Problem 1. *Show that $x^3 + 3x + 1$ is irreducible over $\mathbb{Q}$ and let $\theta \in \mathbb{C}$ be a root. Compute $(1+\theta)(1+\theta+\theta^2)$ and $\frac{1+\theta}{1+\theta+\theta^2}$ in $\mathbb{Q}(\theta)$.*

By the rational roots theorem if rational roots for $x^3 + 3x + 1$ exist then they must be of the form ± 1. However neither of those are roots. Thus $x^3 + 3x + 1$ is irreducible over $\mathbb{Q}$.

Let $\theta \in \mathbb{C}$ be a root of $x^3 + 3x + 1$. Then for the expression $(1+\theta)(1+\theta+\theta^2)$ we have:

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

For the next expression, $\frac{1+\theta}{1+\theta+\theta^2}$, the multiplicative inverse of the bottom $1+\theta+\theta^2$ is $\frac{3}{7}\theta^2 - \frac{2}{7}\theta + \frac{8}{7}$. This can be found be multiplying $1+\theta+\theta^2$ by $(c + b\theta + c\theta^2)$ and extracting a system of linear equations. Then we have:

$$\begin{aligned}\frac{1+\theta}{1+\theta+\theta^2} &= (1+\theta)\left(\frac{3}{7}\theta^2 - \frac{2}{7}\theta + \frac{8}{7}\right) \\ &= \frac{3}{7}\theta^3 + \frac{1}{7}\theta^2 + \frac{6}{7}\theta + \frac{8}{7} \\ &= \frac{1}{7}\theta^2 - \frac{3}{7}\theta + \frac{5}{7}\end{aligned}$$

Problem 2. *Let $w = e^{\pi i/6}$ so that $w^{12} = 1$, but $w^k \neq 1$ for $1 \leq k < 12$. Find the minimal polynomial $m_{w,\mathbb{Q}}(x)$ and compute $[\mathbb{Q}[w] : \mathbb{Q}]$.*

Begin with the polynomial $x^{12} - 1$ which we now that ω is a root of. This factors as

$$x^{12} - 1 = (x^6 - 1)(x^6 + 1)$$

Since ω of $x^6 + 1$ and not the other we continue with it. This factors as

$$x^6 + 1 = (x^2 + 1)(x^4 - x^2 + 1)$$

As before $x^4 - x^2 + 1$ has ω as a root and the other does not. Now we will show that $x^4 - x^2 + 1$ is irreducible.

By the rational root theorem the only possible rational roots are ± 1. However neither of these are roots. The only way $x^4 - x^2 + 1$ would not be irreducible is if it were the product of quadratics. Now consider $x^4 - x + 1$ as a polynomial with integer coefficients and suppose that

$$x^4 - x^2 + 1 = (ax^2 + bx + c)(dx^2 + ex + f) = adx^4 + (bd + ae)x^3 + (af + be + cd)x^2 + (bf + ce)x + fc$$

where $a, b, c, d, e \in \mathbb{Z}$. This gives us the following system of equations:

$$\begin{aligned}ad &= 1 \\ bd + ae &= 0 \\ af + dc + be &= -1 \\ bf + ce &= 0 \\ fc &= 1\end{aligned}$$

Consider these equations as polynomials in $\mathbb{C}[a, b, c, d, e, f]$. Then consider the ideal

$$\langle ad - 1, bd + ae, af + dc + be + 1, bf + ce, fc - 1\rangle$$

The Gröbner basis for this ideal is $\langle 1\rangle$. Since we are in an algebraically closed field there are no solutions to a set of polynomial equations when the ideal is the whole ring. Thus $x^4 - x^2 + 1$ is not the product of quadratics and as such $x^4 - x^2 + 1$ is irreducible.

Therefore $x^4 - x^2 + 1$ is the minimal polynomial $m_{\omega,\mathbb{Q}}(x)$ and as such $[\mathbb{Q}[\omega] : \mathbb{Q}] = 4$.

Problem 3. *Compute the minimal polynomial $m_{\alpha,F}(x)$ where $\alpha = \sqrt{2} + \sqrt{5}$ and F is each of the following fields:*
(a) $\mathbb{Q}$, *(b)* $\mathbb{Q}[\sqrt{5}]$, *(c)* $\mathbb{Q}[\sqrt{10}]$, *(d)* $\mathbb{Q}[\sqrt{15}]$.

First note that $\mathbb{Q}[\alpha] \cong \mathbb{Q}[\sqrt{2}, \sqrt{5}]$ as the latter has a basis of $(1, \sqrt{2}, \sqrt{5}, \sqrt{10})$ and we can construct this basis in $\mathbb{Q}[\alpha]$. To see this we can construct $\mathbb{Q}[\sqrt{5}]$ by

$$\sqrt{2} = \frac{(\alpha^2 - 7)\alpha - 2\alpha}{8}$$

Then we can readily construct the rest.

(a) The minimal polynomial is $x^4 - 14x^2 + 9$. The fact that this is irreducible follows from the tower theorem as $[\mathbb{Q}[\sqrt{5}] : \mathbb{Q}] = 2$ and $[\mathbb{Q}[\sqrt{5}][\sqrt{2}] : \mathbb{Q}[\sqrt{5}]] = 2$ giving us that $[\mathbb{Q}[\sqrt{5}][\sqrt{2}] : \mathbb{Q}] = 4$. Since we have found a fourth degree polynomial that has α as a root we are done.

(b) The minimal polynomial is $x^2 - \sqrt{5}x + 2$. As above the irreducibility follows from the degree of the extension being two and us finding a polynomial with α as a root.

(c) The minimal polynomial is $x^2 - (7 + \sqrt{10})$. To show that it is irreducible note that $\mathbb{Q}[\sqrt{10}][\alpha] = \mathbb{Q}[\sqrt{2}, \sqrt{5}]$ because as above we have

$$\sqrt{2} = \frac{\sqrt{10}\alpha - 2\alpha}{8}$$

By the tower theorem the degree $[\mathbb{Q}[\sqrt{10}] : \mathbb{Q}] = 2$ as it cannot 1 nor can it be 4 as that would imply that $[\mathbb{Q}[\sqrt{10}][\alpha] : \mathbb{Q}[\sqrt{10}]] = 1$. However since $\sqrt{2} \notin \mathbb{Q}[\sqrt{10}]$ this cannot occur. Thus the degree must be two and since we have found a polynomial that has degree 2 with α as a root it must be our minimal polynomial.

(d) The minimal polynomial will be $x^4 - 14x^2 + 9$ as well. The fact that it is irreducible will follow from it being irreducible over $\mathbb{Q}$ if $\sqrt{15}$ is not in the span of $\{1, \alpha\}$.

To show this suppose that

$$\sqrt{15} = a + b\sqrt{2} + c\sqrt{5} + d\sqrt{10}$$

If we square both sides we get

$$15 = a^2 + 2\sqrt{2}ab + 2\sqrt{5}ac + 2\sqrt{10}ad + 2b^2 + 2\sqrt{10}bc + 4\sqrt{5}bd + 5c^2 + 10\sqrt{2}cd + 10d^2$$

This gives us the system of equations

$$\begin{aligned} a^2 + 2b^2 + 5c^2 + 10d^2 - 15 &= 0 \\ 2ab + 10cd &= 0 \\ 2ac + 4bd &= 0 \\ 2ad + 2bc &= 0 \end{aligned}$$

This system of equations has no solution over $\mathbb{Q}$. Thus the degree of the extension $\mathbb{Q}[\sqrt{15}]$ by α is the same as $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 4$. Since we have a monic polynomial with α as the root that is of the proper degree it must be the minimal polynomial.

Problem 4. *Compute the minimal polynomial $m_{\alpha,\mathbb{Q}}(x)$ where $\alpha = \sqrt{2} + \sqrt[3]{5}$.*

Consider the polynomial $f(x) = x^6 - 6x^4 - 10x^3 + 12x^2 - 60x + 17$. Then $f(\alpha) = 0$. Now we wish to show that $f(x)$ is irreducible. By the rational roots theorem if any rational roots exist then they will be of the form ± 17 neither of which are roots. Therefore if $f(x)$ is reducible it will either be the product of two cubics or the product of a quartic and a quadratic.

Suppose that $f(x)$ was the product of two cubics. Then we would have

$$x^6 - 6x^4 - 10x^3 + 12x^2 - 60x + 17 = (x^3 + ax^2 + bx + c)(x^3 + dx^2 + ex + f)$$

If we multiply out the latter terms we can extract the system of equations

$$\begin{aligned} a + d &= 0 \\ ad + b + e + 6 &= 0 \\ ad + be + c + f + 10 &= 0 \\ af + eb + cd - 12 &= 0 \\ bf + ec + 60 &= 0 \\ cf - 17 &= 0 \end{aligned}$$

If we consider the ideal

$$\langle a + d, , ad + b + e, ad + be + c + f + 10, af + eb + cd - 12, bf + ec + 60, cf - 17\rangle \subset \mathbb{C}[a, b, c, d, e, f]$$

the Gröbner basis of this ideal is $\langle 1\rangle$ which implies that there are no solutions to the equation. Thus $f(x)$ cannot be the product of two cubics.

Similarly suppose that $f(x)$ was the product of a quartic and a quadratic. Then

$$x^6 - 6x^4 - 10x^3 + 12x^2 - 60x + 17 = (x^4 + ax^3 + bx^2 + cx + d)(x^2 + ex + f)$$

$$= x^6 + (a + e)\, x^5 + (ae + b + f)\, x^4 + (be + af + c)\, x^3 + (ce + bf + d)\, x^2 + (de + cf)\, x + df$$

This gives us the system of equations

$$\begin{aligned} a + e &= 0 \\ ae + b + f + 6 &= 0 \\ be + af + c + 10 &= 0 \\ ce + bf + d - 12 &= 0 \\ de + cf + 60 &= 0 \\ df - 17 &= 0 \end{aligned}$$

As before consider the ideal

$$\langle df - 17, de + cf + 60, ce + bf + d - 12, be + af + c + 10, ae + b + f + 6\rangle \subset \mathbb{C}[a, b, c, d, e, f]$$

The Gröbner basis for this ideal is $\langle 1\rangle$ which implies that there are no solutions. Therefore $f(x)$ cannot be expressed as the product of a quartic and a quadratic.

Therefore $f(x)$ is irreducible and as such is in fact the minimal polynomial for α.

Problem 5. *If K is a field extension of the field of F and $\alpha \in K$ has a minimal polynomial $f(x) \in F[x]$ of odd degree, prove that $F(\alpha) = F(\alpha^2)$. Determine whether the condition on $f(x)$ is necessary for $F(\alpha) = F(\alpha^2)$.*

Proof. First note that $F \subset F(\alpha^2) \subset F(\alpha)$ as $\alpha^2 \in F(\alpha)$. Then using the tower theorem we know that

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

By assumption we know that $[F(\alpha) : F]$ is odd. Moreover we have that $[F(\alpha) : F(\alpha^2)] = [F(\alpha^2)(\alpha) : F(\alpha^2)]$. The degree $[F(\alpha^2)(\alpha) : F(\alpha^2)]$ will be less than or equal to 2 since $x^2 - \alpha^2$ has α as root. However it cannot be 2 since this would contradict $[F(\alpha) : F]$ being odd. As such the minimal polynomial for $F(\alpha)$ over $F(\alpha^2)$ must be linear, which implies that $\alpha \in F(\alpha^2)$ and therefore $F(\alpha) = F(\alpha^2)$. □

The condition is not necessary. Consider the polynomial

$$(x - e^{2\pi i/3})(x - e^{4\pi i/3}) = x^2 + x + 1$$

Note that both roots are squares of each other making their extensions equal. However $x^2 + x + 1$ is irreducible making the degree even.

Problem 6. *6 Let K be an extension field of F that is algebraic over F. Show that any subring R of K which contains F, i.e., $F \subseteq R \subseteq K$, is a field. Hence, prove that any subring of a finite dimensional extension field K/F containing F is a subfield.*

Proof. As R is a subring of the field K we know that it fulfills all the properties of a field except possibly multiplicative inverses. Let $r \in R$. Since K is algebraic over F there is an irreducible polynomial $f(x) = \sum_0^n a_i x^i$ where r is a root of $f(x)$. Consider

$$f(r) = \sum_0^n a_i r^i = 0$$

The constant term will be nonzero as f is irreducible. As such move a_0 to the right and factor to get

$$r \sum_1^n a_i r^{i-1} = -a_0$$

Since $-a_0 \in F$ it has an inverse. Thus

$$r \cdot \frac{1}{-a_0} \sum_1^n a_i r^{i-1} = 1$$

and $\frac{1}{-a_0} \sum_1^n a_i r^{i-1}$ is the multiplicative inverse to r. This implies that R must be a field.

Since finite dimensional field extension are algebraic it follows that any subring of a finite dimensional field extension K/f containing F is a subfield. □

Problem 7. *Suppose that $K = F(\alpha)$ is a finite simple extension of the field F. Define an F-linear transformation $T_\alpha : K \to K$ by $T_\alpha(\beta) = \alpha\beta$ for all $\beta \in K$. Show that the minimal polynomial of α over F is the characteristic polynomial of T_α, that is*

$$m_{\alpha,F}(x) = det(xI - T_\alpha).$$

Proof. First let $n := [F(\alpha) : F]$ and let $\sum_0^n r_i x_i$ be the minimal polynomial for $F(\alpha)$. Let $\beta = \sum_0^{n-1} c_i \alpha^i \in F(\alpha)$ where $c_i \in F$. Then

$$T_\alpha(\beta) = \sum_0^{n-1} c_i \alpha^{i+1}$$

Using minimal polynomial to remove the α^n we can simplify the expression to

$$T_\alpha(\beta) = \sum_0^{n-2} (c_i - c_{n-1} r_{i+1}) \alpha^{i+1} - c_{n-1} r_0$$

which gives us that the matrix for T_α is

$$[T_\alpha] = \begin{pmatrix} 0 & 0 & \cdots & 0 & -r_0 \\ 1 & 0 & \cdots & 0 & -r_1 \\ 0 & 1 & \cdots & 0 & -r_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 1 & -r_{n-1} \end{pmatrix}$$

Note that this matrix is a companion matrix for the rational canonical form which implies that the determinant of

$$xI - [T_\alpha] = \begin{pmatrix} x & 0 & \cdots & 0 & -r_0 \\ 1 & x & \cdots & 0 & -r_1 \\ 0 & 1 & \cdots & 0 & -r_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 1 & x - r_{n-1} \end{pmatrix}$$

is precisely $\sum_0^n r_i x^i$ completing the proof.

□