1. Let $f(x) = x^3 + 3x^2 + 3x - 1 \in \mathbb{Q}[x]$.

(a) Find the remainder of x^4 when divided by $f(x)$.

(b) Find the reminder of $(x^2 + 1)^3$ when divided by $f(x)$.

(c) Find polynomials $u(x)$, $v(x) \in \mathbb{Q}[x]$, with $\deg(u(x)) \leqslant 2$ which solve

$$x^2 \cdot u(x) + v(x)f(x) = 1.$$

Solution.

(a) By polynomial long division we have :

$$x^4 = (x - 3) \cdot (x^3 + 3x^2 + 3x - 1) + (6x^2 + 10x - 3).$$

Thus, the remainder is $6x^2 + 10x - 3$.

(b) We again use polynomial long division to compute that

$$(x^2 + 1)^3 = (x^3 - 3x^2 + 9x - 17) \cdot (x^3 + 3x^2 + 3x - 1) + (24x^2 + 60x - 16),$$

so that the remainder when dividing $(x^2 + 1)^3$ by $f(x)$ is $24x^2 + 60x - 16$.

(c) The extended gcd algorithm gives the solution

$$x^2 \cdot (3x^2 + 10x + 12) - (1 + 3x) \cdot f(x) = 1.$$

2. Let α be the real number $\alpha = 2^{1/3} - 1$. To as many decimal places as you can (well, at least 8, and no more than 20), evaluate the following real numbers:

(a) α^4;

(b) $(\alpha^2 + 1)^3$;

(c) $1/\alpha^2$;

(d) $3\alpha^2 + 10\alpha + 12$;

(e) $24\alpha^2 + 60\alpha - 16$;

(f) $6\alpha^2 + 10\alpha - 3$.

Now,

(g) explain why some of the numbers this question were the same (question 1 may help).

Solution. We have $\alpha = 0.259921049894873164767211\ldots$, so that

(a) $\alpha^4 = 0.0045642120194505189760\ldots$

(b) $(\alpha^2+1)^3 = 1.2166778459752653712\ldots$

(c) $1/\alpha^2 = 14.801887355484091083\ldots$

(d) $3\alpha^2 + 10\alpha + 12 = 14.801887355484091083\ldots$

(e) $24\alpha^2 + 60\alpha - 16 = 1.2166778459752653712\ldots$

(f) $6\alpha^2 + 10\alpha - 3 = 0.0045642120194505189760\ldots$

(g) The decimal expansions suggest that (a)=(f), (b)=(e), and (c)=(d). Let us see that this is actually true.

Let us first note that since $\alpha + 1 = \sqrt[3]{2}$, and since the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $g(x) = x^3 - 1$, the minimal polynomial of α over $\mathbb{Q}$ is

$$g(x+1) = (x+1)^3 - 2 = x^3 + 3x^2 + 3x - 1 = f(x).$$

Second, consider the evalution homomorphism $\varphi_\alpha \colon \mathbb{Q}[x] \longrightarrow \mathbb{Q}(\alpha)$ given by $h(x) \mapsto h(\alpha)$ for each $h(x) \in \mathbb{Q}[x]$. By definition of the minimal polynomial, $\mathrm{Ker}(\varphi_\alpha)$ is generated by $f(x)$.

Applying φ_α to the equality

$$x^4 = (x-3)\cdot f(x) + 6x^2 + 10x - 3$$

from Question 1(a) gives

$$\alpha^4 = (\alpha-3)\cdot f(\alpha) + 6\alpha^2 + 10\alpha - 3 = (\alpha-3)\cdot 0 + 6\alpha^2 + 10\alpha - 3 = 6\alpha^2 + 10\alpha - 3.$$

Applying φ_α to the equality

$$(x^2+1)^3 = (x^3 - 3x^2 + 9x - 17)\cdot(x^3 + 3x^2 + 3x - 1) + (24x^2 + 60x - 16),$$

from Question 1(b) gives

$$\begin{aligned} (\alpha^2+1)^3 &= (\alpha^3 - 3\alpha^2 + 9\alpha - 17)\cdot f(\alpha) + (24\alpha^2 + 60\alpha - 16) \\ &= (\alpha^3 - 3\alpha^2 + 9\alpha - 17)\cdot 0 + (24\alpha^2 + 60\alpha - 16) = 24\alpha^2 + 60\alpha - 16 \end{aligned}.$$

Finally, applying φ_α to the formula

$$x^2 \cdot (3x^2 + 10x + 12) - (1 + 3x) \cdot f(x) = 1$$

from Question 1(c) gives

$$\begin{aligned} 1 &= \alpha^2 \cdot (3\alpha^2 + 10\alpha + 12) - (1 + 3\alpha) \cdot f(\alpha) \\ &= \alpha^2 \cdot (3\alpha^2 + 10\alpha + 12) - (1 + 3\alpha) \cdot 0 = \alpha^2 \cdot (3\alpha^2 + 10\alpha + 12). \end{aligned}$$

Therefore $1/\alpha^2 = 3\alpha^2 + 10\alpha + 12$.

Note: In case it wasn't clear, the purpose of this question was to reinforce the fact that if $K \subseteq L$ are fields, $\alpha \in L$ algebraic over K, and $q(x) \in K[x]$ the minimal polynomial of α over K, then the fields $K[x]/(q(x))$ and $K(\alpha)$ are isomorphic. In particular, arithmetic in $K[x]/(q(x))$ is exactly the same as arithmetic in $K(\alpha)$.

3. In this question we will show that $f(x) = x^4 - 10x^2 + 1$ is the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$. Let $q(x) \in \mathbb{Q}[x]$ be the (at the moment unknown) minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$. It is easy to check that $f(\sqrt{2} + \sqrt{3}) = 0$, which implies that $q(x) \mid f(x)$. To show that $q(x) = f(x)$ we may therefore show either that $f(x)$ is irreducible in $\mathbb{Q}[x]$ or that $\deg(q(x)) = 4$.

We will use equality $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$, proved in the last homework assignment to show that $\deg(q(x)) = 4$.

(a) Using the chain of field extensions $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ explain why $\deg(q(x))$ must be even.

Since $\deg(q(x)) \leqslant 4$, this means that we must have $\deg(q(x)) = 2$ or 4. We now assume that $\deg(q(x)) = 2$ and show how this leads to a contradiction.

(b) Explain why $\deg(q(x)) = 2$ implies that $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$, and similarly that $\mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

(c) Part (b) gives us $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{3})$, and if so we would be able to write $\sqrt{3} = a + b\sqrt{2}$ with $a, b \in \mathbb{Q}$. Square both sides and show how this would lead to a contradiction. (Do not forget to deal with the special cases $a = 0$ or $b = 0$.)

Thus (after finishing (c)) we conclude that $f(x)$ is the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$. Let us also try the other method of showing that $f(x)$ is the minimal polynomial : showing that $f(x)$ is irreducible over $\mathbb{Q}$.

(d) Use one of the irreducibility tests from class to show that $f(x)$ is irreducible over $\mathbb{Q}$. (There is more than one that will work.)

Solution.

(a) We have the tower of fields $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}+\sqrt{3})$. From our theorem on simple extensions we know that $\deg(q(x)) = [\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}]$. By the tower law we therefore have

$$(\dagger) \quad \begin{aligned} \deg(q(x)) &= [\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \\ &= [\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}(\sqrt{2})] \cdot 2, \end{aligned}$$

and so $\deg(q(x))$ is even.

(b) If $\deg(q(x)) = 2$ then equation $(\dagger)$ gives us

$$2 = \deg(q(x)) = 2[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}(\sqrt{2})],$$

which is the same as $[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 1$, and this means that $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

Similarly, we can use the tower of extensions $\mathbb{Q} \subset \mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}(\sqrt{2}+\sqrt{3})$ to get the equation

$$(\ddagger) \quad \begin{aligned} \deg(q(x)) &= [\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}(\sqrt{3})] \cdot [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] \\ &= [\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}(\sqrt{2})] \cdot 2. \end{aligned}$$

Using $(\ddagger)$ we similarly deduce that $\deg(q(x)) = 2$ implies

$$[\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}(\sqrt{3})] = 1,$$

and so $\mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

(c) Suppose that there are $a, b \in \mathbb{Q}$ such that $\sqrt{3} = a + b\sqrt{2}$. We cannot have $b = 0$ since then we would get $\sqrt{3} = a \in \mathbb{Q}$, which isn't true; therefore $b \neq 0$.

We also cannot have $a = 0$, since from $\sqrt{3} = b\sqrt{2}$ we get $\frac{\sqrt{3}}{\sqrt{2}} = b \in \mathbb{Q}$ which again is not true. (You can use the same kind of argument as the one which shows that $\sqrt{2}$ isn't rational, suppose that $\frac{\sqrt{3}}{\sqrt{2}} = p/q \in \mathbb{Q}$ with $\gcd(p, q) = 1$. Squaring both sides and cross multiplying we deduce that q must be divisible by 2. Writing $q = 2q'$ with $q' \in \mathbb{Z}$, and squaring again we conclude that p must also be divisible by 2, contradicting $\gcd(p, q) = 1$.)

Therefore we may assume that $a \neq 0$ and $b \neq 0$. Squaring both sides of $\sqrt{3} = a + b\sqrt{2}$ gives

$$3 = a^2 + 2ab\sqrt{2} + 2.$$

Since $ab \neq 0$ we may rearrange and divide by ab to get $\sqrt{2} = \frac{1-a^2}{2ab} \in \mathbb{Q}$, which is again a contradiction.

From parts (b)+(c) we conclude that $\deg(q(x)) \neq 2$, and so $\deg(q(x)) = 4$, implying that $q(x) = x^4 - 10x^2 + 1$.

(d) There are many other ways of seeing that $x^4 - 10x^2 + 1$ is irreducible over $\mathbb{Q}$. Here are two :

1. Taking on prime values. Set $H = \max(|-10/1|, |1/1|) = 10$. (That is, H is the maximum of the coefficients divided by the leading coefficient.) Since $f(14) = 36457$ is prime, and $14 \geqslant H+2 = 12$, we conclude that $f(x)$ is irreducible over $\mathbb{Q}$ by one of the criteria from class.

2. Reduction mod p. Reducing f mod 2 we obtain $\overline{f}(x) = x^4 + 1 \in \mathbb{F}_2[x]$. This polynomial is reducible in $\mathbb{F}_2[x]$ since $x = 1$ is a root. Factoring we obtain $\overline{f}(x) = (x+1)(x^3+x^2+x+1) \in \mathbb{F}_2[x]$. Let $g(x) = x^3+x^2+x+1$. We next check that $g(x)$ is irreducible in $\mathbb{F}_2[x]$ by checking if $g(x)$ has a root in $\mathbb{F}_2$ (this is okay since $\deg(g(x)) \leqslant 3$). Since $g(0) = 1 \neq 0$, and $g(1) = 1 \neq 0$ we conclude that $g(x)$ irreducible in $\mathbb{F}_2[x]$.

This tells us that if $f(x)$ factors in $\mathbb{Q}[x]$, the irreducible factors must be of degree 1 and 3.

Next we reduce $f(x)$ mod 3 to get $\overline{f}(x) = x^4 + 2x^2 + 1 \in \mathbb{F}_3[x]$. This polynomial is reducible in $\mathbb{F}_3[x]$:

$$x^4 + 2x + 1 = (x^2 + 1)^2.$$

Let $h(x) = x^2 + 1 \in \mathbb{F}_3[x]$. Since $\deg(h(x)) \leqslant 3$ we can check for irreduciblity of $h(x)$ in $\mathbb{F}_3[x]$ by checking if $h(x)$ has roots in $\mathbb{F}_3$. We get $h(0) = 1 \neq 0$, $h(1) = 2 \neq 0$, and $h(2) = 2 \neq 0$, and so $h(x)$ is irreducible in $\mathbb{F}_3[x]$. Therefore, in $\mathbb{F}_3[x]$, $\overline{f}(x)$ is the square of an irreducible quadratic. In particular, it is the product of two irreducible (and equal) quadratics.

This tells us that if $f(x)$ factors over $\mathbb{Q}$ the irreducible factors must be of degrees 2 and 2.

These two possibilities for the degrees of the irreducible factors are incompatible, and therefore $f(x)$ is irreducible over $\mathbb{Q}$.

4. In this question we will explore some aspects of numbers algebraic over a fixed field.

(a) Suppose that $K \subseteq M$ is a field extension, with $[M : K] = d$ (in particular, the degree of the extension is finite). Show that every $\alpha \in M$ is algebraic over K, and satisfies a polynomial of degree $\leqslant d$. (Suggestion: Can $1, \alpha, \ldots, \alpha^d$ be linearly independent over K?)

(b) Let $K \subseteq L$ be a field extension, and $\alpha, \beta \in L$. If β is algebraic over K, show that β is algebraic over $K(\alpha)$.

(c) If $\alpha, \beta \in L$ are both algebraic over K, show that $[K(\alpha, \beta) : K]$ is finite.

(d) If α, $\beta \in L$ are algebraic over K with $\beta \neq 0$, show that $\alpha + \beta$, $\alpha\beta$, and α/β are algebraic over K

(e) Consider the set $\overline{\mathbb{Q}} = \left\{\alpha \in \mathbb{C} \,\middle|\, \alpha \text{ is algebraic over } \mathbb{Q}\right\}$. Show that $\overline{\mathbb{Q}}$ is a field.

(f) Are there irreducible polynomials in $\mathbb{Q}[x]$ of arbitrarily large degree?

(g) Is $[\overline{\mathbb{Q}} : \mathbb{Q}]$ finite or infinite?

(h) Does the converse to (a) hold? I.e., if $K \subseteq M$ is a field extension such that every $\alpha \in M$ is algebraic over K, does this imply that $[M : K]$ is finite?

Solution.

(a) Given $\alpha \in L$, since $\dim_K(L) = [L : K] = d$, the $d + 1$ elements 1, α, $\alpha^2, \ldots,$ α^d cannot be linearly independent over K. Therefore there is a nontrivial linear relation among them, i.e., there exists c_0, c_1, $\ldots$, $c_d \in K$, not all zero, such that

$$c_0 \cdot 1 + c_1 \cdot \alpha + c_2 \cdot \alpha^2 + \cdots + c_d\alpha^d = 0.$$

Let $f(x) = c_0 + c_1x + c_2x^2 + \cdots + c_dx^d \in K[x]$. Since not all the c_i are zero, $f(x)$ is a nonzero polynomial. The relation above tells us that $f(\alpha) = 0$, and therefore α is algebraic over K.

(b) Since β is algebriac over K there is a nonzero polynomial $f(x) \in K[x]$ such that $f(\beta) = 0$. Since $K \subseteq K(\alpha)$, $f(x)$ is also a polynomial in $K(\alpha)[x]$ with $f(\beta) = 0$. Therefore β is algebraic over $K(\alpha)$.

(c) Let $q(x)$ be the minimal polynomial of α over K (this exists since α is algebraic over K) and set $d = \deg(q(x))$. Let $p(x)$ be the minimal polynomial of β over $K(\alpha)$ (this exists since β is algebraic over K, and hence by part (b), also algebraic over $K(\alpha)$), and set $e = \deg(p(x))$. By the tower law for field extensions we have

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

and thus $[K(\alpha, \beta) : K]$ is finite.

(d) The numbers $\alpha + \beta$, $\alpha\beta$ and α/β are all in $K(\alpha, \beta)$. By part (c) the extension $K \subseteq K(\alpha, \beta)$ is finite. By part (a) every element of $K(\alpha, \beta)$ is therefore algebraic over K, and in particular, $\alpha + \beta$, $\alpha\beta$, and α/β are algebraic over K.

(e) By definition, every element of $\overline{\mathbb{Q}}$ is algebraic over $\mathbb{Q}$. By part (d), given any α, $\beta \in \overline{\mathbb{Q}}$, if $\beta \neq 0$ then $\alpha + \beta$, $\alpha\beta$, and α/β are also in $\overline{\mathbb{Q}}$. (And if $\beta = 0$ it is clear that $\alpha + \beta = \alpha$ and $\alpha\beta = 0$ are in $\overline{\mathbb{Q}}$.) Thus $\overline{\mathbb{Q}}$ is a commutative ring in which every nonzero element has a multiplicative inverse, and so $\overline{\mathbb{Q}}$ is a field.

(f) Yes, by Eisenstein's criterion with the prime $p = 2$, the degree n polynomial $x^n - 2$ is irreducible over $\mathbb{Q}$ for every $n \geqslant 1$.

(g) Part (a) showed that if an extension $K \subseteq M$ is finite of degree d, then every element of M satisfies a polynomial of degree $\leqslant d$ over K. By part (f), for any $n \geqslant 1$ the minimal polynomial of $\alpha = \sqrt[n]{2}$ over $\mathbb{Q}$ has degree n. Since $\sqrt[n]{2} \in \overline{\mathbb{Q}}$, we conclude that $[\overline{\mathbb{Q}} : \mathbb{Q}]$ cannot be finite.

(h) The stated converse to (a) does not hold, with $\mathbb{Q} \subseteq \overline{\mathbb{Q}}$ being a counterexample.