The radical as a forced structure : how to split powers from radicals

Yuanjie Liu

Abstract: It is common to regard the n-th root as a value of the one-parameter power family, $x^{1/n} = x^t$ at $t = 1/n$. On the positive reals this collapse is correct: there the power map $p_n : x \mapsto x^n$ is an automorphism and its inverse is single-valued. We show that the collapse is a torsion phenomenon. Once the base group contains the n-th roots of unity $\mu_n = \{x : x^n = 1\}$, the map p_n is no longer injective; its kernel is exactly μ_n, every fiber of p_n is the coset $x \cdot \mu_n$, and the "root of x^n" is not a function but a section of an n-fold cover: a choice among n branches that differ by multiplication with μ_n. Three elementary theorems express this split — kernel, fibers, and the collapse criterion "p_n is injective if and only if μ_n is trivial" — and all three are verified mechanically in Lean 4 with Mathlib, with zero proof gaps. On the computational side we exhibit machine-certified radical values (the golden section solves $x^2 - x - 1 = 0$) and a certified general quadratic solver: a real root of $x^2 - bx - c = 0$ exists exactly when $b^2 + 4c \geq 0$, and in that case both radical roots are exhibited and the polynomial is shown to factor. The same programme advances to the cubic: surjectivity of the cube map on $\mathbb{R}$ (intermediate value) holds inside the proof system, and the Cardano construction [1] exhibits a real root of $x^3 + px + q = 0$ whenever the discriminant is nonnegative. Every statement in the main deduction is machine-checked; the boundary between executable integer arithmetic and certified, non-executable real statements is stated explicitly.

Keywords: radical function, power map, roots of unity, torsion, quotient and section, formal verification
AMS 2000 subject classifications: 12F10, 03B35, 26A09

> *"Eternity is a long time."*
>
> — *Isaac Asimov,* Foundation

1. Question, inputs, and logical order

Write p_n for the map $x \mapsto x^n$ on a multiplicative structure. The statement that interests us is the received identification

$$\text{"the } n\text{-th root is the power } x^{1/n}\text{, i.e. } p_{1/n}\text{"}. \tag{1}$$

As a statement about positive reals it is unproblematic : for every $x > 0$ there is a unique $y > 0$ with $y^n = x$, and one writes $y = x^{1/n} = \exp(\frac{1}{n} \ln x)$ [2]. But the equation $y^n = x$ does not have a unique solution in general, and where it does not, the symbol $x^{1/n}$ silently selects one solution among several. The present paper asks what is lost by that selection.

We will use three kinds of statements, in the spirit of a compile-first exposition :

Convention. On the positive reals the fractional-power collapse (1) holds because $\mu_n \cap \mathbb{R}_+ = 1$; this is a fact about a torsion-free group, spelled out in Section 3.

Independent Researcher ; yuanjieliu65@gmail.com

Exact deductions. Over a commutative group G, the map p_n is a group endomorphism. Its kernel is the subgroup $\mu_n = \{x \in G : x^n = 1\}$ of n-th roots of unity; every fiber of p_n is a coset of μ_n; and p_n is injective exactly when μ_n is trivial. These are Theorems 3–6.

Machine-checked content. The three theorems, the radical examples, and the quadratic solver of Section 6 are formalized in Lean 4 [3] with Mathlib [4], inside the NODS repository (module `Nods.Theories.Radical`, wired into the main build, zero proof gaps). The original Riemann material of the template file from which this article's layout is taken is entirely removed; no number-theoretic conjecture is touched here.

2. Setting : power maps and roots of unity

Fix a commutative group G, written multiplicatively, and $n \in \mathbb{N}$. We use two objects.

Definition 1 (Power map)**.** *$p_n \colon G \to G$ denotes $p_n(x) = x^n$.*

Definition 2 (Roots of unity)**.** *$\mu_n(G) = \{x \in G : x^n = 1\}$ is the subgroup of n-th roots of unity.*

That $\mu_n(G)$ is a subgroup is immediate from commutativity ($(xy)^n = x^n y^n$) and from $(x^{-1})^n = (x^n)^{-1}$. Its elements are the *torsion* of exponent n; $\mu_n(G) = \{1\}$ is the statement that G has no nontrivial n-th root of unity.

p_n is a group homomorphism : $p_n(xy) = (xy)^n = x^n y^n = p_n(x)p_n(y)$, again by commutativity.

3. The collapse and its failure

On $G = \mathbb{R}_+$ (positive reals, multiplication), the equation $x^n = 1$ has only the solution 1; indeed x^n is strictly increasing. Hence p_n is injective and, being a group endomorphism of $\mathbb{R}_+$ with no kernel, it is an automorphism : every y has exactly one n-th root, the fractional power $y^{1/n}$. The collapse (1) is exactly the statement that this inverse is *unique*, and uniqueness is the absence of torsion.

Over $\mathbb{C}^\times$ the same equation has n solutions, namely the regular n-gon $\mu_n(\mathbb{C}^\times) = \{e^{2\pi i k/n} : 0 \le k < n\}$, a cyclic group of order n [5]. The failure of injectivity is measured by this group. The next section states the mechanism once, for every commutative group.

4. Power as quotient, radical as section

Theorem 3 (Kernel is the group of roots of unity)**.** *For every commutative group G and every n,* $\ker p_n = \mu_n(G)$.

Démonstration. An element x lies in the kernel of p_n iff $p_n(x) = 1$ iff $x^n = 1$ iff $x \in \mu_n(G)$. □

Theorem 4 (Fibers are cosets)**.** *For every commutative group G, every n, and all $x, z \in G$,*

$$z^n = x^n \quad \Longleftrightarrow \quad \exists \zeta \in G,\ \zeta^n = 1 \ \wedge\ z = x\zeta.$$

Equivalently, the fiber of p_n over x^n is the coset $x \cdot \mu_n(G)$.

Démonstration. ($\Leftarrow$) If $z = x\zeta$ with $\zeta^n = 1$, then $z^n = (x\zeta)^n = x^n \zeta^n = x^n$ by commutativity. ($\Rightarrow$) If $z^n = x^n$, put $\zeta = x^{-1}z$. Then $\zeta^n = (x^{-1}z)^n = (x^n)^{-1}z^n = 1$ and $z = x\zeta$. □

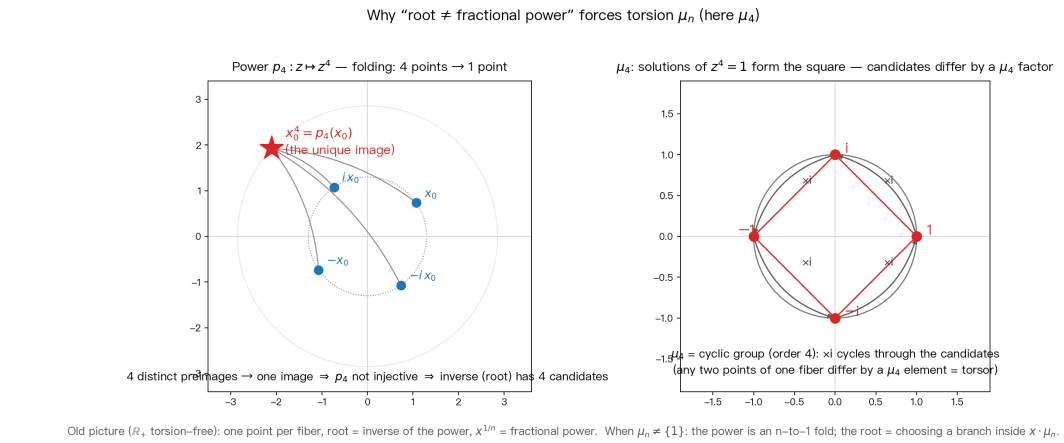

FIGURE 1. *Left : p_4 folds four distinct points into one image, so the inverse (the radical) has four candidates. Right : the four candidates are not isolated ; they form the square μ_4, the kernel of p_4, and multiplication by i cycles through them.*

Corollary 5. *If x^n has one n-th root x_0, then it has exactly $|\mu_n(G)|$ of them, namely ζx_0 with $\zeta \in \mu_n(G)$. Over a field containing μ_n this number is n.*

Theorem 6 (Collapse criterion)**.** *For every commutative group G and every n, p_n is injective if and only if $\mu_n(G) = \{1\}$.*

Démonstration. By Theorem 3, $\ker p_n = \mu_n(G)$; a group homomorphism is injective iff its kernel is trivial. □

The content of the three theorems is a division of labour between two structural roles.

— *Power is a quotient.* p_n collapses the orbit of x under multiplication by μ_n to a single point ; it is the projection of G onto G/μ_n (up to the canonical identification). Its kernel is nontrivial exactly when torsion is present.

— *The radical is a section.* A “root” is a choice of one preimage under p_n. Globally this choice cannot be made continuously or canonically ; it exists only branch by branch, and the branches differ by the deck group μ_n. The fractional power $x^{1/n} = e^{(\ln x)/n}$ is the section on the principal branch — the branch on which the torsion is invisible. This is why (1) “works” on $\mathbb{R}_+$ and fails on $\mathbb{C}^\times$: not because the algebra changes, but because the cover is trivial there.

Figure 1 visualizes both roles for $n = 4$: four points $z \in x_0\mu_4$ are folded by p_4 into one image x_0^4, and the four candidates differ by the square $\mu_4 = \{1, i, -1, -i\}$.

5. What torsion forces : explaining a number

Corollary 5 has a concrete reading. Over $\mathbb{Q}$, the equation $x^2 = 2$ has no solution at all ; this is a machine-checked fact, and it is exactly the sense in which the radical is a *forced* object rather than a chosen symbol :

— no $n \in \mathbb{N}$ satisfies $n^2 = 2$;

— no $q \in \mathbb{Q}$ satisfies $q^2 = 2$;
— over the reals, $\sqrt{2}$ exists and $(\sqrt{2})^2 = 2$, and the exponential/logarithm path gives the different exact formula $e^{\ln 2} = 2$.

The same number admits *different* exact constructions along the four classical families, and which families succeed depends on the number : 25 is 5^2 (power) and $\sqrt{25} = 5$ (radical, executable integer square root) ; 2 is not a square at all and is only reached by radical or transcendental formulas ; the golden section $\varphi = (1+\sqrt{5})/2$ is exhibited as a radical solution of $x^2 - x - 1 = 0$ and verified to satisfy $\varphi^2 = \varphi + 1$. These are statements, not heuristics ; each is checked by the proof system.

6. Certified radicals and a general quadratic solver

The examples of Section 5 are instances of a general solver. Fix real b, c and the equation

$$x^2 - bx - c = 0, \qquad \Delta = b^2 + 4c. \tag{2}$$

Theorem 7 (Quadratic radical solver)**.** *Let $\Delta = b^2 + 4c \geq 0$. Put $r_+ = (b + \sqrt{\Delta})/2$ and $r_- = (b - \sqrt{\Delta})/2$. Then*

1. *$r_+^2 - br_+ - c = 0$ and $r_-^2 - br_- - c = 0$;*
2. *for every x, $x^2 - bx - c = (x - r_+)(x - r_-)$ — there are no other roots ;*
3. *if $\Delta < 0$ there is no real root at all.*

Consequently a real root exists if and only if $\Delta \geq 0$.

Démonstration. All claims are obtained by expanding and using $(\sqrt{\Delta})^2 = \Delta$, which is the defining property of the real square root ; item 1 and item 2 are pure ring identities after that substitution, and item 3 is completing the square : $(2x - b)^2 = \Delta$, impossible for $\Delta < 0$. □

Theorem 8 (Cubic radical solution of Cardano)**.** *Let $\Delta_3 = (q/2)^2 + (p/3)^3 \geq 0$. Then $x^3 + px + q = 0$ has a real root, constructed as follows. Put $s = \sqrt{\Delta_3}$, choose u with $u^3 = -q/2 + s$ (possible because the cube map is surjective on $\mathbb{R}$), and set $v = -p/(3u)$. Then $v^3 = -q/2 - s$, $uv = -p/3$, and $u + v$ is a root.*

Démonstration. $u^3 + v^3 = -q$ together with $3uv = -p$ gives $(u+v)^3 = u^3 + v^3 + 3uv(u+v) = -q - p(u+v)$, hence $(u+v)^3 + p(u+v) + q = 0$. The identity $v^3 = -q/2 - s$ follows from $(q/2)^2 - s^2 = -(p/3)^3$ and $u \neq 0$ by direct calculation (the case $u = 0$ forces $p = 0$, reducing to $x^3 + q$). Note that v cannot be chosen as an *independent* cube root of $-q/2 - s$: then uv would differ by a cube root of unity — the third appearance of the torsion split of Section 4, which machine verification forces us to face. □

The statements are machine-checked. Two boundaries are stated explicitly.

— *Executability.* On $\mathbb{N}$ the integer square root $\sqrt{25} = 5$ is computed and reduced by the proof system itself (`norm_num`). On $\mathbb{R}$ the square root is defined by completeness and is not executable ; the reductions above (for example $\sqrt{16} = 4$ via $\sqrt{a^2} = |a|$) are certified theorems, not numeric iterations. We do not claim a numeric radical evaluator ; we claim certified radical statements.

— *The next degree.* The same programme now needs a general cubic (with an x^2 term, first reduced to the depressed form by a translation) and a quartic (Ferrari, via a cubic resolvent); these two steps are not yet formalized. From degree 5 the general equation escapes the radicals (Abel–Ruffini [6]); stating that boundary precisely is the Galois half [7] of the programme and is not claimed here.

7. Formalization notes

All statements marked are proved in Lean 4 [3] with Mathlib [4], in the module `Nods.Theories.Radical` of the NODS repository. Technical choices :

— theorems are stated over an arbitrary commutative group G (`CommGroup`), which makes the collapse criterion meaningful as an equivalence and not as an accident of $\mathbb{R}_+$;
— the power map is the Mathlib homomorphism `powMonoidHom`; the roots of unity form a self-defined subgroup `nRoots`;
— the proofs are short and do not use excluded middle beyond Mathlib's standard library : Theorem 3 is definitional, Theorem 4 is one calculation in each direction, Theorem 6 follows from the standard kernel-trivial-iff-injective lemma;
— the analytic primitive of the cubic — surjectivity of the cube map on $\mathbb{R}$ — comes from Mathlib's intermediate value theorem (`intermediate_value_Icc`), see Theorem 8; the non-executability of `Real.sqrt` is unchanged;
— the module is imported by the main file and the full build is green; grep confirms zero `sorry` in the source tree.

The template of this article (layout class `jsfds`, bilingual conventions) was taken from the author's earlier preprint; its mathematical content has been completely replaced by the material above.

8. Conclusion

The identification of the n-th root with a fractional power is not false; it is local. It holds exactly on the branch where the cover is trivial, i.e. where $\mu_n = \{1\}$. Over a group that carries the n-th roots of unity, power and radical are two different structural roles — a quotient by μ_n and a section of the resulting n-fold cover — and the torsion subgroup μ_n is the exact measure of the difference, because removing it collapses the distinction (Theorem 6). Three short theorems, radical examples, and certified quadratic and cubic solvers carry this statement through a proof system end to end, with the boundary between executable arithmetic and certified real analysis stated where it occurs.

References

[1] Girolamo Cardano. *Artis Magnae, Sive de Regulis Algebraicis*. Johannes Petreius, Nuremberg, 1545.
[2] Leonhard Euler. *Introductio in analysin infinitorum*. Marc-Michel Bousquet, Lausanne, 1748.
[3] Leonardo de Moura, Soonho Kong, Jeremy Avigad, Floris van Doorn, and Jakob von Raumer. The Lean theorem prover (system description). In *Automated Deduction — CADE-25*, volume 9195 of *LNCS*, pages 378–388. Springer, 2015.

[4] The mathlib Community. The lean mathematical library. In *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020)*, pages 367–381. ACM, 2020.
[5] Carl Friedrich Gauss. *Disquisitiones Arithmeticae*. Gerhard Fleischer, Leipzig, 1801.
[6] Niels Henrik Abel. Mémoire sur les équations algébriques, où l'on démontre l'impossibilité de la résolution de l'équation générale du cinquième degré, 1824. Christiania ; reprinted in Œuvres complètes, vol. 1, 1881.
[7] Évariste Galois. Mémoire sur les conditions de résolubilité des équations par radicaux. *Journal de Mathématiques Pures et Appliquées*, 11 :417–433, 1846.