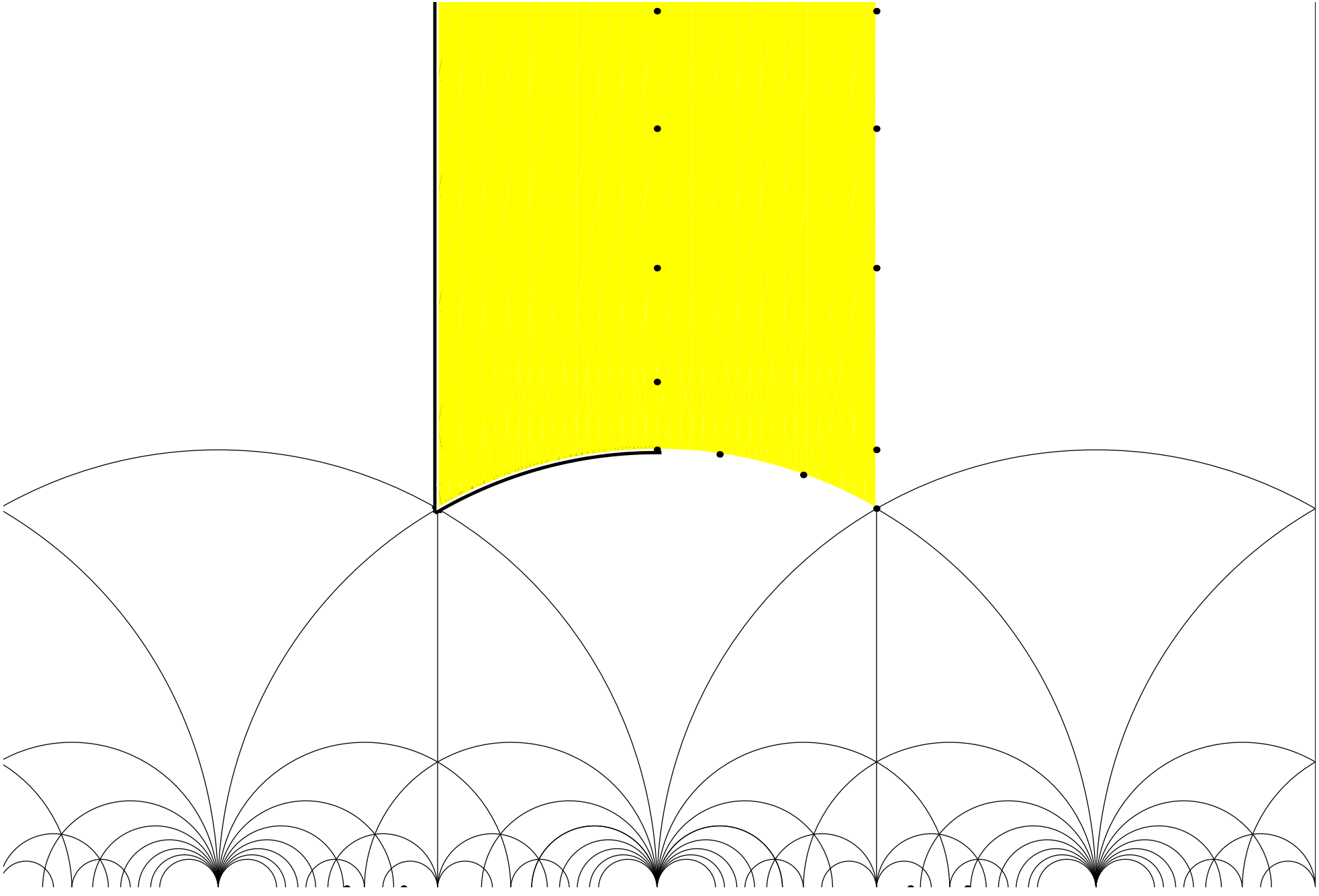
Back to solving the quintic, depression and Galois primes

Semjon Adlaj

CC FRC "Informatics and Control" of the RAS, Moscow, Russia

PCA annual conference 2018, April 16-21

The fundamental domain (for $\Gamma\backslash(\mathbb{H}\cup\mathbb{P}^1(\mathbb{Q}))$)



An explicit analytic fast inverse of the modular invariant

An explicit analytic inverse k of the modular invariant j was given in [2] as a composition

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

where

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

$$k_2(x) := \frac{3}{2}\left(\frac{x}{k_3(x)} + k_3(x)\right) - 1,$$

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

and $M(x)$ is the arithmetic-geometric mean of 1 and x.

Key properties of the inverse of the modular invariant

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 $\mathrm{PSL}(2,\mathbb{Z})$. 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 $\mathrm{PSL}(2,\mathbb{Z})$ 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,

$$\forall x \in \mathbb{C},\ j \circ k\,(x) = x,$$ [1]

for the modular invariant j does not separate points, in its domain, as long as they differ by the action of the modular group $\mathrm{PSL}(2,\mathbb{Z})$, and no troubles arise in extending the latter equality to the whole Riemann sphere, including the point at (complex) infinity.

---

[1] 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.

Verifying the formula for the inverse k at 0 and 1: the image (under j) of the "corners" of the fundamental domain

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 $j(i) = 1$.[2] So, we point out that the (set) values of the composition, $k_1 \circ k_2$ at 0 and 1, coincide with set values of the elliptic moduli β at $\tau = \zeta$ and $\tau = i$, which, respectively, are the four values $\beta \in \{\pm i\zeta, \pm i\zeta^2\}$ and the six values $\beta \in \{\pm i, \pm 1/\sqrt{2}, \pm\sqrt{2}\}$. 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 $i \in k(1) = k_0 \circ k_1(1/2)$.[3]

---

[2] We denoted by ζ a primitive cube root of unity, so $\zeta^3 = 1 \neq \zeta$.

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

The modular equation

Assume, unless indicated otherwise, 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, Φ_n is symmetric in its two variables, that is $\Phi_n(x, z) = \Phi_n(z, x)$. When τ is 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 $\mathbb{Q}(j(\tau))$,[4] and we shall call its roots, *the roots of the modular equation of level n*.

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

The modular equation of level 3 and 5

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

$$\Phi_3^*(x,y) = x^3y^3 - 2232\,(x^3y^2+x^2y^3) - x^4 - y^4 + 1069956\,(x^3y+xy^3) - 2587918086\,x^2y^2 - 36864000\,(x^3+y^3) - 8900222976000\,(x^2y+y^2x) - 452984832000000\,(x^2+y^2) + 770845966336000000\,xy - 1855425871872000000000\,(x+y).$$ (Smith 1879)

$$\Phi_5(x,y) = 8916100448256\,x^5y^5 - 19194382909440\,(x^5y^4+y^5x^4) + 13589034024960\,(x^5y^3+y^5x^3) - 4974647446705766400\,x^4y^4 - 3505336473600\,(x^5y^2+y^5x^2) - 186414787904261990400\,(x^4y^3+y^4x^3) - x^6 - y^6 + 246683410950\,(x^5y+y^5x) - 38308360977981121537 5\,(x^4y^2+y^4x^2) + 4412069655129148352461 00\,x^3y^3 - 1136117760\,(x^5+y^5) - 74387615108118528000\,(x^4y+y^4x) - 1556625512637738181376000\,(x^3y^2+y^3x^2) - 430254526762844160\,(x^4+y^4) + 64453772899964735127552000\,(x^3y+y^3x) - 171164406023355050901504 0000\,x^2y^2 - 54313315434020926285414400\,(x^3+y^3) - 70845528472506632188723 20000\,(x^2y+y^2x) - 75060841692705007463301 1200\,(x^2+y^2) + 29617595563122405481849552896\,xy - 34577955606487609104138240 00\,(x+y) - 53096261712733607223623680 00.$$

$$\Phi_5^*(x,y) = x^5y^5 - 3720\,(x^5y^4+y^4x^5) + 4550940\,(x^5y^3+y^5x^3) - 1665999364600\,x^4y^4 - 2028551200\,(x^5y^2+y^5x^2) - 107878928185336800(x^4y^3+y^4x^3) - x^6 - y^6 + 246683410950\,(x^5y+y^5x) - 38308360977981121537 5\,(x^4y^2+y^4x^2) + 4412069655129148352461 00\,x^3y^3 - 1963211489280\,(x^5+y^5) - 1285417989068288163840 00\,(x^4y+y^4x) - 2689848885838073157741772 8000\,(x^3y^2+y^3x^2) - 1284733132841424456253440\,(x^4+y^4) + 1924579346189282996551082311 68000\,(x^3y+y^3x) - 5110941777552418083110765199360000\,x^2y^2 - 2802447778284395278043215652978 68800\,(x^3+y^3) - 3655473658394962929570647233265664 0000\,(x^2y+y^2x) - 6692500042627997708487149415015068467200\,(x^2+y^2) + 2640734570766205962597157902479787829493 76\,xy - 5327433080342442545042016027335650915123 2000\,(x+y) - 1413599471547213586977534746910713627510046 72000.$$ (Berwick 1916)

The Galois group of the modular equation

In his last letter [4], 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,[5] and observed that it was simple whenever the prime p strictly exceeded the prime 3.

[5] 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 $\mathrm{PSL}(2,\mathbb{F}_p)$, where we assume the index p to denote a prime.

Galois criterion for depressing the degree of the modular equation

A modular equation, of prime level $n \geq 5$, is depressible, from degree $n+1$ to degree n (and no lower), iff (its group) $\mathrm{PSL}(2, \mathbb{Z}_n)$ possesses a subgroup of index n 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},[6] Galois must, in particular, be solely credited for solving the general quintic via exhibiting it as a modular equation of level 5.

[6] For $n = 5, 7, 11$, the subgroup of index n in $\mathrm{PSL}(2, \mathbb{Z}_n)$ turn 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.

Galois constructions of subgroups of G_p of index p

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.

Galois wrote down only the first pair-set for each of the two remaining cases, where $p = 7$ and $p = 11$, respectively: $\{(0,\infty),(1,3),(2,6),(4,5)\}$,$\{(0,\infty),(1,2),(3,6),(4,8),(5,10),(9,7)\}$.

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 $\{(0,\infty),(1,6),(3,7),\ (4,2),(5,8),(9,10)\}$.

Elliptic polynomials as factors of the division polynomial

Denote by $\mathbb{F} := \mathbb{Q}(\beta + 1/\beta)$ the base field of the polynomial r_n, which roots are the first coordinates of the points (on $\mathbb{E}_\beta$) of order n. Call r_n the division polynomial of level n. 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*

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

where the dot is used to indicate the multiplication of the first coordinate to yield the first coordinate of the l-multiple (on $\mathbb{E}_\beta$).

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:

$$r_n(x) = \prod_{m=1}^{n+1} r_{mn}(x).$$

Coelliptic polynomials

The group of automorphisms $\mathrm{Aut}(\mathbb{F}[\gamma_m]/\mathbb{F})$ of each field extension $\mathbb{F}[\gamma_m]/\mathbb{F}$, $1 \leq m \leq n+1$, is cyclic of order $(n-1)/2$. One might, in fact, establish the isomorphism

$$\mathrm{Aut}\left(\mathbb{F}[\gamma_m]/\mathbb{F}\right) \cong \mathbb{Z}_n^{\times}/\{\pm 1\},$$

where the group, on the right hand side of the isomorphism, denoted by $\mathbb{Z}_n^{\times}$ is the multiplicative subgroup of $\mathbb{Z}_n$: the (prime) field of integers modulo n. Put $q(x) := x^2 + (\beta + 1/\beta)\, x + 1$, and to each elliptic polynomial r_{mn} associate a coelliptic polynomial

$$t_m(x) := n\, x\, r_{m\,n}(x)^2 - 2\, q'(x)\, r'_{m\,n}(x)\, r_{m\,n}(x) +$$

$$+4\, q(x)\left(r'_{m\,n}(x)^2 - r''_{m\,n}(x)\, r_{m\,n}(x)\right).$$

Calculating the roots of the modular equation

Now, let (for a fixed $\tau \in \mathcal{D}$) the value of $j(\tau)$ be given by

$$(*) \qquad j(\tau) = \frac{4\left(d^2+1\right)^3}{27\,d^2},\ d^2 = d^2(\beta^2) := (\beta - 1/\beta)^2\,,$$

then the roots of the modular equation, of level n, are

$$(**) \qquad j_m := \frac{4\left(d_m^2+1\right)^3}{27\,d_m^2},\ d_m^2 := d^2(\beta_m^2),$$

$$\beta_m^2 := \frac{s_m(-\beta) - s_m(0)}{s_m(-1/\beta) - s_m(0)},\ 1 \le m \le n+1,$$

where $s_m(\cdot)$ is the n-th degree fractional transformation given by

$$s_m(x) := \frac{t_m(x)}{r_{m\,n}(x)^2}.$$

An action of S_3

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 by

$$S : x \mapsto \frac{1}{x}, \quad T : x \mapsto 1 - x.$$

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 verify that, indeed, the value of one of the roots j_m coincides with $j(n\tau)$, while the rest n of the $n+1$ roots satisfy the relation $j(n\,k\,(j_m)) = j(\tau)$. The elliptic curves $\mathbb{E}_\beta$ and $\mathbb{E}_{\beta_m}$ are said to be related by *cyclic isogeny* of degree n.

Three suppressed and forgotten "snapshots" of history

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.

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 had 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".

In 1851, in a paper published in Annali di Tortolini, Betti futily asked Liouville not to deprive the public any longer of Galois' (unpublished) results. Then, in 1854, Betti showed that Galois' construction yields a solution to the quintic via elliptic functions.

Solving the quintic (1 out of 4)

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 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 $\Gamma/\Gamma_2 \cong S_3$.[7] In particular, β^2 viewed as function on $\mathcal{H}$, is periodic, with period 2. Sohnke, in a remarkable work [6], 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 [3], inspired Hermite [5] 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 latter quotient group coincides with G_2 which is isomorphic with S_3.

Solving the quintic (2 out of 4)

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

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

Solving the quintic (3 out of 4)

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

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

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.

[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 $\tau \mapsto 2/(2-\tau)$.

Solving the quintic (4 out of 4)

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 $2\cdot\gamma_m$, $0 \le m \le 5$, 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].

Two examples (1 out of 6)

Let, for example, $\tau = 2\,i$, $\beta = \left(\sqrt{2}-1\right)^2$. 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) $r_5 r_0$, $r_4 r_1$ and $r_3 r_2$, 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:

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

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

where

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

Two examples (2 out of 6)

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

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

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

one finds out that

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

and, so, a root of our quintic is

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

Two examples (3 out of 6)

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 (*), we might calculate five special values of the modular invariant:

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

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

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

$$j(10\,i) = j_5 = \left(\sqrt{5}+2\right)^{20}\chi(1)^6\left(238\sqrt{5} + 60\sqrt{\sqrt{5}} - \frac{861}{2}\right)^3.$$ [9]

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

Two examples (4 out of 6)

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

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

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 examples (5 out of 6)

Two more special values of the modular invariant are calculated by (reapplying) formula (*) 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 (**), 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 this section, we calculate the corresponding values z_1 and z_2, so put

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

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

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

$$\left. -\epsilon\sqrt{\sqrt{5}}\left(693172512 - 595746414\,\delta\sqrt{2} + 407357424\,\epsilon^2\sqrt{5} - 240819696\,\delta\,\epsilon^2\sqrt{10}\right)\right) =$$

Two examples (6 out of 6)

$$= \frac{1}{8}\left(129569705555681708+57945333889427292\,\epsilon^2\sqrt{5}-\epsilon\sqrt{\sqrt{5}}\left(86648484409011792+38750380257176208\,\epsilon^2\sqrt{5}\right)+\right.$$

$$\left.-9\,\delta\sqrt{2}\left(10179957492752331+4552615392370507\,\epsilon^2\sqrt{5}-\epsilon\sqrt{\sqrt{5}}\left(6807747878350206+3044517405934206\,\epsilon^2\sqrt{5}\right)\right)\right).$$

Now 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 $m \in \{0,\ 2,\ 3,\ 5\}$ and verify that

$$j\left(\frac{5\,i}{4}\right) = z_1(j_0),\ j\left(\frac{20\,i+5}{17}\right) = z_1(j_2),\ j\left(\frac{20\,i-5}{17}\right) = z_1(j_3),\ j\,(20\,i) = z_1(j_5),$$

$$j\left(\frac{5\,i+2}{4}\right) = z_2(j_0),\ j\left(\frac{20\,i+4}{13}\right) = z_2(j_2),\ j\left(\frac{20\,i-4}{13}\right) = z_2(j_3),\ j\left(\frac{10\,i+1}{2}\right) = z_2(j_5).$$

Four special values of the modular invariant

Suppose that j is (correctly) normalized with $j(i) = 1$, then

$$j\left(\frac{4\,(5\,i \pm 1)}{13}\right) =$$

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

$$\left.\left. \pm i\sqrt{\sqrt{5}}\left(693172512 - 595746414\,\sqrt{2} - 407357424\,\sqrt{5} + 240819696\,\sqrt{10}\right)\right)\right)^{3},$$

$$j\left(\frac{5\,(4\,i \pm 1)}{17}\right) =$$

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

$$\left.\left. \pm i\sqrt{\sqrt{5}}\left(693172512 + 595746414\,\sqrt{2} - 407357424\,\sqrt{5} - 240819696\,\sqrt{10}\right)\right)\right)^{3}.$$

Two quotes from "Récoltes et Semailles" by Grothendieck

"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)."

"Mais au delà de ces différences accidentelles, je crois discerner à cette "marginalité" une cause commune, que je sens essentielle. Cette cause, je ne la vois pas dans des circonstances historiques, ni dans des particularités de "tempérament" ou de "caractère" (lesquels sont sans doute aussi différents de lui à moi qu'ils peuvent l'être d'une personne à une autre), et encore moins certes au niveau des "dons" (visiblement prodigieux chez Galois, et comparativement modestes chez moi). S'il y a bien une "parenté essentielle", je la vois à un niveau bien plus humble, bien plus élémentaire."

Several references and two pitifully pathetic (anti)references

1. Адлай С.Ф. *Итерационный алгоритм вычисления эллиптического интеграла* // Задачи исследования устойчивости и стабилизации движения. 2011. С. 104-110.

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`.

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

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

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

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

Кованцов Н. *Математика и романтика*. Киев: Вища школа, 1976, 96 с. (A mundane interpretation of Galois biography.)

Rothman T. *Genius and Biographers: The Fictionalization of Evariste Galois* // The American Mathematical Monthly, vol. 89, 1982, 84-106. (The latter article, sorrowfully, received the Lester R. Ford Writing Award, 1983).