https://henrydukepickle.github.io/js_quintic/

Nobody Solves the Quintic

Abstract. Everybody knows that nobody can solve the quintic. Indeed this insolubility is a well known hard theorem, the high point of a full-semester course on Galois theory, often taken in one's 3rd or 4th year of university mathematics. I'm not sure why so few know that the same theorem can be proven in about 15 minutes using *very* basic and easily understandable topology, accessible to practically anyone.

Definition. A permutation of n elements is just some rearranging of those elements.

Notation. We use cycle notation to write permutations. The cycle $(abcd)$, for instance, permutes a, b, c, d, in a "cycle" – so a goes to b, b to c, c to d, and d back to a.

Example. (12) represents the permutation swapping 1 and 2, and leaving all other elements alone.

Example. (123) represents sending 1 to 2, 2 to 3, and 3 to 1.

Definition. The product of two permutations is the result of applying these permutations in sequence.

Example. The product $(12) * (23) = (132)$.

Example. The product $(12) * (12)$ is the identity permutation, which does nothing.

Definition. The inverse of a permutation is the result of doing that permutation "backwards".

Example. The inverse of (123) is (321).

Definition. The commutator of two operations x and y is $[x, y] := xyx^{-1}y^{-1}$.

Example 1. $[(12),(23)] = (12)(23)(12)^{-1}(23)^{-1} = (123)$ and in general,

$$[(ij),(jk)] = (ijk).$$

Example 2.

$$[(ijk),(jkl)] = (ijk)(jkl)(ijk)^{-1}(jkl)^{-1} = (il)(jk).$$

Example 3. $[(ijk),(klm)] = (ijk)(klm)(ijk)^{-1}(klm)^{-1} = (jkm)$.

Example 4. So, in fact, we have $(123) = [(412),(253)] = [[(341),(152)],[(125),(543)]] = [[[(234),(451)],[(315),(542)]],[[(312),(245)],[(154),(423)]]] = [\,[[[(123),(354)],[(245),(531)]],[[(231),(145)],[(154),(432)]]], [[[(431),(152)],[(124),(435)]],[[(215),(534)],[(142),(253)]]]\,]$.

Solving the Quadratic, $ax^2+bx+c = 0$: $\Delta = b^2-4ac$; $\delta = \sqrt{\Delta}$; $r = \frac{\delta-b}{2a}$.

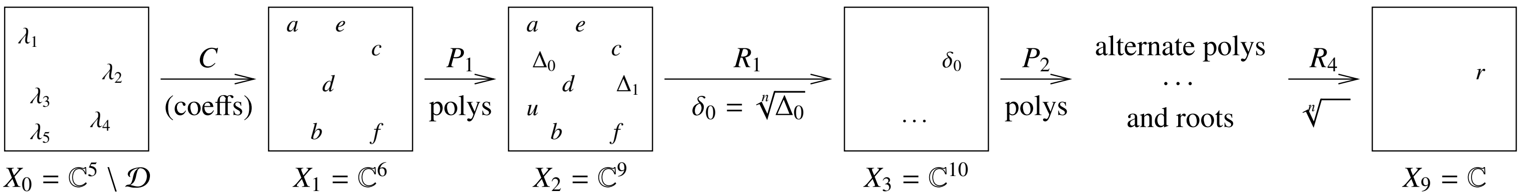
Solving the Cubic, $ax^3+bx^2+cx+d = 0$: $\Delta = 27a^2d^2-18abcd+4ac^3+4b^3d-b^2c^2$; $\delta = \sqrt{\Delta}$; $\Gamma = 27a^2d-9abc+3\sqrt{3}a\delta+2b^3$; $\gamma = \sqrt[3]{\frac{\Gamma}{2}}$; $r = -\frac{\frac{b^2-3ac}{\gamma}+b+\gamma}{3a}$.

Solving the Quartic, $ax^4+bx^3+cx^2+dx+e = 0$: $\Delta_0 = 12ae-3bd+c^2$; $\Delta_1 = -72ace+27ad^2+27b^2e-9bcd+2c^3$; $\Delta_2 = \frac{1}{27}\left(\Delta_1^2-4\Delta_0^3\right)$; $u = \frac{8ac-3b^2}{8a^2}$; $v = \frac{8a^2d-4abc+b^3}{8a^3}$; $\delta_2 = \sqrt{\Delta_2}$; $Q = \frac{1}{2}\left(3\sqrt{3}\delta_2+\Delta_1\right)$; $q = \sqrt[3]{Q}$; $S = \frac{\frac{\Delta_0}{q}+q}{12a} - \frac{u}{6}$; $s = \sqrt{S}$; $\Gamma = -\frac{v}{s} - 4S - 2u$; $\gamma = \sqrt{\Gamma}$; $r = -\frac{b}{4a} + \frac{\gamma}{2} + s$.

Theorem. There is no general formula, using only the basic arithmetic operations and taking roots, for the solution of the quintic equation $ax^5+bx^4+cx^3+dx^2+ex+f = 0$.

Key Point. The "persistent root" of a closed path (path lift, in topological language) may not be closed, yet the persistent root of a commutators of closed paths is always closed.

Proof. Suppose there was a formula, and consider the corresponding "composition of machines" picture:



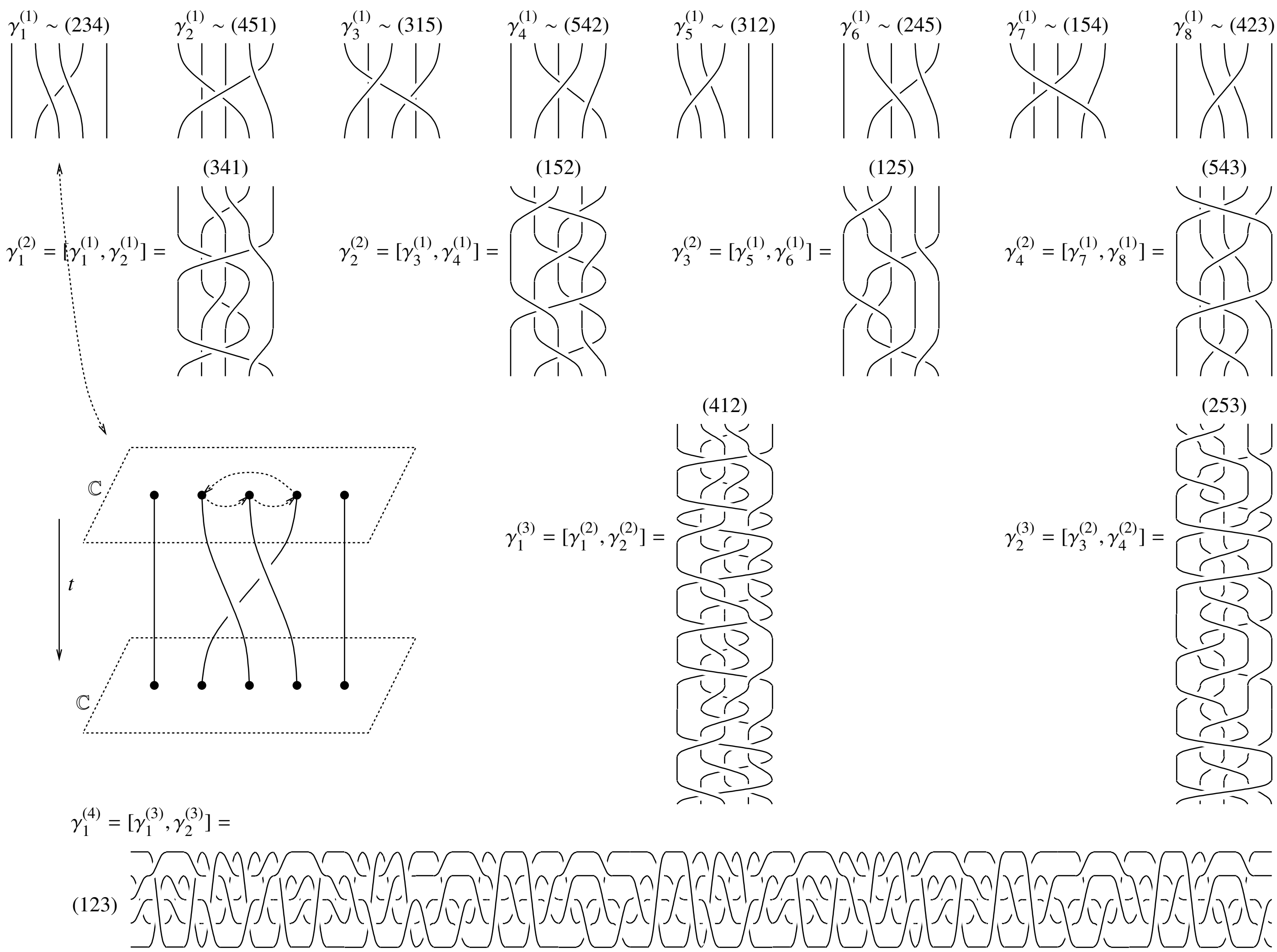
Now let $\gamma_1^{(1)}, \gamma_2^{(1)}, \ldots, \gamma_{16}^{(1)}$, are "musical chairs" paths in X_0 that induce permutations of the roots and set $\gamma_1^{(2)} := [\gamma_1^{(1)}, \gamma_2^{(1)}]$, $\gamma_2^{(2)} := [\gamma_3^{(1)}, \gamma_4^{(1)}]$, …, $\gamma_8^{(2)} := [\gamma_{15}^{(1)}, \gamma_{16}^{(1)}]$, $\gamma_1^{(3)} := [\gamma_1^{(2)}, \gamma_2^{(2)}]$, …, $\gamma_4^{(3)} := [\gamma_7^{(2)}, \gamma_8^{(2)}]$, $\gamma_1^{(4)} := [\gamma_1^{(3)}, \gamma_2^{(3)}]$, $\gamma_2^{(4)} := [\gamma_3^{(3)}, \gamma_4^{(3)}]$, and finally $\gamma^{(5)} := [\gamma_1^{(4)}, \gamma_2^{(4)}]$, as in "Dance of the Roots" on the next page. (Note: no "homotopy" anywhere). We claim that $\gamma^{(5)} /\!\!/ C /\!\!/ P_1 /\!\!/ R_1 /\!\!/ \cdots /\!\!/ R_4$ is a closed path. Indeed

- In X_0, none of the paths is necessarily closed.
- After C, all of the paths are closed.
- After P_1, all of the paths are still closed.
- After R_1, the $\gamma^{(1)}$'s may open up, but the $\gamma^{(2)}$'s remain closed.

…

- At the end, after R_4, $\gamma^{(4)}$'s may open up, but $\gamma^{(5)}$ remains closed.

But if the paths are chosen as in Example 4, $\gamma^{(5)} /\!\!/ C /\!\!/ P_1 /\!\!/ R_1 /\!\!/ \cdots /\!\!/ R_4$ is not a closed path. □



Definition.: The Bring Radical $BR : \mathbb{C} \to \mathbb{C}$ takes in an argument z and returns some root of $x^5 + x + z$.

Note. The Bring Radical, like the typical nth root, cannot be defined as a continuous function, but can similarly be defined in a persistent manner.

Theorem. With the addition of the Bring Radical, the quintic can be solved.

Proof Outline. Take the roots of your quintic to be x_1, x_2, x_3, x_4, x_5. It's possible to find a quintic of the form $y^5 + py + q$ for some $p, q \in \mathbb{C}$ such that the roots y_i of this quintic are each related by some quartic to x_i, so for instance we might have $y_1 = 7x_1^4 + 5x_1^3 + 2x_1^2 + 2$. The quintic $y^5 + py + q$ can be solved using the Bring Radical, and then the roots x_i can be recovered from the calculated roots y_i using the quartic formula.

Corollary. A commutator of closed paths does not necessarily remain a closed path when passed through the Bring Radical. (Otherwise, the proof given above would give us the same contradiction!)

Remark. This proof is stronger in some ways than the traditional proof via Galois Theory. Specifically, in the polynomial steps P_1, P_2... in the machine, we could have also allowed any continuous function, so for instance, exponential functions, trigonometric functions, and any compositions of these functions. The same proof works to show that the quintic remains unsolvable even if these functions are allowed.

Remark. This proof is also weaker in some ways than the traditional proof. Specifically, this proof only outlaws the existence of a general quintic formula, but does not show the existence of *specific* quintics that can't be solved. The traditional proof can show, for instance, that the roots of quintic $3x^5 - 15x + 5$ cannot be expressed using only arithmetic operations and roots.

References. V.I. Arnold, 1960s, hard to locate.

V.B. Alekseev, *Abel's Theorem in Problems and Solutions, Based on the Lecture of Professor V.I. Arnold,* Kluwer 2004.

A. Khovanskii, *Topological Galois Theory, Solvability and Unsolvability of Equations in Finite Terms,* Springer 2014.

B. Katz, *Short Proof of Abel's Theorem that 5th Degree Polynomial Equations Cannot be Solved,* YouTube video, http://youtu.be/RhpVSV6iCko.

Work done under Dr. Dror Bar-Natan at the University of Toronto. Handout and talk based on http://drorbn.net/cumc20.

The Zeroes

Problem. There is a subtle issue in this proof that needs handling. When we claimed that the persistent root of a commutator of closed paths is closed, we must further require that this commutator doesn't at any point cross through the origin.

Definition. In concrete terms, in our proof, this means that at any point where we define a new variable $\delta_n = \sqrt{\Delta_n}$ in our quintic machine, we need to define our initial paths, the ones in X_0, to ensure that no variable Δ_n is 0 anywhere along the path.

Definition. Formally, we can view our machine as a series of nonzero rational functions $\Delta_1, \Delta_2, ...\Delta_m$ and roots of these functions $\delta_1, \delta_2, ...\delta_m$. Specifically, each Δ_i is a nonzero rational function in the roots $\lambda_1, \lambda_2, ...\lambda_5$ and the previous root expressions $\delta_1, \delta_2, ...\delta_{i-1}$, and each root expression δ_i is defined as $\sqrt[n_i]{\Delta_i}$. Note, of course, that there are n_i possible choices for the value of δ_i. We will verify that $\mathbb{C}^5$ remains path-connected, even if we remove the points where any choices of $\delta_1, \delta_2 ...\delta_m$ could have any $\Delta_i = 0$.

Detail. There are many ways to divide the multi-valued function $z \mapsto \sqrt[n]{z}$ into n "branches", that is, n single-valued (discontinuous) functions, such that for any point z, these n functions collectively attain all of the values of $\sqrt[n]{z}$.

Example. For instance, define one branch as choosing the nth root with the lowest (nonnegative) angle above the real axis, and defining the other branches as this initial branch multiplied by $e^{2i\pi(j/n)}$, where $j \in \{1, 2, ...n-1\}$.

Detail. Choose any valid definition for the branches, and for each $\delta_i = \sqrt[n_i]{\Delta_i}$, pick some branch of $\sqrt[n_i]{z}$.

Definition. Now if we let F denote the field of rational functions in the roots $\lambda_1, \lambda_2, ...\lambda_5$, then we want to examine the set

$$\beta := \{\delta_1^{j_1} \delta_2^{j_2} ... \delta_m^{j_m} : 0 \le j_k < n_k\}$$

and then consider the vector space $V := F[\beta]$.

Claim. All rational functions in $\lambda_1, \lambda_2, ...\lambda_5, \delta_1, \delta_2 ...\delta_m$ fall in V.

Proof. Any rational expressions in these variables having at any point a higher power of δ_k than $n_k - 1$ can just be reduced since $\delta_k^{n_k}$ can be simplified to Δ_k, an expression in $\lambda_1, ...\lambda_5, \delta_1, \delta_2, ...\delta_{k-1}$.

Corollary. $\Delta_i \in V$ for all i. Furthermore, $\Delta_i^j \in V$ for all i, j.

Note. V is finite-dimensional over F, having dimension $n_1 n_2 n_3 ... n_m$.

Key Point. Now, fixing i, the set $\{\Delta_i^0, \Delta_i^1, \Delta_i^2, ...\} \subseteq V$, being infinite, must be linearly dependent. Then there is some finite linear combination

$$p_1 \Delta_i^{k_1} + p_2 \Delta_i^{k_2} + ... + p_l \Delta_i^{k_l} = 0.$$

where each p_j is a nonzero rational function and k_j are nonnegative integers with $k_1 < k_2 < ... < k_l$.

Then dividing the entire equation by $\Delta_i^{k_1}$, we get

$$-p_1 = p_2 \Delta_i^{k_2 - k_1} + p_3 \Delta_i^{k_3 - k_1} + ... + p_l \Delta_i^{k_l - k_1}.$$

Note. Since each $k_j - k_1$ is positive when $j > 1$, when Δ_i is 0, the entire sum on the right side reduces to 0, and so $p_1 = 0$ at these points.

Detail. The division by $\Delta_i^{k_1}$ needs to be justified. Starting with $F := \mathbb{C}(\lambda_1, ...\lambda_5)$, we can extend F by splitting the polynomial $T^{n_1} - \Delta_1$ (where T is the variable) to get an extension containing δ_1. We can of course then extend this extension by splitting the polynomial $T^{n_2} - \Delta_2$, since Δ_2 lives in this extension. Continuing in this way we can attain an (algebraic) extension K over F that contains all the δ_i, and so all the Δ_i. Working in K, since Δ_i is nonzero, then $\Delta_i^{k_i}$ is nonzero, so it is safe to divide by $\Delta_i^{k_i}$.

Theorem. If q is a nonzero polynomial in n complex variables, and $Z(q)$ is the set $\{z \in \mathbb{C}^n : q(z) = 0\}$, then $\mathbb{C}^n \setminus Z(q)$ is path-connected.

Lemma. If f is a nonzero polynomial in 1 complex variable, then $\mathbb{C} \setminus Z(f)$ is path-connected. This is just because $Z(f)$ is finite, and $\mathbb{C}$ without a finite set is path-connected.

Proof. Fix $a, b \in \mathbb{C}^n \setminus Z(q)$. Then define $f_q : \mathbb{C} \to \mathbb{C}$ by $f_q(z) = q(a + (b-a)z)$. $f_q(0) = q(a) \neq 0$, and $f_q(1) = q(b) \neq 0$, so both $0, 1$ lie in $\mathbb{C} \setminus Z(f_q)$. Then we can find a path $p : 0 \to 1$ in $\mathbb{C} \setminus Z(f_q)$ by the lemma. Then we define the path $p'(t) := a + (b-a)p(t)$. Now $p'(0) = a + (b-a)p(0) = a$ and $p'(1) = a + (b-a)p(1) = b$, and if $q(p'(t)) = 0$ then $q(a + (b-a)p(t)) = f(p(t)) = 0$, but by definition $f(p(t)) \neq 0$ for all t, so that $p' : a \to b$ is a path not intersecting $Z(q)$.

Reminder. There is a nonzero rational function p_1 that is zero whenever Δ_i is zero.

Corollary. Since p_1 is just a (nonzero) rational function in $\lambda_1, \lambda_2, ...\lambda_5$, $\mathbb{C}^5 \setminus Z(p_1)$ is path-connected.

Corollary. Furthermore, if for every Δ_i we construct the corresponding p_1, call it q_i, so that $Z(\Delta_i) \subseteq Z(q_i)$. Then

$$Z(\Delta_1) \cup Z(\Delta_2) \cup ... \cup Z(\Delta_m) \subseteq Z(q_1) \cup ... \cup Z(q_m) = Z(q_1 q_2 ... q_m).$$

Note. Now we revisit our choice of branch from the start. Since there are finitely many branches for each δ_i, and there are finitely many δ_i, there are finitely many choices of branches we could have made for all the δ_i. Taking the product p of the calculated polynomial $q_1 q_2 ... q_m$ for each choice of branches, we can then note that $Z(p)$ must contain every point where any Δ_i could be 0 for any choice of the δ_j based on the Δ_j.

Conclusion. The set $Z(o)$, by the theorem above, has $\mathbb{C}^5 \setminus Z(p)$ as path-connected (since p is just a finite product of polynomials, it is a polynomial), so we can always choose our paths in $\mathbb{C}^5$ to avoid $Z(p)$ and thus avoid $Z(\Delta_i)$ for all i, for any choice of the δ_i based on the Δ_i.