hexagon:2610.00428v1

Every Algebraic Number is a Critical Value of an Integer Polynomial

by RJ Acuña

Abstract

We arrived at an independent proof of Petrov's theorem. For every irreducible $f \in \mathbb{Z}[x]$ of positive degree there are $g \in \mathbb{Z}[x]$ and an irreducible $F \in \mathbb{Z}[x]$ of positive degree with $F \mid g'$ and $F^2 \mid f \circ g$. Equivalently, every algebraic number is a critical value of an integer polynomial, so the set of critical values of $\mathbb{Z}[x]$ is exactly $\overline{\mathbb{Q}}$. The construction is explicit. We classify $g \in \mathbb{Z}[x]$ with critical value α, and find a lower bound for $\deg g$. The proof was assisted by AI, and has been formalized in Lean.

1 Introduction

A critical value of a nonconstant $g \in \mathbb{Z}[x]$ is a number α with $g(\beta) = \alpha$ and $g'(\beta) = 0$ for some β. Since $\overline{\mathbb{Q}}$ is closed under polynomial evaluation, every critical value is algebraic. Schwarz, Vologodsky and Walcher posed the problem of establishing the reverse implication [SVW17]. This note solves the problem.

Petrov's Theorem. *Let f be an irreducible integral polynomial of positive degree. Then there exist F and g in $\mathbb{Z}[x]$, with F irreducible and of positive degree, such that*

$$F \mid g' \quad \textit{and} \quad F^2 \mid f \circ g.$$

The construction in §2 was derived independently. Petrov's theorem [Pet21] was found later. The corollary is the statement in the title.

Corollary 1. *The set of critical values is exactly $\overline{\mathbb{Q}}$.*

pf. Write $f = m_\alpha$. If $g(\beta) = \alpha$ and $g'(\beta) = 0$ then β is a double root of $f \circ g$, since $(f \circ g)' = (f' \circ g)\, g'$, so $m_\beta \mid g'$ and $m_\beta^2 \mid f \circ g$. Conversely take F and g from Petrov's theorem. A root β of F has $g'(\beta) = 0$ and $f(g(\beta)) = 0$, so $g(\beta)$ is a conjugate of α, and conjugation gives α itself. ∎

2 The construction

Let f be irreducible of degree $n \geq 1$ and α a root. Write $f(x) = \sum_{k=0}^{n} a_k x^{n-k}$, so that $a_n = f(0)$. If $f = x$, then $g = x^2$ and $F = x$ work. Otherwise $f(0) \neq 0$, and since $\gcd(f, f') = 1$ in $\mathbb{Q}[x]$, the elimination ideal $(f, f') \cap \mathbb{Z}$ is nonzero. Let $u, v \in \mathbb{Z}[x]$ and $\rho \in \mathbb{Z}$, $\rho \neq 0$, be such that $u\, f + v\, f' = \rho$, and set $M := \rho\, a_n$, $F(x) := f(Mx)/a_n$ and $W(x) := \big(v(0)F(x) - v(Mx)\big)/\rho$. The polynomial claimed by Petrov's theorem is

$$g(x) := Mx + f(Mx)\, W(x). \tag{1}$$

pf. Write $F(x) = \sum_{k=0}^{n} A_k x^{n-k}$. From $A_k = a_k M^{n-k}/a_n$ we get $A_n = 1$ and $A_k = a_k \rho^{n-k} a_n^{n-k-1}$ for $k < n$, so $F \in \mathbb{Z}[x]$ with $F(0) = 1$, which gives $W(0) = 0$. And ρ divides M and every A_k with $k < n$, so it divides $v(0)F(x) - v(Mx)$ and $W \in \mathbb{Z}[x]$. Therefore g is an integral polynomial.

Let $\beta = \alpha/M$, a root of F. Therefore $g(\beta) = \alpha$, and $\rho W(\beta) = -v(\alpha)$. Then

$$\begin{aligned} g'(\alpha/M) &= M + \rho\, a_n f'(\alpha)\, W(\alpha/M) + \cancel{f(\alpha)}\, W'(\alpha/M) \\ &= M - a_n f'(\alpha) v(\alpha) = 0, \end{aligned}$$

because $u(\alpha)\cancel{f(\alpha)} + v(\alpha) f'(\alpha) = \rho$. Hence β is a double root of $f \circ g$, and F is irreducible, so $F \mid g'$ and $F^2 \mid f \circ g$ by Gauss. ∎

Any ρ will do, but $M = \rho\, a_n$ multiplies into every coefficient of F, W and g, so the reduced resultant gives the answer with the smallest coefficients.

3 Classification

We say a polynomial p is reducible if it is not primitive, or $p = fg$ with $\deg f, \deg g < \deg p$, and irreducible otherwise. For $\alpha \in \overline{\mathbb{Q}}$ we normalize the minimal polynomial m_α with positive leading coefficient for uniqueness. Say that α is a critical value for $\beta \in \overline{\mathbb{Q}}$ if some $g \in \mathbb{Z}[x]$ has $g(\beta) = \alpha$ and $g'(\beta) = 0$, and call such a g a solution for β. Here we classify which g can appear for a given α. Let $P \in \mathbb{Z}[x]$ with $\deg P > 0$. By the fundamental theorem of algebra, $P(x) - \alpha$ has a root β. Moreover this root is algebraic because it is a root of $m_\alpha \circ P \in \mathbb{Z}[x]$.

Theorem 1. *Let $P \in \mathbb{Z}[x]$ be nonconstant, let β be a root of $P - \alpha$, and write $m_\alpha \circ P = m_\beta\, h$ with $h \in \mathbb{Z}[x]$. Then α is a critical value for β if and only if*

$$m'_\alpha(\alpha) \mid h(\beta) \ \text{ in } \mathbb{Z}[\beta].$$

In that case, for $Q \in \mathbb{Z}[x]$ with $Q(\beta) = -h(\beta)/m'_\alpha(\alpha)$, $g_0 = P + m_\beta Q$ is a solution for β, and the solutions g for β are exactly $g \in g_0 + m_\beta^2\,\mathbb{Z}[x]$.

pf. By Gauss's lemma m_β divides $m_\alpha \circ P$ in $\mathbb{Z}[x]$, since m_β is irreducible. Differentiating $m_\alpha \circ P = m_\beta h$ and evaluating at β gives $m'_\alpha(\alpha)P'(\beta) = m'_\beta(\beta)h(\beta)$, where $m'_\alpha(\alpha), m'_\beta(\beta) \neq 0$, so the two divisibilities are equivalent and $-h(\beta)/m'_\alpha(\alpha)$ equals $-P'(\beta)/m'_\beta(\beta)$. Now $g_0(\beta) = P(\beta) = \alpha$ and

$$g_0'(\beta) = P'(\beta) + m'_\beta(\beta)Q(\beta) = 0.$$

If g is a solution for β then $g - P$ vanishes at β, so $g = P + m_\beta q$ with $q \in \mathbb{Z}[x]$, and $0 = g'(\beta) = P'(\beta) + m'_\beta(\beta)q(\beta)$ gives the divisibility and $q(\beta) = Q(\beta)$, so $m_\beta \mid q - Q$ and $g \in g_0 + m_\beta^2\mathbb{Z}[x]$; conversely every $g_0 + m_\beta^2 r$ has value α and derivative 0 at β. ■

Since the solutions for α are cosets $g \in g_0 + m_\beta^2\,\mathbb{Z}[x]$, $\deg g$ is unbounded above. So the natural question is what is the smallest $\deg g$ for α; we do not answer that question, but we provide the following lower bound.

Proposition 1. *If g is a nonconstant solution for β, then* $\deg g > \deg \alpha$.

pf. Since $\alpha = g(\beta)$, $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\beta)$, so $\deg \beta \geq \deg \alpha$. And $g' \neq 0$ vanishes at β, so $m_\beta \mid g'$ and $\deg g - 1 \geq \deg \beta$.■

Each line below is a closed identity, checkable by expansion.

Example 1 ($f = qx - p$, $p \neq 0$, $\gcd(p, q) = 1$). Here $f' = q$ and $p = qx - f$, so $(f, f') \cap \mathbb{Z} = \mathbb{Z}$ and $\rho = 1$. Choose $a, b \in \mathbb{Z}$ with $ap + bq = 1$ and take $u = -a$, $v = ax + b$. Then $f(0) = -p$, $M = -p$, $F = qx + 1$, $W = x$, and

$$g = -pqx^2 - 2px, \qquad g' = -2p\,(qx + 1), \qquad f \circ g = -p\,(qx + 1)^2.$$

Example 2 ($f = ax^2 + bx + c$). This is irreducible of degree 2 exactly when $a \neq 0$, $\gcd(a, b, c) = 1$, and $D := b^2 - 4ac$ is not a square. Since $(f')^2 = 4af + D$,

$$\rho = \operatorname{Res}(f, f') = -aD, \qquad u = 4a^2, \qquad v = -af',$$

so $M = -acD$ and

$$F = a^3cD^2x^2 - abD\,x + 1, \qquad W = a^3bcD\,x^2 - a(b^2 - 2ac)\,x,$$

$$g = a^6bc^3D^3x^4 - 2a^4c^2(b^2 - ac)D^2x^3 + a^2bc(b^2 - ac)D\,x^2 - 2ac(b^2 - 3ac)\,x,$$

with $g' = 2ac\big(2a^2bcD\,x - (b^2 - 3ac)\big)F$. For $b = 0$ the quartic term drops and $\deg g = 3 = n + 1$, the least any solution can have. On $f = x^2 - d$ that cubic is $g(x) = -D_3(4d^2x, d)/(2d)$, a rescaling of the Dickson polynomial $D_3(x, d) = x^3 - 3dx$, whose pair of critical values is classical.

Example 3 ($f = x^3 - x - 1$). The construction gives $M = 23$ and a sextic. Then a search exhibits a quintic. Let θ be a root of f. Then Theorem 1 with $\beta = 1/(\theta^2 - \theta + 2)$, so that $m_\beta = 23x^3 - 23x^2 + 8x - 1$, $P = 46x^2 - 23x + 3$, and $Q = -1058x^2 + 667x - 115$, gives the quintic

$$g = -24334x^5 + 39675x^4 - 26450x^3 + 9085x^2 - 1610x + 118.$$

This is the least possible degree. By Proposition 1 a solution has degree at least 4, and degree 4 cannot happen. In fact no $g \in \mathbb{Q}[x]$ of degree 4 has θ as a critical value. Suppose $g(\beta) = \theta$ and $g'(\beta) = 0$ with $\deg g = 4$. Up to a rational translation of x, g' is a multiple of a depressed cubic, $g' = 4a\,(x^3 + ux + w)$ with $a, u, w \in \mathbb{Q}$, $a \neq 0$, so $g = a\,h + r$ with $h = x^4 + 2ux^2 + 4wx$ and $r \in \mathbb{Q}$, and the critical values of g are $as_i + r$ with $s_i = h(\beta_i)$, where the β_i are the roots of $x^3 + ux + w$. Since $\beta_i^3 = -u\beta_i - w$, $s_i = u\beta_i^2 + 3w\beta_i$, and the characteristic polynomial of this element of $\mathbb{Q}[\beta]/(\beta^3 + u\beta + w)$ is

$$s(z) = z^3 + 2u^2z^2 + (u^4 + 18uw^2)\,z + 2u^3w^2 + 27w^4.$$

Now $s(z)$ is a monic cubic over $\mathbb{Q}$ with root $(\theta - r)/a$, whose minimal polynomial is $a^{-3}f(az + r)$, so $s(z) = a^{-3}f(az + r)$. The z^2 coefficient gives $r = 2au^2/3$, and with it the z and constant coefficients become $-1/a^2 = 18uw^2 - u^4/3$ and $-1/a^3 = 27w^4 - 10u^3w^2 - 2u^6/27$. The first forces $u \neq 0$, so $\sigma = 27w^2/u^3 \in \mathbb{Q}$, and the two equations read $-1/a^2 = -u^4(1-2\sigma)/3$ and $-1/a^3 = u^6(\sigma^2 - 10\sigma - 2)/27$. Cubing the first and squaring the second gives $-1/a^6$ and $1/a^6$ on the left, so adding them, u and a drop out: $(\sigma^2 - 10\sigma - 2)^2 = 27(1 - 2\sigma)^3$, that is, $\sigma^4 + 196\sigma^3 - 228\sigma^2 + 202\sigma - 23 = 0$. This is monic with integer coefficients, so a rational root is an integer dividing 23. But the polynomial takes the values 148 and -648 at $\sigma = \pm 1$ and is nonzero at ± 23. So there is no rational σ, a contradiction.

Example 4 (Dedekind's cubic). $f = x^3 - x^2 - 2x - 8$, the standard example of a field whose ring of integers is not monogenic. Here 2 is a common index divisor [Ded78]. With $u = 21x - 125$, $v = -7x^2 + 44x - 3$, $\rho = 1006$, $f(0) = -8$, $M = -8048$,

$$\begin{aligned} F &= 65158925824x^3 + 8096288x^2 - 2012x + 1, \\ W &= -194310912x^3 + 426544x^2 + 358x, \end{aligned}$$

$$\begin{aligned} g = {} & 101288722414414331904x^6 \\ & - 209759614012620800x^5 - 217370176548864x^4 \\ & - 14767629312x^3 + 2350016x^2 - 10912x. \end{aligned}$$

4 Computerization

The construction of g was provided by AI. However, the crucial step that allowed the agent to provide answers was my proof of Corollary 1. Once I recast the problem as the search for an irreducible polynomial F satisfying the hypotheses of Petrov's theorem, the agent found g for a general linear polynomial (which one can do by hand), then for a general quadratic, then for a general cubic, and finally gave the formula for g for arbitrary f. Previously, all agents I tried failed to construct g for $x^3 - x - 1$. An agent later found Petrov's theorem on MathOverflow after I insisted it should do a deep literature search, including all the classical literature. The development above has been formalized in Lean 4 [MU21] against Mathlib [The20], in about 1,700 lines [Acu26b]. An online calculator [Acu26a] is provided for the reader to verify the construction. It runs the construction in the browser and, if α is real, generates a Desmos plot that allows the reader to check visually that it is a critical value. The implemented program does have a virtue that Petrov's construction doesn't have. Because it uses the reduced resultant, the coefficients come out as small as possible.

References

[Ded78] Richard Dedekind. Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen. *Abhandlungen der Königlichen Gesellschaft der Wissenschaften zu Göttingen*, 1878.

[SVW17] Albert Schwarz, Vadim Vologodsky, and Johannes Walcher. *Integrality of Framing and Geometric Origin of 2-functions*. https://arxiv.org/abs/1702.07135, 2017.

[The20] The mathlib Community. The Lean Mathematical Library. In *Certified Programs and Proofs (CPP 2020)*. ACM, 2020.

[MU21] Leonardo de Moura and Sebastian Ullrich. The Lean 4 Theorem Prover and Programming Language. In *Automated Deduction – CADE 28*, Lecture Notes in Computer Science. Springer, 2021.

[Pet21] Fedor Petrov. Answer to "When $p(x)^2 \mid f(g(x))$?". https://mathoverflow.net/q/397800, 2021.

[Acu26a] RJ Acuña. *Critical values of integer polynomials: an online calculator*. https://rjacuna.github.io/CriticalValues/, 2026.

[Acu26b] RJ Acuña. *CriticalValues: paper, Lean 4 formalization and calculator*. https://github.com/rjacuna/CriticalValues, 2026.

the repository

the calculator