

Q3a: Since $f_3 = \gcd(f_1, f_2)$, there must exist some u, v with $f_3 = v \cdot f_1 + u \cdot f_2$ evaluating at α we get that

$$f_3(\alpha) = u(\alpha)f_1(\alpha) + v(\alpha)f_2(\alpha) = 0 \cdot u(\alpha) + 0 \cdot v(\alpha) = 0$$

Q3b: We define $M = \{\deg(p(x)) : p(\alpha) = 0\}$. This is non-empty by definition, since α is algebraic. It is also bounded below by the property of the degrees of polynomials. Hence by the well ordering principle, there exists a minimal element corresponding to some polynomial $m_\alpha(x)$.

Claim 1: m_α is irreducible.

pf: Suppose not. Then there exist some non constant polynomials, $u(x), v(x)$ such that $u(x) \cdot v(x) = m_\alpha(x)$ By definition of m_α , we know that

$$0 = m_\alpha = u(\alpha) \cdot v(\alpha)$$

So either $u(\alpha) = 0$ or $v(\alpha) = 0$. Since u, v are assumed to be non constant, we have that $\deg(u) < \deg(m_\alpha)$ and $\deg(v) < \deg(m_\alpha)$. This contradicts minimality of m_α ■

Claim 2: Uniqueness of m_α

pf: Suppose that there exists some other v_α of minimal degree with $v_\alpha(\alpha) = 0$. Let $m_\alpha = \sum_{k=0}^n m_k x^k$ and $v_\alpha = \sum_{k=0}^n v_k x^k$, with $v_n, m_n \neq 0$. Note that any linear combination of m_α and v_α will also vanish at α . With this in mind observe the following:

$$v_\alpha(x) + (-v_n \cdot m_n^{-1})m_\alpha(x) = \sum_{k=0}^{n-1} v_k - \frac{v_n}{m_n} m_k x^k$$

By construction, this polynomial has degree strictly less than that of v_α, m_α and will also vanish at α , contradicting minimality of m_α ■

Note that WLOG we can always rescale m_α to be monic.

Claim 3: For any f which vanishes at α is divisible by m_α .

pf: Consider $\gcd(f, m_\alpha) = q(x)$. By previously proven results, we have that $q(x) | m_\alpha(x)$. Hence $\deg(q(x)) \leq \deg(m_\alpha(x))$. By part 3a we have that $q(\alpha) = 0$ and from uniqueness and minimality of $m_\alpha(x)$ we have that $q(x) = m_\alpha(x)$ and hence $m_\alpha(x) | f(x)$ ■

Q3c: From basic calculus we have that such an r satisfying $r^3 = m$ must be an irrational number. By 3b, if q is a polynomial where $q(r) = 0$, then $x^3 - m | q(x)$. Hence it is sufficient to show that $q(x)$ can not be of degree 1 or 2. If q is degree 1, then for some $a, b \in \mathbb{Q}$ we have that

$$q(r) = ar + b = 0 \implies r = -\frac{b}{a}$$

contradicting that r is irrational. If q is of degree 2, then we have that $x^3 - r^3 = (x - r)(x^2 + xr + r^2)$. So $q = x^2 + xr + r^2$. These coefficients are not in \mathbb{Q} so no such polynomial can exist.

Q3d: Consider the $m = 2, n = 9$. It is clear that there is no integer satisfying $k^9 = 2$. We see that $2^{\frac{1}{9}}$ is indeed a root of $x^9 - 2$, but it will also be the root of the polynomial $x^3 - 2^{\frac{1}{3}}$