Solution 11

Field extensions

1. Let $f = X^4 - X - 1 \in \mathbb{Q}[X]$ and $\alpha \in \mathbb{C}$ a root of f. Let $K := \mathbb{Q}(\alpha)$.

   (a) Prove that the polynomial $\overline{f} = X^4 - X - 1 \in \mathbb{F}_2[X]$ is irreducible in $\mathbb{F}_2[X]$.

   (b) Deduce that f is irreducible in $\mathbb{Q}[X]$. Recall: this implies that $\mathbb{Q}[X]/(f) \cong K$.

   (c) Write down the following elements as linear combinations of the $\mathbb{Q}$-basis elements $1, \alpha, \alpha^2, \alpha^3$:

   $$\alpha^{10}, \quad \frac{1}{\alpha}, \quad \frac{1}{\alpha+1}, \quad \frac{\alpha^5}{\alpha^2+2}.$$

   Solution:

   (a) Since $\overline{f}(0) = \overline{f}(1) = 1 \neq 0$, the polynomial $\overline{f}$ has no root in $\mathbb{F}_2$, hence it is not divisible by any degree 1 polynomial. Suppose that $\overline{f} = g \cdot h$ for g, h non-constant polynomials. Then $\deg(g) = \deg(h) = 2$. Comparing leading coefficients and constant terms in g, h and f, we see that $g = X^2 + aX + 1$ and $h = X^2 + bX + 1$ for some $a, b \in \mathbb{F}_2$. Then

   $$X^4 + X + 1 = \overline{f} = gh = X^4 + (a+b)X^3 + abX^2 + (a+b)X + 1$$

   forces $a + b = 0$ and $a + b = 1$ at the same time, a contradiction. Hence $\overline{f}$ is irreducible in $\mathbb{F}_2[X]$.

   (b) A decomposition of f in $\mathbb{Z}[X]$ gives via the map π_2 (as defined in Exercise 2) a decomposition of $\overline{f}$ in $\mathbb{F}_2[X]$ into polynomials of corresponding degrees, so that by (a) f cannot be factored into a product of two non-constant polynomials in $\mathbb{Z}[X]$. Since f is primitive, we can conclude that it is irreducible in $\mathbb{Z}[X]$. By Gauss' Lemma, f is irreducible in $\mathbb{Q}[X]$ as well.

   The evaluation map $\mathrm{ev}_\alpha : \mathbb{Q}[X] \longrightarrow K$ has kernel $\ker(\mathrm{ev}_\alpha) = (\mathrm{irr}(\alpha, \mathbb{Q}))$ as seen in class, and since $f \in \ker(\mathrm{ev}_\alpha)$ we know that $\mathrm{irr}(\alpha, \mathbb{Q}) | f$. As f and $\mathrm{irr}(\alpha, \mathbb{Q})$ are both irreducible, we can conclude that $(\mathrm{irr}(\alpha, \mathbb{Q})) = (f)$ so that by the First Isomorphism Theorem on rings we obtain an isomorphism $\mathbb{Q}[X]/(f) \cong K$.

   (c) For this task, we use constantly the fact that $\alpha^4 = \alpha + 1$.

   - $\alpha^{10} = \alpha^2(\alpha^4)^2 = \alpha^2(\alpha+1)^2 = \alpha^4 + 2\alpha^3 + \alpha^2 = 2\alpha^3 + \alpha^2 + \alpha + 1$.
   - Since $\alpha \cdot \alpha^3 = \alpha + 1$, we realise that $\alpha \cdot (\alpha^3 - 1) = 1$, so that $\alpha^{-1} = \alpha^3 - 1$.

- By the previous computation, we obtain $(\alpha+1)^{-1} = \alpha^{-4} = (\alpha^{-1})^4 = (\alpha^3-1)^4 = (\alpha^6 - 2\alpha^4 + 1)^2$. Since $\alpha^5 = \alpha^2(\alpha+1) = \alpha^2 + \alpha$ and $\alpha^6 = \alpha^3 + \alpha^2$, we can conclude that

$$\begin{aligned}(\alpha+1)^{-1} &= (\alpha^6 - 2\alpha^3 + 1)^2 = (-\alpha^3 + \alpha^2 + 1)^2 \\ &= \alpha^6 + \alpha^4 + 1 - 2\alpha^5 - 2\alpha^3 + 2\alpha^2 \\ &= \alpha^3 + \alpha^2 + \alpha + 1 + 1 - 2\alpha^2 - 2\alpha + 2\alpha^2 - 2\alpha^3 \\ &= -\alpha^3 + \alpha^2 - \alpha + 2.\end{aligned}$$

- We first compute $(\alpha^2+2)^{-1}$. Let $p, q, r, s \in \mathbb{Q}$ and suppose that $p + q\alpha + r\alpha^2 + s\alpha^3 = (\alpha^2+2)^{-1}$. Then

$$\begin{aligned}&(p + q\alpha + r\alpha^2 + s\alpha^3)(\alpha^2+2) = 1 \iff \\ &2p + 2q\alpha + (p+2r)\alpha^2 + (q+2s)\alpha^3 + r\alpha^4 + s\alpha^5 = 1 \iff \\ &2p + 2q\alpha + (p+2r)\alpha^2 + (q+2s)\alpha^3 + r(1+\alpha) + s(\alpha+\alpha^2) = 1 \iff \\ &(2p+r) + (r+s+2q)\alpha + (p+2r+s)\alpha^2 + (q+2s)\alpha^3 = 1 \iff \\ &2p + r = 1 \text{ and } r + s + 2q = p + 2r + s = q + 2s = 0,\end{aligned}$$

  where the last equivalence is due to the fact that $1, \alpha, \alpha^2, \alpha^3$ is a $\mathbb{Q}$-basis of K. Solving the system of equations in $\mathbb{Q}$, we obtain

$$(\alpha^2+2)^{-1} = \frac{7}{11} + \frac{2}{11}\alpha - \frac{3}{11}\alpha^2 - \frac{1}{11}\alpha^3.$$

  Hence

$$\begin{aligned}\frac{\alpha^5}{\alpha^2+2} &= \left(\frac{7}{11}\alpha + \frac{2}{11}\alpha^2 - \frac{3}{11}\alpha^3 - \frac{1}{11}\alpha^4\right)(1+\alpha) \\ &= \left(-\frac{1}{11} + \frac{6}{11}\alpha + \frac{2}{11}\alpha^2 - \frac{3}{11}\alpha^3\right)(1+\alpha) \\ &= -\frac{1}{11} + \frac{5}{11}\alpha + \frac{8}{11}\alpha^2 - \frac{1}{11}\alpha^3 - \frac{3}{11}(1+\alpha) \\ &= -\frac{4}{11} + \frac{2}{11}\alpha + \frac{8}{11}\alpha^2 - \frac{1}{11}\alpha^3.\end{aligned}$$

2. Let p be a prime number. Recall that the canonical projection $\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ induces a surjective ring homomorphism

$$\pi_p : \mathbb{Z}[X] \longrightarrow \mathbb{F}_p[X].$$

   Let $f = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$ be a polynomial such that p divides $a_0, a_1, \ldots, a_{n-1}$, p does not divide a_n and p^2 does not divide a_0.

   (a) Prove that $\pi_p(f)$ is monomial of degree n in $\mathbb{F}_p[X]$.

(b) Prove that f is irreducible in $\mathbb{Q}[X]$ [This result is referred to as *Eisenstein's criterion*]

Solution:

(a) Write $a_k = pa'_k$ for $k = 0, \ldots, n-1$. Recall that π_p is reduction modulo p on coefficients and maps $X \mapsto X$. Then

$$\pi_p(f) = \pi_p(a_n X^n + \sum_{k=0}^{n-1} pa'_k X^k) = \pi_p(a_n)X^n + \sum_{k=0}^{n-1} \pi_p(p)\pi_p(a'_k)X^k = \pi_p(a_n)X^n$$

since $\pi_p(p) = 0$. Since $p \nmid a_n$, we know that $\pi_p(a_n) \neq 0$, so that $\pi_p(f)$ is a monomial of degree n.

(b) Suppose by contradiction that $f = g_0 h_0$ for $g_0, h_0 \in \mathbb{Q}[X]$ non-invertible polynomials. Then g_0 and h_0 are non-constant and by Gauss' Lemma there exist $g, h \in \mathbb{Z}[X]$ of corresponding degree such that $f = gh$. Then $\pi_p(g)\pi_p(h) = \pi_p(f)$ and since $\mathbb{F}_p[X]$ is a UFD we know that $\pi_p(g)$ and $\pi_p(h)$ are monomials whose degrees add up to n. This means by construction of π_p that p divides the constant term of both g and h. Since a_0, the constant term of f, is the product of those two constant terms, we deduce that $p^2 | a_0$, in contradiction with our assumption. Hence f is irreducible in $\mathbb{Q}[X]$.

3. Let $a \in \mathbb{Z} \smallsetminus \{0, \pm 1\}$ be a *square-free* integer, that is, an integer which is not divisible by any perfect square except 1. Prove that, for each $n \in \mathbb{Z}_{>0}$, the polynomial $X^n - a \in \mathbb{Q}[X]$ is irreducible. Conclude that there are irreducible polynomials in $\mathbb{Q}[X]$ of any degree $n \geqslant 1$.

Solution: Let p be a prime factor of a. Since a is squarefree, $p^2 \nmid a$. Then $X^n - a$ satisfies the hypothesis of Eisenstein's criterion for p (Exercise 2), so that it is irreducible in $\mathbb{Q}[X]$. Since $n \geqslant 1$ is arbitrary and $a = 101$ is an example of square free integer, there are irreducible polynomial in $\mathbb{Q}[X]$ of any degree $n \geqslant 1$.

4. Let p be a prime number. Let $\zeta := e^{\frac{2\pi i}{p}} \in \mathbb{C}$ and consider the polynomial

$$f := \frac{X^p - 1}{X - 1} = X^{p-1} + \cdots + X + 1 \in \mathbb{Q}[X].$$

(a) Prove that f is irreducible [*Hint:* $g(X) := f(X + 1)$. Use Exercise 2]

(b) Deduce that $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$. The field $\mathbb{Q}(\zeta)$ is called the *p-th cyclotomic field*.

Solution:

(a) Consider the unique ring homomorphism $\gamma : \mathbb{Q}[X] \longrightarrow \mathbb{Q}[X]$ which sends $\mathbb{Q} \ni a \mapsto a$ and $X \mapsto X + 1$. Clearly, it is a ring isomorphism with inverse

defined via $X \mapsto X-1$. In particular, f is irreducible if and only if $g := \gamma(f)$ is irreducible. We notice that

$$Xg = \gamma(X-1)\gamma(f) = \gamma(X^p - 1) = (X+1)^p - 1,$$

so that

$$g = \sum_{k=1}^{p} \binom{p}{k} X^{k-1} = \sum_{h=0}^{p-1} \binom{p}{h+1} X^h.$$

Since $p \mid \binom{p}{h+1}$ for $h = 0, \ldots, p-2$, while $p \nmid \binom{p}{(p-1)+1} = 1$ and $p^2 \nmid \binom{p}{0+1} = p$, the polynomial g satisfies the hypothesis of Eisenstein's Lemma (Exercise 2), so that it is irreducible in $\mathbb{Q}[X]$. Hence g is irreducible in $\mathbb{Q}[X]$.

(b) First, notice that

$$f(\zeta) = \frac{\zeta^p - 1}{\zeta - 1} = \frac{1-1}{\zeta - 1} = 0.$$

As in Exercise 1(b), since f is irreducible, we can conclude that $\mathbb{Q}[X]/(f) \cong \mathbb{Q}(\zeta)$. This is also an isomorphism of $\mathbb{Q}$-vector spaces, so that $[\mathbb{Q}(\zeta) : \mathbb{Q}] = [\mathbb{Q}[X]/(f) : \mathbb{Q}] = \deg(f) = p - 1$.

5. Let $f = \sum_i a_i X^i \in \mathbb{Z}[X]$. Suppose that $\alpha \in \mathbb{Q}$ is a root of f and write $\alpha = \frac{a}{b}$ for $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$.

(a) Prove that $a | a_0$ and $b | a_n$.

(b) Deduce that $2X^4 + X + 3 \in \mathbb{Q}[X]$ has no roots in $\mathbb{Q}$. Is it irreducible in $\mathbb{Q}[X]$?

Solution:

(a) Since α is a root of f, we see that

$$a_n \frac{a^n}{b^n} + \cdots + a_1 \frac{a}{b} + a_0 = 0.$$

Multiplying both sides by b^n we obtain

$$a_n a^n + \cdots + a_1 a b^{n-1} + a_0 b^n = 0.$$

In particular, $a_n a^n = -b(\sum_{k=0}^{n-1} a_k a^k b^{n-k-1})$ and $a_0 b^n = -a(\sum_{k=1}^{n} a_k a^{k-1} b^{n-k})$, so that $b | a_n a^n$ and $a | a_0 b^n$. Since a and b are coprime, we conclude that $b | a_n$ and $a | a_0$.

(b) Let $f = 2X^4 + X + 3$. By part (a),

$$\{\text{roots of } f \text{ in } \mathbb{Q}\} \subset \left\{ \pm 1, \pm 3, \pm \frac{1}{2}, \pm \frac{3}{2} \right\}.$$

One easily checks that those eight rational numbers are not roots of the given polynomial, so that f has no root in $\mathbb{Q}$. This means that f has no linear factors, but not yet that it is irreducible. In order to decide if it is irreducible, we need to check if it possible to write it as a product of degree-2 polynomials in $\mathbb{Q}[X]$.

Suppose that $f = gh$ for $g, h \in \mathbb{Q}[X]$ of degree 2. By Gauss' Lemma, we can find g and h with integer coefficients. Since the product of the leading coefficients of g and h must be the prime number 2, we can assume without loss of generality that $g = 2X^2 + aX + b$ and $h = X^2 + cX + d$ (the leading coefficients can be chosen to be any two rational numbers with product equal to 2) for $a, b, c, d \in \mathbb{Z}$. Then

$$X^4 + (a + 2c)X^3 + (2d + ac + b)X^2 + (ad + bc)X + bd = 2X^4 + X + 3.$$

Comparing the coefficients of X^3, we see that $a = -2c$, so that a is even. Then, comparing the coefficients of X^2, we see that $b = -2d - ac$ must is even as well. This implies that $ad + bc = 1$ is even as well, contradiction. Hence f is irreducible.

6. Let $x \in \mathbb{R} \setminus \mathbb{Q}$ be algebraic over $\mathbb{Q}$. Let $f = \mathrm{irr}(x, \mathbb{Q})$ and $n = \deg(f)$.

   (a) Show that there exists $c \in \mathbb{R}_{>0}$ such that, for any $\frac{a}{b} \in \mathbb{Q}$ with coprime $a, b \in \mathbb{Z}$, $b > 0$, we have
   $$\left|x - \frac{a}{b}\right| > \frac{c}{b^n}.$$
   [*Hint:* Write $f(\frac{a}{b}) = f(\frac{a}{b}) - f(x) = (\frac{a}{b} - x)f'(y)$ for some y]

   (b) Show that $\alpha := \sum_{n=1}^{\infty} 10^{-n!}$ is an irrational number.

   (c) Show that α is transcendental over $\mathbb{Q}$. [*Hint:* Consider $\frac{a_m}{b_m} = \sum_{n=1}^{m} 10^{-n!}$ and estimate $|\alpha - \frac{a_m}{b_m}|$]

Solution:

(a) Following the hint, we use the mean value theorem and write

$$\left|f\left(\frac{a}{b}\right)\right| = \left|f(x) - f\left(\frac{a}{b}\right)\right| = \left|x - \frac{a}{b}\right| |f'(y)| \tag{1}$$

for some y between $\frac{a}{b}$ and x. If we take $c > 1$, the statement clearly holds for $\left|x - \frac{a}{b}\right| \geqslant 1$. So we can assume that $\left|x - \frac{a}{b}\right| < 1$. Then $|y| < 1 + |x|$ and $|f'(y)| < \frac{1}{c'}$ for some constant $c' > 0$ depending only on x. Hence (1) tells us that

$$\left|x - \frac{a}{b}\right| > c' \left|f\left(\frac{a}{b}\right)\right| = \frac{c'}{b^n} \left|b^n f\left(\frac{a}{b}\right)\right| \geqslant \frac{c'}{b^n}, \tag{2}$$

where the last inequality is due to the fact that $f\left(\frac{a}{b}\right) \neq 0$ since f is irreducible in $\mathbb{Q}$, while $b^n f\left(\frac{a}{b}\right)$ is seen (similarly as in Exercise 5) to be an integer, so that $\left|b^n f\left(\frac{a}{b}\right)\right| \geqslant 1$.

(b) A basic result in number theory states that the decimal expansion of a rational number is eventually periodic. But the decimal expansion of α, which consists of 0's everywhere, except on the positions $n!$ for $n > 1$, can be seen not to be eventually periodic, so that $\alpha \notin \mathbb{Q}$.

(c) Let $a_m = 10^{m!} \sum_{n=1}^{m} 10^{-n!}$ and $b_m = 10^{m!}$. Then

$$\left|\alpha - \frac{a_m}{b_m}\right| = \left|\sum_{n=1}^{\infty} 10^{-n!} - \sum_{n=1}^{m} 10^{-n!}\right| = \sum_{n=m+1}^{\infty} 10^{-n!}$$
$$< 10^{-(m+1)!} \sum_{n=0}^{\infty} 10^{-n} = 10^{-(m+1)!} \frac{10}{9} = \frac{10}{9 b_m^{m+1}} < \frac{1}{b_m^m},$$

so that α cannot be algebraic, because otherwise $m \gg 0$ would give a contradiction.

7. [Transcendence of e] Let $f \in \mathbb{R}[X]$ be a polynomial of degree m. For $t \in \mathbb{R}$, define

$$I_f(t) := \int_0^t e^{t-u} f(u) du.$$

(a) Show that $I_f(t) = e^t \sum_{j=0}^{m} f^{(j)}(0) - \sum_{j=0}^{m} f^{(j)}(t)$. [*Hint:* Induction and integration by parts]

(b) Show that $|I_f(t)| \leqslant |t| e^{|t|} \tilde{f}(|t|)$, where $\tilde{f} = \sum_{i=0}^{m} |a_i| X^i$ if $f = \sum_{i=0}^{m} a_i X^i$.

(c) From now on, we assume by contradiction that e is algebraic over $\mathbb{Q}$. Show that there exist $n \in \mathbb{Z}_{>0}$ and $q_0, \ldots, q_n \in \mathbb{Z}$ with $q_n \neq 0$, such that

$$q_0 + q_1 e + \cdots + q_n e^n = 0.$$

(d) Let p be a prime number and $f_p = X^{p-1}(X-1)^p \cdots (X-n)^p$. Define

$$J_p = \sum_{k=0}^{n} q_k I_{f_p}(k).$$

Show that there exists a constant $c \in \mathbb{R}_{>0}$ independent of p such that

$$|J_p| \leqslant c^p.$$

[*Hint:* Prove that $\tilde{f}_p(k) \leqslant (2n)^m$, where $m = \deg(f_p)$, for $k = 0, \ldots, n$.]

(e) Prove that

$$J_p = -\sum_{j=0}^{m} \sum_{k=0}^{n} q_k f_p^{(j)}(k), \quad \text{where } m = (n+1)p - 1.$$

(f) Using part (e), show that if $p > n$ and $p > |q_0|$, then J_p is an integer divisible by $(p-1)!$ but not by $p!$

(g) Conclude by contradiction that e is transcendental over $\mathbb{Q}$.

Solution:

(a) Let $L_f(t) := e^t \sum_{j=0}^m f^{(j)}(0) - \sum_{j=0}^m f^{(j)}(t)$ for $m = \deg(f)$. We prove that $I_f(t) = L_f(t)$ by induction on $m = \deg(f)$.
For $m = 0$, i.e., when f is constant $r \in \mathbb{R}$,

$$I_f(t) = I_r(t) = r\int_0^t e^{t-u}du = re^t\int_0^t e^{-u}du = re^t(1-e^{-t}),$$
$$L_f(t) = e^t\sum_{j=0}^0 f^{(j)}(0) - \sum_{j=0}^0 f^{(j)}(t) = e^t r - r,$$

which means that $I_f(t) = L_f(t)$ in this case.
Now suppose that the equality has been proven on degree $m-1$ and let us prove it for f of degree m. Via integration by parts and inductive hypothesis we obtain

$$\begin{aligned} I_f(t) &= \int_0^t e^{t-u}f(u)du = [-e^{t-u}f(u)]\big|_{u=0}^{u=t} + \int_0^t e^{t-u}f'(u)du \\ &= -f(t) + e^t f(0) + L_{f'}(t) \\ &= -f(t) + e^t f(0) + e^t\sum_{j=0}^{m-1} f^{(1+j)}(0) - \sum_{j=0}^{m-1} f^{(1+j)}(t) \\ &= -f(t) + e^t f(0) + e^t\sum_{j=1}^{m} f^{(j)}(0) - \sum_{j=1}^{m} f^{(j)}(t) = L_f(t). \end{aligned}$$

This concludes the proof of the given formula by induction.

(b) By triangular equality, for every u in the segment from 0 to t, $|f(u)| \leqslant \tilde{f}(|u|) \leqslant \tilde{f}(|t|)$. Moreover, for those values of u, the values of $t-u$ range in the same segment, so that $|e^{t-u}| = e^{|t-u|} \leqslant e^{|t|}$. Then, denoting by $\mathrm{lh}([0,t])$ the length of the segment from 0 to t, by basic calculus we obtain that

$$|I_f(t)| = \left|\int_0^t e^{t-u}f(u)du\right| \leqslant \mathrm{lh}([0,t])|e^{t-u}f(u)| \leqslant |t|e^{|t|}\tilde{f}(|t|)$$

(c) If e is algebraic over $\mathbb{Q}$, then there exist $n \geqslant 0$ and $q'_0, \ldots, q'_n \in \mathbb{Q}$, coefficients of the minimal polynomial of e, such that

$$q'_0 + q'_1 e + \cdots + q'_n e^n = 0.$$

Multiplying out all denominators of the rational numbers q'_k, we integers $q_0, \ldots, q_n$ satisfying the desired equality.

(d) If one replaces all minus signs appearing in the product $f_p = X^{p-1}(X-1)^p \cdots (X-n)^p$ with plus signs, one gets a polynomial where each coefficient is a sum of absolute values of integers whose sum is the corresponding coefficient of f_p. Hence each coefficient of $\tilde{f}_p$ has coefficients respectively smaller to those of this polynomial. This implies that $f_p(k) \leqslant k^{p-1}(k+1)^p \cdots (k+n)^p \leqslant (2n)^m$ for $0 \leqslant k \leqslant n$, where $m = (n+1)p - 1$ is the degree of f_p.

By the triangular inequality and part (b),

$$|J_p| \leqslant \sum_{k=0}^{n} |q_k||I_{f_p}(k)| \leqslant \sum_{k=1}^{n} |q_k| k e^k \tilde{f}_p(k) \leqslant \left(\sum_{k=1}^{n} |q_k| k e^k\right)(2n)^m$$
$$\leqslant \left(\sum_{k=1}^{n} |q_k| k e^k\right)((2n)^{n+1})^p \leqslant \left((2n)^{n+1} \sum_{k=1}^{n} |q_k| k e^k\right)^p \leqslant c^p$$

for some constant $c > 0$ independent on p.

(e) Using part (b) and the equation in (c) satisfied by $q_0, \ldots, q_n$ we obtain

$$J_p = \sum_{k=0}^{n} q_k \left(e^k \sum_{j=0}^{m} f_p^{(j)}(0) - \sum_{j=0}^{m} f_p^{(j)}(k)\right)$$
$$= \sum_{j=0}^{m} \sum_{k=0}^{n} q_k \left(e^k f_p^{(j)}(0) - f_p^{(j)}(k)\right)$$
$$= \sum_{j=0}^{m} \left(f_p^{(j)}(0)(\sum_{k=0}^{n} q_k e^k) - \sum_{k=0}^{n} q_k f_p^{(j)}(k)\right) = -\sum_{j=0}^{m} \sum_{k=0}^{n} q_k f_p^{(j)}(k),$$

where $m = (n+1)p - 1$ is indeed the degree of f_p.

(f) For $j \geqslant p$, we have $p! | f_p^{(j)}(k)$. Since $k = 0, \ldots, n$ are all root of multiplicity at least $p-1$ of f_p, we see that $f_p^{(j)}(k) = 0$ for $j < p-1$. For all values of k, except $k = 0$, we actually know that they are roots of multiplicity p, so that for $j = p-1$ and $k \neq 0$ we have $f_p^{(j)}(k) = 0$. This means that all $f_p^{(j)}(k)$ appearing in the sum of part (e) are divisible by $p!$, except eventually $f_p^{(p-1)}(0)$. Hence, using also Leibniz rule we can write, modulo p:

$$J_p \equiv q_0 f_p^{(p-1)}(0) = q_0(p-1)!(-1)^{np}(n!)^p.$$

This number is not divisible by $p!$ if $p > n$ and $p > |q_0|$, but it is divisible by $(p-1)!$.

(g) By the previous part, we see that $|J_p| \geqslant (p-1)!$. By Stirling's formula, $(p-1)! \sim \frac{1}{p}\sqrt{2\pi p}\left(\frac{p}{e}\right)^p$ for $p \to \infty$ meaning that $(p-1)!$ is eventually bigger than c^p for $c > 0$. Since there are infinitely many primes, we can find a prime big enough to get a contradiction.

Hence e is not algebraic, but transcendental.