Exercise 1 Let $E = \mathbb{Q}(\alpha)$, where α is a root of the equation:

$$\alpha^3 + \alpha^2 + \alpha + 2 = 0$$

Express $(\alpha^2 + \alpha + 1)(\alpha^2 + \alpha)$ and $(\alpha - 1)^{-1}$ in the form

$$a\alpha^2 + b\alpha + c \text{ with } a, b, c \in \mathbb{Q}$$

Proof.

$$\begin{aligned}(\alpha^2 + \alpha + 1)(\alpha^2 + \alpha) &= (\alpha^4 + \alpha^3 + \alpha^2) + (\alpha^3 + \alpha^2 + \alpha) &(1)\\ &= \alpha(\alpha^3 + \alpha^2 + \alpha) - 2 &(2)\\ &= -2\alpha - 2 &(3)\end{aligned}$$

Note by polynomial long division we see that:

$$(x - 1)(x^2 + 2x + 3) + 5 = x^3 + x^2 + x + 2 \tag{4}$$

So plugging in α in the above equation we get $(\alpha - 1)(\alpha^2 + 2\alpha + 3) = -5$

$$\begin{aligned}\frac{1}{\alpha - 1} &= \frac{\alpha^2 + 2\alpha + 3}{(\alpha - 1)(\alpha^2 + 2\alpha + 3)} &(5)\\ &= \frac{-1}{5}\alpha^2 + \frac{-2}{5}\alpha + \frac{-3}{5} &(6)\end{aligned}$$

□

Exercise 2 Let $E = F(\alpha)$, where α is algebraic over F, of odd degree. Show that $E = F(\alpha^2)$.

Proof. We will show that $\alpha \in F(\alpha^2)$. First note that this is clear if $n = 1$, since in that case $\alpha \in F$. So we can assume that $3 \leq n = 2m + 1$. Since $\{1, \alpha, \ldots, \alpha^{2m}\}$ is a basis let $a_i \in F$ such that:

$$\alpha^{2m+1} = \sum_{i=0}^{2m} a_i \alpha^i \tag{7}$$

Now we have:

$$\begin{aligned}(\alpha^2)^{m+1} &= \alpha^{2m+2}\\ &= \alpha\alpha^{2m+1}\\ &= \alpha \sum_{i=0}^{2m} a_i \alpha^i\\ &= a_{2m}\alpha^{2m+1} + \sum_{i=0}^{2m-1} a_i \alpha^{i+1}\\ &= \sum_{i=0}^{2m} a_{2m} a_i \alpha^i + \sum_{i=1}^{2m} a_{i-1}\alpha^i\\ (\alpha^2)^{m+1} &= \sum_{i=0}^{2m} (a_{2m}a_i + a_{i-1})\alpha^i \text{ where } a_{-1} = 0 \quad (\dagger)\end{aligned}$$

Let $\beta \in F(\alpha^2)$ be given by $\beta = \sum_{j=0}^{m}(a_{2m}a_{2j} + a_{2j-1})\alpha^{2j}$, all the even terms in †
Now by † we see that:

$$\begin{aligned}(\alpha^2)^{m+1} - \beta + a_{2j-1})\alpha^{2j} &= \sum_{i=0}^{2m}(a_{2m}a_i + a_{i-1})\alpha^i - \sum_{j=0}^{m}(a_{2m}a_{2j} + a_{2j-1})\alpha^{2j}\\ &= \sum_{j=0}^{m}(a_{2m}a_{2j+1} + a_{2j})\alpha^{2j+1} \text{ odd terms in } \dagger\\ &= \alpha(\sum_{j=0}^{m}(a_{2m}a_{2j+1} + a_{2j})\alpha^{2j})\end{aligned}$$

So finitely since we notice that $\sum_{j=0}^{m}(a_{2m}a_{2j+1}+a_{2j})\alpha^{2j} \in F(\alpha^2)$ we have

$$\alpha = \frac{(\alpha^2)^{m+1}-\beta}{\sum_{j=0}^{m}(a_{2m}a_{2j+1}+a_{2j})\alpha^{2j}} \in F(\alpha^2)$$

So $F(\alpha) \subseteq F(\alpha^2) \subseteq F(\alpha) = E$.

□

Exercise 3

Proof. Let $h(X) = \mathrm{Irr}(\beta, F(\alpha), X)$. Then, since $g(X) \in F(\alpha)[X]$ and $g(\beta) = 0$ we have $h(X) \mid g(X)$, so $\deg h \leq \deg g$. So note that:

$$\begin{aligned}[F(\alpha,\beta)\colon F] &= [F(\alpha,\beta)\colon F(\alpha)][F(\alpha)\colon F] \\ &= (\deg h)(\deg f)\end{aligned}$$

But on the other hand we have:

$$[F(\alpha,\beta)\colon F] = [F(\alpha,\beta)\colon F(\beta)]\underbrace{[F(\beta)\colon F]}_{\deg g}$$

Therefore we see that $\deg g \mid (\deg h)(\deg f)$, but since $gcd(\deg g, \deg f) = 1$ we have that $\deg g \mid \deg h$. So we have $\deg g \leq \deg h$. Therefore $\deg g = \deg h$, so $g(X) = ch(X)$ with $c \in F(\alpha)$. But by definition of Irr, $c = 1$. So $g(X) = \mathrm{Irr}(\beta, F(\alpha), X)$ and so is irreducibe in $F(\alpha)[X]$ □

Exercise 4 Let α be the real positive fourth root of 2. Find all intermidiate fields in the extension $\mathbb{Q}(\alpha)$ of $\mathbb{Q}$.

Proof. Notice that $\mathrm{Irr}(\alpha, \mathbb{Q}, X) = X^4 - 2$, so $[\mathbb{Q}(\alpha)\colon \mathbb{Q}] = 4$. Indeed α is a root of this polynomial and by Eisenstein this polynomila is irreducible.We claim that

Now notice that $(\alpha^2)^2 - 2 = \alpha^4 - 2 = 0$, so α^2 is a root of $X^2 - 2$. So we see that $[\mathbb{Q}(\alpha^2)\colon \mathbb{Q}] = 2$. So $\mathbb{Q} \subsetneq \mathbb{Q}(\alpha^2) \subsetneq \mathbb{Q}(\alpha)$.

Now let F be an intermidiate field of $\mathbb{Q}(\alpha)$ and $\mathbb{Q}$, then we have:

$$4 = [\mathbb{Q}(\alpha)\colon \mathbb{Q}] = [\mathbb{Q}(\alpha)\colon F][F\colon \mathbb{Q}]$$

So we see that $[F\colon \mathbb{Q}] \mid 4$, if $[F\colon \mathbb{Q}] = 1$ then $F = \mathbb{Q}$ if $[F\colon \mathbb{Q}] = 4$ then $F = \mathbb{Q}(\alpha)$, so assume that $[F\colon \mathbb{Q}] = 2$, so $[\mathbb{Q}(\alpha)\colon F] = 2$.

Now let's look at $m(X) = \mathrm{Irr}(\alpha, F, X)$ notice that since $F(\alpha) = \mathbb{Q}(\alpha)$ and $[\mathbb{Q}(\alpha)\colon F] = 3$ we see that $\deg m = 2$.

Now by inspection we notice that the roots of $X^4 - 2$ are $i^k\alpha$ where $k = 0, 1, 2, 3$. Now since $X^4 - 2 \in F[X]$ we see that $m(X) \mid X^4 - 2$, furthermore since $m(\alpha) = 0$ we have that $(X - \alpha) \mid m(X)$.

Therefore we see that:

$$m(X) = (X - \alpha)(X - i^k\alpha) \text{ for some } k = 1, 2, 3 \tag{8}$$

Note since $X - \alpha, m(X) \in \mathbb{Q}(\alpha)[X]$ this means that $X - i^k\alpha \in \mathbb{Q}(\alpha)[X]$. So $i^k\alpha \in \mathbb{Q}(\alpha)$, but since $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$ we see that k must be even. So we have that:

$$m(X) = (X - \alpha)(X + \alpha) = X^2 - \alpha^2 \in F[X] \tag{9}$$

So we see that $\alpha^2 \in F$, so $\mathbb{Q}(\alpha^2) \subseteq F$ but since $2 = [\mathbb{Q}(\alpha)\colon \mathbb{Q}(\alpha^2)] = [\mathbb{Q}(\alpha)\colon F][F\colon \mathbb{Q}(\alpha^2)] = 2[F\colon \mathbb{Q}(\alpha^2)]$, so $[F\colon \mathbb{Q}(\alpha^2)] = 1$ so $F = \mathbb{Q}(\alpha^2)$.

So the only intermidiate fields in the extension $\mathbb{Q}(\alpha)$ of $\mathbb{Q}$ are $\mathbb{Q}(\alpha), \mathbb{Q}(\alpha^2), \mathbb{Q}$. □

Exercise 5 If α is a complex root of $X^6 + X^3 + 1$, find all homomorphisms $\sigma\colon \mathbb{Q}(\alpha) \to \mathbb{C}$.

Proof.

Lemma 1. *For any homomorphism $\sigma\colon F \subseteq \mathbb{C} \to \mathbb{C}$, where F is as subfield of $\mathbb{C}$. We have $\sigma(r) = r$ for all $r \in \mathbb{Q}$.*

Proof. Recall $\sigma(1) = 1$, so for all $n \in \mathbb{N}^*$ we have

$$\sigma(n) = \sigma(\underbrace{1 + 1 + \cdots + 1}_{\text{n times}}) = \underbrace{\sigma(1) + \sigma(1) + \cdots + \sigma(1)}_{\text{n times}} = \underbrace{1 + 1 + \cdots + 1}_{\text{n times}} = n$$

Since $\sigma(0) = 0$ and $\sigma(-n) = -\sigma(n)$. We see that for all $n \in \mathbb{Z}$ we have $\sigma(n) = n$.

Therefore we see that $\sigma(\frac{1}{m}) = \sigma(m^{-1}) = (\sigma(m))^{-1} = m^{-1} = \frac{1}{m}$ for all $m \in \mathbb{Z} \setminus \{0\}$. For all $r \in \mathbb{Q}$ there exists $n \in \mathbb{Z}$ and $m \in \mathbb{N}^*$ such that $r = \frac{n}{m}$ and so we have

$$\sigma(r) = \sigma(\frac{n}{m}) = \sigma(n)\sigma(\frac{1}{m}) = \frac{\sigma(n)}{\sigma(m)} = \frac{n}{m} = r$$

□

Lemma 2. *If $\alpha \in \mathbb{C}$ is such that there exists $n \in \mathbb{N}^*$ such that $\alpha^n = 1$ and there doesn't exist a $m \in \mathbb{N}^*$ such that $\alpha^m = 1$, then $\alpha = e^{\frac{2i\pi k}{n}}$ where $\gcd(k, n) = 1$*

Proof. Recall from complex analysis we know that $\alpha = e^{\frac{2i\pi k}{n}}$, for some $0 \leq k \leq n$. Now let $d = \gcd(k, n)$, so let $k_1, n_1 \in \mathbb{N}$ be such that $dk_1 = k$ and $dn_1 = n$,

$\therefore$

$$\alpha^{n_1} = e^{\frac{2i\pi k n_1}{n}} = e^{\frac{2i\pi d k_1 n_1}{n}} = e^{2i\pi k_1} = 1 \tag{10}$$

Since $n_1 \leq n \Rightarrow n_1 = n$ so $d = 1$. □

Lemma 3. *The roots of $X^6 + X^3 + 1$ are of the form $e^{\frac{2i\pi k}{9}}$, where $1 \leq k < 9$ and $\gcd(k, 9) = 1$.*

Proof. By polynomial division we see that:

$$X^9 - 1 = (X^3 - 1)(X^6 + X^3 + 1) \tag{11}$$

So note that the roots of $X^6 + X^3 + 1$ are the roots of $X^9 - 1$ that are not roots of $(X^3 - 1)$ (indeed we can check derivatives to see that these polynomials don't have any multiple roots).

Let β be such that $\beta^9 = 1$ assume that $\beta^n = 1$ for $n < 9$. Then we have $e^{\frac{2\pi ki}{9}}$, for some $0 \leq k < 9$ and we have:

$$\beta^n = e^{\frac{2\pi kni}{9}}$$

So we have $9 \mid kn$. Since both $k, n < 9$ this means that $3 \mid k$, so β is a root of $X^3 - 1$. So the roots of $X^6 + X^3 + 1$ are elements β such that $\beta^9 = 1$ and $\beta^n \neq 1$ for $n < 9$. So by the lemma 2, the roots of this polynomial are:

$$e^{\frac{2i\pi k}{9}} \text{ such that } \gcd(9, k) = 1 \tag{12}$$

□

Let $\sigma \colon \mathbb{Q}(\alpha) \to \mathbb{C}$, be any homomorphism:

By lemma 1:

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

So σ sends α to another root of X^6+X^3+1. Furthermore, let β be a root of X^6+X^3+1 since $\mathbb{Q}(\alpha) = \{\sum_{i=0}^{5} a_i \alpha^i \mid a_i \in \mathbb{Q}\}$, we can define a homomorphism $\sigma_\beta \colon \mathbb{Q}(\alpha) \to \mathbb{C}$, with $\sigma_\beta(\alpha) = \beta$ and $\sigma(r) = r$ for all $r \in \mathbb{Q}$.

So all homomorphisms of from $\mathbb{Q}(\alpha) \to \mathbb{C}$ are the homomorphisms sending α to another root of $X^6 + X^3 + 1$. If we let $\{k_1, k_2, \ldots, k_6\}$ be the coprime integers smaller than 9, where wlog we let $\alpha = e^{\frac{2\pi ik_1}{9}}$, then the homomorphisms are $\sigma_i \colon \mathbb{Q}(\alpha) \to \mathbb{C}$ where $\sigma_i(\alpha) = e^{\frac{2\pi ik_i}{9}}$.

□

Exercise 6

Proof. Note that $((\sqrt{2} + \sqrt{3})^2 - 5)^2 - 24 = (2 + 3 + \sqrt{24} - 5)^2 - 24 = 0$. So $\sqrt{2} + \sqrt{3}$ is algebraic, furthermore since $f(X) = (X^2 - 5)^2 - 24 = X^4 - 10X^2 + 1$, is such that $f(\sqrt{2} + \sqrt{3}) = 0$, we see that $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) \colon \mathbb{Q}] \leq 4$.

$$[\mathbb{Q}(\sqrt{2} + \sqrt{3}) \colon \mathbb{Q}] = [\mathbb{Q}(\sqrt{2} + \sqrt{3}) \colon \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) \colon \mathbb{Q}] = [\mathbb{Q}(\sqrt{2} + \sqrt{3}) \colon \mathbb{Q}(\sqrt{2})]2 \tag{13}$$

Since $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) \colon \mathbb{Q}] \leq 4$ and is even: $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) \colon \mathbb{Q}] = 2$ or $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) \colon \mathbb{Q}] = 4$.

Assume for a contradiction that $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) \colon \mathbb{Q}] = 2$, then we have $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) \colon \mathbb{Q}(\sqrt{2})] = 1$ so we have: $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2})$. So we have $\sqrt{2}, \sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}) \Rightarrow \sqrt{3} \in \mathbb{Q}(\sqrt{2})$.

So there are $a, b \in Q$ such that:

$$\sqrt{3} = a + b\sqrt{2} \Rightarrow 3 = (a + b\sqrt{2})^2 = ((a^2 + 2b^2) + 2ab\sqrt{2} \tag{14}$$

Therefore:

$$\sqrt{2} = \frac{(3 - (a^2 + 2b^2))}{2ab} \in \mathbb{Q} \tag{15}$$

Which is famously false.

Therefore $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) \colon \mathbb{Q}] = 4$ □

Exercise 7

Proof. □

Exercise 8

Proof. □

Exercise 9 Find the splitting field of $f(X) = X^{p^8} - 1$ over the field $\mathbb{Z}/p\mathbb{Z}$.

Proof. Let K be the spitting field of $f(X)$, the for all non-zero $\alpha \in K$ we have $\alpha^{p^8} = 1$, but recall we also have □

Exercise 10 Let α be a real number such that $\alpha^4 = 5$.

(a) Show that $\mathbb{Q}(i\alpha^2)$ is normal over $\mathbb{Q}$

(b) Show that $\mathbb{Q}(\alpha + i\alpha)$ is normal over $\mathbb{Q}(i\alpha^2)$

(c) Show that $\mathbb{Q}(\alpha + i\alpha)$ is not normal over $\mathbb{Q}$

Proof. (a) Note since:

$$(i\alpha^2)^2 = -1\alpha^4 = -5 \tag{16}$$

So $i\alpha^2$ is the root of the polynomial $X^2 + 5 \in \mathbb{Q}[x]$. The other root of this polynomial is $-i\alpha^2$.
So $\mathbb{Q}(i\alpha^2) = \mathbb{Q}(i\alpha^2, -i\alpha^2)$ is the splitting field of $X^2 + 5$, and so it is normal over $\mathbb{Q}$.

(b) Note since:

$$(\alpha + i\alpha)^2 = \alpha^2 + 2i\alpha^2 - \alpha^2 = 2i\alpha^2 \tag{17}$$

So $\alpha + i\alpha$ is a root of the polynomial $X^2 - 2i\alpha^2 \in \mathbb{Q}(i\alpha^2)[X]$, the other root of this polynomial is $-(\alpha + i\alpha)$.
So $\mathbb{Q}(\alpha + i\alpha) = \mathbb{Q}(\alpha + i\alpha, -(\alpha + i\alpha))$ is the splitting field of $X^2 - 2i\alpha^2$. So $\mathbb{Q}(\alpha + i\alpha)$ is normal over $\mathbb{Q}(i\alpha^2)$.

(c) Let:

$$f(X) = (X^2 - 2i\alpha^2)(X^2 + 2i\alpha^2) = X^4 + 20 \tag{18}$$

Note that

$$(-\alpha + i\alpha) = (i(\alpha + i\alpha))^2 = -(\alpha + i\alpha)^2 = -2i\alpha^2 \tag{19}$$

So it is a root of $(X^2 + 2i\alpha^2)$. So the roots of f are $\pm(\alpha + i\alpha)$ and $\pm(-\alpha + i\alpha)$.
Assume for a contradiction that $-\alpha + i\alpha \in \mathbb{Q}(\alpha + i\alpha)$ then:

$$r(\alpha + i\alpha) = -\alpha + i\alpha \text{ for some } r \in \mathbb{Q}$$
$$r(\alpha + i\alpha) = i(\alpha + i\alpha)$$

Therefore, $r = i$ which is not possible since $i \notin \mathbb{Q}$. So $-\alpha + i\alpha \notin \mathbb{Q}(\alpha + i\alpha)$.

Note $X^4 + 20$ is irreducible by Eisenstein, that has a root in $\mathbb{Q}(\alpha + i\alpha)$ but does not split into linear factors in $\mathbb{Q}(\alpha + i\alpha)$. So it is indeed not normal over $\mathbb{Q}$.

□

Exercise 11 Describe the splitting fields of the following polynomials over $\mathbb{Q}$, and find the dgree of each such splitting field.

(a) $X^2 - 2$

(b) $X^2 - 1$

(c) $X^3 - 2$

(d) $(X^3 - 2)(X^2 - 2)$

(e) $X^2 + X + 1$

(f) $X^6 + X^3 + 1$

(g) $X^5 - 7$

Proof. (a) The roots of $X^2 - 2$ are $\pm\sqrt{2}$ so the splitting field of $X^2 - 2$ is $\mathbb{Q}(\sqrt{2})$. The degree is $[\mathbb{Q}(\sqrt{2})\colon \mathbb{Q}] = 2$

(b) The splitting field of $X^2 - 1$ is $\mathbb{Q}$, and $[\mathbb{Q}\colon \mathbb{Q}] = 1$.

(c) Let α be the real root of X^3-2, we know that a real root exists by the intermidiate value theorem. Let ζ_3 be a root of X^2+X+1, then since $X^3-1=(X-1)(X^2+X+1)$, we see that ${\zeta_3}^3-1=0$. Since ζ_3 is a primitive root of unity we can assume wlog that $\zeta_3=e^{\frac{2i\pi}{3}}$

Then notice that:

$$\left({\zeta_3}^i\alpha\right)^3-2={\zeta_3}^{3i}\alpha^3-2=\alpha^3-2=0 \text{ for } i=0,1,2 \tag{20}$$

Note since $\zeta_3\neq\pm1$ we see that $\alpha,\zeta_3\alpha,{\zeta_3}^2\alpha$ are the distinct roots of X^3-2. So the splitting field of X^3-2 over $\mathbb{Q}$ is $\mathbb{Q}(\alpha,\zeta_3\alpha,{\zeta_3}^2\alpha)$.

But notice, since $\alpha,\zeta_3\alpha\in\mathbb{Q}(\alpha,\zeta_3\alpha,{\zeta_3}^2\alpha)$

$$\zeta=\frac{1}{2}(\zeta\alpha)(\alpha^2)\in\mathbb{Q}(\alpha,\zeta\alpha,\zeta^2\alpha) \tag{21}$$

So $\mathbb{Q}(\alpha,\zeta)\subseteq\mathbb{Q}(\alpha,\zeta\alpha,\zeta^2\alpha)$, the other inclusion is clear so $\mathbb{Q}(\alpha,\zeta)$ is the splitting field of X^3-2 over $\mathbb{Q}$.

$$\begin{aligned}[\mathbb{Q}(\alpha,\zeta)\colon\mathbb{Q}]&=[\mathbb{Q}(\alpha,\zeta)\colon\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha)\colon\mathbb{Q}]\\&=3[\mathbb{Q}(\alpha,\zeta)\colon\mathbb{Q}(\alpha)]\end{aligned}$$

Note that since $\frac{d}{dx}X^2+X+1=2X+1$, then then:

$$(-0.5)^2+0.5+1=0.75\leq X^2+X+1 \text{ for all } X\in\mathbb{R} \tag{22}$$

So this function has no roots in $\mathbb{R}$, so $\zeta_3\in\mathbb{C}\setminus\mathbb{R}$, so $\zeta_3\notin\mathbb{Q}(\alpha)\subseteq\mathbb{R}$.

Since $\text{Irr}(\zeta_3,\mathbb{Q}(\alpha),X)\mid X^2+X+1$ and can't be of degree 1, we find that $\text{Irr}(\zeta_3,\mathbb{Q}(\alpha),X)=X^2+X+1$. So

$$[\mathbb{Q}(\alpha,\zeta)\colon\mathbb{Q}]=3\cdot2=6 \tag{23}$$

(d) Recall the roots of $(X^3-2)(X^2-2)$, are $\pm\sqrt{2}$ and $\zeta_3^i\alpha$, for $i=0,1,2$. Where ζ_3 and α have the same definition as in (c).

Any field that contains these roots also contain ζ_3 so contains $\mathbb{Q}(\zeta_3,\alpha.\sqrt{2})$. But $\mathbb{Q}(\zeta_3,\alpha.\sqrt{2})$ contains all the roots of this polynomial so it is indeed the splitting field.

Now since

$$\begin{aligned}[\mathbb{Q}(\alpha,\zeta_3,\sqrt{2})\colon\mathbb{Q}]&=[\mathbb{Q}(\alpha,\zeta_3,\sqrt{2})\colon\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2})\colon\mathbb{Q}]\\&=[\mathbb{Q}(\alpha,\zeta_3,\sqrt{2})\colon\mathbb{Q}(\alpha,\sqrt{2})][\mathbb{Q}(\alpha,\sqrt{2})\colon\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2})\colon\mathbb{Q}]\\&=4[\mathbb{Q}(\alpha,\sqrt{2})\colon\mathbb{Q}(\sqrt{2})]\end{aligned}$$

Note we indeed see that since ζ_3 is imaginary, $\zeta_3\notin\mathbb{Q}(\alpha,\sqrt{2})\subseteq\mathbb{R}$ so $[\mathbb{Q}(\alpha,\zeta_3,\sqrt{2})\colon\mathbb{Q}(\alpha,\sqrt{2})]=2$.

On the other hand notice that:

$$\begin{aligned}[\mathbb{Q}(\alpha,\zeta_3,\sqrt{2})\colon\mathbb{Q}]&=[\mathbb{Q}(\alpha,\zeta_3,\sqrt{2})\colon\mathbb{Q}(\alpha,\zeta_3)][\mathbb{Q}(\alpha,\zeta_3)\colon\mathbb{Q}]\\&=6[\mathbb{Q}(\alpha,\zeta_3,\sqrt{2})\colon\mathbb{Q}(\alpha,\zeta_3)]\end{aligned}$$

So $3\mid[\mathbb{Q}(\alpha,\zeta_3,\sqrt{2})\colon\mathbb{Q}]=4[\mathbb{Q}(\alpha,\sqrt{2})\colon\mathbb{Q}(\sqrt{2})]\Rightarrow3\mid[\mathbb{Q}(\alpha,\sqrt{2})\colon\mathbb{Q}(\sqrt{2})]$.

Since $\text{Irr}(\alpha,\mathbb{Q}(\sqrt{2}),X)\mid X^3-2$, we see that $[\mathbb{Q}(\alpha,\sqrt{2})\colon\mathbb{Q}(\sqrt{2})]\leq3$, therefore $[\mathbb{Q}(\alpha,\sqrt{2})\colon\mathbb{Q}(\sqrt{2})]=3$ so:

$$[\mathbb{Q}(\alpha,\zeta_3,\sqrt{2})\colon\mathbb{Q}]=12 \tag{24}$$

(e) Recall that the roots of X^2+X+1 are ζ_3 and ζ_3^2, where ζ_3 is defined as above. So the splitting field of this polynomial is:

$$\mathbb{Q}(\zeta_3) \tag{25}$$

Furthermore, since $\zeta_3\notin\mathbb{Q}$ we see that $[\mathbb{Q}(\zeta_3)\colon\mathbb{Q}]=2$.

(f) Let $\omega_1, \omega_2, \omega_3$ be the roots of $X^3 - \zeta_3$ and $\gamma_1, \gamma_2, \gamma_3$ be the roots of $X^3 - {\zeta_3}^2$. Note we see that these roots are all distinct by looking at derivatives. We have:

$$(\omega_i)^6 + \omega_i^3 + 1 = \zeta^3 + \zeta + 1 = 0 \text{ and } (\gamma_i)^6 + \gamma_i^3 + 1 = (\zeta^2)^3 + \zeta^2 + 1 = 0 \text{ for } i = 1, 2, 3 \tag{26}$$

Since $\zeta_3 = e^{\frac{2i\pi(1+3k)}{3}}$, for $k \in \mathbb{Z}$. We have that the distinct roots of $X^3 - \zeta_3$ are $e^{\frac{2i\pi(1+3k)}{9}}$, for $k = 0, 1, 2$. More explicitely the roots:

- $e^{\frac{2i\pi}{9}}$
- $e^{\frac{8i\pi}{9}}$
- $e^{\frac{14i\pi}{9}}$

Likewise the distinct roots of $X^3 - {\zeta_3}^2$ are $e^{\frac{2i\pi(2+3k)}{9}}$, for $k = 0, 1, 2$. More explicitely the roots:

- $e^{\frac{4i\pi}{9}}$
- $e^{\frac{10i\pi}{9}}$
- $e^{\frac{16i\pi}{9}}$

Note that any field containing the roots of $X^6 + X^3 + 1$ contains the field $\mathbb{Q}(e^{\frac{2\pi i}{9}})$. Furthermore since:

$$\begin{aligned}
(e^{\frac{2i\pi}{9}})^2 &= e^{\frac{4i\pi}{9}} \\
(e^{\frac{2i\pi}{9}})^4 &= e^{\frac{8i\pi}{9}} \\
(e^{\frac{2i\pi}{9}})^8 &= e^{\frac{16i\pi}{9}} \\
(e^{\frac{2i\pi}{9}})^{-2} &= e^{\frac{-4i\pi}{9}} = e^{2\pi i + \frac{-4i\pi}{9}} = e^{\frac{14i\pi}{9}} \\
(e^{\frac{2i\pi}{9}})^{-4} &= e^{\frac{-8i\pi}{9}} = e^{2\pi i + \frac{-8i\pi}{9}} = e^{\frac{10i\pi}{9}}
\end{aligned}$$

So $\mathbb{Q}(e^{\frac{2\pi i}{9}})$ is contains all the roots of $X^6 + X^3 + 1$ and so is the splitting field over $\mathbb{Q}$. Furthermore, using Eisenstein on $(X+1)^6 + (X+1)^3 + 1$, we see that $X^6 + X^3 + 1$ is irreducible so:

$$[\mathbb{Q}(e^{\frac{2\pi i}{9}}) \colon \mathbb{Q}] = \deg(X^6 + X^3 + 1) = 6$$

(g) $X^5 - 7$

By the intermidiate value theorem, we can see that this polynomial has a real root, call this β. Now let ζ_5 be a root of $X^4 + X^3 + X^2 + X + 1$, note since

$$(\zeta_5)^5 - 1 = ((\zeta_5) - 1)((\zeta_5)^4 + (\zeta_5)^3 + (\zeta_5)^2 + (\zeta_5) + 1) = 0$$

And if $n \leq 5$ is such that $\zeta_5^n = 1$, then we have $(X^n - 1) \mid (X^5 - 1) = (X - 1)(X^4 + X^3 + X^2 + X + 1)$, but from Eisenstein we can see that $X^4 + X^3 + X^2 + X + 1$ is irreducibe and $\zeta + 5 \neq 1$, so we have $X^n - 1 = X^5 - 1$, so $n = 5$.

Then ζ_5 is a primitive root of unity.

So WLOG we can let $\zeta_5 = e^{\frac{2\pi i}{5}}$, now by a similar argument from, (c) we see that the splitting field of $X^5 - 7$ is:

$$\mathbb{Q}(\beta, \zeta_5)$$

And similarly to (c) we conclude that

$$[\mathbb{Q}(\beta, \zeta_5) \colon \mathbb{Q}] = [\mathbb{Q}(\beta, \zeta_5) \colon \mathbb{Q}(\beta)][\mathbb{Q}(\beta) \colon \mathbb{Q}] = 4 \cdot 5 = 20$$

□

Exercise 12 Let K be a finite field with p^n elements, show that every element of K has an unique pth root in K.

Proof. Let $\alpha \in K$ and $f(X) = X^p - \alpha \in K[X]$, let $\beta \in K^a$ be a root of $f(X)$, then notice that we have $\beta^p = \alpha$

Recall that α is a root of the polynomial $g(X) = X^{p^n} - X$:

$$0 = \alpha^{p^n} - \alpha = (\beta^p)^{p^n} - \beta^p = (\beta^{p^n})^p - \beta^p = (\beta^{p^n} - \beta)^p \tag{27}$$

Since K^a is a field this implies that $\beta^{p^n} - \beta = 0$. So we see that β is a root of $g(X)$ so $\beta \in K$.

Now we will show uniqueness assume that β and γ are roots of $f(X)$ so we have:

$$(X - \gamma)^p = X^p - \gamma^p = X^p - \alpha = X^p - \beta^p = (X - \beta)^p \tag{28}$$

So by unique factorization of $K[X]$ we have that $\gamma = \beta$. □

Exercise 13 If the roots of a monic polynomial $f(X) \in k[X]$ in some splitting field are distinct and form a field, then char $k = p$ and $f(X) = X^{p^n} - X$.

Proof. Let $S = \{\alpha \in k^a \mid f(\alpha) = 0\}$, since S is finite and a field there is a p such that: $\underbrace{1 + 1 + \cdots + 1}_{p \text{ times}}$.

So we indeed see that k has characteristic p, now notice that since S is a finite field of characteristic p, then it is of the form $\mathbb{F}_{p^n}$, for some $n \geq 1$. So all elements of S are the roots of a polynomial $X^{p^n} - X$. So we have:

$$f(X) = \prod_{\alpha \in S} (X - \alpha) = X^{p^n} - X \tag{29}$$

□

Exercise 14 Let char$K = p$. Let L be an extension of K, and suppose that $[L\colon K]$ is prime to p. Show that L is separable over K.

Proof. Recall that $[L\colon K] = p^n[L\colon K]_s$, for some $n \in \mathbb{N}$. But we also know that $[L\colon K]$ is prime to p, so $n = 0$. □

Exercise 15 Suppose char $K = p$. Let $a \in K$, if a has no p-th rooth in K, show that $X^{p^n} - a$ is irreducibe in $K[X]$ for all positive integers n.

Proof. □

Exercise 16 Let char $K = p$. Let α be algebraic over K. Show that α is separable if and only if $K(\alpha) = K(\alpha^{p^n})$ for all positive integers n.

Proof. • $\Rightarrow$ Assume that α is separable.

□

Exercise 17 Prove that the following two properties are equivalent:

(a) Every algebraic extension of K is separable

(b) Either char $K = 0$, or char $K = p$ and every element of K has a p-th root in K.

Exercise 18 Show that every element of a finite field can be written as a sum of two squares in that field.

Proof. Let F be a finite field and $\alpha \in F$. □

Exercise 19 Let E be an algebraic extension of F. Show that every subring of E which contains F is actually a field. Is this necessarily true if E is not algebraic over F?

Prove or give a counterexample

Proof. Let $F \subseteq L$ be a subring of E. Let $\alpha \in L \setminus \{0\}$, since α is algebraic over F let

$$p(X) = \text{Irr}(\alpha, F, X) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$$

Since this polynomial is irreducibe we know that $a_0 \neq 0$, since if it was we could factor this polynomial by 0.

So we have:

$$a_0 + a_1\alpha + \cdots + \alpha^n = 0 \Rightarrow -a_0^{-1}(a_1\alpha + \cdots + \alpha^n) = 1 \Rightarrow \alpha \underbrace{(-a_0^{-1}(a_1 + a_2\alpha + \cdots + \alpha^{-1}))}_{\beta} = 1$$

But since $\alpha, a_i \in L$, we see that $\alpha^{-1} = \beta \in L$. So every non-zero element of L is invertible, so L is a field(it is trivially a commutative ring).

Now let us look ath the extension $\mathbb{R}/\mathbb{Q}$, let $x \in \mathbb{R}$ ne transcendental over $\mathbb{Q}$ (we can choose $x = \pi$ if we want, but since $\mathbb{Q}^a$ is countable and $\mathbb{R}$ is uncountable there are an uncountably infinite amount of transcendental numbers in $\mathbb{R}$ over $\mathbb{Q}$).

Let $\mathbb{Q}[x] = \{a_0 + a_1 x + \cdots + a_n x^n \mid n \in \mathbb{N},\ a_i \in \mathbb{Q} \text{ and } a_n \neq 0\}$, this is a subring of $\mathbb{R}$. Assume that this is a field, then there exists $a_i \in \mathbb{Q}$ such that:

$$a_0 + a_1 x + \cdots + a_n x^n = x^{-1} \tag{30}$$

Note that $n > 0$, since $x \notin \mathbb{Q} \Rightarrow x^{-1} \notin \mathbb{Q}$. From this we see that we have:

$$-1 + a_0 x + a_1 x^2 + \cdots + a_n x^{n+1} = 0 \tag{31}$$

So if we let $-1 + \sum_{i=0}^{n} a_i X^{i+1} = q(X) \in \mathbb{Q}[X]$, is a polynomial such that $q(x) = 0$. But this contradicts the fact that X is transcendental. So this statement is not necessarily true if E is not algebraic over F. □

Exercise 20 Let $E = F(x)$ where x is transcendental over F.

(a) Let $K \neq F$ be a subfield of E which contains F. Show that x is algebraic over K.

(b) Let $y = \frac{f(x)}{g(x)}$ be a ration function with relatively prime polynomials $f, g \in F[x]$. Let $n = \max(\deg f, \deg g)$. Suppose $n \geq 1$, prove that:
$$[F(x) \colon F(y)] = n$$

Proof. (a) Let $y \in K \subseteq E$. Furthermore we can assume that $y \notin F$. Recall

$$E = F(x) = \{f(x) \mid f \in F(X) \text{ is a rational function}\}$$

So there is a rational function $f(X)$ such that $f(x) = y$. Let $p(X), q(X) \in F[X]$ such that $f(X) = \frac{p(X)}{q(X)}$, we have:

$$p(x) - q(x)y = 0 \tag{32}$$

So let $s(X) \in E[X]$ be given by $s(X) = p(X) - q(X)y$. Assume that $s(X) = 0$ this means that:

$$p(X) - q(X)y = 0 \Rightarrow p(X) = q(X)y$$

Since $q \neq 0$, this implies that $y \in F$(just compare coefficients), but this is impossible by assumption. So $s(X) \neq 0$ and $s(x) = 0$, so x is algebraic over E.

(b) Since $n \geq 1$, notice that $0 \neq f(X) - g(X)y \in F(y)[X]$. So $\mathrm{Irr}(x, F(y), X) \mid f(X) - g(X)y$.

□

Exercise 21 Let $\mathbb{Z}^+$ be the set of all positive integers, and A an additive abelian group. Let $f \colon \mathbb{Z}^+ \to A$ and $g \colon \mathbb{Z}^+ \to A$ be maps. Suppose that for all n,

$$f(n) = \sum_{d \min n} g(d)$$

Let μ be the Möbius function. Prove that:

$$g(n) = \sum_{d|n} \mu(n/d) f(d)$$

Recall the Möbius fucntion is the function such that:

$$\begin{cases} \mu(1) = 1 \\ \mu(p_1 \cdots p_r) = (-1)^r \text{ if } p_i \text{ are distinct primes} \\ mui(m) = 0 \text{ if } p^2 \mid m \text{ for some prime } p. \end{cases}$$

Proof. □

23. Let k be a finite field with q elements

(a) Define the **zeta function** by:

$$Z(t) = (1-t)^{-1} \prod_{p} (1 - t^{\deg\, p})^{-1} \tag{33}$$

Where p ranges over all irreducible polynomials $p = p(X) \in k[X]$ with leading coefficient 1.

Prove that $Z(t)$ is a rational function and determine this rational function.

(b) Let $\pi_q(n)$ be the number of primes p as in (a) of degree $\leq n$. Prove that

$$\pi_q(m) = \frac{q}{q-1} \frac{q^m}{m} \text{ for } m \to \infty \tag{34}$$