3

Determine the Galois group of $f = (x^2 - 2)(x^2 - 3)(x^2 - 5)$. Determine all subfields of the splitting field of f

Solution. The splitting field of f is clearly $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ and any automorphism of K will map $\sqrt{a} \to \pm\sqrt{a}$ where $a \in \{2, 3, 5\}$ and therefore there are 8 total automorphisms. Now we must show that there are no more than 8, this is done by noting that $|\mathrm{Aut}(K/\mathbb{Q})| \leq [K : \mathbb{Q}] = 8$, furthermore we can conclude that this extensions is Galois. The subfields are

$\mathbb{Q}(\sqrt{a})$ where $a \in \{2, 3, 5, 6, 10, 15, 30\}$

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q}(\sqrt{2}, \sqrt{5}), \mathbb{Q}(\sqrt{3}, \sqrt{5}), \mathbb{Q}(\sqrt{2}, \sqrt{15}), \mathbb{Q}(\sqrt{3}, \sqrt{10}), \mathbb{Q}(\sqrt{5}, \sqrt{6}), \mathbb{Q}(\sqrt{10}, \sqrt{15})$$

□

Question 2.4

Let p be a prime. Determine the elements of the Galois group of $x^p - 2$

Solution. The splitting field of $x^p - 2$ is $K = \mathbb{Q}(\sqrt[p]{2}, \zeta)$ where ζ is the p-th root of unity.

1. Consider $G_1 = \mathrm{Gal}(K/\mathbb{Q}(\zeta))$ and $\tau(\sqrt[p]{2}) = \sqrt[p]{2}\zeta$ and it fixes ζ. The order of τ is p and therefore $G_1 \cong \langle \tau \rangle \cong C_p$
2. Consider $G_2 = \mathrm{Gal}(K/\mathbb{Q}(\sqrt[p]{2}))$ and $\sigma(\zeta) = \zeta^a$ and it fixes $\sqrt[p]{2}$. The order of σ is $p - 1$ because $a^{p-1} \equiv 1 \pmod{p}$ and therefore $G_2 \cong \langle \sigma \rangle \cong C_{p-1}$

Furthermore, we know the following:

1. $[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt[p]{2})][\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}] = (p - 1)p$ is a galois extension and hence $|G| = |\mathrm{Gal}(K/\mathbb{Q})| = p(p - 1)$
2. $|\langle \tau \rangle||\langle \sigma \rangle| = p(p - 1)$
3. $|\langle \tau \rangle \bigcap \langle \sigma \rangle| = 1$

Therefore, using point 2 and 3 and the following $|\langle \tau \rangle \langle \sigma \rangle| = \frac{|\langle \tau \rangle||\langle \sigma \rangle|}{|\langle \tau \rangle \bigcap \langle \sigma \rangle|}$ we have that $G = \langle \tau \rangle \langle \sigma \rangle$. Futhermore we can notice that $K^{G_1}/\mathbb{Q} = \mathbb{Q}(\zeta)/\mathbb{Q}$ is a galois extension because $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1 = |\mathrm{Aut}(\mathbb{Q}(\zeta)/\mathbb{Q})|$ and therefore $G_1 \lhd G$ and therefore we have $G \cong C_p \rtimes C_{p-1}$ □

Question 2.5

Prove that the Galois group of $x^p - 2$ for p a prime is isomorphic to the group of matrices

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$$

where $a, b \in \mathbb{F}_p, a \neq 0$

Solution. Let $G = \mathrm{Gal}(\mathbb{Q}(\sqrt[p]{2}, \zeta)/\mathbb{Q})$. Now notice that any element $\varphi \in G$ is determined by $\varphi(\zeta)$ and $\varphi(\sqrt[p]{2})$, where $\varphi(\zeta) = \zeta^a$ for some $1 \leq i \leq p-1$ and $\varphi(\sqrt[p]{2}) = \sqrt[p]{2}\zeta^b$ for some $0 \leq b \leq p-1$ then we define the map

$$\alpha : G \to \{\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \text{ where } a, b \in \mathbb{F}_p, a \neq 0\}$$

$$\alpha(\varphi) = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$$

This is a homomorphism and bijective, hence an isomorphism □

Question 2.6

Let $K = \mathbb{Q}(\sqrt[8]{2}, i)$ and let $F_1 = \mathbb{Q}(i), F_2 = \mathbb{Q}(\sqrt{2}), F_3 = \mathbb{Q}(-\sqrt{2})$. Prove that $\mathrm{Gal}(K/F_1) \cong \mathbb{Z}_8, \mathrm{Gal}(K/F_2) \cong D_8, \mathrm{Gal}(K/F_3) \cong Q_8$

Solution. We follow the discussion from Chapter 14.2 where we found that

$$\mathrm{Gal}(K/\mathbb{Q}) = \left\langle \sigma, \tau : \sigma^8 = \tau^2 = 1, \sigma\tau = \tau\sigma^3 \right\rangle \text{ where } \sigma = \begin{cases} \sqrt[8]{2} \to \zeta\sqrt[8]{2} \\ i \to i \\ \zeta \to \zeta^5 \end{cases} \quad \text{and } \tau = \begin{cases} \sqrt[8]{2} \to \sqrt[8]{2} \\ i \to -i \\ \zeta \to \zeta^7 \end{cases}$$

1. Clearly σ fixes i therefore $\mathrm{Gal}(K/F_1) = \left\langle \sigma \right\rangle \cong \mathbb{Z}_8$
2. τ fixes $\sqrt{2}$ already, now we need $\sigma^n(\sqrt{2}) = \sigma^n(\sqrt[8]{2})^4 = \sqrt{2}\zeta^{4n}$, we need $\zeta^{4n} = 1 \implies n = 2, 4, 6$, therefore $\mathrm{Gal}(K/F_2) = \{1, \sigma^2, \sigma^4, \sigma^6, \tau, \tau\sigma^2, \tau\sigma^4, \tau\sigma^6\} = \left\langle \sigma^2, \tau \right\rangle$ where $(\sigma^2)^4 = \tau^2 = 1$ and $\sigma^2\tau = \tau\sigma^6$ which describes D_8 and therefore $\mathrm{Gal}(K/F_2) \cong D_8$
3. Note that $\sqrt{-2} = \sqrt{2}i(\sqrt[8]{2})^4 i$, clearly τ will not fix this. We try $\sigma^n((\sqrt[8]{2})^4 i) = \zeta^{4n}\sqrt{2}i$ therefore $n = 2, 4, 6$ from part 2. Next we try $\tau\sigma^n((\sqrt[8]{2})^4 i) = \tau(\zeta^4 n\sqrt{2}i) = -\zeta^{28n}\sqrt{2}i = -\zeta^{4n}\sqrt{2}i$, we need $-\zeta^4 = 1 \implies n = 1, 3, 5, 7$ therefore $\mathrm{Gal}(K/F_3) = \{1, \sigma^2, \sigma^4, \sigma^6, \tau\sigma, \tau\sigma^3, \tau\sigma^5, \tau\sigma^7\} = \left\langle \sigma^2, \tau\sigma^3 \right\rangle$ with the relations $(\sigma^2)^4 = 1, (\sigma^2)^2 = \sigma^4 = (\tau\sigma^3)^2, \tau\sigma^4 = (\sigma^2)^{-1}\tau\sigma^3$ which describes Q_8 and therefore $\mathrm{Gal}(K/F_3) \cong Q_8$

□

Question 2.7 - Unfinished

Determine all the subfields of the splitting field of $x^8 - 2$ which are Galois over $\mathbb{Q}$

Question 2.8 - Unfinished

Suppose K is a Galois extension of F of degree p^n for some prime p and some $n \geq 1$. Show there are Galois extensions of F contained in K of degrees p and p^{n-1}

Question 2.9

Give an example of fields F_1, F_2, F_3 with $\mathbb{Q} \subset F_1 \subset F_2 \subset F_3$, $[F_3 : \mathbb{Q}] = 8$ and each field if Galois over all of its subfields with the exception that F_2 is not Galois over $\mathbb{Q}$

Solution. Take $F_3 = \mathbb{Q}(\sqrt[4]{2}, i), F_2 = \mathbb{Q}(\sqrt[4]{2}), F_1 = \mathbb{Q}(\sqrt{2})$. Then we have that F_3 is Galois over $F_2, F_1, \mathbb{Q}$, F_2 is Galois over F_1 but not Galois over $\mathbb{Q}$ and F_1 is Galois over $\mathbb{Q}$ □

Question 2.10

Determine the Galois group of the splitting field over $\mathbb{Q}$ of $x^8 - 3$

Solution. The splitting field of the polynomial is $K = \mathbb{Q}(\sqrt[8]{3}, \zeta) = \mathbb{Q}(\sqrt[8]{3}, \sqrt{2}, i)$ where ζ is an 8-th root of unity. This extension is of degree 32 because of the following, $[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt[8]{3}, \sqrt{2})][\mathbb{Q}(\sqrt[8]{3}, \sqrt{2}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 32$ because we can show that $\sqrt[8]{3} \notin \mathbb{Q}(\sqrt{2})$.
Any automorphism of $\mathrm{Aut}(K/\mathbb{Q})$ is of the form

$$\sqrt[8]{3} \mapsto \sqrt[8]{3}\zeta^i, 1 \leq i \leq 7, \quad \sqrt{2} \mapsto \pm\sqrt{2}, \quad i \mapsto \pm i$$

Alternatively, consider the generators

1. $\sigma : \sqrt[8]{3} \mapsto \sqrt[8]{3}\zeta$.
2. $\tau_i : \zeta \mapsto \zeta^i$, for $i \in \{3, 5, 7\}$

and work out the relations. Namely, all automorphisms can be written in the form $\sigma^a, \sigma^a\tau_3, \sigma^a\tau_5, \sigma^a\tau_7$ for $0 \leq a \leq 7$, giving exactly 32 automorphisms as desired. □

Question 2.11 - Unfinished

Suppose $f(x) \in \mathbb{Z}[x]$ is an irreducible quartic whose splitting field has Galois group S_4 over $\mathbb{Q}$ (there are many such quartics, cf. Section 6). Let θ be a root of $f(x)$ and set $K = \mathbb{Q}(\theta)$. Prove that K is an extension of $\mathbb{Q}$ of degree 4 which has no proper subfields. Are there any Galois extensions of $\mathbb{Q}$ of degree 4 with no proper subfields?

Question 2.12

Determine the Galois group of the splitting field over $\mathbb{Q}$ of $x^4 - 14x^2 + 9$.

Solution. **Note:** From Question 2.1 we can already see that the splitting field of the polynomial is $\mathbb{Q}(\sqrt{2}+\sqrt{5}) = \mathbb{Q}(\sqrt{2}, \sqrt{5})$ and therefore $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}+\sqrt{5})/\mathbb{Q}) \cong K_4$, now we can just confirm the answer.
Solving for x^2 using the quadratic formula we see that

$$x^2 = \frac{14 \pm \sqrt{14^2 - 4(1)(9)}}{2} = 7 \pm 2\sqrt{10} = (\sqrt{2} \pm \sqrt{5})^2$$

Then, we have that the roots of the polynomial are $\pm\sqrt{2} \pm \sqrt{5}$ and therefore the splitting field of the polynomial is $\mathbb{Q}(\sqrt{2}+\sqrt{5}) = \mathbb{Q}(\sqrt{2}, \sqrt{5})$ which has 4 automorphisms.

Finally, we conclude

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2}+\sqrt{5})/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau = \tau\sigma\} \cong K_4 \text{ where } \sigma = \begin{cases} \sqrt{2} \to \sqrt{2} \\ \sqrt{5} \to -\sqrt{5} \end{cases} \quad \text{and } \tau = \begin{cases} \sqrt{2} \to -\sqrt{2} \\ \sqrt{5} \to \sqrt{5} \end{cases}$$

□

Question 2.13

Prove that if the Galois group of the splitting field of a cubic over $\mathbb{Q}$ is the cyclic group of order 3 then all the roots of the cubic are real.

Solution. Suppose the 3 roots are not all real, then we must have one real root r_1 and 2 complex roots $z, \bar{z}$ in which case the splitting field would be $\mathbb{Q}(r_1, z)$ and we have an automorphism of $\mathrm{Gal}(\mathbb{Q}(r_1,z)/\mathbb{Q})$ which would fix r_1 and send $z \mapsto \bar{z}$ and therefore 2 would divide $|\mathrm{Gal}(\mathbb{Q}(r_1,z)/\mathbb{Q})|$ and hence $\mathrm{Gal}(\mathbb{Q}(r_1,z)/\mathbb{Q}) \ncong \mathbb{Z}_3$ □

Question 2.14

Show that $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ is a cyclic quartic field, i.e, is a Galois extension of degree 4 with cyclic Galois group

Solution. Let $K = \mathbb{Q}(\sqrt{2+\sqrt{2}})$. We find a polynomial with root $x = \sqrt{2+\sqrt{2}}$ using the following $x^2 = 2+\sqrt{2} \implies x^2 - 2 = \sqrt{2} \implies x^4 - 4x^2 + 4 = 2 \implies x^4 - 4x^2 + 2$ which is a degree 4 polynomial and is irreducible by Eisenstein criterion, therefore it is the minimum polynomial of $\sqrt{2+\sqrt{2}}$ over $\mathbb{Q}$. The 4 roots are $\pm\sqrt{2 \pm \sqrt{2}}$ and we can notice that $\sqrt{2-\sqrt{2}} = \frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}} \in K$, so all our roots are contained in K which makes K the splitting field of a separable polynomial (as the roots are distinct) and therefore a Galois Extension of $\mathbb{Q}$, hence $|\mathrm{Aut}(K/\mathbb{Q})| = [K : \mathbb{Q}] = 4$. Furthermore, if $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma(\sqrt{2+\sqrt{2}}) = \sqrt{2-\sqrt{2}}$ we have that

$$\sigma^2(\sqrt{2+\sqrt{2}}) = \sigma(\sqrt{2-\sqrt{2}}) = \sigma(\frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}}) = \frac{\sigma(\sqrt{2})}{\sigma(\sqrt{2+\sqrt{2}})} = \frac{\sigma((\sqrt{2+\sqrt{2}})^2 - 2)}{\sqrt{2-\sqrt{2}}} = \frac{-\sqrt{2}}{\sqrt{2+\sqrt{2}}} = -\sqrt{2-\sqrt{2}}$$

Therefore $\mathrm{ord}(\sigma) > 2$ and it must divide 4, which implies that $\mathrm{ord}(\sigma) = 4$ and therefore $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_4$ □

Question 2.15

(Biquadratic extensions) Let F be a field of characteristic $\neq 2$

(a) If $K = F(\sqrt{D_1}, \sqrt{D_2})$ where $D_1, D_2 \in F$ have the property than none of D_1, D_2, D_1D_2 is a square in F, prove that K/F is a Galois extension with $\mathrm{Gal}(K/F)$ isomorphic to the Klein 4 group

(b) Conversly, suppose K/F is a Galois extension with $\mathrm{Gal}(K/F) \cong K_4$. Prove that $K = F(\sqrt{D_1}, \sqrt{D_2})$ where $D_1, D_2 \in F$ have the property that none of D_1, D_2, D_1D_2 is square in F

Solution.

(a) If D_1, D_2 are not square in F this implies that $[F(\sqrt{D_1}) : F] = [F(\sqrt{D_2}) : F] = 2$ and therefore

$$[K : F] = [K : F(\sqrt{D_1})][F(\sqrt{D_1}) : F] \leq [F(\sqrt{D_1}) : F][F(\sqrt{D_2}) : F] = 4$$

We then have that $[K : F(\sqrt{D_1})] \leq 2$. To show that $[K : F(\sqrt{D_1})] = 2$ we show that $\sqrt{D_2} \notin F(\sqrt{D_1})$. Suppose $\sqrt{D_2} \in F(\sqrt{D_1})$ then we have $\sqrt{D_2} = a + b\sqrt{D_1}$ where $a, b \in F$, this implies $D_2 = a^2 + 2ab\sqrt{D_1} + b^2 D_1$, because D_2 is not square in F we must have $a = 0$ or $b = 0$. If $b = 0$ then $D_2 = a^2$ which means D_2 is a square, a contradiction. If $a = 0$ then $D_2 = b^2 D_1 \implies D_1 D_2 = b^2 D_1^2$ which means $D_1 D_2$ is a square, a contradiction. Hence we conclude $\sqrt{D_2} \notin F(\sqrt{D_1})$ and therefore $[K : F] = 4$. Furthermore, it is easy to see that we have 4 automorphisms of K fixing F

$$Id \quad \sigma = \begin{cases} \sqrt{D_1} \mapsto -\sqrt{D_1} \\ \sqrt{D_2} \mapsto \sqrt{D_2} \end{cases} \qquad \tau = \begin{cases} \sqrt{D_1} \mapsto \sqrt{D_1} \\ \sqrt{D_2} \mapsto -\sqrt{D_2} \end{cases} \qquad \sigma\tau = \tau\sigma = \begin{cases} \sqrt{D_1} \mapsto -\sqrt{D_1} \\ \sqrt{D_2} \mapsto -\sqrt{D_2} \end{cases}$$

and hence we conclude that K/F is a Galois extension with $\mathrm{Gal}(K/F) \cong K_4$

(b) Given that $\mathrm{Gal}(K/F) \cong K_4$ and K_4 has 3 non-trivial subgroups or order 2; $\langle 1, \sigma\rangle, \langle 1, \tau\rangle, \langle 1, \sigma\tau\rangle$ there will be correspondingly 3 subfields E_1, E_2, E_3 of K containing F where they are degree 2 extensions of F. Let $E_1 = F(\sqrt{D_1}), E_2 = F(\sqrt{D_2})$ where D_1, D_2 are not square in F as needed, then the fact that $E_1 \neq E_2 \implies D_1D_2$ is not square in F from part (a), therefore $E_3 = F(\sqrt{D_1D_2})$ is a degree 2 extension of F. Finally, we have that E_1E_2 is a degree 4 extension over F and $E_1, E_2, E_3 \subset E_1E_2 \implies K = E_1E_2 = F(\sqrt{D_1}, \sqrt{D_2})$

□

Question 2.16

(a) Prove that $x^4 - 2x^2 - 2$ is irreducible over $\mathbb{Q}$

(b) Show that the roots of this quartic are

$$\alpha_1 = \sqrt{1+\sqrt{3}} \quad \alpha_3 = -\sqrt{1+\sqrt{3}}$$
$$\alpha_2 = \sqrt{1-\sqrt{3}} \quad \alpha_4 = -\sqrt{1-\sqrt{3}}$$

(c) Let $K_1 = \mathbb{Q}(\alpha_1)$ and $K_2 = \mathbb{Q}(\alpha_2)$. Show that $K_1 \neq K_2$ and $K_1 \cap K_2 = \mathbb{Q}(\sqrt{3}) = F$.

(d) Prove that K_1, K_2 and K_1K_2 are Galois over F with $\mathrm{Gal}(K_1K_2/F)$ the Klein 4-group. Write out the elements of $\mathrm{Gal}(K_1K_2/F)$ explicitly. Determine all the subgroups of the Galois group and give their corresponding fixed subfields of K_1K_2 containing F.

(e) Prove that the splitting field of $x^4 - 2x^2 - 2$ over $\mathbb{Q}$ is of degree 8 with dihedral Galois group

Solution.

(a) Using Eisenstein with $p = 2$ shows that $x^4 - 2x^2 - 2$ is irreducible over $\mathbb{Q}$

(b) $(x - \sqrt{1+\sqrt{3}})(x + \sqrt{1+\sqrt{3}})(x - \sqrt{1-\sqrt{3}})(x + \sqrt{1-\sqrt{3}}) = (x^2 - (1+\sqrt{3}))(x^2 - (1-\sqrt{3})) = x^4 - 2x^2 - 2$

(c) Notice that $1 - \sqrt{3} < 0$ and $\mathbb{Q}(\alpha_1) \subset \mathbb{R}$ and α_2 is a complex number and therefore $\alpha_2 \notin \mathbb{Q}(\alpha_1)$ which implies $K_1 \neq K_2$. Since $K_1 \neq K_2$, then $F = K_1 \cap K_2$ is a proper subfield of K_1 and K_2 which are both degree 4 extensions of $\mathbb{Q}$, hence F has degree 1 or 2, it is easy to see that $\sqrt{3} \in F$ and $\sqrt{3} \notin \mathbb{Q}$ and hence we can conclude $F = \mathbb{Q}(\sqrt{3})$

(d) $[K_1 : F] = \frac{[K_1:\mathbb{Q}]}{[F:\mathbb{Q}]} = \frac{4}{2} = 2$, quadratic extensions are always Galois, similarly K_2 is a Galois extension of F, additionally this shows that $1 \pm \sqrt{3}$ are not squares in F. Let $K = F(\sqrt{1+\sqrt{3}}, \sqrt{1-\sqrt{3}})$ notice that K_1, K_2 are proper subfields of K, hence $K_1K_2 \subset K$. Conversely, we know that $[K_1K_2 : F] \leq [K_1 : F][K_2 : F] = 4$ therefore we must have $K_1K_2 = K$. By the previous exercise we know that $\mathrm{Gal}(K_1K_2/F) \cong K_4$. We can explicitly write out the elements of $\mathrm{Gal}(K_1K_2/F)$ as follows

$$\textit{Identity} \quad \sigma_1 = \begin{cases} \alpha_1 \mapsto -\alpha_1 \\ \alpha_2 \mapsto \alpha_2 \end{cases} \qquad \sigma_2 = \begin{cases} \alpha_1 \mapsto \alpha_1 \\ \alpha_2 \mapsto -\alpha_2 \end{cases} \qquad \sigma_3 = \sigma_1\sigma_2 = \sigma_2\sigma_1 = \begin{cases} \alpha_1 \mapsto -\alpha_1 \\ \alpha_2 \mapsto -\alpha_2 \end{cases}$$

The subgroups are $\langle\sigma_1\rangle, \langle\sigma_2\rangle, \langle\sigma_3\rangle$ with corresponding subfields $F(\alpha_2), F(\alpha_1), F(\alpha_1\alpha_2) = F(\sqrt{-2})$

(e) The splitting field of $x^4 - 2x^2 - 2$ is $K = F(\alpha_1, \alpha_2)$ and we know $[F(\alpha_1, \alpha_2) : F] = 4$ and $[F : \mathbb{Q}] = 2$ from (c) and (d), therefore $[F(\alpha_1, \alpha_2) : \mathbb{Q}] = [F(\alpha_1, \alpha_2) : F][F : \mathbb{Q}] = 8$. All that is left is to show that $\mathrm{Gal}(F(\alpha_1, \alpha_2)/\mathbb{Q}) \cong D_8$

In Chapter 14.6 we learn that $\mathrm{Gal}(F(\alpha_1, \alpha_2)/\mathbb{Q}) \hookrightarrow S_4$, the reason being that a Galois extension permutes the roots. Using this and the fact that D_8 is the only subgroup of S_4 with order 8, we conclude that $\mathrm{Gal}(F(\alpha_1, \alpha_2)/\mathbb{Q}) \cong D_8$

□

Question 2.17

Let K/F be any finite extension and let $\alpha \in K$. Let L be a Galois extension of F containing K and let $H \leq \mathrm{Gal}(L/F)$ be the subgroup corresponding to K. Define the *norm* of α from K to F to be

$$N_{K/F}(\alpha) = \prod_{\sigma} \sigma(\alpha)$$

where the product is taken over all the embeddings of K into an algebraic closure of F (so over a set of coset representatives for H in $\mathrm{Gal}(L/F)$ by the Fundamental Theorem of Galois Theory). This is a product of Galois conjugates of α. In particular, if K/F is Galois this is $\prod_{\sigma \in \mathrm{Gal}(K/F)} \sigma(\alpha)$

(a) Prove that $N_{K/F}(\alpha) \in F$

(b) Prove that $N_{K/F}(\alpha\beta) = N_{K/F}(\alpha)N_{K/F}(\beta)$, so that the norm is a multiplicative map from K to F

(c) Let $K = F(\sqrt{D})$ be a quadratic extension of F. Show that $N_{K/F}(a + b\sqrt{D}) = a^2 - Db^2$

(d) Let $m_\alpha(x) = x^d + \cdots + a_1 x + a_0 \in F[x]$ be the minimal polynomial for $\alpha \in K$ over F. Let $n = [K : F]$. Prove that d divides n, that there are d distinct Galois conjugates of α which are all repeated n/d times in the product above and conclude that $N_{K/F}(\alpha) = (-1)^n a_0^{n/d}$

Solution.

(a) Let $\Omega = \{\sigma \mid \sigma H = H, H \leq \mathrm{Gal}(L/F)\}$ then $N_{K/F}(\alpha) = \prod_{\sigma\in\Omega} \sigma(\alpha)$. Showing that $N_{K/F}(\alpha) \in F$ is analogous to showing that any $\tau \in \mathrm{Gal}(L/F)$ fixes $N_{K/F}(\alpha)$ as F is the fixed field of $\mathrm{Gal}(L/F)$.

Now, let $\tau \in \mathrm{Gal}(L/F)$ we then have

$$\tau(N_{K/F}(\alpha)) = \tau(\prod_{\sigma\in\Omega} \sigma(\alpha)) = \prod_{\sigma\in\Omega} \tau(\sigma(\alpha))$$

We can now notice that if $\tau\sigma_1$ is in the same coset as $\tau\sigma_2$ then $\tau\sigma_1 = \tau\sigma_1 h, h \in H$ which implies that σ_1 is in the same coset as σ_2, therefore $\{\sigma \mid \sigma H = H\} = \{\tau\sigma \mid \tau\sigma H = H\} = \Omega$. Hence we can simplify

$$\tau(N_{K/F}(\alpha)) = \prod_{\sigma\in\Omega} \tau(\sigma(\alpha)) = \prod_{\sigma\in\Omega} \sigma(\alpha) = N_{K/F}(\alpha)$$

We have now shown that $N_{K/F}(\alpha)$ is fixed by arbitrary $\tau \in \mathrm{Gal}(L/F)$

(b) σ is a homomorphism (remember that an embedding is just an injective homomorphism) and therefore

$$N_{K/F}(\alpha\beta) = \prod_{\sigma} \sigma(\alpha\beta) = \prod_{\sigma} \sigma(\alpha)\sigma(\beta) = N_{K/F}(\alpha)N_{K/F}(\beta)$$

(c) If $K = F(\sqrt{D})$ is a quadratic extension then we have 2 embeddings. Namely, σ, τ where σ is identity and τ which fixes F and maps $\sqrt{D} \mapsto -\sqrt{D}$, hence

$$N_{K/F}(a + \sqrt{D}) = \sigma(a + b\sqrt{D})\tau(a + b\sqrt{D}) = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - b^2 D$$

(d) $m_\alpha(x)$ has degree d and therefore $[F(\alpha) : F] = d$ which divides $[K : F] = n$. Let $m_\alpha(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$, where $a_i \in F$. Consider $H = \{\sigma \in G \mid \sigma(\alpha) = \alpha\}$ and notice that it is a subgroup of G. For any $\sigma \in G$, it must be that $\sigma : \alpha \mapsto \alpha_i$, where $\alpha_1 = \alpha, \ldots, \alpha_d$ are the roots of $m_\alpha(x)$. Since K/F is Galois, then any irreducible polynomial over F is separable, and thus we can conclude that the α_i's are distinct.

Now consider G acting on K in the obvious way (That is $\sigma \cdot \alpha = \sigma(\alpha)$). Then notice that $H = \mathrm{Stab}(\alpha)$, and by orbit-stabiliser theorem, we have

$$\begin{aligned} |G| &= |H||\mathcal{O}(\alpha)| \\ n &= |H|(d) \quad \text{there are } d \text{ distinct roots} \\ |H| &= \frac{n}{d} \end{aligned}$$

Then

$$\begin{aligned}N_{K/F}(\alpha) &= \prod_{\sigma\in G}\sigma(\alpha)\\ &= \prod_{i=1}^{d}\prod_{\tau\in H}(\sigma_i\tau)(\alpha)\\ &= \prod_{i=1}^{d}(\sigma_i(\alpha))^{\frac{n}{d}} \qquad \tau(\alpha)=\alpha,\ \forall\tau\in H\\ &= \prod_{i=1}^{d}\alpha_i^{\frac{n}{d}}\end{aligned}$$

Since $a_0 = (-1)^d\prod_{i=1}^{d}\alpha_i$, then it follows that $N_{K/F}(\alpha) = \left(\prod_{i=1}^{d}\alpha_i\right)^{\frac{n}{d}} = \left((-1)^d a_0\right)^{\frac{n}{d}} = (-1)^n a_0^{\frac{n}{d}}$ as desired.

□

3 Chapter 14.3

Question 3.1

Factor $x^8 - x$ into irreducibles in $\mathbb{Z}[x]$ and $\mathbb{F}_2[x]$

Solution. In $\mathbb{Z}[x]$ we have $x^8 - x = x(x^7-1) = x\cdot\Phi_1(x)\cdot\Phi_7(x) = x(x-1)(x^6+x^5+x^4+x^3+x^2+x+1)$. From the discussion of Proposition 18 we have $x^8 - x = x(x-1)(x^3+x+1)(x^3+x^2+1)$ in $\mathbb{F}_2[x]$ □

Question 3.2

Write out the multiplication table for $\mathbb{F}_4$ and $\mathbb{F}_8$

Solution. We know $x^4 - x = x(x-1)(x^2+x+1)$ and $g(x) = x^2+x+1$ is irreducible in $\mathbb{F}_2[x]$. Let θ be a root of $g(x)$, we then have

$$\mathbb{F}_4 \cong \mathbb{F}_2[x]/(x^2+x+1) \cong \mathbb{F}_2(\theta) = \{a+b\theta \mid a,b\in\mathbb{F}_2\} = \{0,1,\theta,1+\theta\}$$

Using $\theta^2+\theta+1=0$ we then have the multiplication table:

$\times$	0	1	θ	$\theta+1$
0	0	0	0	0
1	0	1	θ	$\theta+1$
θ	0	θ	$\theta+1$	1
$\theta+1$	0	$\theta+1$	1	θ

From Question 3.1 we have $x^8 - x = x(x-1)(x^3+x+1)(x^3+x^2+1)$ and $h(x) = x^3+x+1$ is irreducible in $\mathbb{F}_2[x]$, let α be a root of $h(x)$. We then have

$$\mathbb{F}_8 \cong \mathbb{F}_2(\alpha) \cong \mathbb{F}_2[x]/(x^3+x+1) \cong \{a+b\alpha+c\alpha^2 \mid a,b,c\in\mathbb{F}_2\} = \{0,1,\alpha,\alpha+1,\alpha^2,\alpha^2+1,\alpha^2+\alpha,\alpha^2+\alpha+1\}$$

Using $\alpha^3+\alpha+1=0$, we have the multiplication table:

$\times$	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	0	0	0	0	0	0	0
1	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
α	0	α	α^2	$\alpha^2+\alpha$	$\alpha+1$	1	$\alpha^2+\alpha+1$	α^2+1
$\alpha+1$	0	$\alpha+1$	$\alpha^2+\alpha$	α^2+1	$\alpha^2+\alpha+1$	α^2	1	α
α^2	0	α^2	$\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α	α^2+1	1
α^2+1	0	α^2+1	1	α^2	α	$\alpha^2+\alpha+1$	$\alpha+1$	$\alpha^2+\alpha$
$\alpha^2+\alpha$	0	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	1	α^2+1	$\alpha+1$	α	α^2
$\alpha^2+\alpha+1$	0	$\alpha^2+\alpha+1$	α^2+1	α	1	$\alpha^2+\alpha$	α^2	$\alpha+1$

□

Question 3.3

Prove that an algebraically closed field must be infinite

Solution.

(Method 1) Suppose K is a finite algebraically closed field, then $K \cong \mathbb{F}_{p^n} = \{\alpha \mid \alpha^{p^n} - \alpha = 0\}$. Let $\alpha_0, \alpha_1 \cdots \alpha_n$ be the distinct roots and hence all the elements of K, then $f(x) = 1 + \prod_{i=0}^{n}(x - \alpha_i)$ has no root in $K[x]$ which contradicts the assumption that K is algebraically closed.

(Method 2) Alternatively, for a field to be algebraically closed, it necessarily must contain roots of $x^{p^m} - x$ for any m and for any prime p. Since each $x^{p^m} - x$ has p^m distinct roots, then $|\mathbb{F}| \geq p^m$ for any p, m. That is, it must be infinite.

(Method 3) Alternatively, we proceed by contraposition. Fix some arbitrary finite field $\mathbb{F}_{p^n}$. Let q be a prime s.t. $q \nmid n$. By proposition 17, $\exists Q(x) \in \mathbb{F}_p$ irreducible and of degree q. Fix any $\alpha \in \mathbb{F}_{p^n}$. If $Q(\alpha) = 0$, then we have the following.

$$\mathbb{F}_p \subseteq \mathbb{F}_p(\alpha) \subseteq \mathbb{F}_{p^n}$$

where the degree of the first extension is q. But $q \nmid n$ and thus cannot be the case.

□

Question 3.4

Construct the finite field of 16 elements and find a generator for the multiplicative group. How many generators are there?

Solution. A finite field with 16 elements will be isomorphic to $\mathbb{F}_{2^4}$. Again by the discussion of Proposition 18 we have $x^{16} - x = x(x-1)(x^2+x+1)(x^4+x^3+1)(x^4+x+1)(x^4+x^3+x^2+x+1)$ and $f(x) = x^4 + x + 1$ is irreducible in $\mathbb{F}_2[x]$, let θ be a root of $f(x)$, hence we have

$$\mathbb{F}_{16} \cong \mathbb{F}_2[x]/(f(x)) \cong \mathbb{F}_2(\theta) = \{0, 1, \theta, \theta^2, \theta^3, 1+\theta, 1+\theta^2, 1+\theta^3, \theta+\theta^2, \theta+\theta^3, \theta^2+\theta^3, 1+\theta+\theta^2, 1+\theta+\theta^3, 1+\theta^2+\theta^3, \theta+\theta^2+\theta^3, 1+\theta+\theta^2+\theta^3\}$$

Now we can notice that $x^3 \neq x, x^5 = x + x^2 \neq x$ hence $\text{ord}(x) \neq 3$ or 5 but it must divide $15 = |\mathbb{F}_{16}^\times|$, hence $\text{ord}(x) = 15$ and $\langle x \rangle$ generates $\mathbb{F}_{16}^\times$, therefore we conclude $\langle x \rangle \cong \mathbb{Z}_{15}$ and hence there will be $\varphi(15) = 8$ generators, they are $\{x^a \mid \gcd(a, 15) = 1\} = \{x^1, x^2, x^4, x^7, x^8, x^{11}, x^{13}, x^{14}\}$ □

Question 3.5

Exhibit an explicit isomorphism between the splitting fields of $x^3 - x + 1$ and $x^3 - x - 1$ over $\mathbb{F}_3$

Solution. Notice that $f(x) = x^3 - x + 1$ and $g(x) = x^3 - x - 1$ are both irreducible in $\mathbb{F}_3[x]$ because $f(0) = f(1) = f(2) = 1 \neq 0$ and $g(0) = g(1) = g(2) = -1 = 2 \neq 0$, therefore we have

$$\mathbb{F}_{27} \cong \mathbb{F}_3[x]/(f(x)) \cong \mathbb{F}_3[x]/(g(x))$$

Let $\alpha(x) = ax^2 + bx + c$ be a root of $f(x)$ in $\mathbb{F}_3[x]/(g(x))$, then if we map $x \in \mathbb{F}_3/(f(x)) \mapsto \alpha(x)$ we have our isomorphism. Now, we need to find $\alpha(x)$ such that $f(\alpha(x)) = 0$

$$\begin{aligned} f(\alpha(x)) &= (ax^2 + bx + c)^3 - (ax^2 + bx + c) + 1 \\ &= ax^6 + bx^3 + c - ax^2 - bx - c + 1 \quad (d^3 = d \textit{ for } d \in \mathbb{F}_3) \\ &= a(x+1)^2 + b(x+1) + c - ax^2 - bx - c + 1 \quad (x^3 = x + 1 \textit{ in } \mathbb{F}_3/(g(x))) \\ &= ax^2 + 2ax + a + bx + b + c - ax^2 - bx - c + 1 \\ &= 2ax + b + a + 1 = 0 \end{aligned}$$

Therefore we have $a = 0, b = 2$, then we just let $c = 0$ and we have $\alpha(x) = 2x$, we finally have the explicit isomorphism

$$\begin{aligned} \mathbb{F}_3[x]/(f(x)) &\mapsto \mathbb{F}_3[x]/(g(x)) \\ x &\mapsto 2x \end{aligned}$$

$\square$

Question 3.6 - Unfinished

Suppose $K = \mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{D_1}, \sqrt{D_2})$ with $D_1, D_2 \in \mathbb{Z}$, is a biquadratic extension and that $\theta = a + b\sqrt{D_1} + c\sqrt{D_2} + d\sqrt{D_1 D_2}$ where $a, b, c, d \in \mathbb{Z}$ are integers. Prove that the minimal polynomial $m_\theta(x)$ for θ over $\mathbb{Q}$ is irreducible of degree 4 over $\mathbb{Q}$ but is reducible modulo every prime p. In particular show that the polynomial $x^4 - 10x^2 + 1$ is irreducible in $\mathbb{Z}[x]$ but is reducible modulo every prime. [Use the fact that there are no biquadratic extensions over finite fields.]

Question 3.7

Prove that one of 2, 3 or 6 is a square in $\mathbb{F}_p$ for every prime p. Conclude that the polynomial

$$x^6 - 11x^4 + 36x^2 - 36 = (x^2 - 2)(x^2 - 3)(x^2 - 6)$$

has a root modulo p for every prime p but has no root in $\mathbb{Z}$

Solution. Let $\langle x \rangle = \mathbb{F}_p^\times$. Then $a \in \mathbb{F}_p^\times$ is a square if and only if $a = x^{2k} = (x^k)^2$ where $b \in \mathbb{F}_p^\times, k \in \mathbb{Z}$. Now suppose 2 and 3 are not square in $\mathbb{F}_p$, this means $2 = x^{2k_1+1}$ and $3 = x^{2k_2+1}$ where $k_1, k_2 \in \mathbb{Z}$ and therefore $6 = x^{2(k_1+k_2+1)}$ is a square in $\mathbb{F}_p$.
Therefore, 2, 3 or 6 must be a square in $\mathbb{F}_p$ and hence WLOG suppose 2 is a square in $\mathbb{F}_p$ there is an $a \in \mathbb{F}_p$ such that $a^2 - 2 = 0$ which implies a is a root of $(x^2 - 2)(x^2 - 3)(x^2 - 6)$. Furthermore, the real roots of this polynomial are $\pm\sqrt{2}, \pm\sqrt{3}, \pm\sqrt{6}$ which are all not integers, hence the polynomial has no root in $\mathbb{Z}$. $\square$