Computer tools in education, 2018
№ 4: 11–26
http://ipo.spb.ru/journal
doi:10.32603/2071-2340-4-11-26

algorithmic mathematics and mathematical modeling

ON THE SECOND MEMOIR OF ÉVARISTE GALOIS' LAST LETTER

Adlaj S. F.

Federal Research Center "Informatics and Control", Moscow, Russia

Abstract

Évariste Galois' last letter, addressed to Auguste Chevalier, on the eve of the (so-called) duel on May 30, 1832 (which, perhaps, simpler and more accurately described by Alfred, who did not allow a priest to deprive him from the final moments on the following day with his elder brother Évariste, as murder), was written on seven pages and was divided into three memoirs. The first memoir consumes a little less than two pages. It gave rise to what has come to be known as Galois theory (as, in particular, told by Melvin Kiernan). Yet Galois went on with stunningly amazing constructions in the second memoir, which consumed a bit more than two pages. The third (and longest!) memoir begins on the fifth page and remains mysteriously unresolved, yet it undoubtedly inspired Alexander Grothendieck to formulate his period conjecture. The letter is concluded with a paragraph on the latest "principal contemplations", concerning "the applications of the theory of ambiguity to transcendental analysis", where Galois delivers his last puzzle to us, saying that "one recognizes immediately lots of expressions to look for". Unfortunately, the severity of the time pressure upon him permitted only succinct last instructions with no more last examples. Still and disgracefully, many "historians" keep on incessantly and mundanely telling us (and each other) that we ought not "overestimate" the significance of the letter, which was (contrary to their advice) eloquently and veraciously described by Hermann Weyl as "the most substantial piece of writing in the whole literature of mankind"!

Keywords: *Essential elliptic function, depressing the degree of the modular equation, projective special linear group over a prime field, elliptic and coelliptic polynomials, solving the general quintic equation.*

Citation: S. F. Adlaj, "On the Second Memoir of Évariste Galois' Last Letter," *Computer tools in education*, no. 4, pp. 11–26, 2018. doi:10.32603/2071-2340-4-11-26

> The sections of the second memoir dealing with elliptic integrals were never written, nor, apparently, was any part of the third memoir. The outline of this material in the letter to Chevalier was very sketchy, and did not influence later mathematics.[1]

[1] The quote concerns Galois' last letter. It is taken from page 79 of a 154-page survey on [15, The Development of Galois Theory from Lagrange to Artin] by M. B. Kiernan.

1. AN ESSENTIAL ELLIPTIC FUNCTION AND ITS MODULAR INVARIANT

Given a parameter $\beta \in \mathbb{C} \setminus \{-1,0,1\}$, introduce *an essential elliptic function*, as in [1, 2, 4, 6, 9], that is a (meromorphic) function $\mathscr{R} = \mathscr{R}_\beta = \mathscr{R}_\beta(\cdot) = \mathscr{R}(\cdot,\beta)$, possessing a (double) pole at the origin and satisfying the differential equation

$$\mathscr{R}'^2 = 4\mathscr{R}\left(\mathscr{R}+\beta\right)\left(\mathscr{R}+1/\beta\right). \tag{1}$$

Denote the lattice of the function $\mathscr{R}_\beta$ by Λ_β, and call the parameter β *the elliptic modulus*. The map

$$z \mapsto \left(1, \mathscr{R}_\beta(z), \mathscr{R}'_\beta(z)\right),$$

extends, with $0 \mapsto (0,0,1)$, to a map from the period-parallelogram $\mathbb{C}/\Lambda_\beta$ into the complex projective space $\mathrm{P}\mathbb{C}^2$. The (extended) map induces, onto its image $\mathbb{E}_\beta$, which we shall call *the associated elliptic curve*,[2] an isomorphism of Riemann surfaces, as well as, an isomorphism of groups.[3] This map, further, enables an identification (exploiting the j-invariant) of isomorphism classes of projective complex elliptic curves with homothety classes of lattices $\mathscr{L}/\mathbb{C}^\times$, which might, in turn, be identified with the fundamental domain $\Gamma\backslash\mathscr{H}$, for the action of the modular group $\Gamma := \mathrm{PSL}(2,\mathbb{Z})$, upon the upper half plane $\mathscr{H}$, as is well explained in [17]. From now on, we exploit the identification of the points on the torus $\mathbb{C}/\Lambda_\beta$, which might be viewed as the domain of $\mathscr{R}_\beta$, with the points on the elliptic curve $\mathbb{E}_\beta$, which might be viewed as the image of the functional pair $(\mathscr{R}_\beta, \mathscr{R}'_\beta)$. Keeping in mind that the value of the function $\mathscr{R}_\beta$ determines, up to a sign, via equation (1), the value of its derivative $\mathscr{R}'_\beta$, we might further identify a pair of (not necessarily distinct) points on $\mathbb{E}_\beta$, sharing a first coordinate, with their corresponding pair of points in the domain of $\mathscr{R}_\beta$, which image (under $\mathscr{R}_\beta$) coincide with that very first coordinate.
Fix the elliptic modulus β, and express the defining equation for the (already introduced) elliptic curve $\mathbb{E}_\beta$ as

$$\mathbb{E}_\beta : y^2 = 4\,x\,q(x),\ \ q(x) := x^2 + (\beta + 1/\beta)\,x + 1.$$

The justification for such canonical representation of elliptic curves (not to be confused with the Weierstrass normal form) is provided in the afore-indicated references [1, 2, 4, 6, 9].[4] Two distinct points (x_1, y_1) and (x_2, y_2) might be summed (on $\mathbb{E}_\beta$) to a point (x_3, y_3), which first coordinate satisfy *the addition formula*

$$x_3 = \frac{1}{4\,x_1 x_2}\left(\frac{x_1\,y_2 - x_2\,y_1}{x_1 - x_2}\right)^2. \tag{2}$$

Now, denoting by $n \cdot (x,y)$ the multiplication of the point (x,y) by n, and denoting by $(n\cdot x, n\cdot y)$ the n-multiple of the point (x,y) on $\mathbb{E}_\beta$, so that $(n\cdot x, n\cdot y) = n\cdot(x,y)$, *the doubling formula* expresses the first coordinate $2\cdot x$ of the point $2\cdot(x,y)$, as calculated in [1],

$$2\cdot x = \frac{p_2(x)}{q_2(x)},\ \ p_2(x) := \left(\frac{x^2-1}{2}\right)^2,\ \ q_2(x) := x\,q(x). \tag{3}$$

When n is an arbitrary integer, the multiplication by n amounts to successively multiplying by its prime factors (counted with their respective multiplicities), so we want to deduce *a multiplication by an odd prime formula*. Assuming n to be odd (not necessarily prime!), exceeding

[2] Without, necessarily, further specifying whether the association pertains to the elliptic function $\mathscr{R}_\beta$, its lattice Λ_β or the elliptic modulus β.

[3] The curve $\mathbb{E}_\beta$ is, thereby, said to be a one-dimensional complex Lie group.

[4] We shall, furthermore, employ this representation for attaining an explicit inverse of the modular invariant.

2, we might (recursively) deduce such a formula, expressing the first coordinate of the n-odd-multiple point as a degree n^2 fractional transformation of the first coordinate of the point to be multiplied, that is,

$$n \cdot x = \frac{p_n(x)}{q_n(x)},\ p_n(x) := x^{n^2} r_n\left(\frac{1}{x}\right)^2,\ q_n(x) := r_n(x)^2,$$

$$r_n(x) := \frac{(n-1)^2\left(x\, q_{n-1}(x) - p_{n-1}(x)\right)}{n\,(n-2)\, r_{n-2}(x)},\ r_1(x) :\equiv 1. \tag{4}$$

An explicit formula for $n \cdot x$ relies on an explicit formula for $(n-1)\cdot x$ as a fractional transformation with (coprime) polynomials p_{n-1} and q_{n-1} appearing in its numerator and denominator, respectively. Since n is odd, by assumption, the formula for $(n-1)\cdot x$ might always be attained via the doubling formula applied to $\left(\frac{n-1}{2}\right)\cdot x$. Note that the sequence $\{r_n : n \text{ is odd}\}$ need not be extended to include elements r_n with even indices, unlike p_n and q_n which are (successively) defined for all integer indices n (employing the doubling formula whenever the indices are even), and that, furthermore, if we choose the polynomials q_n to be monic for all even n then so do become all (subsequent) polynomials r_n (and q_n). The roots of each r_n are precisely the first coordinates of the points, aside from the identity point, on $\mathbb{E}_\beta$, of order dividing n, so, in particular, the degree of r_n is $(n^2-1)/2$, and if m divides n then the polynomial $r_m(x)$ divides the polynomial $r_n(x)$.

The (monic) polynomial r_n, which we have just introduced, has its coefficients in the field $\mathbb{F} := \mathbb{Q}(\beta+1/\beta)$, that is, the field of rational functions in the transcendental (or algebraic) element $\beta+1/\beta$, over the field of rational numbers $\mathbb{Q}$.[5] When n is an odd prime, as we now opt as being the default assumption, the roots of r_n are the first coordinates of the points of order n on $\mathbb{E}_\beta$. The assumption which will not be lifted (throughout this paper) that $\beta^2 \in \mathbb{C}\setminus\{0,1\}$ guarantees that the roots (of r_n) are pairwise distinct. We shall call the polynomial r_n *the division polynomial of level* n, and, whenever an emphasis on its dependence upon the elliptic modulus β is desired, we shall denote it as $r_n(\cdot,\beta)$, still being at large viewing it either as a function of two variables or as a β-parametric polynomial function in a single variable.

The field $\mathbb{F}[\gamma_m]$, obtained by adjoining a root γ_m of r_n to the base field $\mathbb{F}$, is the splitting field for *the elliptic polynomial of level* n:

$$r_{mn}(x) := \prod_{l=1}^{(n-1)/2} \left(x - l\cdot\gamma_m\right).$$

The polynomial r_{mn} divides r_n, and the first index (m) of r_{mn} might be employed to designate $n+1$ pairwise coprime elliptic polynomial factors of r_n:

$$r_n(x) = \prod_{m=0}^{n} r_{mn}(x).$$[6]

Put $d(x) := x - 1/x$, and $d^2(x) := x + 1/x - 2$. Let d^2 denote the discriminant of the quadratic polynomial $q(x)$, which coincides with the discriminant of the cubic polynomial $q_2(x)$, so $d^2 = d(\beta)^2 = d^2(\beta^2)$. The homothety class of the lattice Λ_β is represented by a (unique) point τ in the

[5] No further restriction is imposed upon assuming that the coefficients of polynomials, in $\beta+1/\beta$, appearing in the numerator and the denominator of a rational expression, in $\mathbb{F}$, are integers.

[6] The elliptic polynomials were introduced in 2014 at the 7th annula 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".

fundamental domain $\Gamma\backslash\mathscr{H}$, as we already mentioned. The (Klein) modular invariant j, which maps the upper half plane $\mathscr{H}$ onto $\mathbb{C}$, is a modular form of weight zero. Its domain might be extended to include all rational real points, as well as, the point at (complex) infinity. All these points map (under j) to (complex) infinity. We shall emphasize that the modular invariant j is a (holomorphic) bijection between the (or any) extended fundamental domain and the Riemann sphere $\mathbb{C}\cup\infty$.[7] The domain of j might be further extended to include the lower half plane via setting $j(-\tau) = j(\tau)$. The value of j at a point τ, corresponding to the homothety class of the lattice Λ_β is

$$j(\tau) = \frac{4\left(d^2+1\right)^3}{27\,d^2}, \tag{5}$$

and since the said discriminant d^2 is invariant under the substitutions $\beta \mapsto -\beta$ and $\beta \mapsto 1/\beta$, so must be $j(\tau)$. Moreover, $j(\tau)$ is invariant under the substitutions $\beta^2 \mapsto 1-\beta^2$. Thus, the homothety class of the lattice Λ_β as β^2 undergoes the inversions (meaning linear fractional transformations of order 2)

$$S : x \mapsto \frac{1}{x},\ \ T : x \mapsto 1-x, \tag{6}$$

is preserved. The latter two inversions generate a (6 element) group isomorphic with the symmetry group S_3 of a triangle. The three functional (trigonometric) pairs

$$\{-\tan^2, -\cot^2\},\ \{\sin^2, \cos^2\},\ \{\csc^2, \sec^2\}$$

might be viewed as the three vertices, which are rotated via either the composition $S\circ T$ or its inverse $T\circ S$. The first vertex is invariant under the action of S which transposes the second vertex with the third, while the second vertex is invariant under the action of T which transposes the third vertex with the first, and the third is invariant under the action of the third inversion

$$S\circ T\circ S = T\circ S\circ T : x \mapsto \frac{x}{x-1}$$

which transposes the first vertex with the second. Generally, twelve distinct values of β correspond to a single point τ in the fundamental domain. The exceptions are the values, corresponding to the *corners* of the fundamental domain. These are the six values $\beta \in \{\pm i, \pm 1/\sqrt{2}, \pm\sqrt{2}\}$, corresponding to $\tau = i := \sqrt{-1}$, and the four values $\beta \in \{\pm i\zeta, \pm i\zeta^2\}$, corresponding to $\tau = \zeta$.[8] An isomorphism between elliptic curves as their elliptic modulus β undergoes permissible transformations (generated by S and T) might explicitly be given as a linear map between first coordinates. Evidently, the isomorphism corresponding to the transformation $\beta \to 1/\beta$ is given by the identity map $x \mapsto x$, and the isomorphism corresponding to the transformation $\beta \to -\beta$ is given by the map $x \mapsto -x$. The isomorphism corresponding to the transformation $\beta \to \sqrt{1-\beta^2}$ is given by the map $x \mapsto -(\beta x+1)/\sqrt{1-\beta^2}$. Alternatively denoting the elliptic modulus β by $\sin\theta$,[9] the latter map between first coordinates:

$$l(x) = -x\tan\theta - \sec\theta \tag{7}$$

is said to induce an isomorphism of elliptic curves, as the elliptic modulus β undergoes the transformation $\sin\theta \to \cos\theta$.[10]

[7] The latter statement merely defines a modular form of weight zero.

[8] A reformulation involving α (instead of β) would be less cumbersome, perhaps, and so we give it here. Generally, six distinct values of α correspond to a single point τ in the fundamental domain. The exceptions are the three values $\alpha \in \{0, \pm 1/\sqrt{2}\}$, corresponding to $\tau = i$, and the two values $\alpha \in \{\pm 1/\sqrt{3}\}$, corresponding to $\tau = \zeta$.

[9] The angle θ is then called *the modular angle*.

[10] One readily verifies that the inverse of the linear map l is $l^{-1}(x) = -x\cot\theta - \csc\theta$ correspond to the (reverse) transformation of the elliptic modulus $\cos\theta \to \sin\theta$.

Since two elliptic moduli β and $1/\beta$ correspond to a single elliptic function $\mathscr{R}_\beta$ (and to a single elliptic curve $\mathbb{E}_\beta$), only six elliptic functions $\mathscr{R}$ correspond to twelve values of the elliptic modulus, corresponding to a single point τ in the fundamental domain. Only three distinct functions $\mathscr{R}$ correspond to the exceptional value $\tau = i$, and only two distinct functions $\mathscr{R}$ correspond to the exceptional value $\tau = \zeta$. The term elliptic modulus, endowed upon the parameter β, is now seen to coincide with the same term appearing in connection with the Jacobi elliptic functions. The Jacobi elliptic sine function, corresponding to elliptic modulus β and denoted by $\mathrm{sn}_\beta = \mathrm{sn}_\beta(\cdot)$, satisfies the differential equation

$$\mathrm{sn}_\beta'^2 = \left(1-\mathrm{sn}_\beta^2\right)\left(1-\beta^2\mathrm{sn}_\beta^2\right),$$

and coincides, up to homothety and translation (of its argument), with a square root of the function $\mathscr{R}$ (analytically continued). Explicitly,

$$\beta\,\mathrm{sn}_\beta\left(\frac{z}{\sqrt{\beta}}\right)^2 = \frac{1}{\mathscr{R}_{-\beta}(z)} = \mathscr{R}\left(z+\sqrt{\beta}\,z_0,-\beta\right),$$ [11] $$z_0 := \frac{\pi i}{2M(\beta)},$$

where $M(x)$ is the arithmetic-geometric mean of 1 and x; enlightening details about the function M are presented in [12]. As the elliptic modulus $\beta = \sin\theta$ undergoes the transformations, which we earlier discussed, corresponding elliptic functions $\mathscr{R}(\cdot,-\sin\theta)$, $\mathscr{R}(\cdot, i\tan\theta)$ and $\mathscr{R}(\cdot,-\sec\theta)$ coincide, up to homothety, translation and multiplicative constants, with the squares of the Jacobi elliptic functions sn_β, cn_β and dn_β. Putting $\kappa := 2i\csc(2\theta)$, the squares of the latter two Jacobi elliptic functions might be, explicitly, expressed as

$$\mathrm{cn}_\beta(z)^2 = 1-\frac{\kappa}{\mathscr{R}\left(z/\sqrt{\kappa},\, i\tan\theta\right)+i\tan\theta} = i\cot\theta\,\mathscr{R}\left(\frac{z+z_0}{\sqrt{\kappa}},\, i\tan\theta\right),$$

$$\mathrm{dn}_\beta(z)^2 = 1+\frac{\sin\theta\tan\theta}{\mathscr{R}\left(\sqrt{-\cos\theta}\,z,\,-\sec\theta\right)-\sec\theta} = \cos\theta\,\mathscr{R}\left(\sqrt{-\cos\theta}\,(z+z_0)\,,\,-\sec\theta\right).$$

Respectively, they satisfy the differential equations:

$$\mathrm{cn}_\beta'^2 = \left(1-\mathrm{cn}_\beta^2\right)\left(1-\beta^2+\beta^2\mathrm{cn}_\beta^2\right),\ \mathrm{dn}_\beta'^2 = \left(1-\mathrm{dn}_\beta^2\right)\left(\beta^2-1+\mathrm{dn}_\beta^2\right),$$

as well as, the functional equations:

$$\mathrm{sn}_\beta^2+\mathrm{cn}_\beta^2 \equiv 1 \equiv \beta^2\mathrm{sn}_\beta^2+\mathrm{dn}_\beta^2.$$

Here, one must also bear in mind a simple and basic functional equation:

$$\mathscr{R}(iz,\beta) = -\mathscr{R}(z,-\beta).$$

2. AN EXPLICIT FAST INVERSION OF THE MODULAR INVARIANT

An explicit fast inverse k of the modular invariant j was given in [3] as a composition

$$k := k_0\circ k_1\circ k_2,$$

[11] Note that the leftmost side of the equality is unaltered by switching from a branch of the square root function, applied to β, in the expression for the argument of the (known to be odd) function sn_β, to the other.

where

$$k_0(x) := \frac{i\,M\left(\sqrt{1-x^2}\right)}{M(x)},\ k_1(x) := \frac{\sqrt{x+4}-\sqrt{x}}{2},\ k_2(x) := \frac{3}{2}\left(\frac{x}{k_3(x)} + k_3(x)\right) - 1,$$

$$k_3(x) := \sqrt[3]{\sqrt{x^2-x^3}-x}.$$

Strictly speaking, the function M is (doubly) infinitely-valued as its calculation entails choosing one of two branches of the square root function at infinitely many steps. Consequently, the function k is, as well, an infinitely-valued function. However, its values, up to a sign, differ by the action of the modular group Γ. We mean that by flipping the sign, if necessary, we might assume that the function k never assumes values in the lower half plane, and, furthermore, its values might be brought via the action of the modular group Γ to a single value in the (or any) fundamental domain. In other words, while k is not strictly a left inverse of j, it is a right inverse, that is,

$$\forall x \in \mathbb{C},\ j \circ k(x) = x,$$[12]

for the modular invariant j does not separate points, in its domain, as long as they differ by the action of the modular group Γ, and no troubles arise in extending the latter equality to the whole Riemann sphere, including the point at (complex) infinity.

Before we move on to the modular equation, we must clarify the calculation of the inverse function k for the two special values of j at the corners: $j(\zeta) = 0$ and $j(i) = 1$. So, we point out that the (set) values of the composition, $k_1 \circ k_2$ at 0 and 1, coincide with exceptional (set) values of β at $\tau = \zeta$ and $\tau = i$, respectively. Certainly, k_2 has a removable singularity at zero and must be evaluated to -1 there, whereas $k_2(1) = 1/2$. Thus, $\zeta \in k(0) = k_0 \circ k_1(-1)$, and $i \in k(1) = k_0 \circ k_1(1/2)$.[13]

An elementary proof of the fast inversion formula, being discussed here, is given in [16].

3. EXPLICITLY AND EFFICIENTLY SOLVING THE MODULAR EQUATION

Recalling our default assumption that n is an odd prime, the functional pair $(j(\tau), j(n\tau))$ is known to be algebraically dependent (over $\mathbb{Q}$), and is said to satisfy *the modular polynomial of level n*, that is

$$\Phi_n(j(\tau), j(n\tau)) \equiv 0,$$

where the modular polynomial Φ_n possesses integer (rational) coefficients. Moreover, as explained in [18], Φ_n is symmetric in its two variables, that is $\Phi_n(x,z) = \Phi_n(z,x)$.[14] When τ is

[12] An analogy is afforded by a branch of the logarithmic function which is (regradless of the choice of the branch) a right (but not left) inverse of the exponential function. While the values of the logarithm, at a given point, constitute a discrete subset of a line, the values of the functions k and M do not. We have already indicated that the function M is (doubly) infinitely-valued, suggesting that its values (at a given point) constitute a discrete subset of $\mathbb{C}$ (not contained in any one-dimensinal subset over $\mathbb{R}$), and so is the function k.

[13] Implying, unsurprisingly, that the values 0 and 1 are fixed by the (identity) function $j \circ k$.

[14] For a couple examples, the modular polynomials $\Phi_3^*(x,y)$ and $\Phi_5^*(x,y)$, of degrees 3 and 5, were calculated by Smith (1879) and Berwick (1916), respectively:
$\Phi_3^*(x,y) = x^3y^3 - 2232\,(x^3y^2 + x^2y^3) - x^4 - y^4 + 1069956\,(x^3y + xy^3) - 2587918086\,x^2y^2 - 36864000\,(x^3 + y^3) - 8900222976000\,(x^2y + y^2x) - 452984832000000\,(x^2 + y^2) + 770845966336000000\,x\,y - 1855425871872000000000\,(x+y)$,
$\Phi_5^*(x,y) = x^5y^5 - 3720\,(x^5y^4 + y^4x^5) + 4550940\,(x^5y^3 + y^5x^3) - 1665999364600\,x^4y^4 - 2028551200\,(x^5y^2 + y^5x^2) - 107878928185336800\,(x^4y^3 + y^4x^3) - x^6 - y^6 + 246683410950\,(x^5y + y^5x) - 383083609779811215375\,(x^4y^2 + y^4x^2) + 441206965512914835246100\,x^3y^3 - 1963211489280\,(x^5 + y^5) - 128541798906828816384000\,(x^4y +$

fixed, and so is $j(\tau)$, the polynomial $\Phi_n(j(\tau),x)$ might be viewed as a polynomial in a single variable x over the (base) field $\mathbb{Q}(j(\tau))$,[15] and we shall call its roots, *the roots of the modular equation of level* n.

Now, let the value of $j(\tau)$ be given by equation (5) then the values

$$j_m := \frac{4\left(d_m^2+1\right)^3}{27\,d_m^2},\ d_m^2 := d^2(\beta_m^2),\ \beta_m^2 := \frac{s_m(-\beta)-s_m(0)}{s_m(-1/\beta)-s_m(0)},\ 0 \le m \le n, \tag{8}$$

$$s_m(x) := n\,x - \frac{(6\,x^2+\alpha\,x+2)\,r'_{m\,n}(x)}{r_{m\,n}(x)},^{16}\ \alpha := 4\left(\beta+\frac{1}{\beta}\right),$$

are the $(n+1)$ roots of the modular equation of level n.[17] Evidently, each such root j_m is invariant as β_m^2 is subjected to the action of the triangle group S_3, which is generated by the two inversions S and T given in (6). This action on β_m^2 corresponds to the action of S_3 as the permutation group of the three symbols $\{0,\beta,1/\beta\}$, appearing on the right hand side of the defining expression for β_m^2. One might be satisfied to verify that a value of one of the roots j_m would coincide with $j(n\tau)$. The elliptic curves $\mathbb{E}_\beta$ and $\mathbb{E}_{\beta_m}$ are said to be related by *cyclic isogeny* of degree n.

The projective special linear group $G_n := \mathrm{PSL}(2,\mathbb{Z}_\mathrm{n})$, where $\mathbb{Z}_n$ is the (prime) field of integers modulo n (which we had earlier introduced), is the Galois group of the modular equation of level n. Not merely a Galois group in the conventional sense, but is the Galois group in a most spectacular sense. Galois, who was apparently the discoverer of finite fields, indicated, in his last letter [13], sufficient and necessary condition for *depressing* the degree of the modular equation of prime level.[18] For this very purpose he did introduce the, being discussed, projective special linear groups over prime fields G_n, and observed that they were simple for all primes strictly exceeding the prime 3.[19] For primes $n \ge 5$, he pointed out the three exceptions for which the groups G_n possessed subgroups of indices coinciding with the cardinality of the field n. These

$y^4 x) - 26898488858380731577417728000\ (x^3 y^2 + y^3 x^2) - 1284733132841424456253440\ (x^4 + y^4) + 192457934618928299655108231168000\ (x^3 y + y^3 x) - 5110941777552418083110765199360000\ x^2 y^2 - 280244777828439527804321565297868800\ (x^3 + y^3) - 36554736583949629295706472332656640000\ (x^2 y + y^2 x) - 6692500042627997708487149415015068467200\ (x^2 + y^2) + 264073457076620596259715790247978782949376\ x\ y - 53274330803424425450420160273356509151232000\ (x+y) - 141359947154721358697753474691071362751004672000.$

Our reason for using the asterisk is to point out that $j(i)$ was assumed to equal 12^3. There is no sound justification for this "popular choice", and so if we switch to the "correct" normalization with $j(i) = 1$, then the corresponding polynomials $\Phi_3(x,y)$ and $\Phi_5(x,y)$ become:

$\Phi_3(x,y) = 2176782336\ x^3 y^3 - 2811677184\ (x^3 y^2 + y^3 x^2) - 729\ (x^4 + y^4) + 779997924\ (x^3 y + y^3 x) - 1886592284694\ x^2 y^2 - 15552000\ (x^3 + y^3) - 3754781568000\ (x^2 y + y^2 x) - 110592000000\ (x^2 + y^2) + 188194816000000\ x\ y - 262144000000000\ (x+y),$

$\Phi_5(x,y) = 8916100448256\ x^5 y^5 - 19194382909440\ (x^5 y^4 + y^5 x^4) + 13589034024960\ (x^5 y^3 + y^5 x^3) - 4974647446705766400\ x^4 y^4 - 3505336473600\ (x^5 y^2 + y^5 x^2) - 1864147879042619904\,00\ (x^4 y^3 + y^4 x^3) - x^6 - y^6 + 246683410950\ (x^5 y + y^5 x) - 383083609779811215375\ (x^4 y^2 + y^4 x^2) + 441206965512914835246100\ x^3 y^3 - 1136117760\ (x^5 + y^5) - 74387615108118528000\ (x^4 y + y^4 x) - 155662551263777381813760\,00\ (x^3 y^2 + y^3 x^2) - 430254526762844160\ (x^4 + y^4) + 6445377289996473512755200\,0\ (x^3 y + y^3 x) - 17116440602335505090150400\,00\ x^2 y^2 - 543133154340209262854144\,00\ (x^3 + y^3) - 70845528472506632188723200\,00\ (x^2 y + y^2 x) - 7506084169270500746330112\,00\ (x^2 + y^2) + 29617595563122405481849552896\ x\ y - 345779556064876091041382\,4000\ (x+y) - 530962617127336072236236\,8000.$

Aided with computers, Andrew V. Sutherland went on to calculate the coefficients of three hundred modular polynomials, which he made generously accessible at https://math.mit.edu/~drew/ClassicalModPolys.html.

[15] So, in fact, it might be viewed as a polynomial over the ring $\mathbb{Z}[j(\tau)]$.

[16] As before, the prime mark denotes differentiation with respect to the argument x, as β is assumed to be fixed.

[17] More details are given in author's article "Multiplication and division on elliptic curves, torsion points and roots of modular equations", which is accessible at http://www.ccas.ru/depart/mechanics/TUMUS/Adlaj/ECMD.pdf.

[18] The nowadays-established term "depressing" means lowering. 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.

[19] The very concept of simplicity, being again introduced by Galois, provides the basic principle in classifying (finite)

were the primes 5, 7 and 11. For any prime n strictly exceeding 11, proper subgroups of index $n+1$, and no lower (as Galois had also shown), are guaranteed to exist in G_n. Equivalently said,[20] a modular equation, of prime level $n \geq 5$, is depressible, from degree $n+1$ to degree n (and no lower), iff $n \in \{5,7,11\}$. Via explicitly constructing a permutation representation for the three exceptional groups, embedding them, respectively, in the three alternating groups A_5, A_7 and A_{11},[21] Galois must, in particular, be solely credited for solving the general quintic via exhibiting it as a modular equation of level 5.

4. AN APPLICATION: SOLVING THE QUINTIC

While Galois' contribution for formulating sufficient and necessary criterion for solubility of an algebraic equation via radicals was brought to light by Liouville, his decisive contribution to actually solving the quintic (before Hermite and Klein did) is, surprisingly, too poorly recognized (if not at all unrecognised!).[22] Betti, in 1851 [10], futily asked Liouville not to deprive the public any longer of Galois' (unpublished) results, and, in 1854 [11], went on to show that Galois' construction yields a solution to the quintic via elliptic functions.[23] One might associate with each quintic, given in Bring-Jerrard form, a corresponding value for the (Jacobi) elliptic modulus β, as Hermite did, in 1858 [14], implementing this very Galois' construction, which time has come to clarify. 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.[24] Galois did not (in his last letter) write down

groups. We note here that the projective special linear group is simple for all finite, not necessarily prime, fields except the fields $\mathbb{Z}_2$ and $\mathbb{Z}_3$. Galois, thereby, initiated 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).

[20] The equivalence, of statement that follows to the few statements preceding it, was established by Galois.

[21] For $n = 5,7,11$, the subgroup of index n in G_n turns out to be isomorphic to A_4, S_4 and A_5, respectively. These are precisely the symmetry groups of the platonic solids. The tetrahedron, being self-dual, has A_4 as its symmetry group. S_4 is the symmetry group for the hexahedron and the octahedron, whereas A_5 is the symmetry group for the dodecahedron and the icosahedron.

[22] Galois' brother Alfred and schoolmate Auguste Chevalier managed to involve Liouville (who was 135 weeks elder to Galois) in disentangling the manuscripts, which they faithfully copied and forwarded to several mathematicians (including Gauss and Jacobi). Liouville acknowledged in September 1843 that he "recognized the entire correctness of the method", which was, subsequently (in 1846), published in the Journal de Mathématiques Pures et Appliquées XI, giving birth to Galois theory. Liouville declared an intention to proceed with publishing the rest of Galois' papers. Yet, most unfortunately, subsequent publication never ensued, and neither Gauss nor Jacobi has ever fulfilled Galois modest request to merely announce the significance (tacitly alleviating the burden of judging the correctness) of his (not necessarily published) contributions. In 1847, Liouville published (instead) his own paper "Leçons sur les fonctions doublement périodiques".

[23] 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)."

[24] 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 $n = 7$ or $n = 11$, allows an alternative, as will, next, be exhibited.

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 $n=7$ and $n=11$, 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 $n=5$, an alternative might be presented for $n=7$, which is $\{(0,\infty), (1,5), (2,3), (4,6)\}$, and for $n=11$, 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 Γ, consisting of linear fractional transformations congruent to the identity modulo 2, is β^2. A fundamental domain $\Gamma_2\backslash\mathscr{H}$ for the action of Γ_2, might be obtained by subjecting a fundamental domain $\Gamma\backslash\mathscr{H}$ (of Γ) to the action of the quotient group $\Gamma/\Gamma_2 \cong S_3$.[25] In particular, β^2 viewed as function on $\mathscr{H}$, is periodic, with period 2. The definition of the modular equation, initially introduced for the invariant j, might be extended to other invariants such as β^2 or $\beta^{1/4}$. Sohnke, in a remarkable work [19], 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).[26] The modular polynomial for $\beta^{1/4}$, of level 5, is

$$\phi_5(x,y) := x^6 - y^6 + 5\,x^2\,y^2\,(x^2-y^2) + 4\,x\,y\,(1-x^4\,y^4),^{27} \tag{9}$$

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 $\tau\in\mathscr{H}$, 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

$$x^5 - x + c,\;\; c := \frac{2\,(1+\beta^2)}{5^{5/4}\,\sqrt{\beta(1-\beta^2)}} = \frac{2\,(1+y^8)}{5^{5/4}\,y^2\,\sqrt{1-y^8}},^{28}$$

is

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

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

[26] 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!

[27] A diligent reader would notice a sign discrepancy in our equation once compared with the equation derived in [19].

[28] 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 $\Gamma_2\backslash\mathscr{H}$ 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 $r_{m5}(x) =: x^2 - \lambda_m x + \mu_m$, $0 \le m \le 5$. 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 $y_m^8 = \beta_m^2$, as given in (8), might be rewritten for the special case $n = 5$ 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

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

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

The roots γ_m and $2\cdot\gamma_m$, $0 \le m \le 5$, 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 (2) along with the doubling formula (3).

Let us conclude with a couple of examples, so let $\tau = 2i$, $\beta = \left(\sqrt{2} - 1\right)^2$. The corresponding quintic is

$$x^5 - x + \frac{3\sqrt{2\sqrt{2}}}{5\sqrt{\sqrt{5}}}.$$

The corresponding division polynomial $r_5(x)$ factors over $\mathbb{Q}[\sqrt{5}]$ into three quartic polynomial-factors:

$$r_5(x) = \left(x^4 + 4\left(3 + \sqrt{5}\right)x^3 + 6\left(5 + 2\sqrt{5}\right)x^2 - 4\left(29 + 13\sqrt{5}\right)x + 9 + 4\sqrt{5}\right)$$

$$\left(x^4 + \frac{18\,x^2}{5} + \frac{8\,x}{5} + \frac{1}{5}\right)\left(x^4 + 4\left(3 - \sqrt{5}\right)x^3 + 6\left(5 - 2\sqrt{5}\right)x^2 - 4\left(29 - 13\sqrt{5}\right)x + 9 - 4\sqrt{5}\right).$$

Each (quartic) factor is an elliptic polynomial pair product. They are (with their argument omitted) $r_{55}r_{50}$, $r_{54}r_{51}$ and $r_{53}r_{52}$, respectively. The (corresponding) modular polynomial $\phi_5\left(x, y = \beta^{1/4} = \sqrt{\sqrt{2} - 1}\right)$ factors, over $\mathbb{Q}[y]$, into a quadratic and a quartic polynomial-factor:

$$\phi_5(x, y) = \left(x^2 + y^{-2}\right)\left(x^4 + 4\,y^3\left(1 - y^2 x^2\right)x - 2\,y^4 x^2 - y^8\right),$$

and the six roots (of the modular polynomial) might be accordingly expressed and ordered:

$$y_0 = -\sqrt{\frac{\sqrt{2}\left(2 + \sqrt{5}\right) - \chi(-1)}{\chi(1)}},\ y_1 = -i\sqrt{\sqrt{2} + 1},\ y_2 = \sqrt{\frac{\sqrt{2}\left(2 - \sqrt{5}\right) - \chi(i)}{\chi(-i)}}.$$

$$y_3 = \sqrt{\frac{\sqrt{2}\left(2 - \sqrt{5}\right) - \chi(-i)}{\chi(i)}},\ y_4 = i\sqrt{\sqrt{2} + 1},\ y_5 = \sqrt{\frac{\sqrt{2}\left(2 + \sqrt{5}\right) - \chi(1)}{\chi(-1)}},$$ [29]

[29] The image of the square root is assumed, here (but not necessarily earlier!), to be unambigiously taken in the right half-plane, including the boundary of the upper quadrant but excluding it for the lower quadrant.

where

$$\chi(\epsilon) := 3 + 2\sqrt{\sqrt{5}\,\epsilon}.$$

Exploiting the identities

$$\beta = \left(\sqrt{2}-1\right)^2 = \left(\sqrt{10}-3\right)\left(\sqrt{5}-2\right)\left(3\sqrt{2}+\sqrt{5}-2\right),$$

$$\chi(1)\,\chi(-1) = \left(\sqrt{5}-2\right)^2 = \left(3\sqrt{2}+\sqrt{5}+2\right)\left(3\sqrt{2}-\sqrt{5}-2\right).$$

$$\chi(i)\,\chi(-i) = \left(\sqrt{5}+2\right)^2 = \left(3\sqrt{2}+\sqrt{5}-2\right)\left(3\sqrt{2}-\sqrt{5}+2\right),$$

along with the alternative expressions

$$y_0 = -\frac{\sqrt{-(i+1)\chi(i)}+\sqrt{(i-1)\chi(-i)}}{\sqrt{2\,\chi(1)}},\ y_5 = \frac{\sqrt{(i-1)\chi(i)}+\sqrt{-(i+1)\chi(-i)}}{\sqrt{2\,\chi(-1)}},$$

$$y_2 = \frac{\sqrt{2\,\chi(-i)}}{\sqrt{(1+i)\chi(1)}-\sqrt{(1-i)\chi(-1)}},\ y_3 = \frac{\sqrt{2\,\chi(i)}}{\sqrt{(1-i)\chi(1)}-\sqrt{(1+i)\chi(-1)}},$$

one finds out that

$$x_1 = -8\sqrt{5}\,\beta,$$

and, so, a root of our quintic is

$$\frac{-8\sqrt{5}\,\beta}{2\sqrt{5\sqrt{5}\,\beta(1-\beta^2)}} = \frac{-2}{\sqrt{\sqrt{10}}}.$$

Along the way, we might calculate the (five) discriminants

$$d^2(\beta^2) = d^2(\beta_1^2) = d^2(\beta_4^2) = 32,$$

$$d^2(\beta_0^2) = \frac{32\,\chi(-1)}{\chi(1)^5},\ d^2(\beta_2^2) = \frac{32\,\chi(i)}{\chi(-i)^5},\ d^2(\beta_3^2) = \frac{32\,\chi(-i)}{\chi(i)^5},\ d^2(\beta_5^2) = \frac{32\,\chi(1)}{\chi(-1)^5},$$

observing that they are sixth powers of the respective values

$$2^{5/6},\ \frac{\sqrt{5}-1}{2^{1/6}\chi(1)},\ \frac{\sqrt{5}+1}{2^{1/6}\chi(-i)},\ \frac{\sqrt{5}+1}{2^{1/6}\chi(i)},\ \frac{\sqrt{5}-1}{2^{1/6}\chi(-1)},$$

and, so using equation (5), we might calculate five special values of the modular invariant:

$$j\left(\frac{5\,i}{2}\right) = j_0 = \left(\sqrt{5}+2\right)^{20}\chi(-1)^6\left(238\sqrt{5}-60\sqrt{\sqrt{5}}-\frac{861}{2}\right)^3,\ j(2\,i) = j_1 = j_4 = \left(\frac{11}{2}\right)^3,$$

$$j\left(\frac{5\,i-1}{4}\right) = j_2 = -\left(\sqrt{5}-2\right)^{20}\chi(i)^6\left(238\sqrt{5}-60\sqrt{\sqrt{5}\,i}+\frac{861}{2}\right)^3,$$

$$j\left(\frac{5\,i+1}{4}\right) = j_3 = -\left(\sqrt{5}-2\right)^{20}\chi(-i)^6\left(238\sqrt{5}+60\sqrt{\sqrt{5}\,i}+\frac{861}{2}\right)^3,$$

$$j(10\,i) = j_5 = \left(\sqrt{5}+2\right)^{20}\chi(1)^6\left(238\sqrt{5}+60\sqrt{\sqrt{5}}-\frac{861}{2}\right)^3.$$ [30]

[30] These special values might be expressed as cubes if one notes that $\sqrt{5}\pm 2 = \left(\sqrt{5}\pm 1\right)^3/8$.

We might now let $\tau = i$, $\beta = \sqrt{2}$, and observe that the modular polynomial $\phi_5\left(x, y = \beta^{1/4} = \sqrt{\sqrt{\sqrt{2}}}\right)$ factors, over $\mathbb{Q}[y]$, into a quadratic and a quartic polynomial-factor:

$$\phi_5\left(x, y = \sqrt{\sqrt{\sqrt{2}}}\right) = \left(x^2 - y^5 x + y^2\right)\left(x^4 - 3\,y^5 x^3 - 2\,y^2 x^2 + y^7 x - y^4\right),$$

before confirming that the roots of the latter quartic polynomial-factor

$$\frac{\epsilon^2\sqrt{5}+1}{y^3\left(\epsilon\sqrt{\sqrt{5}}-1\right)},\ \epsilon = \{1, -i, i, -1\},$$

are, respectively, obtainable as fourth roots of the values

$$\frac{\sqrt{2}\left(\epsilon^2\sqrt{5}+2\right)}{\chi(-\epsilon)},$$

which, in turn, are (as they ought to be) the images of the four afore-calculated values β_0, β_2, β_3 and β_5 (where β was $3-2\sqrt{2}$) if subjected to the (fourth order) linear fractional transformation

$$\frac{1+\beta_m}{1-\beta_m},\ m \in \{0, 2, 3, 5\}.$$

The four corresponding values of the discriminants are

$$d^2\left(\frac{2\left(\epsilon^2\sqrt{5}+2\right)^2}{\chi(-\epsilon)^2}\right) = \frac{\chi(\epsilon)^5}{2\,\chi(-\epsilon)} = 32\left(\frac{\chi(\epsilon)}{\sqrt{5}-\epsilon^2}\right)^6.$$

Two more special values of the modular invariant are calculated by (reapplying) formula (5) to a discriminant from, firstly, the complex-conjugate ($\epsilon = \pm i$) pair, and, secondly, the real-valued ($\epsilon = \pm 1$) pair:

$$j\left(\frac{5\,i+1}{2}\right) = \left(\frac{2927-1323\sqrt{5}}{2}\right)^3,\ j(5\,i) = \left(\frac{2927+1323\sqrt{5}}{2}\right)^3.$$

One might infer, from equation (8), that the modular polynomial, of level 2, $\Phi_2(x, z)$ vanishes at

$$(x, z_l) = \frac{4}{27}\left(\frac{\left(d^2+1\right)^3}{d^2}, \frac{\left(d_l^2+1\right)^3}{d_l^2}\right),\ l \in \{0, 1, 2\},$$

where

$$\left(d_0^2, d_1^2, d_2^2\right) = 16\left(\frac{1}{d^2}, -\frac{d}{\beta^3}, \beta^3 d\right),\ d = d(\beta) = \beta - \frac{1}{\beta}.$$

For $x \in \{j_0, j_2, j_3, j_5\}$ we have already calculated the (two) corresponding values z_0. Concluding, we calculate the corresponding values z_1 and z_2, so put

$$\psi(\delta,\epsilon) := \frac{\sqrt{5}+1}{8\,\chi(\epsilon)^6}\left(57272 - 34011\,\delta\sqrt{2} + 4\left(101 - 5463\,\delta\sqrt{2}\right)\epsilon^2\sqrt{5} + \right.$$

$$\left. -18\left(800 + 111\,\delta\sqrt{2} + 4\left(100 + 27\,\delta\sqrt{2}\right)\epsilon^2\sqrt{5}\right)\epsilon\sqrt{\sqrt{5}}\right) =$$

$$\frac{\left(\epsilon^2\sqrt{5}+1\right)^{37}}{2^{39}}\Bigl(1190448488-858585699\,\delta\sqrt{2}+540309076\,\epsilon^2\sqrt{5}-374537880\,\delta\,\epsilon^2\sqrt{10}+$$

$$-\epsilon\sqrt{\sqrt{5}}\Bigl(693172512-595746414\,\delta\sqrt{2}+407357424\,\epsilon^2\sqrt{5}-240819696\,\delta\,\epsilon^2\sqrt{10}\Bigr)\Bigr),$$

and observe that

$$z_1(j_m)=\frac{4}{27}\left(\frac{2^{8/3}d(\beta_m)^{2/3}}{\beta_m^2}-\frac{\beta_m}{2^{4/3}d(\beta_m)^{1/3}}\right)^3=\psi(-1,\epsilon)^3,$$

$$z_2(j_m)=\frac{4}{27}\left(2^{8/3}\beta_m^2\,d(\beta_m)^{2/3}+\frac{1}{2^{4/3}\beta_m\,d(\beta_m)^{1/3}}\right)^3=\psi(1,\epsilon)^3,$$

where $\epsilon\in\{1,-i,i,-1\}$ correspond, respectively, to $m\in\{0,2,3,5\}$, as before, and verify that

$$j\left(\frac{5\,i}{4}\right)=z_1(j_0)=\psi(-1,1)^3,\ j\left(\frac{20\,i+5}{17}\right)=z_1(j_2)=\psi(-1,-i)^3,$$

$$j\left(\frac{20\,i-5}{17}\right)=z_1(j_3)=\psi(-1,i)^3,\ j\,(20\,i)=z_1(j_5)=\psi(-1,-1)^3,$$

$$j\left(\frac{5\,i+2}{4}\right)=z_2(j_0)=\psi(1,1)^3,\ j\left(\frac{20\,i+4}{13}\right)=z_2(j_2)=\psi(1,-i)^3,$$

$$j\left(\frac{20\,i-4}{13}\right)=z_2(j_3)=\psi(1,i)^3,\ j\left(\frac{10\,i+1}{2}\right)=z_2(j_5)=\psi(1,-1)^3.$$

Few of these special values were first presented in [5].

5. CONCLUSION

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,[31] and Galois is merely mentioned, along with Abel, for determining that the quintic is not generally solvable via radicals. With this paper, we hope that this (crippled) view of Galois (deeply constructive and far from fully appreciated) theory would finally come to an end. A recent exapmle concerns an expression, for "the speed of precession" of a freely moving triaxial rigid body, which attainment relied on identifying the function field where such a general expression would lie, based on exploring its symmetries [7]. Only a (minor) consequence of such Galois guided algebraic approach, was identifying a Galois axis fixed within a triaxial rigid body and distinct from any of its three main axes of inertia. Marvelously, Galois axis rotates uniformly during the critical motion (whether or not such motion is said to be either stable or unstable and whether or not the body "flips"), as shown in [8].

[31] 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.

References

1. S. F. Adlaj, "Iteratsionnyi algoritm vychisleniya ellipticheskogo integrala" [Iterative elliptic integral algorithm], *Zadachi issledovaniya ustoichivosti i stabilizatsii dvizheniya*, pp. 104–110, 2011, [Online]. Available: http://www.ccas.ru/depart/mechanics/TUMUS/z_SBORNIKI/issues/2011_4Adlaj.pdf (in Russian).
2. S. Adlaj, "Eighth lattice points," arXiv:1110.1743 [math.GM], Oct. 2011.
3. S. Adlaj, "An inverse of the modular invariant," arXiv:1110.3274 [math.GM], Oct. 2011.
4. S. Adlaj, "Mechanical interpretation of negative and imaginary tension of a tether in a linear parallel force field," in *Selected works of International Scientific Conference on Mechanics “Sixth Polyakhov Readings,”* St. Petersburg, Russia, Jan. 31–Feb. 3, 2012, pp. 13–18.
5. S. Adlaj, "Torsion points on elliptic curves and modular polynomial symmetries," presented on at the Joined MSU-CCRAS Computer Algebra Seminar, Moscow, Russia, Sep. 24, 2014 [Online]. Available: http://www.ccas.ru/sabramov/seminar/lib/exe/fetch.php?media=adlaj140924.pdf.
6. S. Adlaj, "An analytic unifying formula of oscillatory and rotary motion of a simple pendulum," in *Special edition dedicated to the 70th birthday of J. J. Sławianowski*, Sofia, Bulgaria: Avangard Prima, 2015, pp. 160–171.
7. S. Adlaj, "Dzhanibekov’s flipping nut and Feynman’s wobbling plate," in *Polynomial Computer Algebra International Conference*, St. Petersburg, Russia, Apr. 18–23 2016, pp. 10–14 [Online]. Available at http://pca.pdmi.ras.ru/2016/abstracts_files/PCA2016SA.pdf.
8. S. F. Adlaj, S. A. Berestova, N. E. Misyura, and E. A. Mityushov "Illustrations of rigid body motion along a separatrix in the case of Euler-Poinsot," *Computer tools in education*, no. 2, 2018, pp. 5–13; doi:10.32603/2071-2340-2-5-13.
9. S. F. Adlaj, *Ravnovesie niti v lineinom parallel’nom pole sil: Klassifikatsiya i issledovanie ustoichivosti ravnovesnykh form niti v lineinom parallel’nom pole sil* [Thread balance in a linear parallel field of forces: Classification and study of the stability of the equilibrium forms of a thread in a linear parallel field of forces], LAMBERT Academic Publishing, 2018.
10. E. Betti, "Sopra la risolubilità per radicali delle equazioni algebriche irriduttibili di grado primo," *Dagli Annali di Scienze matimatiche e fisiche*, **II** (Roma, 1851), pp. 5–19.
11. E. Betti, "Un teorema sulla risoluzione analitica delle equazioni algebriche," *Dagli Annali di Scienze matimatiche e fisiche*, **V** (Roma, 1854), pp. 10–17.
12. D. Cox, "The arithmetic-geometric mean of Gauss," *L’Enseignement Mathématique*, vol. 30, 1984, pp. 275–330; doi:10.1007/978-3-319-32377-0_3.
13. É. Galois, "Lettre de Galois à M. Auguste Chevalier," *Journal de Mathématiques Pures et Appliquées* XI, 1846, pp. 408–415.
14. C. Hermite, "Sur la résolution de l’équation du cinquième degré," *Comptes Rendus de l’Académie des Sciences*,, XLVI (I), 1858, pp. 508–515.
15. M. B. Kiernan, "The development of Galois theory from Lagrange to Artin. Communicated by M. Kline," *Arch. Rational Mech.*, vol. 8, no 1–2, 1971; doi:10.1007/BF00327219.
16. H. Ruhland, "The Inverse of the Modular Invariant," [Online]. Available: http://www.ccas.ru/depart/mechanics/TUMUS/Adlaj/TheInverse.pdf.
17. J-P. Serre, *A Course in Arithmetic*, New York: Springer-Verlag, 1973.
18. G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton, NJ: Princeton University Press, 1981.
19. L. A. Sohnke, "Aequationes modulares pro transformatione Functionum Ellipticarum," *Journal für die reine und angewandte Mathematik*, vol. 16, 1837, pp. 97–130, [Online]. Available: http://eudml.org/doc/146989

Received 19.06.2018, the final version — 26.07.2018.

Компьютерные инструменты в образовании, 2018
№ 4: 11–26
УДК: 511.238
http://ipo.spb.ru/journal
doi:10.32603/2071-2340-4-11-26

О ВТОРОМ МЕМУАРЕ ПОСЛЕДНЕГО ПИСЬМА ЭВАРИСТА ГАЛУА

Адлай С. Ф.

Федеральный научно-исследовательский центр «Информатика и управление»
Российской академии наук, Москва, Россия

Аннотация

Последнее письмо Эвариста Галуа, адресованное Огюсту Шевалье, накануне (так называемой) дуэли 30 мая 1832 года (которая, пожалуй, проще и точнее была охарактеризована как убийство Альфредом, не допустившим на следующий день священника к своему старшему брату Эваристу в его последние мгновения), было написано на семи страницах и разделено на три мемуара. Первый мемуар занимает чуть меньше двух страниц. Впоследствии сей мемуар стал известен как теория Галуа (о которой, в частности, рассказал Мелвин Кирнан). Однако, Галуа продолжил своё письмо потрясающе удивительными конструкциями во втором мемуаре, который занял чуть более двух страниц. Третий (и самый длинный!) мемуар начинается на пятой странице и остаётся загадочным и нерасшифрованным, но он, несомненно, вдохновил Александра Гротендика сформулировать свою гипотезу о периодах. Письмо заканчивается абзацем о последних «главных размышлениях», касающихся «приложений теории неоднозначности к трансцендентному анализу», где Галуа преподносит нам последнюю загадку, говоря, что «мы можем тотчас же рассмотреть большое множество выражений». К сожалению, неумолимость давлеющего времени не позволила ему привести какие-либо конкретные примеры, а смогла лишь дать краткие последние инструкции, о том, что делать с письмом. Несмотря на это, многие «историки» назойливо и примитивно твердят нам (и друг другу), что мы не должны «переоценивать» значение письма, которое (вопреки их советам) красноречиво и правдиво описывалось Германом Вейлем как «самая значимая рукопись во всей истории человечества»!

Ключевые слова: *эссенциальная эллиптическая функция, понижение степени модулярного уравнения, проективная специальная линейная группа над простым полем, эллиптические и коэллиптические полиномы, решение общего квинтического уравнения.*

Цитирование: Adlaj S. F. On the Second Memoir of Évariste Galois’ Last Letter // Компьютерные инструменты в образовании. 2018. № 4. С. 11–26. doi:10.32603/2071-2340-4-11-26

Поступила в редакцию 19.06.2018, окончательный вариант — 26.07.2018.

Адлай Семён Франкович, научный сотрудник, Сектор теории устойчивости и механики управляемых систем, Отделение моделирования сложных физических и технических систем, Вычислительный центр

им А. А. Дородницына ФИЦ ИУ РАН; 119333, Россия, Москва, ул. Вавилова, д. 40, semjonadlaj@gmail.com

Semjon F. Adlaj,
Scientific Researcher, Section of Stability Theory and Mechanics of Controlled Systems, Division of Complex Physical and Technical Systems Modeling, Computing Center of the Federal Research Center "Informatics and Control", Russian Academy of Sciences;
119333, Russia, Moscow, Vavilov Street 40,
semjonadlaj@gmail.com