Nice cubic polynomials: symmetry and arithmetic of the Lagrange resolvent

Jean-François Burnol* Jürgen Gilg**

February 22, 2021

1 Introduction

This paper is an introduction to "$\mathbb{Q}$-nice" polynomials: polynomials P with rational coefficients such that both P and P' only have rational roots. For example:

$$\begin{aligned} P &= X(X-3)(X-8)\\ Q &= X(X-25)(X-88)(X-165)\\ R &= (X-141)(X-193)(X+167)^2\\ S &= X(X-36)(X-57)(X-92)(X-156) \end{aligned}$$

all are nice polynomials: R is from [7], Q and S were copied from [10]; in the latter reference the roots are scaled for the derivative to also have integer roots: for Q, one needs to double the roots, for S one needs to multiply them by 5, and $X(X-3)(X-8)$ must be replaced by $X(X-9)(X-24)$ to let the derivative also have integer roots.

Caldwell [6] found parametrized families of nice polynomials with four distinct roots in degree 4. These polynomials were symmetrical (with respect to average of the roots), and [6] also gave the first five examples of nice non-symmetric degree four polynomials with distinct roots. More examples were found by Evard [10].

A stronger requirement defines "rational-derived" polynomials: those polynomials P with rational coefficients and rational roots, whose derivatives of all orders only have rational roots. This is the case of P above (of course as P'' is of degree one) but neither of Q nor of S as their second derivatives do not factorize over $\mathbb{Q}$. Remarkably R is rational-derived and for a time it was even conjectured that all rational-derived degree

*Lille, France
**Stuttgart, Germany

four polynomials with at least three distinct roots could be obtained from R by affine transformations [7]. This was shown to be false first by Galvin and MacDougall who found two other examples (see [13] for some explanations on their computer based approach) and then by Buchholz and Kelly who obtained infinitely many non-equivalent examples parametrized by a rank one subgroup of the group of rational points on a certain elliptic curve ([3]).

One is also interested in P and its derivative or higher derivatives having only integer roots: hence the notions of $\mathbb{Z}$-nice or $\mathbb{Z}$-derived polynomials (cf [4] for the terminology; in the literature "nice" has been used it seems mainly to mean $\mathbb{Z}$-nice; and "totally nice" to mean "$\mathbb{Z}$-derived"). From Vieta's formulae relating roots to coefficients, the average $x(P)$ of all (complex) roots (counted with multiplicities) verifies $x(P) = x(P')$. So for P of degree d which is $\mathbb{Z}$-nice, both $dx(P)$ and $(d-1)x(P)$ are integers, hence the average $x(P)$ of the roots must be itself an integer. This $x(P)$ is also the root of $P^{(d-1)}$. So for $d = 3$ any $\mathbb{Z}$-nice polynomial (such as $X(X-9)(X-24)$ whose average of the roots is 11) is $\mathbb{Z}$-derived.

In higher degrees the generic examples of "rational-derived" polynomials are the degree d polynomials with rational roots, one of them being of multiplicity at least $d-1$: translating to put the multiple root at the origin we have thus $P = eX^{d-1}(X-y) = eX^d - eyX^{d-1}$ and all higher derivatives keep this shape (with varying d, e and y), thus the roots are always rational.

There is actually a conjecture ([7]) that for $d \geq 5$, these are the sole examples. Although the degree $d = 4$ case is now known to be more complex than hoped for in [7], the $d \geq 5$ conjecture follows, according to results of Buchholz and MacDougall [4] combined with those of Flynn [11], from the hypothesis that there does not exist a rational-derived polynomial of degree four with distinct roots. Nowadays, the study is still on-going in degrees four and higher, see among others [1] and [9].

We will mainly focus on degree 3 however, where all is known, and accessible via undergraduate algebra: certainly many amateurs and professionals alike have encountered and solved the problem privately; earliest references we could find are Chapple [8] (1960) and Zuser [15] (1963). Other references include [2], [5], [12]. We could not access [8] nor [12] but only [13] which summarizes relevant information.

Here is how our treatment differs from what we could find in the literature:

- we explain (in arbitrary degree) the precise relation between rational and integer notions of equivalence classes,
- we give in degree three the complete one-to-one enumeration of these classes; the precise and complete description turns out to involve an interesting incarnation of

the dihedral group D_{12} of order 12 as a group of homographic transformations.

- we obtain the parametrization of nice cubics in two independent "elementary" ways, which do not rely on an analysis of the $a^2 - ab + b^2 = \square$ diophantine equation using Pythagorean triples or the chord-slope method to parametrize the ellipse $a^2 - ab + b^2 = 1$. Our second "effortless" method takes place in the field $\mathbb{Q}(j)$ generated by cube roots of unity. This is also closely related with the dihedral group mentioned in the first item.

We will handle cubic polynomials via the idea of the Lagrange resolvent. We do not need to know the Cardano's formulae nor even to know how the Lagrange approach, which prefigures ideas of Galois theory, allows to obtain them. But we will focus first on the "ambiguities" (hence "symmetry" in the title) of the resolvent, then on its "arithmetic". In particular we will deduce the parametrization of nice cubics from the fact that the unit-norm equation $N(y) = y\overline{y} = 1$ in $\mathbb{Q}(j)$ has for solutions $y = z/\overline{z}$, $z \in \mathbb{Q}(j)$. Here $j = \exp(2\pi i/3)$, $1 + j + j^2 = 0$.

And our characterization can be summarized as follows: a cubic polynomial with rational coefficients is nice if and only if the Lagrange resolvent is in $\mathbb{Q}(j)$ and is, modulo the multiplicative action by $\mathbb{Q}^*$, a square in this field.

The Gaussian theory of factorization in $\mathbb{Z}[j]$ would provide an alternative approach (see e.g. [14] for algebraic number theory) but we have decided to limit the scope of this paper to common knowledge undergraduate algebra techniques only. Some working familiarity with homographic transformations and with elementary group theory will be helpful.

We have included various graphs to illustrate the manipulated concepts. We hope that this text will motivate readers into pursuing their own researches into the conjectures related to degree four and higher.

2 Equivalence classes of nice polynomials

Definition 1. *A polynomial P is $\mathbb{Q}$-nice if itself and its first derivative both have all their (complex) roots in the field of rational numbers. It is also required that all coefficients of P be rational.*

Constant and degree one polynomials with rational coefficients are (a bit boring) examples of nice polynomials. Under the condition of rationality of the roots one only has (thanks to Vieta's formulae) to look at the polynomial highest degree coefficient to know if all its coefficients are rational.

Definition 2. *A polynomial P is $\mathbb{Z}$-nice if P and P' both have integer coefficients and roots.*

Let Q monic of degree $d \geq 1$ with rational roots $x_1, \ldots, x_d$ (with possible multiplicities) and such that Q' also has only rational roots $y_1, \ldots, y_{d-1}$. If N is a positive integer multiple of all of the denominators of the x_i then $P = \prod_i (X - Nx_i)$ has integer coefficients; the roots of P' are the Ny_i, $1 \leq i \leq d-1$. So if N is suitably chosen, P is $\mathbb{Z}$-nice. And Q is recoverable from P as $Q(X) = N^{-d}P(NX)$. We will give a more precise statement later.

Let's now formalize that certain simple transformations preserve the "niceness".

Definition 3. *Two $\mathbb{Q}$-nice polynomials Q_1 and Q_2 are equivalent if $Q_2(X) = \nu Q_1((X - \mu)/\lambda)$ for some rational numbers $\lambda \neq 0$, $\nu \neq 0$, and μ.*

In other words the roots of Q_2 (hence resp. of Q_2') are obtained from those of Q_1 (resp. Q_1') by the invertible rational affine transformation $x \mapsto \lambda x + \mu$. This is indeed an equivalence relation.

In the integer case, we limit to invertible integer affine transformations $x \mapsto \pm x + \mu$ to define $\mathbb{Z}$-equivalence classes. Notice that we still allow in this definition $\nu \in \mathbb{Q}^*$, in effect ignoring the leading coefficient.

Definition 4. *Two $\mathbb{Z}$-nice polynomials P_1 and P_2 are ($\mathbb{Z}$) equivalent if $P_2(X) = \nu P_1((X - \mu)/\lambda)$ with $\lambda = \pm 1$, $\mu \in \mathbb{Z}$, and $\nu \in \mathbb{Q}^*$.*

We will use the notation $C(Q)$ for the equivalence class of a $\mathbb{Q}$-nice Q and $C_{\mathbb{Z}}(P)$ for the $\mathbb{Z}$-equivalence class of a $\mathbb{Z}$-nice P. Integer equivalence classes can be indexed by a positive integer, the "level":

Definition 5. *The level $\ell(P)$ of a $\mathbb{Z}$-nice polynomial P of degree d is the greatest common divisor of the differences $x_i - x_j$ of roots of P and of the differences $x_i - y_j$ between roots of P and roots of P'. Equivalently it is* $\gcd(x_1 - x_d, \ldots, x_{d-1} - x_d, y_1 - x_d, \ldots, y_{d-1} - x_d)$ *where x_d is any given root of P.*

The level is constant on any $\mathbb{Z}$-equivalence class. The nice polynomials of zero level are the monomials $\nu(X - x_d)^d$ (which includes all polynomials of degree at most 1). Polynomials with at least two distinct roots have positive levels.

Definition 6. *If $P_2(X) = \nu P_1((X - \mu)/\lambda)$ for some $\mu \in \mathbb{Z}$, $\nu \in \mathbb{Q}^*$ and $\lambda \in \mathbb{Z} \setminus \{0\}$, we say that P_2 "is generated" from P_1.*

If P_2 is generated from P_1, i.e. its roots are obtained from those of P_1 by the integer affine transform $x \mapsto \lambda x + \mu$, then $\ell(P_2) = |\lambda|\ell(P_1)$ and the equality $\ell(P_2) = \ell(P_1)$, in case P_1 has at least two distinct roots hence has non-zero level, thus happens if and only

if $\lambda = \pm 1$, i.e. if P_1 and P_2 are $\mathbb{Z}$-equivalent (if $\ell(P_1) = 0$ then P_1 and P_2 are indeed $\mathbb{Z}$-equivalent, but the λ did not have to be ± 1).

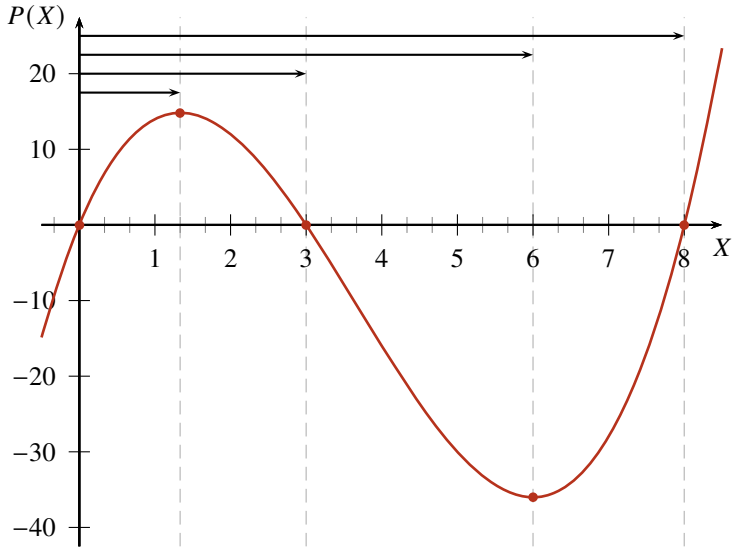

Figure 1: Roots of $X(X-3)(X-8)$ and its $\gcd(\frac{4}{3}, 3, 6, 8) = \frac{\gcd(4,9,18,24)}{3} = \frac{1}{3}$ level

Here is the main result relating the two types of equivalence classes:

Theorem 1. *For any equivalence class C of $\mathbb{Q}$-nice polynomials of degree $d > 1$, except $C(X^d)$, and any integer $\ell > 0$, the $\mathbb{Z}$-nice polynomials of level ℓ contained in C are a single (non-empty) $\mathbb{Z}$-equivalence class.*

In particular there exists a $\mathbb{Z}$-nice polynomial P_0 of level 1, all such $\mathbb{Z}$-nice polynomials in C of level 1 are a single $\mathbb{Z}$-equivalence class and P_0 generates all $\mathbb{Z}$-nice polynomials in C. Notice also as corollary that any $\mathbb{Z}$-nice polynomial with level $\ell > 1$ can be generated from a $\mathbb{Z}$-nice polynomial with level 1.

To present the proof of the theorem conveniently, let us first recall that the notion of gcd extends to rational numbers: if $q_1, \ldots, q_r$ are given, there exists a unique non-negative rational number q such that:

$$\{n_1 q_1 + \cdots + n_r q_r, n_1, \ldots, n_r \in \mathbb{Z}\} = q\mathbb{Z} \tag{1}$$

We write $q = \gcd(q_1, \ldots, q_r)$. If $N \in \mathbb{N}$ is such that all Nq_i's are in $\mathbb{Z}$, then $q = \gcd(Nq_1, \ldots, Nq_r)/N$, as is easily verified (once one knows how the usual gcd of integers relates to $\mathbb{Z}$-ideals and multi-term Bézout identities). This allows to extend the notion of level:

Definition 7. *The (fractional) level $\ell(Q)$ of a $\mathbb{Q}$-nice polynomial Q is the* gcd *of the differences $x_i - x_j$ of roots of Q and of their differences $x_i - y_j$ with the roots of Q'.*

As per integer polyomials, the level scales under $Q_1(X) = \nu Q((X-\mu)/\lambda)$ equivalence transformations: $\ell(Q_1) = |\lambda|\ell(Q)$.

Proof of Theorem 1. From any $\mathbb{Q}$-nice polynomial of non-zero level $\lambda = \ell(Q)$ (i.e. a polynomial with at least two distinct roots, which we have ensured by excluding the class of X^d) we can obtain a polynomial Q_1 of level 1 via $Q_1(X) = Q(\lambda X)$. Writing $x_1, \ldots, x_d, y_1, \ldots, y_{d-1}$ for the roots of Q_1 and its derivative, this implies that all of $x_i - x_d$, $y_j - x_d$ are integers. So $Q_2 = Q_1(x + x_d)$ only has integer roots (one of them being 0) and its derivative too. Multiplying it by a constant to turn it into a monic polynomial, we obtain P_0 with integer coefficients (from being monic with integer roots). So P_0 is a $\mathbb{Z}$-nice polynomial of level 1 in the equivalence class of Q. From now on x_i, $1 \le i < d$, $x_d = 0$, and y_j, $1 \le j < d$ denote the roots of P_0 and of its derivative. They are integers, with no common divisor > 1.

We now prove that any $\mathbb{Z}$-nice P in C is generated by such a P_0. Let P be another monic $\mathbb{Z}$-nice polynomial in C. Let u_i, $1 \le i \le d$ be its roots and v_j, $1 \le j < d$ be the roots of its derivative P'. There exists a $\mathbb{Q}$-affine transformation $x \mapsto \lambda x + \mu$ mapping the roots of P_0 (resp. P_0') to those of P (resp. P'). After re-enumerating the roots of P and P' we can assume $u_i = \lambda x_i + \mu$ for $1 \le i \le d$ and $v_j = \lambda y_j + \mu$ for $1 \le j < d$. In particular $u_d = \mu$ (as $x_d = 0$), so $\mu \in \mathbb{Z}$. Hence all λx_i, λy_i, are integers. As $x_d = 0$, and $\ell(P_0) = 1$, there is a Bézout identity expressing 1 as $\mathbb{Z}$-linear combination of the x_i, $1 \le i < d$, and y_j, $1 \le j < d$. Multiplying by λ, we see that it is an integer. So P is indeed generated from P_0 by a $\mathbb{Z}$-affine transformation (invertible in $\mathbb{Q}$, not necessarily in $\mathbb{Z}$). Notice that $\ell(P) = |\lambda|$ with the notations above.

If conversely P_0 can be generated from P, this means that its roots are the images of those of P by a $\mathbb{Z}$-affine transformation, $x \mapsto \lambda' x + \mu'$. The minimal distance between two distinct roots of P_0 is thus $|\lambda'|$ times the minimal distance between two distinct roots of P which itself is $|\lambda|$ times the minimal distance between two distinct roots of P_0. Hence $|\lambda\lambda'| = 1$. And P is $\mathbb{Z}$-equivalent to P_0. We have used here that in C no polynomial is a monomial.

Let now P_1 be another $\mathbb{Z}$-nice polynomial of level 1 in C. Translating it to let it become P_2 which vanishes at 0, the proof done for P_0 shows that P_2 generates all $\mathbb{Z}$-nice polynomials in C, hence in particular P_0. So P_0 and P_2, are, by the previous paragraph, $\mathbb{Z}$-equivalent. So P_0 and P_1 are $\mathbb{Z}$-equivalent.

We have proven so far that $\mathbb{Z}$-nice polynomials of level 1 exist in C and are a single $\mathbb{Z}$-class; and that any other $\mathbb{Z}$-nice polynomial is generated by P_0 of level 1. Let P_2 and P_3 be two such polynomials of the same level $\ell > 0$. The roots of P_2 are obtained from those of P_0 by an affine transformation $x \mapsto \epsilon\ell x + \mu$, and those of P_3 by $x \mapsto \epsilon'\ell x + \mu'$ with $\epsilon = \pm 1$, $\epsilon' = \pm 1$. So the roots of P_3 are obtained from those of P_2 by $x \mapsto \epsilon\epsilon' x - \epsilon\epsilon'\mu' + \mu$

and they are in the same $\mathbb{Z}$-class.

This completes the proof of Theorem 1. □

Let's handle degree two case. A polynomial is $\mathbb{Q}$-nice if and only if its two roots are rational. Any polynomial with rational roots is either in $C(X^2)$ or $C(X(X-1))$ (there is an affine transformation mapping 0 and 1 to two arbitrary distinct roots). As per the integer case, $C_{\mathbb{Z}}(X^2)$ contains all polynomials with an integer double root. On the other hand, according to Theorem 1 the $\mathbb{Z}$-nice polynomials in $C(X(X-1))$ are partitioned into $\mathbb{Z}$-classes indexed by the positive integer level. The level of $Q = X(X-1)$ is $1/2$, so we look at $Q_1 = Q(X/2) = X(X-2)/4$ and make it monic, obtaining $P_0 = X(X-2)$ as a representative of the $\mathbb{Z}$-class of $\mathbb{Z}$-nice level 1 polynomials in $C(Q)$. All other $\mathbb{Z}$-nice polynomials in $C(Q)$ are generated from P_0, i.e. of the shape $P = \nu(X-\mu)(X-\mu-2\lambda)$ with $\lambda, \nu \neq 0$ and μ being integers. In other terms, the difference (or the sum) of the roots is even. This can naturally be also be obtained directly, which is left as exercise to the reader!

3 The precise classification of nice cubic polynomials

Let's turn to degree 3. Again $C(X^3)$ is the single $\mathbb{Q}$-class of monomials, and $C_{\mathbb{Z}}(X^3)$ also contains all $\mathbb{Z}$-nice monomials. If Q has a double root, there is an affine transformation mapping 0 to the multiple root and 1 to the other one, so $C(X^2(X-1))$ contains all $\mathbb{Q}$-nice polynomials having a double root. The level of $Q = X^3 - X^2$ is computed from the roots 0, 1 of Q and 0, $2/3$ of Q' to be $1/3$. So we consider $Q_1 = Q(X/3) = (X^3 - 3X^2)/27$, then $P_0 = X^3 - 3X^2 = X^2(X-3)$. This P_0 is of level 1. We conclude from Theorem 1 that the $\mathbb{Z}$-nice cubic polynomials with a double root are partitioned into $\mathbb{Z}$-classes indexed one-by-one by positive integer levels ℓ, with representatives $X^2(X-3\ell)$.

The real work is for polynomials with three distinct roots. The following (which includes polynomials with multiple roots) is known:

- Chapple (1960, [8]): let p, q, r, s be four rational numbers in arithmetic progression. Then $X(X-pr)(X-qs)$ is a nice rational cubic and this gives all equivalence classes.
- Zuser (1963, [15]): let u and v be two rational numbers. Then $(X-u^2)(X-2uv)(X-v^2)$ is a nice rational cubic and this gives all equivalence classes.

We could not access the original Chapple publication, only an extract given in [13], so we have formulated it using our language of equivalence classes. And Zuser studied $\mathbb{Z}$ nice polynomials and obtained their description from those with roots at 0, $u^2 - 2uv$, $v^2 - 2uv$,

with u and v integers, but the $(X-u^2)(X-2uv)(X-v^2)$ form is a nice memorable form, which we thus call the "Zuser form", even if it is used as here with u and v rational.

Taking $p=1$, $q=2$, $r=3$, $s=4$ in Chapple's formula, we get $Q=X(X-3)(X-8)$. The derivative is $Q'=3X^2-22X+24=3(X-4/3)(X-6)$, and the fractional level of Q is thus $1/3$. To ensure integer roots for the derivative we thus have to rescale by 3, obtaining $X(X-9)(X-24)$, whose derivative roots are 4 and 18. We will establish that this P has the smallest possible separation 14 between the roots of its derivatives.

We will explain later that generally speaking with a four-term Chapple arithmetic progression p, q, r, s consisting of integers (or u and v taken to be integers in Zuser parametrization) we may have to multiply the roots by 3 in order to ensure that the derivative also has integer roots (thus, Chapple arithmetic progression would have to be scaled by $\sqrt{3}$ to also account for $\mathbb{Z}$ nice polynomials).

Taking Zuser's formula with $u=1$ and $v=3$ (as $v=2$ gives double root) we get $(X-1)(X-6)(X-9)$; and with $u=1$, $v=-2$ we get $(X-1)(X+4)(X-4)$. All three of $X(X-3)(X-8)$, $(X-1)(X-6)(X-9)$ and $(X-1)(X+4)(X-4)$ are equivalent up to translation by an integer, replacement of X by $-X$, and of P by $-P$ to let it be monic again. The derivative has an integer root, but the other is in $\frac{1}{3}\mathbb{Z}$, not in $\mathbb{Z}$. After rescaling we obtain polynomials all in $C_{\mathbb{Z}}(X(X-9)(X-24))$.

The Chapple and Zuser forms are indeed elementarily equivalent. To explain this, let us change notations and write $p-2q$, $p-q$, p, $p+q$, for the four-term Chapple arithmetic progression. The Chapple polynomial has roots at 0, p^2-2pq, p^2-q^2. The map $x\longrightarrow p^2-x$ transforms them into the roots p^2, $2pq$, q^2, as in Zuser's parametrization.

Let $w=\frac{p}{q}$. To have distinct roots, we need $q\neq 0$ and $w\notin\{-1,0,\frac{1}{2},1,2\}$. The Chapple and Zuser polynomials are $\mathbb{Q}$-equivalent to $X(X-1)(X-a)$ with $a=\frac{p^2-2pq}{p^2-q^2}=\frac{w^2-2w}{w^2-1}=\frac{2w-w^2}{1-w^2}$ and the condition $a\notin\{0,1,\infty\}$ is the same as $w\notin\{-1,0,\frac{1}{2},1,2,\infty\}$.

Here is a parametrization of $\mathbb{Q}$-nice cubics with distinct roots (the proof will be given later):

Theorem 2. *For any $w\in\mathbb{Q}\setminus\{-1,0,\frac{1}{2},1,2\}$, the polynomial $X(X-1)(X-a)$ with $a=\frac{2w-w^2}{1-w^2}$ is a nice rational cubic with distinct roots and this gives all such polynomials up to $\mathbb{Q}$-equivalence.*

More precisely, the equivalence classes of nice rational cubics with distinct roots are via this association of $X(X-1)(X-a)$ to w in one-to-one correspondence with the rational numbers $w\in(0,1/(2+\sqrt{3}))$.

The second part of the statement corresponds to the choice of one of the two w-intervals mapping to $0<a<\frac{1}{2}$. This $0<w<2-\sqrt{3}$ constraint arises if one insists into stating a one-to-one enumeration of the equivalence classes, which does not seem to have been the

case in the literature (probably from being too obvious and going without saying). The next statement goes into more details about what happens without the constraint:

Theorem 3. *For a given $0 < w_0 < 2 - \sqrt{3}$, there are in total twelve w's in $\mathbb{Q}$ such that $X(X-1)(X-a)$, $a(w) = (2w-w^2)/(1-w^2)$, define the same $\mathbb{Q}$-class as $a(w_0)$. They are the orbit of w_0 under an action on $\mathbb{R} \cup \{\infty\}$ of the dihedral group D_{12} via homographies*:

$$\begin{gathered} w_0, \frac{2w_0-1}{w_0+1}, \frac{w_0-1}{w_0}, \frac{w_0-2}{2w_0-1}, \frac{1}{1-w_0}, \frac{w_0+1}{2-w_0}, \\ \frac{w_0}{w_0-1}, \frac{2w_0-1}{w_0-2}, 1-w_0, \frac{2-w_0}{w_0+1}, w_0^{-1}, \frac{w_0+1}{2w_0-1} \end{gathered} \tag{2}$$

where the first six correspond to the images under the cyclic sub-group of order 6 of D_{12}. The central element of D_{12} is the transform $w \mapsto \frac{w-2}{2w-1}$ which exchanges the two w's giving a common a. The six transforms on the second line are the other elements of order 2 in D_{12}.

For example the twelve values w which give polynomials $X(X-1)(X-\frac{w^2-2w}{w^2-1})$ in the same $\mathbb{Q}$-equivalence class as $X(X-9)(X-24)$ are $w = \frac{1}{5}, -\frac{1}{2}, -4, 3, \frac{5}{4}, \frac{2}{3}, -\frac{1}{4}, \frac{1}{3}, \frac{4}{5}, \frac{3}{2}, 5$, and -2. They correspond to the a values $\frac{3}{8}, -\frac{5}{3}, \frac{8}{5}, -\frac{3}{5}, \frac{5}{8}, \frac{8}{3}$, where $\frac{3}{8}$ is the sole representative in $(0, \frac{1}{2})$.

The following general table of correspondence holds:

w	$1-w$	$\frac{1}{w}$	$\frac{w}{w-1}$	$\frac{1}{1-w}$	$\frac{w-1}{w}$
$a = \frac{w^2-2w}{w^2-1}$	$\frac{1}{a}$	$1-a$	$\frac{a}{a-1}$	$\frac{a-1}{a}$	$\frac{1}{1-a}$

Its explanation will emerge from the interpretation of $w \mapsto a$ obtained in the last section of this paper, which will provide the proof of Theorem 3.

Theorem 4. *The $\mathbb{Z}$-classes of $\mathbb{Z}$-nice polynomials with distinct roots are in one-to-one correspondence with the triples (q, p, ℓ) of integers verifying*:

- $0 < p < (2-\sqrt{3})q$,
- $(p, q) = 1$,
- $\ell > 0$,

where a representative polynomial of the class indexed by (q, p, ℓ) is

$$(X - \ell 3^\epsilon p^2)(X - \ell 3^\epsilon 2pq)(X - \ell 3^\epsilon q^2)\,,$$

with $\epsilon = 0$ if $3 \mid p+q$ and 1 if $3 \nmid p+q$. Its derivative has its roots at respectively $\ell 3^\epsilon pq$ and $\ell 3^\epsilon (2p^2+pq+2q^2)/3$.

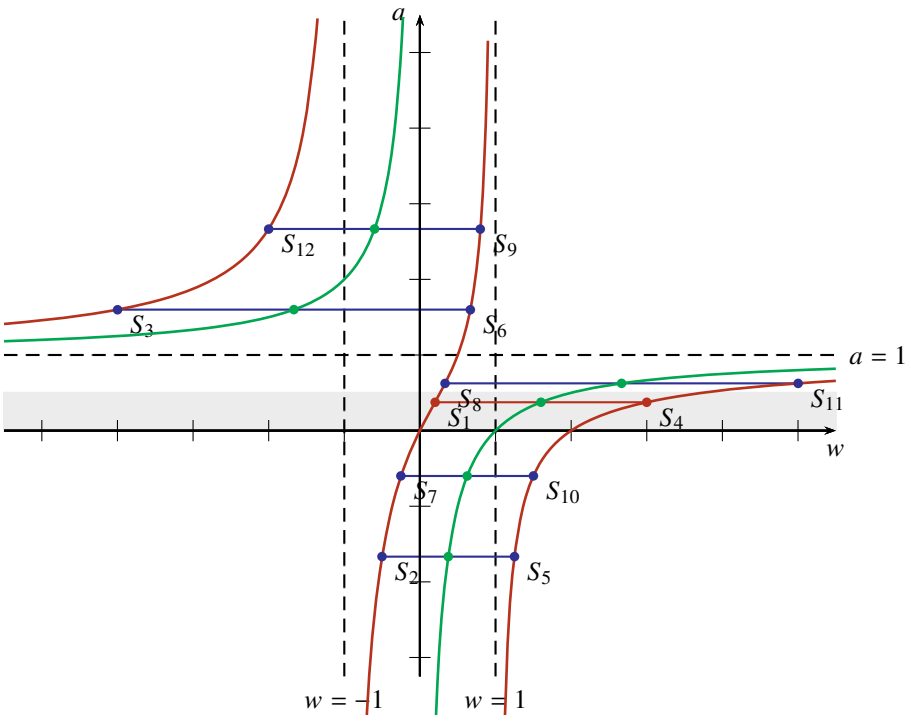

Figure 2: The $w \mapsto a = \frac{w^2-2w}{w^2-1}$ map

The marked points correspond to the twelve values of w in the order of Theorem 3, starting with $S_1 = (w = \frac{1}{5}, a = \frac{3}{8})$. The two values w_1 and w_2 with same image a verify $s = \frac{w_1+w_2}{2} = (1-a)^{-1}$, hence $a = \frac{s-1}{s}$ whose graph is the green line. The fact that $w \mapsto \frac{w-2}{2w-1}$ exchanges w_1 and w_2 is not represented graphically.

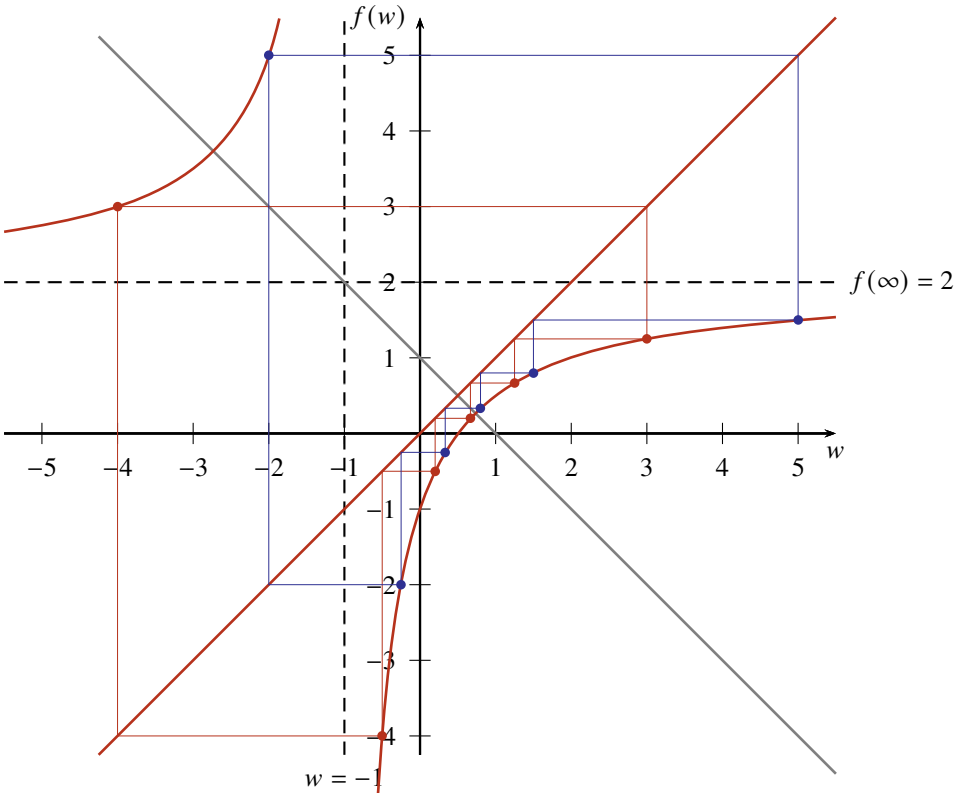

Figure 3: The $f(w) = \frac{2w-1}{w+1}$ cyclic homography of order 6 and two of its orbits

Together they are a single orbit of a D_{12} group of homographies, and these 12 values of w's are those such that $X(X-1)(X-a(w))$ is in the same $\mathbb{Q}$-class as $X(X-3)(X-8)$.

Indicated is an axis of symmetry corresponding to the fact that the graph is invariant under $(x, y) \mapsto (1-y, 1-x)$, i.e. that $1 - w = f(1 - f(w))$. Writing $\sigma(w) = 1 - w$, this corresponds to $\sigma = f\sigma f$, or $(f\sigma)^2 = \mathrm{Id}$. More generally, $\{\sigma, f\sigma, f^2\sigma, f^3\sigma, f^4\sigma, f^5\sigma\}$ give all order 2 elements in D_{12} distinct from the central element. They are the transforms on the second line in Theorem 3 (shifted by 2 mod 6). Looking at the list we see by same reasoning that also the functional equation $w^{-1} = f(f(w)^{-1})$ for example holds, which means that the graph is invariant under $(x, y) \mapsto (y^{-1}, x^{-1})$.

The authors are not aware of a previous publication of this precise result. Zuser statements ([15]) are very close, but he did not consider the problem of enumerating the equivalence classes of the $\mathbb{Z}$-nice polynomials, only how to construct $\mathbb{Z}$-nice polynomials, so in particular the restriction $0 < p < q/(2+\sqrt{3})$ is nowhere in sight.

Corollary 5. *Among all $\mathbb{Z}$-nice polynomials with distinct roots, those having the smallest separation between the roots of the derivative are the polynomials $\mathbb{Z}$-equivalent to $(X-1)(X-10)(X-25)$. This minimal separation is 14.*

Proof of corollary. According to Theorem 4, the separation S of the roots of the derivative for the chosen representative of each class is $S = \ell 3^\epsilon 2(q^2-qp+p^2)/3$. Clearly we have to take $\ell = 1$ to start with. And $0 < p < q/(2+\sqrt{3})$, $\epsilon = 1$ if $3 \nmid p+q$, $\epsilon = 0$ if $3 \mid p+q$. We observe that $q^2-qp+p^2 = (q-p/2)^2+3p^2/4$, and as $q > \frac{7}{2}p$, $q^2-qp+p^2 > (9+\frac{3}{4})p^2$. For $p = 2$ this is greater than 39, and $S > 26$ then. To achieve a smaller S we thus must take $p = 1$, which gives $S = 3^\epsilon 2(q^2-q+1)/3$. This increases strictly with q, so is minimal among those allowed q's ($q > 2+\sqrt{3}$, i.e. $q \geq 4$) with $3 \nmid p+q = 1+q$ for $q = 4$ which gives then $S = 3 \cdot 2 \cdot 13/3 = 26$. And the smallest allowed $q \equiv 2 \pmod 3$ is $q = 5$ giving $S = 1 \cdot 2 \cdot 21/3 = 14$. There is thus a unique $\mathbb{Z}$-class realizing this minimum and it is obtained for $p = 1$, $q = 5$, (hence $3^\epsilon = 1$), and $\ell = 1$. □

4 Deduction of the integer case from the rational case

Before proving Theorem 2 and Theorem 3, we first explain Theorem 4 as a corollary to Theorem 1 and Theorem 2.

Let us for $Q = X(X-1)(X-a) = X^3-(1+a)X^2+aX$ obtain the roots of its derivative $Q' = 3X^2-2(1+a)X+a$. The (reduced) discriminant is $\Delta = (1+a)^2-3a = 1-a+a^2$. We are going to cheat a little here and, rather than replacing immediately a by its expression in terms of w, first factorize over $\mathbb{C}$ this Δ. The result is $(a+j)(a+j^2) = |a+j|^2$, with $j = \exp(2\pi i/3)$ (hence $j^3 = 1$, $j+j^2 = -1$). Let us pursue using only now w:

$$a+j = \frac{2w-w^2+j-jw^2}{1-w^2} = \frac{j+2w-(1+j)w^2}{1-w^2}$$
$$= \frac{j+2w+j^2w^2}{1-w^2} = \frac{j^2(j^2+2jw+w^2)}{1-w^2} = j^2\frac{(w+j)^2}{1-w^2}$$

So $\Delta = |a+j|^2 = |w+j|^4/(1-w^2)^2 = (w^2-w+1)^2/(1-w^2)^2$ is a rational square. The roots of Q' are thus indeed rational numbers $r < s$: (here $0 < w < 2-\sqrt{3} < 1$)

$$r = \frac{1+a-\sqrt{\Delta}}{3} = \frac{1-w^2+2w-w^2-(w^2-w+1)}{3(1-w^2)} = \frac{3w(1-w)}{3(1-w^2)} = \frac{w}{1+w}$$
$$s = \frac{1+a+\sqrt{\Delta}}{3} = \frac{1-w^2+2w-w^2+(w^2-w+1)}{3(1-w^2)} = \frac{2+w-w^2}{3(1-w^2)} = \frac{2-w}{3(1-w)}$$

It is interesting that r and s are homographic in w, hence in one-to-one correspondence with it; in fact taking a root of Q' as parameter is also a way to achieve the rational parametrization of the nice polynomials as we will comment upon later.

There remains the task of computing the level of Q, which has roots at 0, 1, a, and whose derivative has roots at r and s. For this we write $w = p/q$ with $(p,q) = 1$, $q > 0$ (let us recall $0 < w < 2-\sqrt{3}$, in particular $0 < p < q$). We have to compute $\ell(Q) = \gcd(1, a, r, s)$, which can be done (using homogeneity under multiplication by $3(q^2-p^2) = 3q^2(1-w^2)$) in terms of an integer gcd:

$$\ell(Q) = \frac{\gcd(3(q^2-p^2), 3(2qp-p^2), 3(qp-p^2), 2q^2+qp-p^2)}{3(q^2-p^2)}$$

Let's rewrite the numerator as $\gcd(i,j,k,l)$ with

$$\begin{pmatrix} 3 & 0 & -3 \\ 0 & 6 & -3 \\ 0 & 3 & -3 \\ 2 & 1 & -1 \end{pmatrix} \begin{pmatrix} q^2 \\ qp \\ p^2 \end{pmatrix} = \begin{pmatrix} i \\ j \\ k \\ l \end{pmatrix}$$

We see that $\frac{1}{3}i$, $\frac{1}{3}j$ and $\frac{1}{3}k$ are computed in terms of q^2, qp, p^2 by an integer transformation of determinant -1, hence its inverse also has integer coefficients and $3q^2$, $3qp$ and $3p^2$ are integer linear combinations of i, j, and k. Thus $\gcd(i,j,k)$ divides $\gcd(3q^2, 3p^2) = 3$, and consequently is equal to 3. As $l \equiv -(p+q)^2 \pmod 3$ we conclude that the numerator gcd is

- 1 if $3 \nmid p+q$,
- 3 if $3 \mid p+q$.

Consequently $\ell(Q) = (3(q^2-p^2))^{-1}$ in the first case and $(q^2-p^2)^{-1}$ in the second case.

We compute also $(q^2-p^2)a = (q^2-p^2)\frac{2w-w^2}{1-w^2} = 2pq-p^2$. To obtain a level 1 $\mathbb{Z}$-nice polynomial in the class of $X(X-1)(X-a)$ we thus only have to choose the monic polynomial having its roots at 0, $3^\epsilon(q^2-p^2)$ and $3^\epsilon(2pq-p^2)$ where $\epsilon = 1$ if $3 \nmid p+q$ and $\epsilon = 0$ if $3 \mid p+q$. According to Theorem 1 this is a representative in $C(X(X-1)(X-a))$ of the unique $\mathbb{Z}$-equivalence class of nice level 1 polynomials there.

To obtain a representative of the level ℓ solutions we only need to rescale by ℓ the roots. We then translate by $\ell 3^\epsilon p^2$ to obtain the roots in the form stated in Theorem 4. The roots of the derivative are also scaled then shifted by $\ell 3^\epsilon p^2$. For r, resp. s this gives first $\ell 3^\epsilon p(q-p)$ resp. $\ell 3^\epsilon(2q^2+qp-p^2)/3$, then after translation we obtain $\ell 3^\epsilon pq$ and $\ell 3^\epsilon(2q^2+qp+2p^2)/3$, and this completes the proof of Theorem 4.

5 The "effortless" way to find all nice rational cubics

In this section we will obtain "effortlessly" a construction (equivalent to the one of Theorem 2) of all equivalence classes of $\mathbb{Q}$-nice polynomials with distinct roots. Let $Q = X(X-1)(X-a)$ be in the class (we can always map two roots to 0 and 1). We already computed $Q' = 3X^2 - 2(1+a)X + a$. Now, let r be one of its supposedly rational roots. Tautologically:

$$3r^2 - 2(1+a)r + a = 0 \implies a = \frac{3r^2 - 2r}{2r - 1} \tag{3}$$

It can never happen that $r = \frac{1}{2}$ if the left hand side holds. But this is a parametrization! We only have to exclude those r for which $a = 0$, $a = 1$, or $a = \infty$.

Let thus $r \in \mathbb{Q} \setminus \{0, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, 1\}$ be given and let a be defined by (3). Then $a \in \mathbb{Q} \setminus \{0, 1\}$, and r is a rational root of Q'_a with $Q_a = X(X-1)(X-a)$. The other root s is also rational as $r + s = \frac{2}{3}(1+a)$. So $X(X-1)(X-a)$ is a $\mathbb{Q}$-nice cubic polynomial!

We have, with no effort whatsoever, obtained the first part of the following theorem:

Theorem 6. *For any $r \in \mathbb{Q} \setminus \{0, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, 1\}$, the polynomial $X(X-1)(X-a)$ with $a = \frac{r(2-3r)}{1-2r}$ is a nice rational cubic with distinct roots and this gives all such polynomials up to $\mathbb{Q}$-equivalence.*

More precisely, the equivalence classes of nice rational cubics with distinct roots are via this association of $X(X-1)(X-a)$ to r in one-to-one correspondence with the rational numbers $r \in (0, 1/(3+\sqrt{3}))$.

Proof. The first part is already known. For the second part, we admit temporarily that any equivalence class of nice cubics with distinct roots contains a unique representative $X(X-1)(X-a)$ with $0 < a < \frac{1}{2}$. We will prove this next in Theorem 7.

The map $r \mapsto r(3r-2)/(2r-1)$ is strictly increasing (cf its graph): with $y = 2r - 1$ it is $(3y + 2 - 1/y)/4$ whose y derivative is $(3 + y^{-2})/4$. So $r \mapsto a$ is a bijection of $(0, (3+\sqrt{3})^{-1})$ with $(0, \frac{1}{2})$. As one antecedent of a is known to be rational, the other also is, so we can always impose the condition $0 < r < 1/(3+\sqrt{3})$. □

As an aside, the other root s is expressible as a homographic transform or r. Indeed:

$$\left.\begin{aligned} r + s &= \frac{2}{3}(1+a) \\ rs &= \frac{1}{3}a \end{aligned}\right\} \implies 6rs - 3(r+s) + 2 = 0 \implies \begin{cases} s = \dfrac{3r-2}{6r-3} \\ r = \dfrac{3s-2}{6s-3} \end{cases} \tag{4}$$

Using affine transformations of the roots we can follow this chain:

$$\begin{aligned}(0,1,\frac{(3r-2)r}{2r-1}) &\to (0,2r-1,3r^2-2r)\\ &\to (0,6r-3,9r^2-6r)\\ &\to (1,2(3r-1),(3r-1)^2)=(1,2\zeta,\zeta^2)\\ &\to (1-\zeta^2,2\zeta-\zeta^2,0)\\ &\to (1,\frac{2\zeta-\zeta^2}{1-\zeta^2},0)\ ,\end{aligned} \tag{5}$$

to exhibit in the same class a representative $X(X-1)(X-b)$ with $b=\frac{2\zeta-\zeta^2}{1-\zeta^2}$ as in Theorem 2, with $\zeta=3r-1$. Of course the excluded values of r match with those of ζ.

This establishes that the first part of Theorem 2 is equivalent with the first part of the "effortless" Theorem 6. In other terms we have obtained out of thin air a proof of Theorem 2, except for the range condition. This range condition follows as in the proof of Theorem 6 once we have the next statement:

Theorem 7. *In any $\mathbb{Q}$-equivalence class of cubic polynomials having distinct roots there is one and only one $X(X-1)(X-a)$ with $0<a<\frac{1}{2}$.*

Proof. We start by defining an action of the permutation group $\mathcal{S}_3$ on $\mathbb{R}\setminus\{0,1\}$. Let $x_1=0$, $x_2=1$, $x_3=a\neq 0,1$. For any permutation $\sigma\in\mathcal{S}_3$, we consider the affine transformation which maps $x_{\sigma(1)}$ to 0, and $x_{\sigma(2)}$ to 1, i.e. $x\mapsto f_\sigma(x)=(x-x_{\sigma(1)})/(x_{\sigma(2)}-x_{\sigma(1)})$. Let us define the image of $x_{\sigma(3)}$ as a transform of a:

$$a\cdot\sigma=\frac{x_{\sigma(3)}-x_{\sigma(1)}}{x_{\sigma(2)}-x_{\sigma(1)}}$$

For example with the transposition $\sigma=\tau_{12}$, we obtain $a\cdot\tau_{12}=(a-1)/(0-1)=1-a$. And similarly $a\cdot\tau_{23}=(1-0)/(a-0)=1/a$. And naturally $a\cdot e=a$.

For any σ, we compute:

$$a\cdot\sigma\tau_{12}=\frac{x_{\sigma\tau_{12}(3)}-x_{\sigma\tau_{12}(1)}}{x_{\sigma\tau_{12}(2)}-x_{\sigma\tau_{12}(1)}}=\frac{x_{\sigma(3)}-x_{\sigma(2)}}{x_{\sigma(1)}-x_{\sigma(2)}}=1-\frac{x_{\sigma(3)}-x_{\sigma(1)}}{x_{\sigma(2)}-x_{\sigma(1)}}=(a\cdot\sigma)\cdot\tau_{12}$$

$$a\cdot\sigma\tau_{23}=\frac{x_{\sigma\tau_{23}(3)}-x_{\sigma\tau_{23}(1)}}{x_{\sigma\tau_{23}(2)}-x_{\sigma\tau_{23}(1)}}=\frac{x_{\sigma(2)}-x_{\sigma(1)}}{x_{\sigma(3)}-x_{\sigma(1)}}=\left(\frac{x_{\sigma(3)}-x_{\sigma(1)}}{x_{\sigma(2)}-x_{\sigma(1)}}\right)^{-1}=(a\cdot\sigma)\cdot\tau_{23}$$

Iterating we get also for example $a\cdot\sigma\tau_{12}\tau_{23}=(a\cdot\sigma\tau_{12})\cdot\tau_{23}=((a\cdot\sigma)\cdot\tau_{12})\cdot\tau_{23}=(a\cdot\sigma)\cdot\tau_{12}\tau_{23}$. Any permutation τ can be written as an iterated product of the transpositions τ_{12} and τ_{23}, so via a recurrence (! not very long actually, but the method of deduction would apply to any group generated by two elements once the above and $a\cdot e=a$ are known)

$$\forall\sigma,\tau\qquad a\cdot\sigma\tau=(a\cdot\sigma)\cdot\tau$$

In other words we have defined a group action of $\mathcal{S}_3$ on (the right of) $\mathbb{R} \setminus \{0,1\}$. If $X(X-1)(X-a)$ is a nice polynomial, then any $X(X-1)(X-b)$ in its equivalence class must be such that $\{0,1,b\}$ is the image of $\{0,1,a\}$ by some affine transformation f, i.e. there exists a permutation g of the cardinality 3 set $\{0,1,a\}$ such that $0 = f(g(0))$, $1 = f(g(1))$, $b = f(g(a))$. Which is the same as saying that $f = f_\sigma$ for some $\sigma \in \mathcal{S}_3$ and then $b = a \cdot \sigma$.

Doing the computations one finds that the orbit of a under this action of $\mathcal{S}_3$ is $\{a, 1-a, 1/a, a/(a-1), 1/(1-a), (a-1)/a\}$, i.e. $\mathcal{S}_3$ acts (faithfully) by homographic transformations (which allows to extend the action to all of $\mathbb{R} \cup \{\infty\}$).

The images of $(0, \frac{1}{2})$ under the six homographic transformations are $(0, \frac{1}{2})$, $(\frac{1}{2}, 1)$, $(2, \infty)$, $(-\infty, -1)$, $(1, 2)$, and $(-1, 0)$. This builds up a partition of $(\mathbb{R} \cup \{\infty\}) \setminus (\{0, 1, \infty\} \cup \{-1, \frac{1}{2}, 2\})$. Thus any orbit there has cardinality 6 and possesses exactly one point in $(0, \frac{1}{2})$. As the values $a = 0, 1, \infty$ are excluded, and also $a = -1, \frac{1}{2}, 2$ which do not give nice polynomials, this completes the proof. □

Most of the above is intuitively obvious, and may be judged as "going without saying" but in our experience the precise write-up (not admitting without proof that we really have a group action of $\mathcal{S}_3$) will probably be challenging to students. It was not needed for establishing the theorem to understand the group action, we could have simply commented upon the properties of $\{a, 1-a, 1/a, a/(a-1), 1/(1-a), (a-1)/a\}$. But we deliberately want to emphasize group theory here. Theorem 2 (and Theorem 6) are now completely proven.

6 Lagrange's resolvent and its dihedral ambiguities

Let P be a cubic polynomial, with complex roots x_1, x_2, x_3. Lagrange considers $y_1 = x_1 + x_2 j + x_3 j^2$ and $y_2 = x_1 + x_2 j^2 + x_3 j$, with $j = \exp(2\pi i/3)$ and shows that in $y_1^3 + y_2^3$ and $y_1 y_2$ one can assemble the roots in symmetrical polynomials, hence one can express them in terms of the coefficients of P. This means that one only needs to solve a quadratic equation to obtain $\{y_1^3, y_2^3\}$ as a set. One then obtains y_1 from choosing one of the two elements, then extracting a cube root, which means that we expect 6 possibilities in general. y_2 is then known from $y_1 y_2$. Besides $x_1 + x_2 + x_3$ is known. So we obtain then x_1, x_2, x_3 up to a 6-fold ambiguity, which, we expect, matches the 6-fold ambiguity from permuting the roots. We do not comment more here on those aspects whose elucidation comes from Galois theory.

We will focus on polynomials with real roots, then y_1 and y_2 are complex conjugate, i.e. symmetrical in the real line. This symmetry is an element of the dihedral group D_6 of

isometries of the equilateral triangle with vertices 1, j, j^2. We know that D_6 is isomorphic to $\mathcal{S}_3$ when considering its action on the vertices of the triangle, once they are enumerated. We choose the enumeration $M_1 = 1$, $M_2 = j$, $M_3 = j^2$. Elements of D_6 act on the complex plane by symmetries and rotations, which are $\mathbb{R}$-linear. We will use the notation f_σ for the $\mathbb{R}$-linear map on $\mathbb{C}$ which does $f_\sigma(M_i) = M_{\sigma i}$ (we have abbreviated $\sigma i = \sigma(i)$). As $f_{\sigma\tau} = f_\sigma \circ f_\tau$ this is a left action of $\mathcal{S}_3$ on $\mathbb{C}$ realizing an isomorphism $\mathcal{S}_3 \simeq D_6$. Then:

$$\begin{aligned} x_{\sigma 1}M_1 + x_{\sigma 2}M_2 + x_{\sigma 3}M_3 &= x_1 M_{\sigma^{-1}1} + x_2 M_{\sigma^{-1}2} + x_3 M_{\sigma^{-1}3} \\ &= f_{\sigma^{-1}}(x_1 M_1 + x_2 M_2 + x_3 M_3)\,, \end{aligned}$$

which we can rewrite as $y_1(\sigma) = y_1 \cdot \sigma$, where σ acts on the right on $\mathbb{C}$ via $f_{\sigma^{-1}}$ and $y_1(\sigma)$ is the Lagrange resolvent value for roots which have been permuted by $\sigma \in \mathcal{S}_3$ (as acting on their indices; some roots may coincide). So $y_1(\sigma\tau) = y_1(\sigma) \cdot \tau$.

Let us now suppose that x_1, x_2 and x_3 are the roots of some $\mathbb{Q}$-nice polynomial Q. The Lagrange resolvent y_1 is an element of the field $\mathbb{Q}(j)$. Let us point out the special elements $\omega := j + 1 = \exp(\pi i/3)$, $-1 = \omega^3$, and $j^2 + 1 = \exp(-\pi i/3) = \omega^5$ which together with 1, j, j^2 are the sixth roots of unity (see the figure). They are the "units" of the ring $\mathbb{Z}[j]$ considered by Gauss in the infancy of algebraic number theory. We also point out that $2 + j = 1 + \omega$ has argument $\pi/6$, it is on the bissector of $\mathbb{R}^+$ and $\mathbb{R}^+\omega$: $(2 + j)^2 = 4 + 4j + j^2 = 3 + 3j = 3\omega$.

The indirect isometries in D_6 are the orthogonal symmetries in the lines $\mathbb{R}\,(M_2 \leftrightarrow M_3)$, $\mathbb{R}\omega = \mathbb{R}j^2$ $(M_1 \leftrightarrow M_2)$, and $\mathbb{R}j = \mathbb{R}\omega^5$ $(M_1 \leftrightarrow M_3)$. If Q has a triple root, then $y_1 = 0$. If it has a double root, in the orbit there will be some $x + xj$, i.e. $y_1 \neq 0$ is on one of the three lines of symmetries of the triangle and its orbit has only three points. If Q has distinct roots, the orbit has six points, with a unique representative in the angular sector delimited by the positive real axis and $\mathbb{R}^+\omega$, i.e. $y_1 = v + uj$, $0 < u < v$.

How does the Lagrange resolvent change on the equivalence class C of Q? A translation of the roots does not modify y_1. A rescaling scales y_1 by a rational factor: we separate this into a scaling by a *positive* rational number, and a possible $y \mapsto -y$ change. A permutation of the roots corresponds to the action of the dihedral group $\mathcal{S}_3 \simeq D_6$. The group generated by D_6 and $z \mapsto -z$ is the group of isometries of the hexagon of the sixth-roots of unity, D_{12}. The fundamental domain is "half" of the one for D_6. First let us observe that $(X - 2)(X - 1)X$ is not a nice polynomial so $(2 + j)\mathbb{Q}^*$ can never hold the Lagrange resolvent of a nice polynomial. So, for C whose polynomials have distinct roots, a unique representative up to positive rescaling can be found in the angular sector delimited by the positive real axis and $\mathbb{R}^+ \exp(\pi i/6) = \mathbb{R}^+(2+j)$, i.e. $y_1 = b+aj$, $0 < 2a < b$. Normalizing so that $b = 1$, this gives $y_1 = 1 + aj$, $0 < a < \frac{1}{2}$. This matches with Theorem 7.

The quantity y_1y_2 is greatly relevant to the study of nice polynomials.

$$\begin{aligned} y_1y_2 &= (x_1 + x_2j + x_3j^2)(x_1 + x_2j^2 + x_3j) \\ &= x_1^2 + x_2^2 + x_3^2 - x_1x_2 - x_2x_3 - x_3x_1 \qquad (j + j^2 = -1) \end{aligned}$$

This has an interpretation as the reduced discriminant of the *derivative* of $P = (X-x_1)(X-x_2)(X-x_3)$:

$$\begin{aligned} P' &= 3X^2 - 2(x_1 + x_2 + x_3)X + (x_1x_2 + x_2x_3 + x_3x_1) \\ \implies \Delta &= (x_1 + x_2 + x_3)^2 - 3(x_1x_2 + x_2x_3 + x_3x_1) = y_1y_2 \end{aligned}$$

So, for x_1, x_2, x_3 rational roots, P is a nice rational polynomial if and only if $y_1y_2 = y_1\overline{y_1}$ is a rational square. We are thus brought to a question in the number field $\mathbb{Q}(j)$: which elements $y \in \mathbb{Q}(j)$ have a norm $N(y) = y\overline{y}$ which is a rational square? If $N(y) = t^2$ (and $y \neq 0$), then $N(y/t) = 1$, and the problem is equivalent to understanding which elements $y \in \mathbb{Q}(j)$ have norm 1, i.e. are on the unit circle. Here are the answers:

Theorem 8. *An element $y \in \mathbb{Q}(j)$ is such that $N(y)$ is a rational square if and only there exists $t \in \mathbb{Q}$, and $z \in \mathbb{Q}(j)$ such that $y = tz^2$.*

Theorem 9. *An element $y \in \mathbb{Q}(j)$ is of norm 1 if and only if it can be written as $z/\overline{z}$ for some $z \in \mathbb{Q}(j)^*$.*

These two theorems have their natural home in algebraic number theory (the beautiful Gauss theory of factorization of primes in $\mathbb{Z}[j]$ and $\mathbb{Z}[i]$ started it all), but this is beyond the scope we have imposed ourselves for this paper, and we seek an alternate route. Let us first confirm our indication that they are mutually equivalent:

Proof of equivalence. Assume Theorem 8 and let y such that $N(y) = 1$. In particular it is a square so $y = tz^2$ and $1 = t^2N(z)^2$, so $t = \pm(z\overline{z})^{-1}$, and $y = \pm z^2/(z\overline{z}) = \pm z/\overline{z}$. To conclude, we observe that $i\sqrt{3} = j + (1 + j) \in \mathbb{Q}(j)$ and the quotient with its conjugate is -1.

Conversely, let's assume Theorem 9 and let y be such that $N(y) = t^2$. We can assume $y \neq 0$, then y/t has norm 1, so $y/t = z/\overline{z} = z^2/N(z)$, $y = tN(z)^{-1}z^2$ is a rational times a square. □

Theorem 9 has a natural approach via the parametrization of rational points on an ellipse: if $y = a + bj$, then $N(y) = a^2 + b^2 - ab$ so we are looking at the ellipse equation $a^2 + b^2 - ab = 1$. As this ellipse already has known points (the six points corresponding to the roots of unity $\langle\omega\rangle$), the well-known "slope of chord" parametrization method would help us describe the rational solutions. But we will not repeat this here as it is done in most papers dealing with nice cubics, such as Zuser [15].

We would like some "effortless" way of understanding this topic! It would be a bit of a cheat to exploit our "effortless"-acquired understanding of nice polynomials, which, as we explained, is intimately associated with the $y\overline{y} = \square$ equation. We want another approach. The key observation here is that the equation $y = z/\overline{z}$ is a homogeneous $\mathbb{Q}$-*linear* constraint on the unknown $z \in \mathbb{Q}(j)$. So the theory of linear systems will solve this: we only have to compute some determinant. We can even do this abstractly:

Proof of Theorem 9. Let f_y be the $\mathbb{Q}$-linear endomorphism of $\mathbb{Q}(j)$ defined by $f_y(z) = y\overline{z}$. Then $f_y^2(z) = N(y)z$. So, if $N(y) = 1$ (in particular $y \neq 0$), then $(f_y - \mathrm{Id}) \circ (f_y + \mathrm{Id}) = f_y^2 - \mathrm{Id} = 0$. If the equation $f_y(z) = z$ has no non-zero solution then $f_y - \mathrm{Id}$ is injective and we obtain $f_y = -\mathrm{Id}$ which is wrong: certainly $\overline{z}/z$ is not constant on $\mathbb{Q}(j)^*$. So there is a non-zero z with $f_y(z) = z$. □

If we express things with a matrix using the $(1, j)$ basis we obtain for f_y associated to $y = \alpha + \beta j$ the $\begin{pmatrix} \alpha & -\alpha+\beta \\ \beta & -\alpha \end{pmatrix}$ matrix whose determinant is $-\alpha^2 + \alpha\beta - \beta^2 = -N(y)$, and whose trace is zero. The characteristic equation is $\lambda^2 = N(y)$ and it has rational solutions if and only $N(y)$ is a rational square (which could be used for a proof of Theorem 8).

Let us recapitulate what we have so far: nice cubic polynomials $Q = (X - x_1)(X - x_2)(X - x_3)$ are characterized from the fact that the Lagrange resolvent $y(Q) = x_1 + x_2 j + x_3 j^2$ verifies $N(y) = \square$, or equivalently from Theorem 8 that $y = tz^2$ for some $t \in \mathbb{Q}$, $z \in \mathbb{Q}(j)$. There is a D_6 ambiguity in $y(Q)$ and if we consider equivalence classes it becomes a $D_6 \times \mathbb{Q}^* = D_{12} \times \mathbb{Q}^{*+}$ ambiguity. Assuming that the roots are distinct, $y = \beta + \alpha j$ is necessarily with $\beta \neq 0$, and modulo $\mathbb{Q}^*$, we can replace it with $1 + aj$, $a = \alpha/\beta$. This means taking the intercept of $\mathbb{Q}y$ with the line D going through 1 and $\omega = 1 + j$. We will call D the a-line. Then $D \cup \{\infty\}$ is in natural bijection with $\mathbb{Q}(j)^*/\mathbb{Q}^*$, and we will use the notation $[y]$ for the point $1 + aj$ on D corresponding to $y = \beta + \alpha j$.

We can compute the induced $\mathcal{S}_3 \simeq D_6$ left-action on the a-line:

$$
\begin{aligned}
[\tau_{12}(1 + aj)] &= [j + a] = [1 + a^{-1} j] \\
[\tau_{23}(1 + aj)] &= [1 + aj^2] = [1 - a - aj] = [1 + a/(a - 1)j] \\
[\tau_{13}(1 + aj)] &= [j^2 + aj] = [-1 + (a - 1)j] = [1 + (1 - a)j] \\
[j(1 + aj)] &= [-a + (1 - a)j] = [1 + (a - 1)/aj] \\
[j^2(1 + aj)] &= [a - 1 - j] = [1 + (1 - a)^{-1} j].
\end{aligned}
$$

It has the same orbits as the right action considered in the proof of Theorem 7 but we leave it to the reader as an exercise to elucidate the inner automorphism ϕ of $\mathcal{S}_3$ such that $[\phi(\sigma^{-1})(1 + aj)] = [1 + (a \cdot \sigma)j]$...

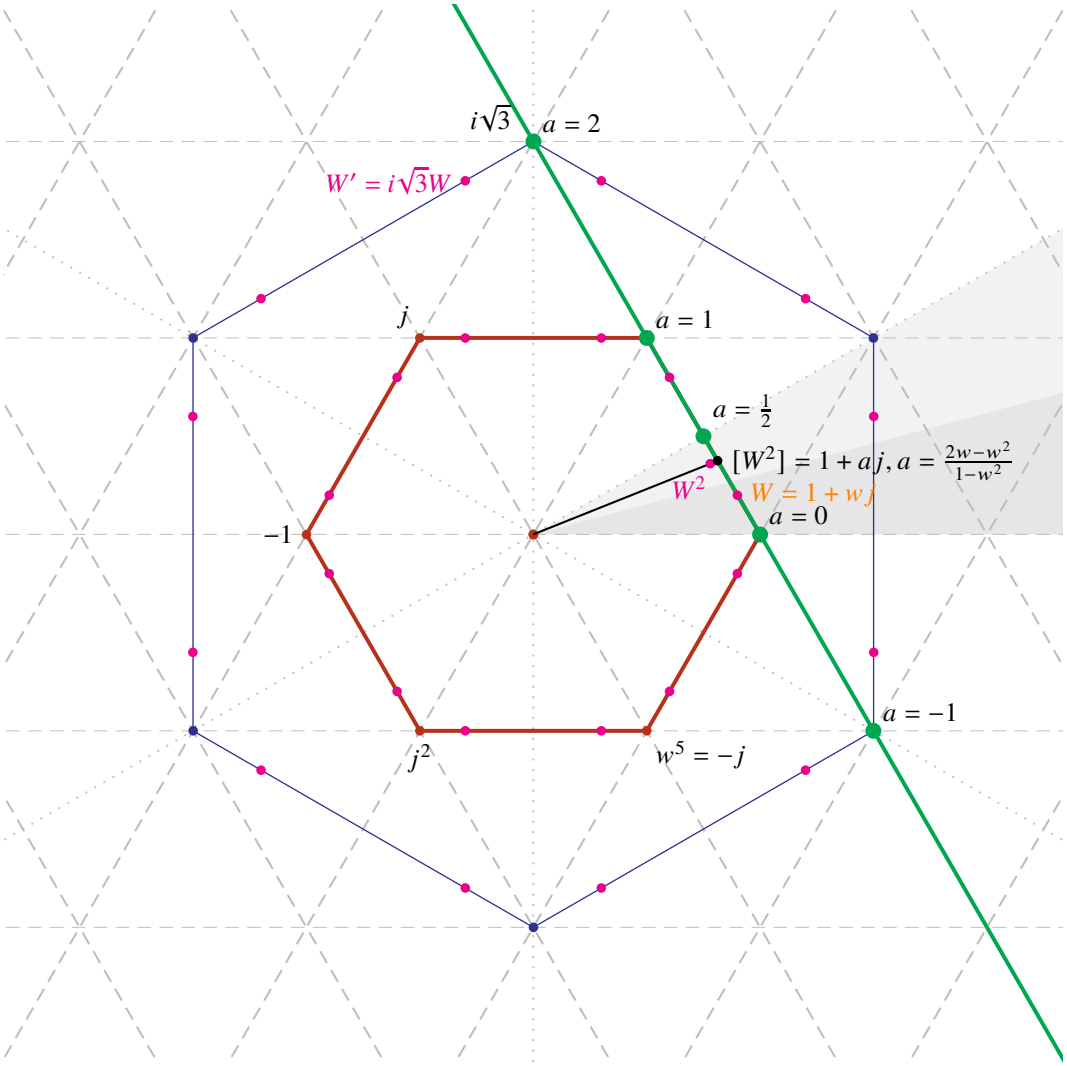

Figure 4: Hexagonal lattice in complex plane and orbits of dihedral group

The $w \mapsto a$ map parametrizing nice cubic polynomials is simply the squaring map in complex plane as applied to elements of $\mathbb{Q}(j)$, and then projectivized to the quotient $\mathbb{Q}(j)/\mathbb{Q}^*$.

From a point W in complex plane not on the symmetry lines of the unit hexagon, six points are obtained via the action of the symmetries D_6 of the equilateral triangle of cube roots of unity; and twelve points from the group D_{12} of symmetries of the hexagon, which also contains $z \mapsto -z$. Central projection from the origin to the line $1 + \mathbb{R}j$ then gives $12/2 = 6$ points $1 + wj$ (they are indeed distinct). Squaring the $1 + wj$ (or the points of the W-orbit) in complex plane and projecting gives 6 points $1 + aj$ (they are distinct). If w is rational, then the a's are also.

The picture is with $w = \frac{1}{5}$, which gives $a = \frac{3}{8}$.

Another D_{12} orbit in the complex plane is obtained from first one by applying a rotation by a right angle and scaling by $\sqrt{3}$, which replaces W by W'. So after projection we now have twelve values of w. The square+project operation gives the same already obtained 6 values for $1 + aj$ ($(i\sqrt{3}z)^2 = -3z^2$ gives same image as z^2). Altogether this means there are twelve $w \in \mathbb{Q}$ giving the six a's of a D_6 orbit on $1 + \mathbb{Q}j \cup \{\infty\}$.

These twelve w values are the orbit of the projective action on the $1 + \mathbb{R}j$ line of $D_{24}/\{\pm \mathrm{Id}\}$ where D_{24} is the group of symmetries of the dodecagon. The action in the plane of D_{24} (which adds $z \mapsto iz$ to D_{12}) does not leave stable $\mathbb{Q}(j)$ as $i \notin \mathbb{Q}(j)$. But $i\sqrt{3} \in \mathbb{Q}(j)$, so the induced projective action on $1 + \mathbb{R}j \cup \{\infty\}$ leaves stable $1 + \mathbb{Q}j \cup \{\infty\}$.

The shaded angular sector of opening angle 30° is a fundamental domain for the action of D_{12} and its bottom half of opening angle 15° is fundamental domain for D_{24}, which maps to the $0 < w < 2 - \sqrt{3}$ range in Theorem 2.

The equation $y = 1 + aj = tz^2 = t(v + uj)^2 = t(v^2 + 2vuj + u^2j^2)$ becomes:

$$\left.\begin{aligned} 1 &= t(v^2 - u^2) \\ a &= t(2vu - u^2) \end{aligned}\right\} \implies a = \frac{2vu - u^2}{v^2 - u^2} = \frac{2w - w^2}{1 - w^2} \qquad (w = \frac{u}{v})$$

which is precisely the parametrization from Theorem 2 of nice cubics $Q = X(X-1)(X-a)$. It can not happen that $v = 0$, as this would give $y = tu^2j^2$ which is on one the three lines of symmetries of $\{1, j, j^2\}$ corresponding to polynomials with multiple roots. In terms of w, $[y] = [(1+wj)^2]$, in other words we are simply inducing on $D \cup \{\infty\} \simeq \mathbb{Q}(j)^*/\mathbb{Q}^*$ the squaring operation of $\mathbb{Q}(j)$.

Let us examine what happens if we replace z by points of its D_6 orbit in the $y = tz^2$ relation: $t(jz)^2 = j^2y$, $t(j^2z)^2 = jy$, $t(\overline{z})^2 = \overline{y}$, $t(j\overline{z})^2 = j^2\overline{y}$, $t(j^2\overline{z})^2 = j\overline{y}$: they are mapped to the six points of the y orbit. More precisely the above establishes

$$t(\sigma \cdot z)^2 = (\tau_{23}\sigma\tau_{23}) \cdot tz^2 \ ,$$

as τ_{23} does the exchange $j \leftrightarrow j^2$ (or is seen as complex conjugation). This explains the correspondence table given previously between the D_6-orbit of w and the one of $a = (w^2 - 2w)/(w^2 - 1)$.

The expression $a = \frac{2w-w^2}{1-w^2}$ is two-to-one: $(1 - a)w^2 - 2w + a = 0$. If w_1 and w_2 are the two roots, then we can eliminate a from $w_1 + w_2 = 2/(1 - a)$, $w_1w_2 = a/(1 - a) = -1 + 1/(1 - a)$:

$$2w_1w_2 - w_1 - w_2 + 2 = 0 \implies \begin{cases} w_1 &= \dfrac{w_2 - 2}{2w_2 - 1} \\ w_2 &= \dfrac{w_1 - 2}{2w_1 - 1} \end{cases}$$

This corresponds to the induced action on the $1 + wj$ line via the $\mathbb{Q}$-linear map $v + uj \mapsto (2u-v)+(u-2v)j = u(2+j)-v(1+2j) = uj(2j^2+1)-v(1+2j) = -(1+2j)(v+uj) = -i\sqrt{3}(v + uj)$. Let us denote by ρ this induced action on the quotient $\mathbb{Q}(j)^*/\mathbb{Q}^*$. Then $\rho^2 = \mathrm{Id}$. Let use examine what is the group generated by this homography of order two and the previously studied D_6 action (which we expressed in the a-notation).

As ρ is induced by a complex multiplication, as are the 3-cycle elements of D_6, they commute. The composition $\rho\tau_{23}$ is induced from $z \mapsto -i\sqrt{3}\overline{z} = -\overline{(-i\sqrt{3})z}$, and as the sign -1 disappears in the quotient by $\mathbb{Q}^*$, this is same as $\tau_{23}\rho$. As D_6 is generated by the elements accounted for so-far, this means that ρ commutes with the full D_6 action on $\mathbb{Q}(j)^*/\mathbb{Q}^*$.

So we obtain a group $G \simeq D_6 \times \mathbb{Z}/2\mathbb{Z}$ acting on the w-line $\mathbb{Q}(j)^*/\mathbb{Q}^*$. This group is of cardinality 12, because it contains an isomorphic copy of D_6, and ρ isn't there (as it commutes with all of D_6). It is thus isomorphic with D_{12}, which also has a structure

$D_6 \times \mathbb{Z}/2\mathbb{Z}$ where it is $z \mapsto -z$ which plays the role of the order two element commuting with D_6. Any $1 + wj$ with $w \notin \{-1, 0, \frac{1}{2}, 1, 2, \infty\}$ has an orbit of full cardinality: the squaring map $[(1 + wj)^2] = [1 + aj]$ has two antecedents for each image ($(1 - a)w^2 - 2w + a = 0$ has reduced discriminant $1 - a + a^2 > 0$, also works for $a = \infty$, then $w = \pm 1$, but not for the two $a \in \{\omega, \overline{\omega}\}$ special complex values: and indeed it is a well known algebro-analytico-geometric fact that the projective line can not have a non-ramified connected covering), and we have shown that the D_6-orbit on the $[1 + wj]$ line maps (not covariantly) to the D_6-orbit on the $[1 + aj]$ (projective) line, which has cardinality 6 if $a \notin \{0, 1, \infty\}$ and $a \notin \{-1, \frac{1}{2}, 2\}$, but the latter values are excluded for nice polynomials (they can not be obtained for $w \in \mathbb{Q}$), and the former values correspond to $w = -1, 0, \frac{1}{2}, 1, 2, \infty$.

Let us list explicitly the twelve homographic images of $w \notin \{-1, 0, \frac{1}{2}, 1, 2, \infty\}$. There is a unique cyclic group of order 6 in D_{12}, and it has two generators which will be given by the actions of $\rho\sigma$ where $\sigma = (123)$ (i.e. multiplication by j) or (132) (multiplication by j^2). We choose the latter (because $-j^2 = \omega$ would rotate in the direct trigonometrical sense). We know that ρ acts as the homography associated with $\left(\begin{smallmatrix} 1 & -2 \\ 2 & -1 \end{smallmatrix}\right)$, and we checked that the multiplication by j^2 induces $w \mapsto (1-w)^{-1}$ on the projective line, i.e. is associated with $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 1 \end{smallmatrix}\right)$. So $\lambda = \rho\sigma$ of order 6 acts as the homography $w \mapsto \frac{2w-1}{w+1}$ (we computed this from the product of the two 2×2 matrices above). Iterating, we obtain the following images induced by direct transforms on the complex plane:

$$w, \frac{2w-1}{w+1}, \frac{w-1}{w}, \frac{w-2}{2w-1}, \frac{1}{1-w}, \frac{w+1}{2-w} \tag{6}$$

The other 6 can be obtained from composing with any one of the three symmetries in D_6, for example τ_{23}, which acts like complex conjugation $j \mapsto j^2 = -1 - j$ which gives on $[1 + wj]$ the homography with matrix $\left(\begin{smallmatrix} 1 & 0 \\ 1 & -1 \end{smallmatrix}\right)$. Here are thus the images induced from indirect transforms on the plane:

$$\frac{w}{w-1}, \frac{2w-1}{w-2}, 1-w, \frac{2-w}{w+1}, w^{-1}, \frac{w+1}{2w-1} \ . \tag{7}$$

The pairs (w_1, w_2) which map to the same a are to be found at indices differing by 3 modulo 6 in these two lists (because λ^3 is the central element which realizes $w_2 = \rho(w_1)$, $w_1 = \rho(w_2)$). This completes the proof of Theorem 3.

We end with a re-interpretation of this D_{12}. Let us consider the dodecagon whose vertices are the twelfth-roots of unity. Its symmetry group is the dihedral group of cardinality 24, D_{24}, whose center $\mathcal{Z}$ consists of the two transforms $z \mapsto z$, and $z \mapsto -z$. Projectivizing its action to the a-line $1 + \mathbb{R}j$, we obtain a faithful action of $D_{24}/\mathcal{Z}$. The map $D_6 \to D_{24}/\mathcal{Z}$ is injective but from D_{12} it is two-to-one as $\mathcal{Z} \subset D_{12}$. The cardinality 12 group $D_{24}/\mathcal{Z}$ is however isomorphic to D_{12}, as the action ρ of (projectivized) multiplication by i is a central element: $\overline{iz} = -i\overline{z}$ becomes $[\overline{iz}] = [i\overline{z}]$ which means that

ρ commutes with the element of D_6 originating in complex conjugation on the plane and as it commutes with those originating in rotations, it commutes with all of D_6. In the plane the image of the hexagon of sixth roots of unity by an element g of D_{24} is either itself (if $g \in D_{12}$) or the hexagon with the other six vertices of the dodecagon. So the elements of $D_{24}/\mathcal{Z}$ not in (the image of) D_6 are those which exchange the two cardinality 3 orbits $\{0, 1, \infty\}$ and $\{-1, \frac{1}{2}, 2\}$ of the D_6 homographies. The central element ρ is the one which maps 0 to 2, 1 to -1 and ∞ to $\frac{1}{2}$. Let us prove that it is the only non trivial homography g (even allowing complex coefficients) which commutes with the $\mathcal{S}_3 \simeq D_6$ group of $\{0, 1, \infty\}$-preserving homographies: as there is only one other cardinality 3 orbit $\{-1, \frac{1}{2}, 2\}$, such a g must map $\{0, 1, \infty\}$ to either itself, but then it would be an element of the center of $\mathcal{S}_3$ hence the identity, or to $\{-1, \frac{1}{2}, 2\}$. And for the same reason it must map $\{-1, \frac{1}{2}, 2\}$ to $\{0, 1, \infty\}$, so if we have two solutions g_1 and g_2, then $g_2 \circ g_1$ maps $\{0, 1, \infty\}$ to itself and commutes with $\mathcal{S}_3$ hence must be the identity. So in particular $g^2 = \mathrm{Id}$, and g is unique, if it exists. And it exists from the $D_{24}/\mathcal{Z}$ construction or direct verification once it has been found to be $t \mapsto \frac{t-2}{2t-1}$.

One can also prove this unicity using matrices, but attention that commutativity of two homographies only means that representative matrices either commute or anti-commute!

List of Figures

References

[1] A. Bremner and B. Carrillo, *On K-derived quartics*, Journal of Number Theory 168 (2016) 276–291.

[2] T. Bruggeman and T. Gush, *Nice cubic polynomials for curve sketching*, Math. Magazine, 53(4) (1980) 233–234.

[3] R. H. Buchholz and S. M. Kelly, *Rational derived quartics*, Bull. Austral. Math. Soc. 51, No. 1 (1995), 121–132.

[4] R. H. Buchholz and J. A. MacDougall, *When Newton met Diophantus: A study of rational-derived polynomials and their extensions to quadratic fields*, J. Number Theory 81 (2000) 210–233.

[5] J. Buddenhagen, C. Ford, and M. May, *Nice cubic polynomials, Pythagorean triples, and the law of cosines*, Math. Mag. 65 (1992) 244–249.

[6] C. K. Caldwell, *Nice polynomials of degree 4*, Math. Spectrum 23(2) (1990) 36–39.

[7] C. E. Carroll, *Polynomials all of whose derivatives have integer roots*, Amer. Math. Monthly, 96(2) (1989) 129–130.

[8] M. Chapple, *A cubic equation with rational roots such that it and its derived equation also has rational roots*, Bull. Math. Teachers Secondary Schools, 11 (1960) 5–7, 1960, (re-published in Aust. Senior Math. J. 4(1) (1990) 57–60).

[9] A. Choudhry, *A diophantine problem from calculus*, J. Number Theory 153 (2015) 354–363.

[10] J.-C. Evard, *Polynomials whose roots and critical points are integers*, arXiv:math/0407256

[11] E. V. Flynn, *On $\mathbb{Q}$-derived polynomials*, Proc. Edinburgh Math. Soc. (2) 44(1) (2001) 103–110.

[12] W. Galvin, *'Nice' cubic polynomials with 'nice' derivatives*, Austral. Senior Math. J. 8 (1990) 17–21.

[13] W. P. Galvin and J. A. MacDougall, *'Nice' Quartic Polynomials – The Sequel*, Austral. Senior Math. J. 8 (1994) 23–27.

[14] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed. Springer-Verlag, GTM Series 84 (2010)

[15] K. Zuser, *Über eine gewisse Klasse von ganzen rationalen Funktionen 3. Grades* (in German), Elem. Math. 18 (1963) 101–104.

Jean-François Burnol
Lille
France

Jürgen Gilg
Stuttgart
Germany