Back to solving the quintic, depression and Galois primes

Semjon Adlaj

Abstract. Évariste Galois is best known for proving the insolubility of the general quintic via radicals. There, he (merely) confirmed the ingenious insights of Carl Gauss, Paolo Ruffini and Niels Abel. Yet, Galois went on (spectacularly alone) to formulate both necessary and sufficient criterion for solubility of a general algebraic equation via radicals. Even more, he was undeniably the first to actually solve the general quintic via exhibiting it as a modular equation of level 5. We aim and (hopefully) succeed at lifting any remaining doubts, concerning the latter (persistently hardly ever known) claim. And along with presenting Galois construction for depressing the degree of the modular equation of level 5, 7 or 11, we show that such construction is unique for the (Galois) prime 5, but one more construction is possible for each of the two remaining Galois primes 7 and 11.

In his last letter [5], eloquently described by Hermann Weyl as "the most substantial piece of writing in the whole literature of mankind", Évariste Galois indicated sufficient and necessary condition for depressing the degree of the modular equation of prime level. For this purpose he introduced the projective special linear group over a prime field, which we denote by G_p,[1] and observed that it was simple whenever the prime p strictly exceeded the prime 3.[2] He pointed out the three exceptional primes for which the group G_p possessed a subgroup of index, coinciding with p. These were the primes 5, 7 and 11. For any prime p strictly exceeding 11 only subgroups of index $p+1$, and no lower, are guaranteed to exist. Equivalently said, a modular equation, of prime level $p \geq 5$,

[1] The group G_p might be viewed as the Galois group (in the common sense) of its corresponding algebraic equations, as we shall further clarify. The standard notation for G_p is PSL(2,$\mathbb{F}_p$), where we assume the index p to denote a prime.

[2] The very concept of simplicity, being introduced by Galois, is the basis for classifying groups. The classification of finite simple groups, which referred to as "an enormous theorem", was (prematurely) announced in 1981 (by Daniel Gorenstein) before it was completed in 2004 (by Michael Aschbacher and Stephen Smith).

is depressable,[3] from degree $p+1$ to degree p, iff $p \in \{5,7,11\}$. Via explicitly constructing the subgroups, corresponding to these three exceptional primes, Galois must, in particular, be solely credited for actually solving the general quintic via exhibiting it as a modular equation of level 5. While Galois' contribution for formulating sufficient and necessary criterion for solubility of an algebraic equation via radicals is acknowledged, his decisive contribution to actually solving the quintic (before Hermite and Klein) is, surprisingly, too poorly recognized (if not at all unrecognized)! Betti, in 1851 [3], futily asked Liouville not to deprive the public any longer of Galois' (unpublished) results, and, in 1854 [4], went on to show that Galois' construction yields a solution to the quintic via elliptic functions.[4] One might associate with each quintic, given in Bring-Jerrard form, a corresponding value for the (Jacobi) elliptic modulus β, as Hermite did, in 1958 [6], implementing this very Galois' construction (thereby enabling an efficient algorithm for calculating the roots via values of an elliptic function at points placed apart by multiples of fifth-period). The group G_5 acts (naturally) on the projective line $\mathrm{P}\mathbb{Z}_5$, which six elements we shall, following Galois, label as 0,1,2,3,4 and ∞. Then collecting them in a triple-pair $\{(0,\infty),(1,4),(2,3)\}$, the group G_5 is seen to generate four more triple-pairs $\{(1,\infty),(2,0),(3,4)\}$,$\{(2,\infty),(3,1),(4,0)\}$,$\{(3,\infty),(4,2),(0,1)\}$,$\{(4,\infty),(0,3),(1,2)\}$. Together, the five triple-pairs constitute the five-element set upon which G_5 acts.[5] Galois did not (in his last letter) write down the four triple-pairs, which we did write after the first, and we now, guided by his conciseness and brevity, confine ourselves to writing down only the first pair-set that he presented for each of the two remaining cases, where $p = 7$ and $p = 11$, respectively: $\{(0,\infty),(1,3),(2,6),(4,5)\}$ and $\{(0,\infty),(1,2),(3,6),(4,8),(5,10),(9,7)\}$. Unlike the case $p = 5$, an alternative might be presented for the case $p = 7$, which is $\{(0,\infty),(1,5),(2,3),(4,6)\}$, and for the case $p = 11$, which is $\{(0,\infty),(1,6),(3,7),(4,2),(5,8),(9,10)\}$. The "absolute invariant" for the action of the subgroup Γ_2, of the modular group $\Gamma := \mathrm{PSL}(2,\mathbb{Z})$, consisting of linear fractional transformations congruent to the identity modulo 2, is the square (of the elliptic

[3] This well-established term means lowerable. Its conception is a simple (yet ingenious) idea with which Galois alone must be fully credited, and, as we shall soon see, is the single most crucial (yet rarely brought to awareness) step towards actually solving the quintic.

[4] In 1830, Galois competed with Abel and Jacobi for the grand prize of the French Academy of Sciences. Abel (posthumously) and Jacobi were awarded (jointly) the prize, whereas all references to Galois' work (along with the work itself!) have (mysteriously) disappeared. The very fact that Galois' lost works contained contributions to Abelian integrals is either unknown (to many) or deemed (by some) no longer relevant to our contemporary knowledge. For the sake of being fair to a few exceptional mathematicians, we must cite (without translating to English) Grothendick (as a representative), who (in his autobiographical book Récoltes et Semailles) graciously admits that "Je suis persuadé d'ailleurs qu'un Galois serait allé bien plus loin encore que je n'ai été. D'une part à cause de ses dons tout à fait exceptionnels (que je n'ai pas reçus en partage, quant à moi)."

[5] Indeed, it is the five-element set (not merely a five-element set) which Hermite had no choice but to employ. Galois' construction for each of the two remaining cases, where $p = 7$ or $p = 11$, allows an alternative, as will, next, be exhibited.

modulus) β^2. A fundamental domain $\Gamma_2\backslash\mathcal{H}$, for the action of Γ_2 (on the upper half-plane $\mathcal{H}$), might be obtained by subjecting a fundamental domain $\Gamma\backslash\mathcal{H}$ (of Γ) to the action of the quotient group $\Gamma/\Gamma_2 \cong S_3$.[6] In particular, β^2 viewed as function on $\mathcal{H}$, is periodic, with period 2. Sohnke, in a remarkable work [7], had determined the modular equations for $\beta^{1/4}$, for all odd primes up to, and including, the prime 19. That work, along with Betti's work, inspired Hermite to (successfully) relate a (general) quintic, in Bring-Jerrard form, to a modular equation of level 5, yet he had little choice but to admit the importance of a sole Galois idea (in depressing the degree of the modular equation).[7] The modular polynomial for $\beta^{1/4}$, of level 5, is

$$\phi_5(x,y) := x^6 - y^6 + 5\,x^2y^2\,(x^2-y^2) + 4\,x\,y\,(1-x^4y^4),$$

and the period of $\beta^{1/4}$ (as an analytically continued function) is 16. Denoting the roots of $\phi_5(x,\, y=\beta^{1/4}(\tau))$, for a fixed $\tau\in\mathcal{H}$, by

$$y_5 = \beta^{1/4}(5\,\tau),\ \ y_m = -\beta^{1/4}\left(\frac{\tau+16\,m}{5}\right),\ \ 0\le m\le 4,$$

one calculates the minimal polynomial for $x_1 := (y_5-y_0)(y_4-y_1)(y_3-y_2)\,y$. It turns out to be

$$x^5 - 2000\,\beta^2\,(1-\beta^2)^2\,x + 1600\sqrt{5}\,\beta^2\,(1-\beta^2)^2\,(1+\beta^2).$$

Thereby, a root of the quintic

$$x^5 - x + c,\ \ c := \frac{2\,(1+\beta^2)}{5^{5/4}\sqrt{\beta(1-\beta^2)}} = \frac{2\,(1+y^8)}{5^{5/4}\,y^2\sqrt{1-y^8}},^{8}$$

is

$$\frac{\sqrt{5}\,c\,x_1}{4\,(1+\beta^2)} = \frac{x_1}{2\sqrt{5\sqrt{5}\,\beta(1-\beta^2)}} = \frac{(y_5-y_0)(y_4-y_1)(y_3-y_2)}{2\,y\sqrt{5\sqrt{5}\,(1-y^8)}},$$

[6] The latter quotient group coincides with G_2 which is isomorphic with S_3.

[7] Hermite had apparently adopted Cauchy's catholic and monarchist ideology, much in contrast to Galois' passionate rejection of social prejudice. In 1849, Hermite submitted a memoir to the French Academy of Sciences on doubly periodic functions, crediting Cauchy, but a priority dispute with Liouville prevented its publication. Hermite was then elected to the French Academy of Sciences on July 14, 1856, and (likely) acquainted, by Cauchy, with ideas stemming from (but not attributed to) Galois "lost" papers. T. Rothman made a pitiful attempt in "Genius and Biographers: The Fictionalization of Evariste Galois", which appeared in the American Mathematical Monthly, vol. 89, 1982, pp. 84-106 (and, sorrowly, received the Lester R. Ford Writing Award in 1983) to salvage Cauchy's reputation (unknowingly) suggesting further evidence of Cauchy's cowardice, and surprising us, along the way, with many (unusual but ill substantiated and biased) judgements telling us much about T. Rothman himself, but hardly anything trustworthy about anyone else!

[8] One must note that the constant coefficient c is invariant under the inversions $\beta\mapsto -1/\beta$ and $\beta\mapsto(1-\beta)/(1+\beta)$. Here, the composition of the latter two inversions is another inversion. The corresponding four-point orbit in a fundamental domain $\Gamma_2\backslash\mathcal{H}$ is generated via the mapping $\tau\mapsto 2/(2-\tau)$.

and so is expressible via the coefficients λ_m and μ_m of the elliptic polynomials $r_{m5}(x) = x^2 - \lambda_m x + \mu_m$, $0 \le m \le 5$.[9] In fact, the polynomials r_{m5} might be so ordered so that, for each m, the value β_m^2 coincides with y_m^8. The (general) expression for $y_m^8 = \beta_m^2$ might be written as

$$y_m^8 = \frac{s(\lambda_m,\, \mu_m,\, \beta)}{\beta^4 s(\lambda_m,\, \mu_m,\, 1/\beta)},$$

where

$$s(\lambda,\, \mu,\, x) = \left(\frac{1+\lambda\, x}{\mu} + x^2\right)\left(4\,\lambda + \left(\frac{2\,\lambda^2}{\mu} + 4 + 5\,\mu\right)x + \lambda\left(\frac{2}{\mu} + 3\right)x^2 + x^3\right),$$

and the coefficients $\lambda_m = \gamma_m + (2\cdot\gamma_m)$ and $\mu_m = \gamma_m(2\cdot\gamma_m)$ satisfy

$$\prod_{m=0}^{5}\left(x^2 - \lambda_m\, x + \mu_m\right) = x^{12} + \frac{62\, x^{10}}{5} - 21\, x^8 - 60\, x^6 - 25\, x^4 - 10\, x^2 + \frac{1}{5} +$$

$$+ \, \alpha\, x^3\left(x^8 + 4\, x^6 - 18\, x^4 - \frac{92\, x^2}{5} - 7\right) + \, \alpha^2 x^4\left(\frac{x^6}{5} - 3\, x^2 - 2\right) - \frac{\alpha^3 x^5}{5} = r_5(x),$$

where $\alpha := 4(\beta + 1/\beta)$. The roots γ_m and $2\cdot\gamma_m$,[10] $0 \le m \le 5$, of the division polynomial r_5 might be highly efficiently calculated via the algorithm provided in [1]. Calculating a pair, say γ_0 and γ_5, suffices, of course, for calculating all twelve roots via applying the addition formula along with the doubling formula, as told in [2].

Nowadays, oblivion has entirely replaced marvelling at Galois key step, towards solving the quintic, in depressing the degree of the modular equation, of level 5, from 6 to 5,[11] and Galois is merely mentioned, along with Abel, for determining that the quintic is not solvable via radicals. We hope that this (crippled) view of Galois (deeply constructive) theory would finally come to an end.

References

[1] Adlaj S. *Iterative algorithm for computing an elliptic integral* // Issues on motion stability and stabilization (2011), 104-110 (in Russian).

[2] Adlaj S. *Multiplication and division on elliptic curves, torsion points and roots of modular equations.* Available at `http://www.ccas.ru/depart/mechanics/TUMUS/Adlaj/ECCD.pdf`.

[9] The elliptic polynomials were presented, in 2014, at the 7th PCA conference (http://pca.pdmi.ras.ru/2014/program) in a talk titled “Modular polynomial symmetries”, and at the 17th workshop on Computer Algebra (http://compalg.jinr.ru/Dubna2014/abstracts.html) in a talk titled “Elliptic and coelliptic polynomials”. Details are provided in [2].

[10] Consistently with the notation employed in [2], $2\cdot\gamma_m$ signifies that the doubling formula has been applied to γ_m.

[11] For example, S. Vlăduţ (wrongfully) attributes, in his book “Kronecker’s Jugendtraum and Modular Functions” (published by Gordon and Breach in 1991), to Hermite showing the equivalence of the general quintic to the modular equation of level 5.

[3] Betti E. *Sopra la risolubilità per radicali delle equazioni algebriche irriduttibili di grado primo* // Dagli Annali di Scienze matimatiche e fisiche, t. II (Roma, 1851): 5-19.

[4] Betti E. *Un teorema sulla risoluzione analitica delle equazioni algebriche* // Dagli Annali di Scienze matimatiche e fisiche, t. V (Roma, 1854): 10-17.

[5] Galois É. *"Lettre de Galois à M. Auguste Chevalier"* // Journal de Mathématiques Pures et Appliquées XI (1846): 408–415.

[6] Hermite C. *"Sur la résolution de l'équation du cinquième degré"* // Comptes Rendus de l'Académie des Sciences XLVI(I) (1858): 508–515.

[7] Sohnke L. *Equationes Modulares pro transformatione functionum Ellipticarum* // Journal de M. Crelle, t. XVI (1836): 97-130.

Semjon Adlaj
Section of Stability Theory and Mechanics of Controlled Systems
Department of Mechanics
Division of Complex Physical and Technical Systems Modeling
Computing Center of the Federal Research Center "Informatics and Control"
Russian Academy of Sciences
Russia 119333, Moscow, Vavilov Street 40.
e-mail: SemjonAdlaj@gmail.com