

Abstract. The commutator of two elements x and y in a group G is $xyx^{-1}y^{-1}$. That is, x followed by y followed by the inverse of x followed by the inverse of y . In my talk I will tell you how commutators are related to the following four riddles:

1. Can you send a secure message to a person you have never communicated with before (neither privately nor publicly), using a messenger you do not trust?
2. Can you hang a picture on a string on the wall using n nails, so that if you remove any one of them, the picture will fall?
3. Can you draw an n -component link (a knot made of n non-intersecting circles) so that if you remove any one of those n components, the remaining $(n - 1)$ will fall apart?
4. Can you solve the quintic in radicals? Is there a formula for the zeros of a degree 5 polynomial in terms of its coefficients, using only the operations on a scientific calculator?

Definition. The commutator of two elements x and y in a group G is $[x, y] := xyx^{-1}y^{-1}$.

Example 1. In S_3 , $[(12), (23)] = (12)(23)(12)^{-1}(23)^{-1} = (123)$ and in general in $S_{\geq 3}$,

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

Example 2. In $S_{\geq 4}$,

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

Example 3. In $S_{\geq 5}$,

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

Example 4. So, in fact, in S_5 , $(123) = [(412), (253)] = [[(341), (152)], [(125), (543)]] = [[[(234), (451)], [(315), (542)]], [[(312), (245)], [(154), (423)]]] = [[[[(123), (354)], [(245), (531)]]], [[(231), (145)], [(154), (432)]]], [[[(431), (152)], [(124), (435)]], [[(215), (534)], [(142), (253)]]]].$

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

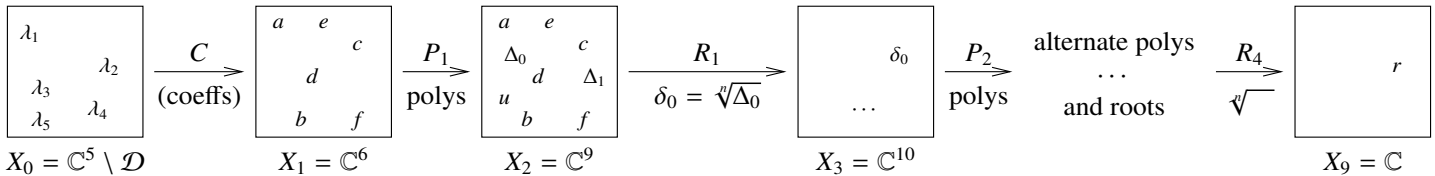
Solving the Cubic, $ax^3 + bx^2 + cx + d = 0$: $\Delta = 27a^2d^2 - 18abcd + 4ac^3 + 4b^3d - b^2c^2$; $\delta = \sqrt{\Delta}$; $\Gamma = 27a^2d - 9abc + 3\sqrt{3}a\delta + 2b^3$; $\gamma = \sqrt[3]{\frac{\Gamma}{2}}$; $r = -\frac{b^2 - 3ac + b + \gamma}{3a}$.

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

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 if $\gamma_1^{(1)}, \gamma_2^{(1)}, \dots, \gamma_{16}^{(1)}$, are paths in X_0 that induce permutations of the roots and we set $\gamma_1^{(2)} := [\gamma_1^{(1)}, \gamma_2^{(1)}]$, $\gamma_2^{(2)} := [\gamma_3^{(1)}, \gamma_4^{(1)}]$, \dots , $\gamma_8^{(2)} := [\gamma_{15}^{(1)}, \gamma_{16}^{(1)}]$, $\gamma_1^{(3)} := [\gamma_1^{(2)}, \gamma_2^{(2)}]$, \dots , $\gamma_4^{(3)} := [\gamma_7^{(2)}, \gamma_8^{(2)}]$, $\gamma_1^{(4)} := [\gamma_1^{(3)}, \gamma_2^{(3)}]$, $\gamma_2^{(4)} := [\gamma_3^{(3)}, \gamma_4^{(3)}]$, and finally $\gamma^{(5)} := [\gamma_1^{(4)}, \gamma_2^{(4)}]$ (all of those, commutators of “long paths”; I don’t know the word “homotopy”), then $\gamma^{(5)} // C // P_1 // R_1 // \dots // R_4$ 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, $\gamma^{(5)} // C // P_1 // R_1 // \dots // R_4$ is not a closed path. □



V.I. Arnold

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>.

