A SHORT ELEMENTARY PROOF OF THE INSOLVABILITY OF THE EQUATION OF DEGREE 5

A. SKOPENKOV

ABSTRACT. We present short elementary proofs of the well-known Ruffini-Abel-Galois theorems on insolvability of algebraic equations in radicals. This proof is obtained from existing expositions by stripping away material not required for the proof (but presumably required elsewhere). In particular, we do not use the terms 'Galois group' and even 'group'. However, our presentation is a good way to learn (or recall) the starting idea of Galois theory: to look at how the symmetry of a polynomial is decreased when a radical is extracted. So the note provides a bridge (by showing that there is no gap) between elementary mathematics and Galois theory. The note is accessible to students familiar with polynomials, complex numbers and permutations; so the note might be interesting easy reading for professional mathematicians.

Contents

Statement and proof	1
Discussion	4
References	g

STATEMENT AND PROOF

Take a subset $X \subset \mathbb{C}$ containing number 1. A complex number a is called **expressible** by radicals from X if a can be obtained from X using operations of addition, subtraction, multiplication, division by a non-zero number and taking the n-th root, where n is a positive integer. Or, in other words, if some set containing a can be obtained from X using the following operations. To a given set $M \subset \mathbb{C}$ containing numbers $x, y \in M$ one can add

numbers x + y, x - y, xy, number x/y when $y \neq 0$,

and any number $r \in \mathbb{C}$ such that $r^n = x$ for some integer n > 0.

Theorem 1. For every $n \geq 5$ there are $a_0, \ldots, a_{n-1} \in \mathbb{C}$ such that no root of the equation $x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = 0$ is expressible by radicals from $\{1, a_0, \ldots, a_{n-1}\}$.

In this note we present a short direct proof of this result, cf. Remark 7. By a proof I mean a 'real' proof using elementary mathematics, not a deduction from some non-elementary results whose proofs contain (in a longer and less motivated form) a 'real' proof. This proof is interesting because it contains an idea of an algorithm for recognition of solvability in radicals (Remark 12). Some discussion is presented in [ECG] and after the proof.

Moscow Institute of Physics and Technology and Independent University of Moscow. E-mail: skopenko@mccme.ru. Homepage: www.mccme.ru/~skopenko.

Supported in part by the D. Zimin Dynasty Foundation and Simons-IUM fellowship.

This text is based on the author's lectures at Moscow 'olympic' school (2015-2018), math circle 'Olympiades and Mathematics' (2015-2018) and Summer Conference of Tournament of Towns (2018). I am grateful to I. Bogdanov, G. Chelnokov, A. Esterov, A. Kanunnikov, F. Petrov and V. Volkov for useful discussions, and to A.B. Sossinsky for correcting English in some historical remarks.

We first prove a weaker insolvability result, the Ruffini Theorem 2 below. The idea of proof is that certain symmetry is kept through extraction of radical (Lemma 3 below). We then deduce Theorem 1 from the Ruffini Theorem 2. The deduction is based on the Rationalization Lemma 4 below, which is also important because it illustrates one of the main ideas of Galois' (and maybe Abel's) work: if an equation is solvable in radicals at all, then it is solvable in radicals using Lagrange resolutions, see Remark 12. The Rationalization Lemma 4 uses the Conjugation Lemma 5.b below, which introduces the idea of a field automorphism in the simple particular case of conjugation sufficient for Theorem 1.

Denote

$$\varepsilon_k := \cos \frac{2\pi}{k} + i \sin \frac{2\pi}{k}, \quad \mathbb{Q}_{\varepsilon} := \bigcup_{k=3}^{\infty} \mathbb{Q}(\varepsilon_3, \varepsilon_4, \dots, \varepsilon_k) \quad \text{and} \quad \vec{y} := (y_1, \dots, y_n).$$

We use the standard notation $F[u_1, \ldots, u_n]$ and $F(u_1, \ldots, u_n)$ for the sets of polynomials and rational fractions (i.e., formal ratios of polynomials) with coefficients in F. Define an extension of a field $F \subset \mathbb{C}$ by numbers $r_1, \ldots, r_s \in \mathbb{C}$ as

$$F(r_1, \ldots, r_s) := \{ P(r_1, \ldots, r_s) : P \in F(u_1, \ldots, u_s) \}.$$

If for every j = 1, ..., s there is an integer k_j such that $r_j^{k_j} \in F(r_1, ..., r_{j-1})$, then the extension is called **a radical extension**.

Theorem 2 (Ruffini). For every $n \geq 5$ there are $a_0, \ldots, a_{n-1} \in \mathbb{C}$ such that no root of the equation $x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = 0$ is contained in any radical extension of $\mathbb{Q}_{\varepsilon}(a_{n-1}, \ldots, a_0)$ contained in $\mathbb{Q}_{\varepsilon}(\vec{x})$, where x_1, \ldots, x_n are the roots of the equation.

For a permutation α denote

$$\vec{u}_{\alpha} := (u_{\alpha(1)}, \dots, u_{\alpha(n)}).$$

A rational fraction $P \in \mathbb{C}(\vec{u})$ is **even-symmetric** if $P(\vec{u}) = P(\vec{u}_{(abc)})$ for every cycle (abc) of length $3.^2$

Lemma 3. If P is a rational fraction of $n \geq 5$ variables with coefficients in \mathbb{C} , and P^k is even-symmetric for some integer k, then P is even-symmetric.

Proof. We may assume that k is a prime and $P \neq 0$.

Let a, b, c, d, e be arbitrary different elements of $\{1, \ldots, n\}$.

First assume that $k \neq 3$. Since

$$P^{k}(\vec{u}) = P^{k}(\vec{u}_{(abc)}), \text{ we have } \prod_{i=0}^{k-1} (P(\vec{u}) - \varepsilon_{k}^{j} P(\vec{u}_{(abc)})) = 0.$$

Since P is a non-zero rational fraction, there is

$$j = j(abc) \in \mathbb{Z}$$
 such that $P(\vec{u}) = \varepsilon_k^j P(\vec{u}_{(abc)})$.

Then

$$P(\vec{u}) = \varepsilon_k^j P(\vec{u}_{(abc)}) = \varepsilon_k^{2j} P(\vec{u}_{(abc)^2}) = \varepsilon_k^{3j} P(\vec{u}).$$

Hence $j \equiv 0 \mod k$, i.e. $P(\vec{u}) = P(\vec{u}_{(abc)})$.

For k = 3 let $\sigma := (ab)(de) = (abe)(bed)$. Then analogously $0 \equiv j(\sigma^2) \equiv 2j(\sigma) \mod 3$. Hence $j(\sigma) \equiv 0 \mod 3$, i.e. $P(\vec{u}) = P(\vec{u}_{\sigma})$. Analogously $P(\vec{u}) = P(\vec{u}_{(ac)(de)})$. Since (ab)(de)(ac)(de) = (abc), we have $P(\vec{u}) = P(\vec{u}_{(abc)})$.

¹In order to understand the main idea one can replace $\mathbb{Q}_{\varepsilon}(\vec{x})$ by $\mathbb{Q}[\vec{x}]$. Theorem 2 holds, with analogous proof, if we replace \mathbb{Q}_{ε} by any countable field.

²A permutation is *even* if it is a composition of an even number of transpositions. Being even-symmetric is equivalent to $P(\vec{u}) = P(\vec{u}_{\alpha})$ for every even permutation α of $\{1, \ldots, n\}$. Indeed, any even permutation is composition of permutations of the form (ab)(bc) = (abc) and (ab)(cd) = (abc)(bcd).

Proof of the Ruffini Theorem 2. Numbers $x_1, \ldots, x_n \in \mathbb{C}$ are called algebraically independent over \mathbb{Q}_{ε} if $P(\vec{x}) \neq 0$ for every non-zero polynomial P with coefficients in \mathbb{Q}_{ε} . By induction on n there are n algebraically independent numbers x_1, \ldots, x_n over \mathbb{Q}_{ε} . The inductive step follows because \mathbb{C} is uncountable, while the set of roots of polynomials with coefficients in $\mathbb{Q}_{\varepsilon}(x_1, \ldots, x_{n-1})$ is countable.

Denote the coefficients of the unitary polynomial with roots x_1, \ldots, x_n by

$$a_{n-1} := -(x_1 + \ldots + x_n), \quad \ldots, \quad a_0 = (-1)^n x_1 \cdot \ldots \cdot x_n.$$

Assume to the contrary that there is a radical extension $\mathbb{Q}_{\varepsilon}(\vec{a}, r_1, \dots, r_s)$ of $\mathbb{Q}_{\varepsilon}(\vec{a}) := \mathbb{Q}_{\varepsilon}(a_{n-1}, \dots, a_0)$, which both contains x_1 and is contained in $\mathbb{Q}_{\varepsilon}(\vec{x})$. Using Lemma 3, by induction on j we obtain that r_j is the value at \vec{x} of an even-symmetric rational fraction for every $j = 1, \dots, s$. Since $x_1 \in \mathbb{Q}_{\varepsilon}(\vec{a}, r_1, \dots, r_s)$, we see that x_1 is also the value at \vec{x} of an even-symmetric rational fraction. Since x_1, \dots, x_n are algebraically independent over \mathbb{Q}_{ε} , the only such rational fraction is $P(u_1, \dots, u_n) = u_1$. This is not even-symmetric because the cycle (123) carries u_1 to $u_2 \neq u_1$. A contradiction.

Theorem 1 is reduced to the Ruffini Theorem 2 by inductively constructing a radical extension F of $\mathbb{Q}_{\varepsilon}(a_{n-1},\ldots,a_0)$ such that $x_1 \in F \subset \mathbb{Q}_{\varepsilon}(\vec{x})$, from a radical extension of $\mathbb{Q}(a_{n-1},\ldots,a_0)$ containing x_1 . The inductive step is based on the following statement.

Lemma 4 (Rationalization). Let n be an integer, $x_1, \ldots, x_n, r \in \mathbb{C}$ numbers, k a prime and $F \subset \mathbb{C}$ a field containing elementary symmetric polynomials of x_1, \ldots, x_n and also ε_k , r^k but not r. If $F(r) \cap \mathbb{Q}_{\varepsilon}(\vec{x}) \not\subset F$, then there is $\rho \in \mathbb{Q}_{\varepsilon}(\vec{x})$ such that $\rho^k \in F$ and $F(\rho) = F(r)$.

This lemma asserts that if F(r) contains more (values of) rational fractions of x_1, \ldots, x_n with coefficients in \mathbb{Q}_{ε} than F, then already r is (or can be made) such a rational fraction.

For a proof we need two lemmas.

Lemma 5. Let k be a prime, $r \in \mathbb{C}$ a number and $F \subset \mathbb{C}$ a field containing ε_k , r^k but not r. (a) (Irreducibility) Then the polynomial $z^k - r^k \in F[z]$ is irreducible over F.

(b) (Conjugation) If $Q \in F[z]$ a polynomial and Q(r) = 0, then $Q(r\varepsilon_k^j) = 0$ for every $j = 1, \ldots, k-1$.

Proof of (a). All the roots of the polynomial $z^k - r^k$ are $r, r\varepsilon_k, r\varepsilon_k^2, \ldots, r\varepsilon_k^{k-1}$. Then the free coefficient of a factor of $z^k - r^k$ is the product of some m of these roots. Since ε_k , we obtain $r^m \in F$. For a proper factor, if it existed, 0 < m < k. Since k is a prime, ka + mb = 1 for some integers a, b. Then $r = (r^k)^a (r^m)^b \in F$. A contradiction.

Proof of (b). Since Q(r) = 0, the remainder of division of Q by $z^k - r^k$ assumes value 0 at r. Since the degree of this remainder is less than k, by (a) this remainder is zero. Thus Q is divisible by $z^k - r^k$. For every $j = 0, 1, \ldots, k-1$ since $(r\varepsilon_k^j)^k = r^k$, we obtain $Q(r\varepsilon_k^j) = 0$. \square

Proof of the Rationalization Lemma 4. By assumption there is a rational fraction $T \in \mathbb{Q}_{\varepsilon}(\vec{u})$ such that $T(\vec{x}) \in F(r) - F$. By the Irreducibility Lemma 5.a F(r) = F[r]. Hence

$$T(\vec{x}) = P(r) = p_0 + p_1 r + \ldots + p_{k-1} r^{k-1}$$

for some polynomial $P \in F[z]$ of degree less than k. Since $P(r) \notin F$, there is l such that 0 < l < k and the coefficient $p_l \in F$ of z^l in P is non-zero. We have

$$\rho := p_l r^l = \frac{P(r) + \varepsilon_k^{-l} P(r \varepsilon_k) + \varepsilon_k^{-2l} P(r \varepsilon_k^2) \dots + \varepsilon_k^{(1-k)l} P(r \varepsilon_k^{k-1})}{k}.$$

Define the resolution polynomial $Q(t) := \prod_{\alpha \in S_n} (t - T(\vec{x}_{\alpha}))$, where S_n is the set of all permutations of $\{1, \ldots, n\}$. Since $T(\vec{x}) = P(r)$, we have Q(P(r)) = 0. The coefficients of Q as a polynomial of t are symmetric in x_1, \ldots, x_n . Since F contains elementary symmetric polynomials of x_1, \ldots, x_n ,

it follows that $Q(t) \in F[t]$. Thus $Q(P(z)) \in F[z]$. Take any j = 1, ..., k-1. Then by the Conjugation Lemma 5.b $Q(P(r\varepsilon_k^j)) = 0$. Thus $P(r\varepsilon_k^j) = T(\vec{x}_\alpha)$ for some permutation $\alpha = \alpha_j$. Hence the above formula for ρ shows that $\rho \in \mathbb{Q}_{\varepsilon}(\vec{x})$.

We have $\rho^k = p_l^k(r^k)^l \in F$ and $\rho = p_l r^l \in F(r)$. Since k is a prime and l is not divisible by k, there are integers a and b such that ak + bl = 1. Since F(r) is a field, we have $r = (r^k)^a (r^l)^b = (r^k)^a \rho^b p_l^{-b} \in F(\rho)$. Hence $F(r) = F(\rho)$.

Proof of Theorem 1. Take $a_0, \ldots, a_{n-1} \in \mathbb{C}$ given by the Ruffini Theorem 2. Assume to the contrary that some root x_1 of the equation is contained in some radical extension of $\mathbb{Q}(\vec{a}) := \mathbb{Q}(a_{n-1}, \ldots, a_0)$. Then x_1 is contained in some radical extension of $\mathbb{Q}_{\varepsilon}(\vec{a})$.

Take a radical extension $\mathbb{Q}_{\varepsilon}(\vec{a}, r_1, \dots, r_s)$ of $\mathbb{Q}_{\varepsilon}(\vec{a})$ containing x_1 , with minimal s. Since s is minimal, $x_1 \notin F_{s-1} := \mathbb{Q}_{\varepsilon}(\vec{a}, r_1, \dots, r_{s-1})$. Then by the Rationalization Lemma 4 there is $\rho \in \mathbb{Q}_{\varepsilon}(\vec{x})$ such that $\mathbb{Q}_{\varepsilon}(\vec{a}, r_1, \dots, r_s) = F_{s-1}(\rho)$ and $\rho^{k_s} \in F_{s-1}$.

Take a radical extension $\mathbb{Q}_{\varepsilon}(\vec{a}, r'_1, \dots, r'_{s'})$ of $\mathbb{Q}_{\varepsilon}(\vec{a})$ containing ρ , with minimal s'. Then s' < s. Repeat the previous argument (or proceed by induction on s) to obtain a radical extension $\mathbb{Q}_{\varepsilon}(\vec{a}, \rho_1, \dots, \rho_t)$ of $\mathbb{Q}_{\varepsilon}(\vec{a})$ containing x_1 and such that $\rho_j \in \mathbb{Q}_{\varepsilon}(\vec{x})$ for every $j = 1, \dots, t$. Then $\mathbb{Q}_{\varepsilon}(\vec{a}, \rho_1, \dots, \rho_t) \subset \mathbb{Q}_{\varepsilon}(\vec{x})$ is a radical extension of $\mathbb{Q}_{\varepsilon}(\vec{a})$ containing x_1 . This contradicts to the Ruffini Theorem 2.

DISCUSSION

Remark 6 (Comparison with other expositions). The direct expositions of [FT, L, PS, Ko, B, Ka, R, P, St94] were more useful to me (in spite of some drawbacks mentioned below) than 'theoretical' expositions in standard textbooks. The latter start with several hundreds pages of definitions and results whose role in the proof of the insolvability theorem is not clear at the moment of their formulations. It would not have been possible to write the present note if the above-mentioned direct expositions did not exist.

The above-given proof of the Ruffini Theorem 2 and Theorem 1 is based on, but different from, [Ko, L] and [PS]³, respectively.

The above-given proof of the Ruffini Theorem has the same idea as the proof of [St94]. This idea is presented above in a more elementary way by looking at the symmetry of a polynomial not at an automorphism of a field. Still, I like that proof and present it in Remark 11.

The exposition here is different from [A, FT, Sk11] (even at the level of formulations, see Remark 7). The two approaches are 'dual': here the symmetry group of a polynomial is decreased after the extraction of a radical, while in [A, FT, Sk11] the group of permutations of roots is *increased* after the extraction of a radical (cf. the proof of Remark 11).

In [Sk17, T] a stronger Kronecker's Theorem is proved; the proof is more complicated.

The exposition of [L] is highly illuminating; it does not claim to be rigorous (and is not).

Before studying the Ruffini Theorem 2 a reader might want to learn its simpler *real* analogue [ECG]. A real analogue of Theorem 1 is also simpler [Sk17, §5.5.3] but uses the ideas of the Irreducibility and Conjugation Lemma 5 in a different way.

See more general remarks and references in [Sk17, §5.1.3 and §5.2.1].

Remark 7 (On statements of the insolvability theorems). I was surprised not to find a rigorous statement of the Abel-Ruffini Theorem in Wikipedia (English, French, German, Russian, Italian, in 2015-2018). Abel's own paper (see a translation in [P]) does not contain a rigorous formulation in the sense of modern mathematics (same holds for [P]). A possible reason is that the Abel-Ruffini Theorem is not so easy to state, see below.

 $^{^{3}}$ Cf. footnote 6. Besides, in [PS] the solvability in radicals of the polynomial G used in the proof of Theorem 4 (p. 219) is not defined. So instead of Theorem 3 and the first part of the proof of Theorem 4 one needs to use more general results. These results are not stated. The exact meaning of 'we are dealing with a general polynomial of degree n' is not clear (p. 220, after the formula for ρ_1).

There are different insolvability theorems:

- the easiest-to-state insolvability of a specific equation: no root of the equation $x^5-4x+2=0$ is contained in any radical extension of \mathbb{Q} (Galois Theorem),
 - an easy-to-state existence of a specific insolvable equation (Theorem 1),
- a harder-to-state non-existence of a formula for solution of any equation (the Abel-Ruffini Theorem, see the Functional and the Formal Abel-Ruffini Theorems of Remarks 8 and 10).

Galois Theorem is much harder than Theorem 1 and the Abel-Ruffini Theorem.⁴ Theorem 1 is easier both to state and to prove than the Functional and the Formal Abel-Ruffini Theorems. So some readers might want to ignore the statement of the latter.

Remark 8 (the Functional Abel-Ruffini Theorem). The exposition of [FT, 5.2, 5.3 and Theorem 5.1], [A, Sk11] uses the following statement of the Ruffini-Abel Theorem, cf. [Es].

We may represent solution of a quadratic equation $x^2 + px + q = 0$ by a sequence of formulas

$$f_1^2 = p^2 - 4q$$
, $x = (f_1 - p)/2$.

We may represent solution of a cubic equation $x^3 + px + q = 0$ by a sequence of formulas

$$f_1^2 = \left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2$$
, $f_2^3 = -\frac{q}{2} + f_1$, $f_3^3 = -\frac{q}{2} - f_1$, $x = f_2 + f_3$.

(See comments on the extraction of complex roots in [FT, §5.2].)

These examples motivate the following definition.

Denote the elementary symmetric polynomials in variables u_1, \ldots, u_n by

$$\sigma_1(u_1,\ldots,u_n):=u_1+\ldots+u_n, \quad \ldots, \quad \sigma_n(u_1,\ldots,u_n)=u_1\cdot\ldots\cdot u_n.$$

A radical n-formula is a collection of

- primes k_1, \ldots, k_s ,
- rational fractions P_0, P_1, \ldots, P_s with complex coefficients and in $n, n+1, \ldots, n+s$ variables, respectively, and
 - functions $f_1, \ldots, f_s : \mathbb{C}^n \to \mathbb{C}$ (which are not assumed to be continuous) such that for every numbers $x_1, \ldots, x_n \in \mathbb{C}$

$$\begin{cases}
f_1^{k_1} = P_0(\sigma_1, \dots, \sigma_n) \\
f_2^{k_2} = P_1(\sigma_1, \dots, \sigma_n, f_1) \\
\dots \\
f_s^{k_s} = P_{s-1}(\sigma_1, \dots, \sigma_n, f_1, \dots, f_{s-1}) \\
x_1 = P_s(\sigma_1, \dots, \sigma_n, f_1, \dots, f_s)
\end{cases}$$

In these formulas the argument (x_1, \ldots, x_n) of polynomials $\sigma_1, \ldots, \sigma_n$ and functions f_1, \ldots, f_s is omitted; the equalities are equalities of functions; we assume that the values $P_j(\sigma_1, \ldots, \sigma_n, f_1, \ldots, f_j)$ are defined.

E.g. there is a radical 2-formula: take

$$s = 1$$
, $k_1 = 2$, $f_1(x_1, x_2) = x_1 - x_2$, $P_0(y_1, y_2) = y_1^2 - 4y_2$ and $P_1(y_1, y_2, z_1) = \frac{y_1 + z_1}{2}$; check that $f_1^2(x_1, x_2) = P_0(x_1 + x_2, x_1x_2)$ and $x_1 = P_1(x_1 + x_2, x_1x_2, f_1(x_1, x_2))$.

⁴'For all that Abel's methods could prove, every particular quintic equation might be soluble, with a special formula for each equation' [St15]. This says that even Theorem 1 is much harder than the Abel-Ruffini Theorem (hence the name of Theorem 1). This is unfair from the point of view of modern mathematics because of the proof presented here, all the ideas except existence of algebraically independent numbers were known to Abel or are due to him. Although proof of the existence uses ideas unfamiliar to Abel, this proof is simple FMPV (=from modern point of view). So if we name Abel-Ruffini Theorem after Abel and Ruffini in spite of neither having even a precise statement FMPV, it might be fair to name Theorem 1 'the Strong, or the numeric, Abel-Ruffini Theorem' (such a name does not mean that this result was proved by Abel-Ruffini).

Functional Abel-Ruffini Theorem. For every $n \geq 5$ there is no radical n-formula.

This result follows from Theorem 1. A different proof is presented [A, FT, Sk11]. That proof uses topological ideas, which could be an advantage for a professional but makes the proof less accessible for a beginner. (E.g because one has to prove that certain multi-valued functions have the monodromy property [A, 2.10, 2.11]).⁵

Remark 9 (the Formal Ruffini Theorem). A rational (or Ruffini) radical n-formula is defined in the same way as a radical n-formula of Remark 8, except that 'functions $f_1, \ldots, f_s : \mathbb{C}^n \to \mathbb{C}$ (which are not assumed to be continuous)' is replaced by 'rational fractions $f_1, \ldots, f_s \in \mathbb{C}(x_1, \ldots, x_n)$ ', and 'equalities of functions' is replaced by 'equalities of rational fractions'.

E.g. the previous example of a radical 2-formula is a rational radical 2-formula.

Formal Ruffini Theorem. For every $n \geq 5$ there is no rational radical n-formula. This holds by the Ruffini Theorem 2, or can analogously be derived from Lemma 3.

Remark 10 (the Formal Abel-Ruffini Theorem). Let us present a formalization of the statement of the Abel-Ruffini Theorem in [R, §2,§4], [St94, Theorem 3], [B, §1 and Theorem 6.3].

Let n be a positive integer. Denote $F_0 := \mathbb{C}(v_1, \ldots, v_n)$. A formal radical n-formula is a collection of primes k_1, \ldots, k_s and polynomials $P_j \in F_0[y_1, \ldots, y_j], j = 0, \ldots, s-1$, such that the polynomial $G(y_j) := y_j^{k_j} - P_{j-1}(v_1, \ldots, v_n, y_1, \ldots, y_{j-1})$ is irreducible over F_{j-1} , where F_1, \ldots, F_s are defined inductively by $F_j := F_{j-1}[y_j]/G(y_j)$.

(Here are details for the definition of F_j . Two polynomials $A, B \in F_{j-1}[y_j]$ are called *congruent modulo* G if a-b is divisible by G. Let F_j be the set of congruence classes. Since

⁵Proof of the Functional Abel Theorem in [Sk15] is incomplete because the definition of an f-formula in [Sk15] before Lemma 7 is meaningless for a non-symmetric polynomial $f \in \mathbb{C}[u_1, \ldots, u_n]$. Merging the fields into $\mathbb{C}(u_1, \ldots, u_n)$ can make the polynomial $y_j^{k_j} - P_{j-1}$ reducible, even if it was irreducible over $\mathbb{C}(\sigma_1, \ldots, \sigma_n)$ for the elementary symmetric polynomials $\sigma_1, \ldots, \sigma_n$ of u_1, \ldots, u_n . E.g. the polynomial $y^2 - (u_1 + u_2)^2 + 4u_1u_2$ is reducible over $\mathbb{C}(u_1, u_2)$, although $y^2 - v_1^2 + 4v_2$ is irreducible over $\mathbb{C}(v_1, v_2)$.

This gap, as well as the gap mentioned in footnote 8, are yet another examples that mistakes come not from explicitly wrong statements, but from lack of accurate definitions (or from use of not well-defined objects). Cf. [MM]. For this reason, nowadays accurate definitions are required to recognize a proof as complete.

⁶ This formalization was not given in [R, St94, B] (so, formally, [R, St94, B] do not contain a rigorous formulation of the Abel-Ruffini Theorem). Indeed, the objects $\sqrt[p_i]{\alpha_i}$ in [R, §2] and f_{k-1}^{1/m_k} in [B, §1], as well as 'equals' in the phrase 'The adjunction is called radical if some positive integer power α^m of α equals to an element $f \in F$ ' [St94, p. 23] is not defined. (The object α_i is not a complex number because E_0 is $\mathbb{C}(s_1, \ldots, s_n)$ in the simplest formulation of the Abel-Ruffini Theorem there; the object f_{k-1} is an algebraic function not a complex number; α^m is not equal to f in the only previously defined field $F(\alpha)$ that contains both elements). The object E_i^* in [R, §2] is also not defined, but it might be a typo and E_i is meant.

In [St94] it is not specified whether x_1, \ldots, x_n are numbers or variables (since they appear in statements without quantifiers, and since algebraic independent numbers are not mentioned, they have to be variables). Analogous problem appears in [PS]. There is no 'equation (5.1)'; presumably equation in p. 215 is meant. It is not defined what is meant by 'the coefficients are considered as independent variables over \mathbb{Q} '. It is not defined what is meant by 'the roots of a polynomial (5.1) with variable coefficients', so definition of $\Delta(F)$ is not clear. Presumably $\Delta = \mathbb{Q}(\sigma_1, \ldots, \sigma_n)$ and $\Delta(F) = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ or, in the notation of this note, $\Delta(F) = \mathbb{Q}(u_1, \ldots, u_n)$ for variables u_1, \ldots, u_n . But then it is not defined what is meant by $\sqrt[s]{a_1}$, where $a_1 \in \mathbb{Q}(u_1, \ldots, u_n)$. So the main notion of solvability in radicals is not defined (p. 215). The exact meaning of 'we may assume that the roots are independent variables' is not given (p. 220).

The formalization of $\sqrt[p_i]{\alpha_i}$ suggested in [Sk15, definition of a formal radical formula before Lemma 7] in incorrect because it was not required that the polynomial $y_j^{k_j} - p_{j-1}$ is irreducible over $F_{j-1}(y_j)$. (That formalization appeared not in the statement but in the proof of the Abel-Ruffini Theorem.) Such a polynomial is reducible e.g. for n = s = 2, $p_0(y) = p_1(y) = y^2$.

For a modern mathematician it is easy, although it does require some accuracy, to formally define $\sqrt[n]{\alpha_i}$ (or f_{k-1}^{1/m_k} or 'equal' or $\sqrt[s]{a_1}$), for some values of p_i , α_i not for all values as it seems to be assumed in [R, St94, B, PS]. (E.g. for $F = \mathbb{Q}(\sqrt[3]{2})$ the ring $F[y]/(y^3 - 2)$ is not a field; in other words, extension of F by $\varepsilon_3\sqrt[3]{2}$ is not isomorphic to $F[y]/(y^3 - 2)$.) See the definition of a formal radical n-formula in Remark 10.

the polynomial G is irreducible over F_{j-1} , the addition and the multiplication on F_{j-1} give an addition and a multiplication on F_j in an obvious way.)

Examples. (a) For n=2 take the formal radical 2-formula $y_1^2=v_1^2-v_2$ (or, formally, s=1, $k_1=2$, $P_0(v_1,v_2)=v_1^2-v_2$). Denote by [z] the congruence class of z. Then $[v_1+y_1],[v_1-y_1]\in F_1$ are the roots of the equation $x^2-2v_1x+v_2=0$.

(b) For $F_0 := \mathbb{C}(p,q)$ take the formal radical 2-formula $y_1^2 = p^3 + q^2$, $y_2^3 = y_1 - q$. Then

$$\left[y_2 - y_2^2(y_1 + q)p^{-2}\right], \quad \left[\varepsilon_3 y_2 - \varepsilon_3^2 y_2^2(y_1 + q)p^{-2}\right], \quad \left[\varepsilon_3^2 y_2 - \varepsilon_3 y_2^2(y_1 + q)p^{-2}\right] \quad \in \quad F_2.$$

are the roots of the equation $x^3 + 3px + 2q = 0$ (because $[y_2y_2^2(y_1+q)p^{-2}] = [(y_1-q)(y_1+q)p^{-2}] = [p] \in F_2$).

Formal Abel-Ruffini Theorem. For every $n \ge 5$ there is no formal radical n-formula for which the equation $x^n - v_1 x^{n-1} + \ldots + (-1)^{n-1} v_{n-1} x + (-1)^n v_n = 0$ has n distinct roots in F_s .

This follows from Theorem 1, or is proved analogously to that result (having a formal radical n-formula allows not to consider algebraically independent numbers but to work with variables not with numbers from the start). This also follows from the Functional Abel-Ruffini Theorem of Remark 8. It would be interesting to know if there is a short converse deduction (i.e. 'Formal implies Functional'), i.e. a short proof that a radical n-formula gives a formal radical n-formula.⁷

Remark 11 (Alternative proof of a weaker version of Theorem 1). Here we present a proof from [St94], filling a gap there and shortening the proof by further stripping the standard approach away.

Theorem. For every $n \geq 5$ there are $a_0, \ldots, a_{n-1} \in \mathbb{C}$ such that some root of the equation $x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = 0$ is not expressible by radicals from $\{a_0, \ldots, a_{n-1}\}$.

This is weaker than Theorem 1. It would be interesting to know if this result easily implies Theorem 1, cf. [Sk17, Main Lemma (c) (Decomposition) in §5.5.4].

For $x_1, \ldots, x_n \in \mathbb{C}$ a field $F \supset \mathbb{Q}(\vec{x})$ is called *even-symmetric* over a subfield $B \subset F$ if for every even permutation α of $\{1, \ldots, n\}$ there is an automorphism of F which maps every element of B to itself and maps x_j to $x_{\alpha(j)}$ for every j.

Symmetrization Lemma. There are $x_1, \ldots, x_n \in \mathbb{C}$ such that for every radical extension F of $\mathbb{Q}_{\varepsilon}(\vec{x})$ there is a radical extension \overline{F} of F which is even-symmetric over \mathbb{Q}_{ε} .

Proof. Analogously to the proof of the Ruffini Theorem 2 take $x_1, \ldots, x_n \in \mathbb{C}$ algebraically independent over \mathbb{Q}_{ε} .

Then the proof is by the induction on the number s from the definition of a radical extension. The base s=0 is trivial: for $F=\mathbb{Q}_{\varepsilon}(\vec{x})$ take $\overline{F}=F$.

This was stated without proof in [Sk15], which is a gap. The naive way of constructing a formal radical formula does not work. Indeed, let $f_1(x_1, x_2) = |x_1 - x_2|$ and $f_2(x_1, x_2) = x_1 - x_2$. Then $f_1^2 = \sigma_1^2 - 4\sigma_2$, $f_2^2 = f_1^2$ is a radical 2-formula, but a collection $k_1 = k_2 = 2$ and $P_0 = v_1^2 - 4v_2$, $P_1 = y_1^2$ is not a formal radical 2-formula.

⁸ The proof of this lemma given in [St94, Proof of Theorem 1] is incomplete. First, the notion of radical expression used in the proof is not defined in [St94], see footnote 6. Second, the bijection σ in that proof is not defined on the adjoined radical. If $F(r) \cap \mathbb{Q}_{\varepsilon}(\vec{x}) \not\subset F$, we cannot set $\psi_{\alpha}(r)$ to be any k-th power root r_{α} of $\psi_{\alpha}(r^k)$ because then ψ_{α} need not be well-defined, for there could be rational functions $P \in F(z)$ and $Q \in \mathbb{Q}_{\varepsilon}(\vec{u})$ such that $P(r) = Q(\vec{x})$ but $P(r_{\alpha}) \neq Q(\vec{x}_{\alpha})$. This problem is resolved above by application of the Rationalization Lemma 4, and thus by working over \mathbb{Q}_{ε} not over \mathbb{Q} . (I am grateful to J. Stillwell for his confirmation that there is an error in [St94].)

The Rationalization Lemma 4 represents a significant new idea required to deduce Theorem 1 from the Ruffini Theorem 2. However the argument of [St94] can be modified (without introduction of new ideas) to provide a complete proof of the Ruffini Theorem 2.

The 'roots of unity' assumption of [St94, Theorem 2] is not checked in [St94, proof of Theorem 3]. So the argument in [St94, p. 25 above] is in fact part of the proof of [St94, Theorem 3], although it is not included in [St94, proof of Theorem 3].

In order to prove the inductive step assume that a radical extension F of $\mathbb{Q}_{\varepsilon}(\vec{x})$ is even-symmetric over \mathbb{Q}_{ε} , that $r \in \mathbb{C} - F$ and $r^k \in F$ for an integer k. For every even permutation α take an automorphism $\psi_{\alpha} : F \to F$ which maps every element of \mathbb{Q}_{ε} to itself and x_j to $x_{\alpha(j)}$ for every j.

If $F(r) \cap \mathbb{Q}_{\varepsilon}(\vec{x}) \not\subset F$, then by the Rationalization Lemma 4 there is $\rho \in \mathbb{Q}_{\varepsilon}(\vec{x})$ such that $\rho^k \in F$ and $F(\rho) = F(r)$. Take a rational fraction $P \in \mathbb{Q}_{\varepsilon}(\vec{u})$ such that $\rho = P(\vec{x})$. Extend ψ_{α} to $\overline{F} := F(\rho) = F(r)$ by setting $\psi_{\alpha}(\rho) := P(\vec{x}_{\alpha})$. This is well-defined by the Irreducibility Lemma 5.a because $\psi_{\alpha}(P(\vec{x})^k) = P(\vec{x}_{\alpha})^k$.

If $F(r) \cap \mathbb{Q}_{\varepsilon}(\vec{x}) \subset F$, then for every even permutation α take any $r_{\alpha} \in \mathbb{C}$ such that $r_{\alpha}^{k} = \psi_{\alpha}(r^{k})$. Take a minimal set $\beta_{1}, \ldots, \beta_{t}$ of even permutations such that $\overline{F} := F(r_{\beta_{1}}, \ldots, r_{\beta_{t}})$ contains r_{α} for every even permutation α . Extend ψ_{α} to \overline{F} by setting $\psi_{\alpha}(r_{\beta_{j}}) := r_{\alpha\beta_{j}}$. The extension is well-defined by the Irreducibility Lemma 5.a.

The extended ψ_{α} maps every element of \mathbb{Q}_{ε} to itself and maps x_j to $x_{\alpha(j)}$ for every j. The inductive step is proved.

Extraction of Radical Lemma (analogue of Lemma 3). Assume that $n \geq 5$ and k are integers, $x_1, \ldots, x_n \in \mathbb{C}$, a field $F \supset \mathbb{Q}(\vec{x})$ is even-symmetric over a subfield $B \subset F$, $r \in F - B$ and $r^k, \varepsilon_k \in B$. Then F is even-symmetric over B(r).

Proof. Let a, b, c, d, e be arbitrary different elements of $\{1, \ldots, n\}$. It suffices to prove that F is (abc)-symmetric over B(r), i.e. that there is an automorphism of F which maps every element of B(r) to itself and x_j to $x_{(abc)(j)}$ for every j. Recall that

$$(abc) = (dac)^{-1}(ceb)^{-1}(dac)(ceb).$$

Since F is even-symmetric over B, there are automorphisms α, β of F such that

- $\bullet \ \alpha(x_d, x_a, x_c) = (x_a, x_c, x_d),$
- $\bullet \ \beta(x_c, x_e, x_b) = (x_e, x_b, x_c),$
- $\alpha(y) = y$ for every $y \in B$ or $y = x_j, j \notin \{d, a, c\}$, and
- $\beta(y) = y$ for every $y \in B$ or $y = x_j, j \notin \{c, e, b\}$.

Since $r^k \in B$, we have $\alpha(r^k) = \beta(r^k) = r^k$. Hence there are integers p, q such that $\alpha(r) = \varepsilon_k^p r$ and $\beta(r) = \varepsilon_k^q r$. Since $\varepsilon_k \in B$, we have $\alpha^{-1}(r) = \varepsilon_k^{-p} r$ and $\beta^{-1}(r) = \varepsilon_k^{-q} r$. Therefore $\alpha^{-1}\beta^{-1}\alpha\beta(r) = r$. Hence the automorphism $\alpha^{-1}\beta^{-1}\alpha\beta$ of F is as required.

Alternative proof of the above Theorem (cf. proof of the Ruffini Theorem 2). Take $x_1, \ldots, x_n \in \mathbb{C}$ given by the Symmetrization Lemma. Denote the coefficients of the unitary polynomial with roots x_1, \ldots, x_n by a_{n-1}, \ldots, a_0 . Assume to the contrary that x_1, \ldots, x_n are contained in some radical extension of $\mathbb{Q}(\vec{a}) := \mathbb{Q}(a_{n-1}, \ldots, a_0)$. Then x_1, \ldots, x_n are contained in some radical extension F of $\mathbb{Q}_{\varepsilon}(\vec{a})$. Hence F is also a radical extension of $\mathbb{Q}_{\varepsilon}(\vec{a})$. Therefore there is a radical extension \overline{F} of F which is even-symmetric over \mathbb{Q}_{ε} . Since a_{n-1}, \ldots, a_0 are symmetric polynomials of x_1, \ldots, x_n , the field \overline{F} is even-symmetric over $\mathbb{Q}_{\varepsilon}(\vec{a})$. Since F is a radical extension of $\mathbb{Q}_{\varepsilon}(\vec{a})$, the field \overline{F} is also a radical extension of $\mathbb{Q}_{\varepsilon}(\vec{a})$, i.e. $\overline{F} = \mathbb{Q}_{\varepsilon}(\vec{a}, r_1, \ldots, r_s)$ for some x_1, \ldots, x_s . By induction on x_1, \ldots, x_s by induction of Radical Lemma one proves that x_1, \ldots, x_s because even permutation x_1, \ldots, x_s for every x_1, \ldots, x_s . For x_1, \ldots, x_s is a contradiction because even permutation x_1, \ldots, x_s for every x_1, \ldots, x_s for x_1, \ldots, x_s for x_1, \ldots, x_s for x_1, \ldots, x_s for every x_2, \ldots, x_s for x_1, \ldots, x_s for x_2, \ldots, x_s for x_3, \ldots, x_s for x_1, \ldots, x_s for x_1, \ldots, x_s for every x_2, \ldots, x_s for x_1, \ldots, x_s for x_2, \ldots, x_s for x_3, \ldots, x_s for x_1, \ldots, x_s for every x_1, \ldots, x_s for x_2, \ldots, x_s for x_3, \ldots, x_s for x_1, \ldots, x_s for every x_1, \ldots, x_s for x_2, \ldots, x_s for x_1, \ldots, x_s for x_2, \ldots, x_s for x_3, \ldots, x_s for x_1, \ldots, x_s for x_2, \ldots, x_s for $x_3, \ldots,$

Remark 12 (A solvability criterion and an algorithm). There is an algorithm deciding, for $a_{n-1}, \ldots, a_0 \in \mathbb{Q}$, whether all the roots of the equation $x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = 0$ are expressible by radicals from $\{1\}$.

This is implied by the following criterion, together with an estimation on the number of operations. (This estimation can easily be extracted from the proof, the idea is to observe that the 'symmetry subgroup' of S_n cannot be changed more than $\log_2 n! < n \log_2 n$ times.)

⁹Here we do not assume that are x_1, \ldots, x_n algebraically independent over \mathbb{Q}_{ε} , although we apply the Lemma in that situation.

Galois Solvability Criterion (conjecture). For every $a_{n-1}, \ldots, a_0 \in \mathbb{Q}$ all the roots of the equation $A(x) := x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = 0$ are expressible by radicals from $\{1\}$ if and only if a set of degree 1 polynomials over \mathbb{Q} can be obtained from $\{A\}$ using the following operations:

- (factorization) if one of our polynomials equals to P_1P_2 for some non-constant $P_1, P_2 \in \mathbb{Q}[x]$, then replace P_1P_2 by P_1 and P_2 ;
- (extracting a root) if one of our polynomials equals to $P(x^k)$ for some $P \in \mathbb{Q}[x]$, then replace $P(x^k)$ by P(x);
 - (taking Galois resolvent) replace one of our polynomials P by the polynomial

$$\prod_{\alpha \in \Sigma_q} (x - \varepsilon_q y_{\alpha(1)} - \varepsilon_q^2 y_{\alpha(2)} - \dots - \varepsilon_q^k y_{\alpha(q)}),$$

where y_1, \ldots, y_q are all the roots of P. (The coefficients of this product are symmetric in y_1, \ldots, y_k , so they are rational, i.e. y_1, \ldots, y_k are 'not required' to calculate the coefficients.)

I would be grateful if a specialist in algebra could confirm that this criterion is correct (and is equivalent to the Galois Solvability Criterion in its usual textbook formulation, please give a reference), or describe required changes. (I asked some specialists since July 2017, but so far obtained no answer.)

I conjecture that for every $a_{n-1}, \ldots, a_0 \in \mathbb{C}$ analogous results holds for $a_{n-1}, \ldots, a_0 \in \mathbb{C}$ with $\{1\}$ replaced by $\{1, a_{n-1}, \ldots, a_0\}$.

References

- [A] V. Alexeev, Abel's theorem in problems and solutions, Kluwer A.P., New York, 2004.
- [B] J. Brown, Abel and the insolvability of the quintic, http://www.math.caltech.edu/~jimlb/abel.pdf.
- [ECG] Toward algorithms of solving algebraic equations, presented by A. Enne, A. Chilikov, A. Glebov, A. Skopenkov, B. Vukorepa, https://www.turgor.ru/lktg/2018/5/index.html.
- [Es] A. Esterov, Galois theory for general systems of polynomial equations, arXiv:1801.08260.
- [FT] D. Fuchs, S. Tabachnikov, Mathematical Omnibus. AMS, 2007.
- [Ka] A. Kanunnikov, Elements of Galois theory: solvability of algebraic equations in radicals (in Russian), http://www.mathnet.ru/conf1015.
- [Ko] V. Kolosov, Theorems and Problems of Algebra, Combinatorics and Number Theory (in Russian), Gelios, Moscow, 2001.
- [L] L. Lerner, Galois Theory without abstract algebra, arXiv:1108.4593.
- [MM] K.S. Makarychev and Y.S. Makarychev. The importance of being formal. Mathematical Intelligencer, 23:1 (2001) 4142. http://ttic.uchicago.edu/~yury/papers/formal.pdf.
- [P] P. Pesic, Abel's Proof, The MIT Press, 2004, Cambridge, Massachusetts, London, England.
- [PS] V. Prasolov and Yu. Solovyov, Elliptic Functions and Elliptic Integrals, AMS, 1997.
- [R] M. I. Rosen, Niels Hendrik Abel and Equations of the Fifth Degree, Amer. Math. Monthly, 102:6 (1995) 495-505.
- [Sk11] A. Skopenkov, A simple proof of the Abel-Ruffini theorem (in Russian), Mat. Prosveschenie, 15 (2011) 113-126, arXiv:1102.2100.
- [Sk15] A. Skopenkov, A short elementary proof of the Ruffini-Abel Theorem (previous version of this note), arXiv:1508.03317v1.
- [Sk17] A. Skopenkov, Some more proofs from the Book: solvability and insolvability of equations in radicals, arXiv:0804.4357v6. Russian version published as §5 of: Elements of mathematics via problems: from olympiades and math circles to a profession, editors A. Zaslavsky, A. Skopenkov, and M. Skopenkov. MCCME, Moscow, 2018, http://www.mccme.ru/circles/oim/sturm.pdf. English version to appear as §9 of: A. Skopenkov, Elements of mathematics via problems: from olympiades and math circles to a profession, Algebra (tentative title), AMS, RI.
- [St94] J. Stillwell, Galois theory for beginners, Amer. Math. Monthly, 101 (1994), 22-27.
- [St15] I. Stewart, Historical Introduction, in: Galois Theory (4th ed.), CRC Press (2015).
- [T] V. Tikhomirov, Abel and his great theorem (in Russian), Kvant, 2003, N1.