On polynomials of
Birch-Chowla-Hall-Schinzel-Davenport-Stothers-Zannier-Beukers-Stewart
and weighted plane trees

Alexander Zvonkin
(University of Bordeaux, France)

Joint work with
Fedor Pakovich
Ben-Gurion University of the Negev, Be'er Sheva, Israel
Nikolai Adrianov
Moscow State University, Russia

RuFiDiM-3, Petrozavodsk, Russia
September 15, 2014

I. Polynomials

1965: B. J. Birch, S. Chowla, M. Hall Jr., A. Schinzel

Let A and B be two coprime polynomials, $A, B \in \mathbb{C}[x]$. What is the minimum possible degree of the difference $R = A^3 - B^2$?

Example (N. Elkies, 2000)

$$\begin{aligned}
P &= (x^{10} - 2x^9 + 33x^8 - 12x^7 + 378x^6 + 336x^5 + 2862x^4 \\
&\quad + 2652x^3 + 14\,397x^2 + 9922x + 18\,553)^3, \\[1em]
Q &= (x^{15} - 3x^{14} + 51x^{13} - 67x^{12} + 969x^{11} + 33x^{10} + 10\,963x^9 \\
&\quad + 9729x^8 + 96\,507x^7 + 108\,631x^6 + 580\,785x^5 + 700\,503x^4 \\
&\quad + 2\,102\,099x^3 + 1\,877\,667x^2 + 3\,904\,161x + 1\,164\,691)^2, \\[1em]
R &= P - Q \\[1em]
&= 2^6\, 3^{15}(5x^6 - 6x^5 + 111x^4 + 64x^3 + 795x^2 + 1254x + 5477).
\end{aligned}$$

Remark. The fact that in this example the coefficients are rational numbers is a great chance. To find them, we had to solve a huge system of algebraic equations, most of them of degree 3. The coefficients might be algebraic numbers.

Two conjectures (1965): Let

$$\deg A = 2k, \quad \deg B = 3k,$$

so that

$$\deg A^3 = \deg B^2 = 6k;$$

then

1. $\deg(A^3 - B^2) \geq k + 1$;
2. this bound is attained.

In the previous example $k = 5$.

1965: The first conjecture proved by H. Davenport.

1981: W. W. Stothers proved that the bound is attained for all k.

We see that the second conjecture turned out to be more difficult: it remained open for 16 years. There were also several publication in between.

1995: The problem is generalized (and solved) by U. Zannier:

Let two partitions of an integer n be given:

$$\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_p), \qquad \beta = (\beta_1, \beta_2, \ldots, \beta_q),$$

$$\sum_{i=1}^{p} \alpha_i = \sum_{j=1}^{q} \beta_j = n,$$

and let P and Q be two coprime polynomials of degree n with complex coefficients, such that

$$P(x) = \prod_{i=1}^{p} (x - a_i)^{\alpha_i}, \qquad Q(x) = \prod_{j=1}^{q} (x - b_j)^{\beta_j}.$$

Denote $R = P - Q$.

Question: What is the minimum possible degree of R?

In the initial problem $\alpha = (3, 3, \ldots, 3)$, $\beta = (2, 2, \ldots, 2)$.

Two technical assumptions:

1. The greatest common divisor of $\alpha_1, \ldots, \alpha_p, \beta_1, \ldots, \beta_q$ is 1.

2. $p + q \le n + 1$.

(We can do without them, but the statements would become more cumbersome.)

Theorem (U. Zannier, 1995)

1. $\deg R \ge (n+1) - (p+q)$.

2. This bound is attained for any pair of partitions $\alpha, \beta \vdash n$ satisfying the above assumptions.

In the above example, $n = 6k$, $p = 2k$, $q = 3k$.

2010: F. Beukers, C. Stewart: Search for polynomials A and B such that

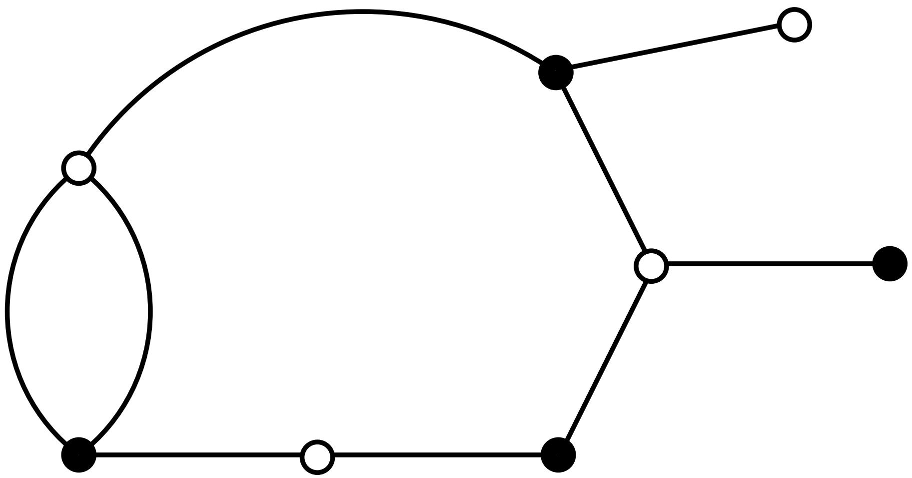
1. The degree of the difference $A^k - B^l$ attains its minimum;

2. $\underline{A \text{ and } B \text{ have rational coefficients}}$.

Several infinite series and several sporadic examples.

II. Maps

All our maps will be **plane** and **bicolored**.

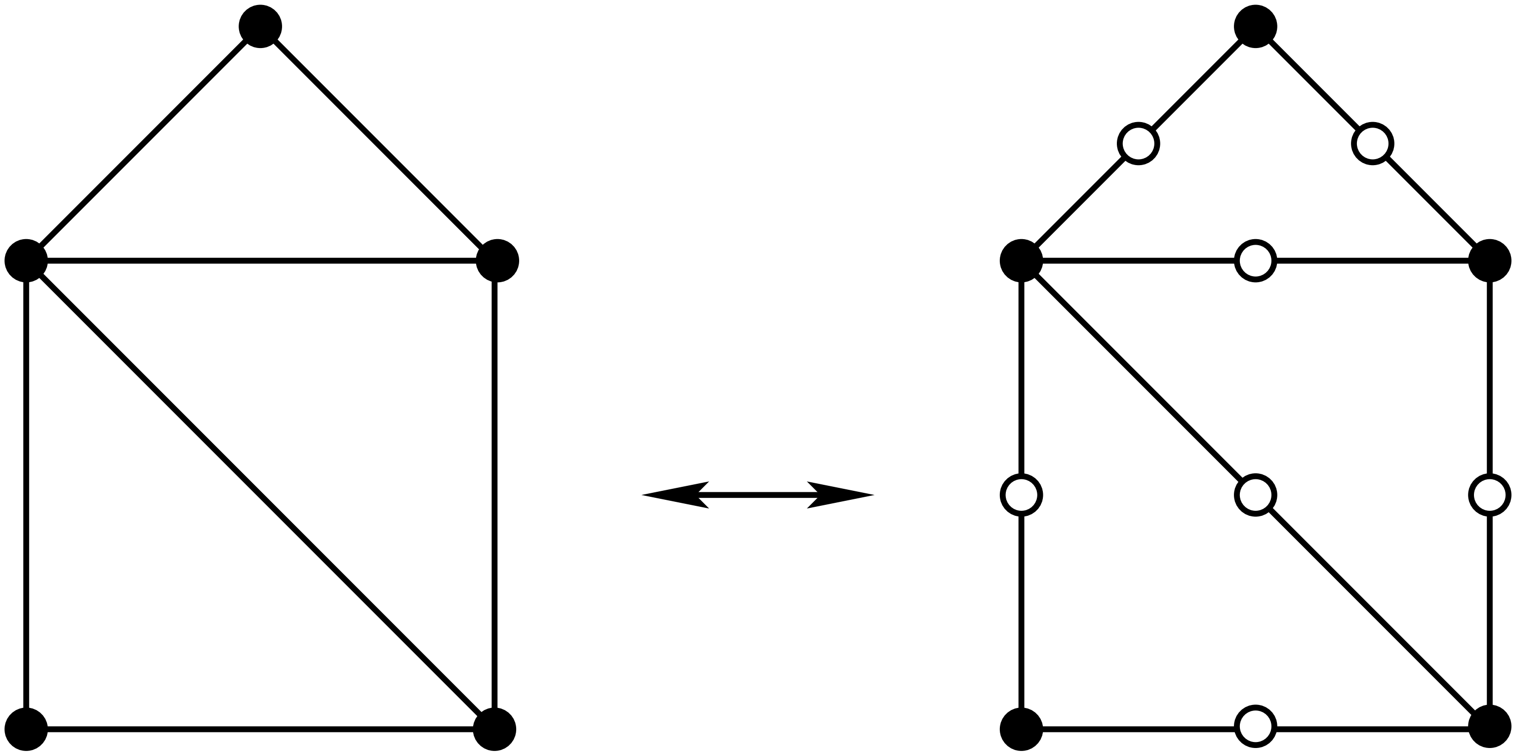


A **face degree** is defined as a **half** of the number of surrounding edges.

Thus, the sum of degrees of black vertices, of white vertices, and of the faces, is equal to the number of edges.

The number of edges is the **degree of the map**.

Convention. When <u>**all white vertices are of degree 2**</u> we do not draw them explicitly.
We may even "forget" about them and think of "ordinary" maps, with only black vertices.



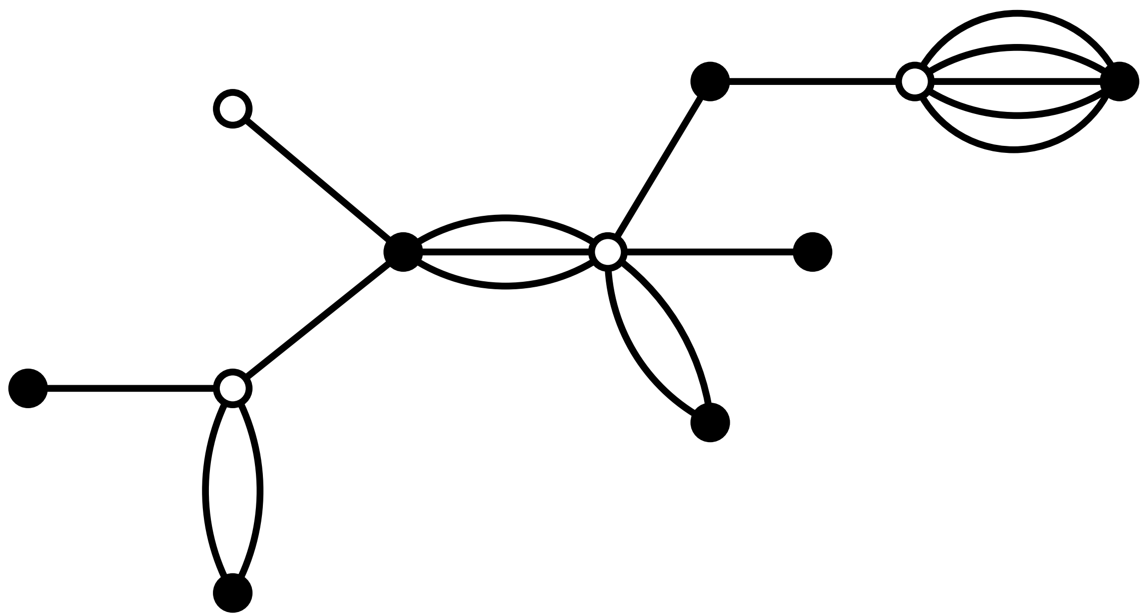
Remark. Two notions of the face degree are coherent. The degree of the map is computed according the bicolored model.

In this talk we are specially interested in the

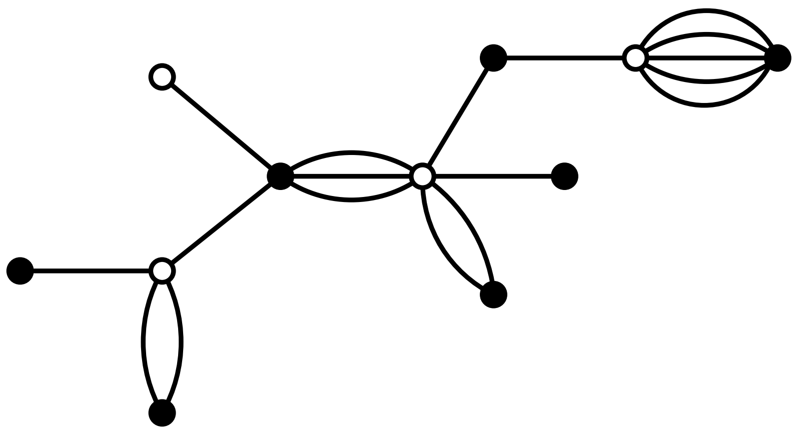
maps with all their faces

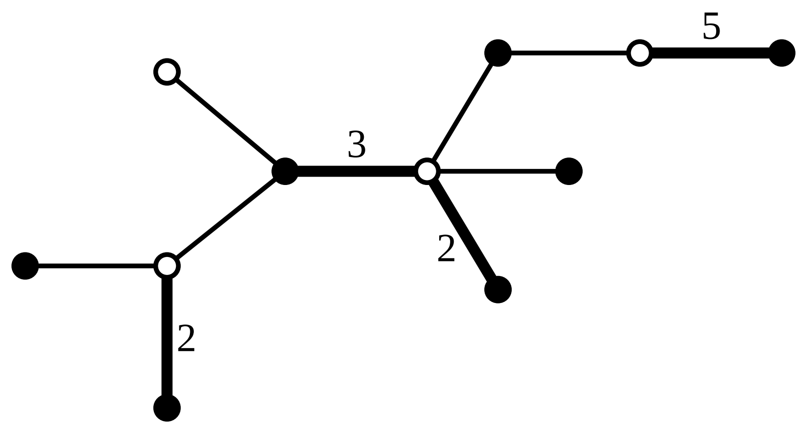
(except the outer one)

being of degree 1:



It is much easier to handle the corresponding **weighted trees**:





The **weight of an edge** is a positive integer.

The **degree of a vertex** is the sum of the weights of the edges incident to this vertex.

The **total weight** of a tree is equal to the degree of the underlying map.

III. Belyi functions

Let $\overline{\mathbb{C}}$ denote the complex Riemann sphere, $\overline{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$, and let $f : \overline{\mathbb{C}} \to \overline{\mathbb{C}}$ be a rational function with complex coefficients.

A **critical value** of f is a point $y \in \overline{\mathbb{C}}$ such that the equation

$$f(x) = y$$

has multiple roots.

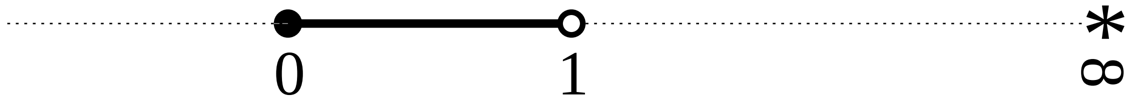
Belyi function is a rational function which has only **three critical values**, namely,

$$y = 0, \quad y = 1, \quad \text{and} \quad y = \infty.$$

The choice of $0, 1, \infty$ is a mere tradition. Indeed, any three points can be placed to any three given positions by making a linear fractional transformation.

Let us take a Belyi function f and consider the preimage

$$M = f^{-1}([0,1]).$$



Then we get the following object:

- M is a bicolored map with n edges, where $n = \deg f$.
- Black vertices are the points $x \in f^{-1}(0)$, and their degrees are equal to the multiplicities of the roots of $f(x) = 0$.
- White vertices are the points $x \in f^{-1}(1)$, and their degrees are equal to the multiplicities of the roots of $f(x) = 1$.
- Inside each face there is exactly one pole $x \in f^{-1}(\infty)$, and the degree of the face is equal to the multiplicity of this pole.

- **For any bicolored plane map M there exists a Belyi function f such that M is isomorphic to $f^{-1}([0,1])$.**

  This function is unique up to a linear fractional transformation of the variable x.

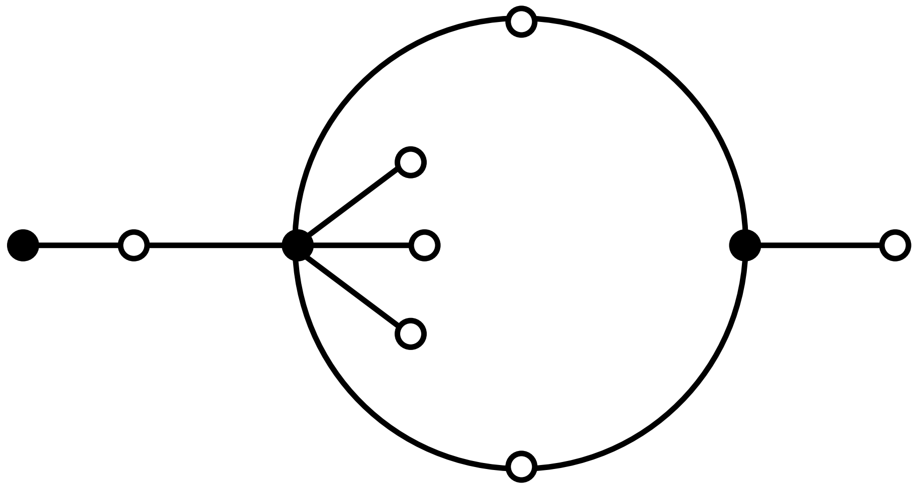
- This statement is a particular case of **Riemann's Existence Theorem**.

- The coefficients of f can be made **algebraic numbers**.

- A striking consequence: the **Galois group** $\Gamma = \mathrm{Aut}(\overline{\mathbb{Q}}|\mathbb{Q})$ acts on maps.

- The **theory of dessins d'enfants** ("children's drawings" in French) studies combinatorial invariants of this action, but not only. . .

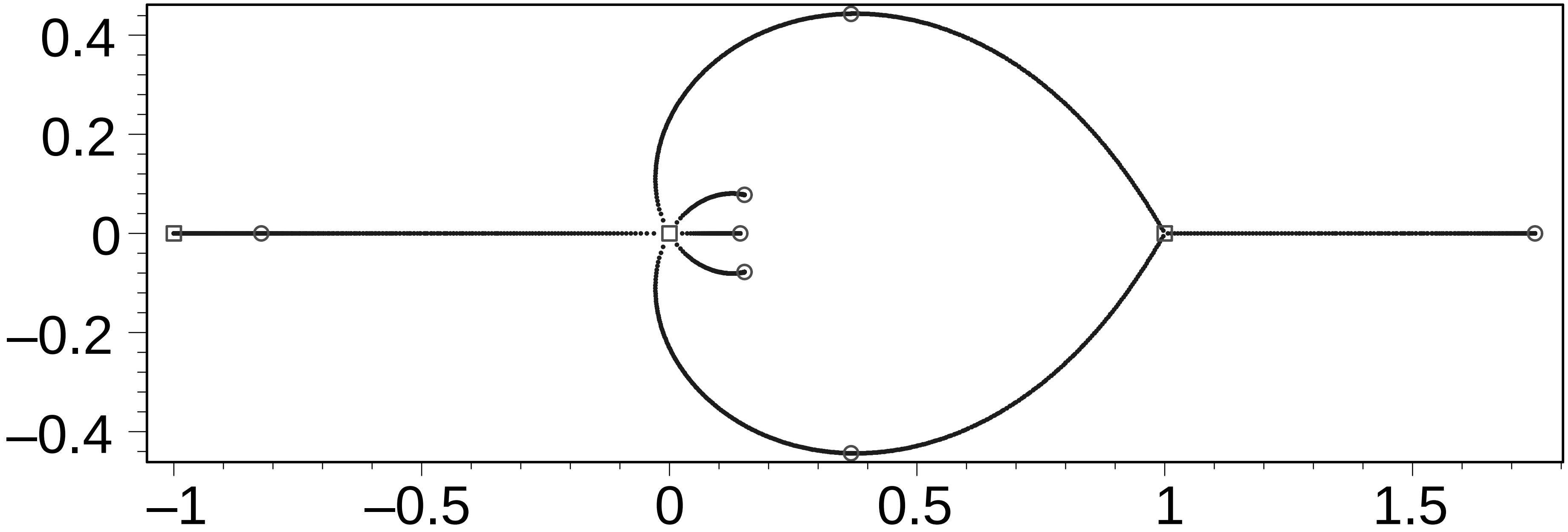
Example



$$f(x) = \frac{50000}{27} \cdot \frac{x^6\,(x-1)^3\,(x+1)}{(x^2+4\,x-1)^5}\,,$$

$$f(x)-1 = \frac{1}{27} \cdot \frac{(11\,x^3+x^2-3\,x+3)^2\,(7\,x-1)\,(59\,x^3-121\,x^2+33\,x-3)}{(x^2+4\,x-1)^5}\,.$$

No other critical values except 0, 1 and ∞.



The **dessin d'enfant** obtained as $f^{-1}([0,1])$ for

$$f(x) = \frac{50\,000}{27} \cdot \frac{x^6\,(x-1)^3\,(x+1)}{(x^2+4\,x-1)^5}.$$

IV. Back to polynomials

Recall that

$$P(x) = \prod_{i=1}^{p} (x - a_i)^{\alpha_i}, \quad Q(x) = \prod_{j=1}^{q} (x - b_j)^{\beta_j}, \quad P - Q = R.$$

Instead of $P - Q = R$ let us write $P - R = Q$ and divide by R:

$$f = \frac{P}{R}, \qquad f - 1 = \frac{Q}{R}.$$

- $f = 0 \;\Leftrightarrow\; P = 0$, hence 0 is a critical value of f;

- $f = 1 \;\Leftrightarrow\; Q = 0$, hence 1 is a critical value of f;

- $f = \infty$ has a multiple root at infinity (if $\deg R < \deg P - 1$); hence ∞ is a critical value.

What if f is a Belyi function? What is the corresponding map?

The map M corresponding to f has the following characteristics:

- it has $p+q$ vertices (p black ones and q white ones);
- the number of edges is $n = \deg f$;
- Euler's formula:

$$(p+q) - n + \#(\text{faces}) = 2,$$

  hence

$$\#(\text{faces}) = (n+2) - (p+q);$$

- faces correspond to poles;
  the pole at ∞ corresponds to the outer face;
  other poles are roots of R (which is the denominator of f);
- <u>Conclusion</u>: the polynomial R has $(n+1) - (p+q)$ distinct roots.

Suite:

- the polynomial R has $(n+1)-(p+q)$ distinct roots;

- hence, $\deg R \geq (n+1)-(p+q)$;

- this lower bound is attained if and only if the roots of R are simple (that is, not multiple),

- which means that all the faces of the map M except the outer one are of degree 1.

Remark. The Riemann-Hurwitz formula implies that if f is *not* a Belyi function, that is, if it has more than three critical values, than the above bound cannot be attained.

First result (A. Z.) A great simplification of Zannier's proof.

For a given (α, β), the existence of a tree implies the attainablity of the lower bound for $\deg R$.

It is much easier to draw trees than to work directly with polynomials.

For number theorists it took 30 years: 1965 . . . 1995.

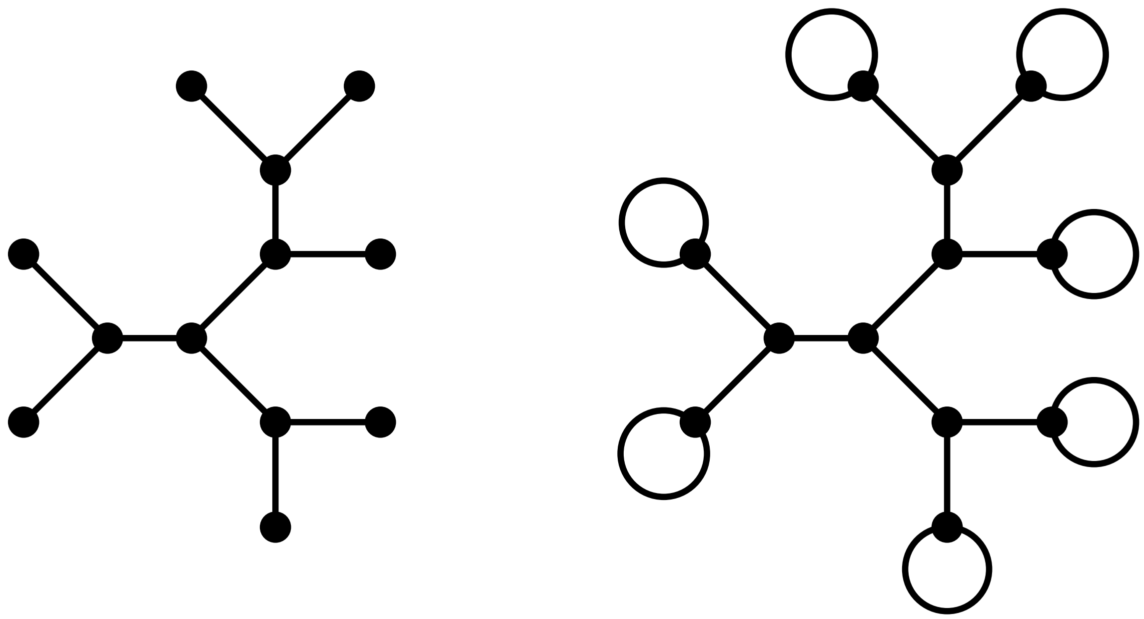
Let us look how it works in the particular case $A^3 - B^2$.

We should draw a map with the following characteristics:

- all its black vertices are of degree 3;
- all its white vertices are of degree 2 (so forget them and think of "ordianry" maps with only black vertices);
- all its faces except the outer one are of degree 1.

Recall that it is a problem which was studied by (at least) five famous mathematicians and a number of less famous but also very good mathematicians, and which remained open for 16 years (from 1965 to 1981).

Solution:



First stage Second stage

(1) Draw a tree with inner nodes of degree 3. (2) Attach a loop to each leaf. Theorem id proved. $\square$

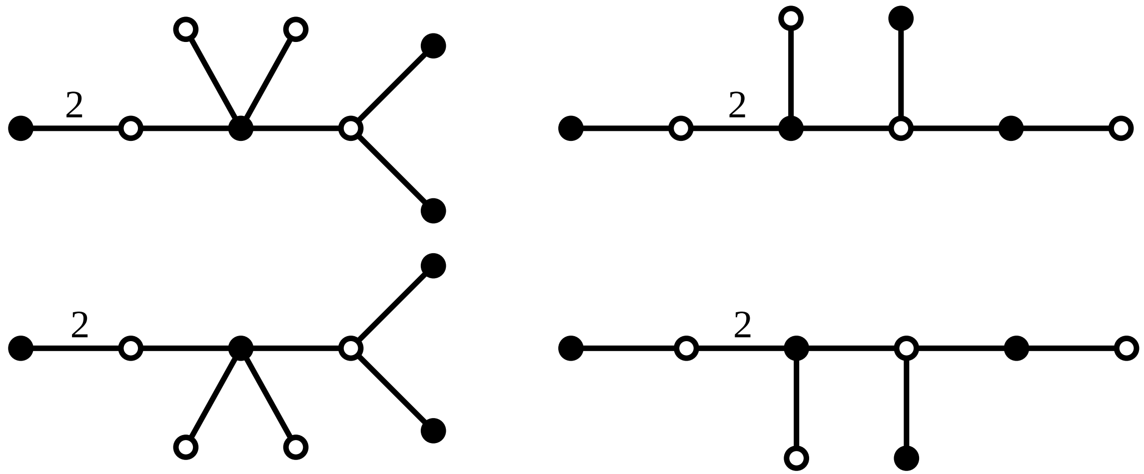
The general case of arbitrary partitions $\alpha, \beta \vdash n$ is slightly more involved but not much more difficult.

V. Galois theory (and combinatorics)

Let us admit certain facts from the theory of **dessins d'enfants**.

Usually, the coefficients of our polynomials are algebraic numbers.

Example: a Galois orbit of degree 4



$$\begin{aligned} P &= x^4(x+1)^2(x^2+ax+b) \\ Q &= (x^2+cx+d)^3(x^2+ex+f) \\ R &= gx+h \end{aligned}$$

$$a, b, c, d, e, f, g, h \in \mathbb{Q}\left(\sqrt{-455+952\sqrt{-14}}\right).$$

There are six more trees with the same set of black and white degrees. They form a Galois orbit of degree 6.

Proposition. If, for a given pair of partitions (α, β), the corresponding tree is unique, then the polynomials P, Q, R are defined over $\mathbb{Q}$.

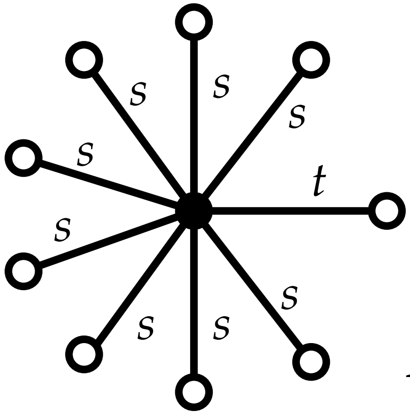
We call such trees **unitrees**.

"Defined over $\mathbb{Q}$" means that there *exist* polynomials with rational coefficients.

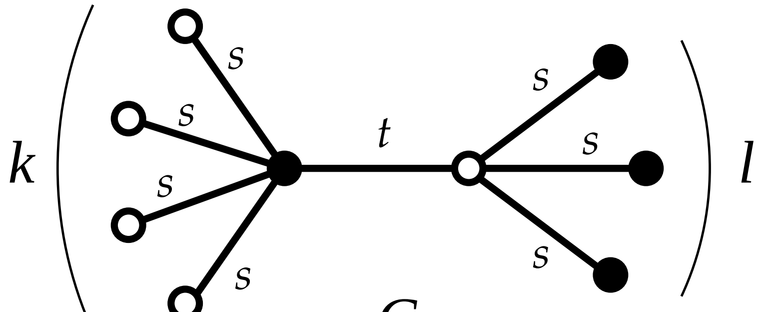
Second result (F. Pakovich, A. Z.): A complete classification of unitrees. There are:

- 10 infinite series, and
- 10 sporadic trees.

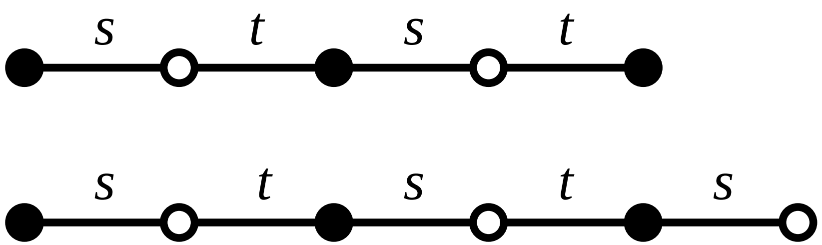
A very long and cumbersome proof. **Pictures follow. . .**



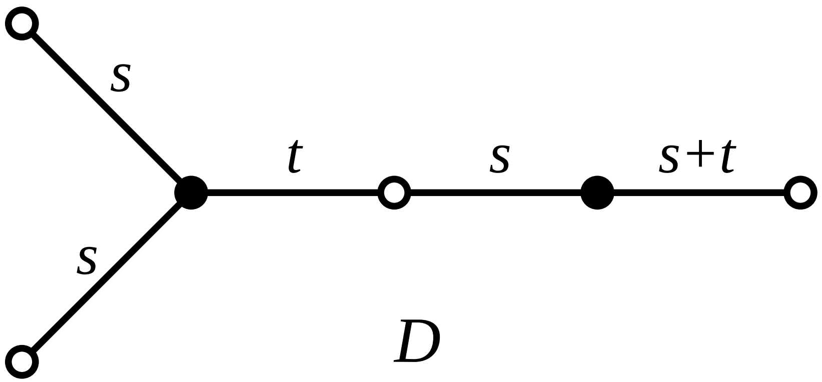
A



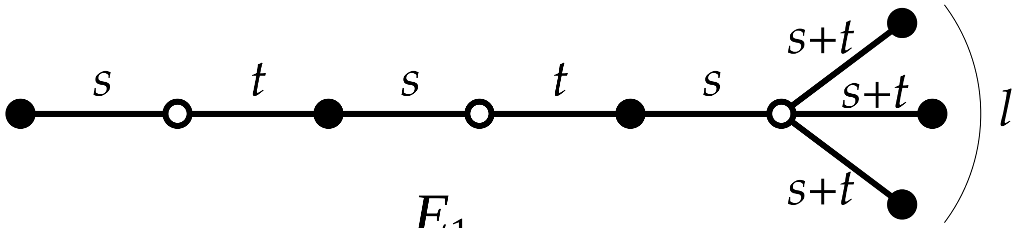
C



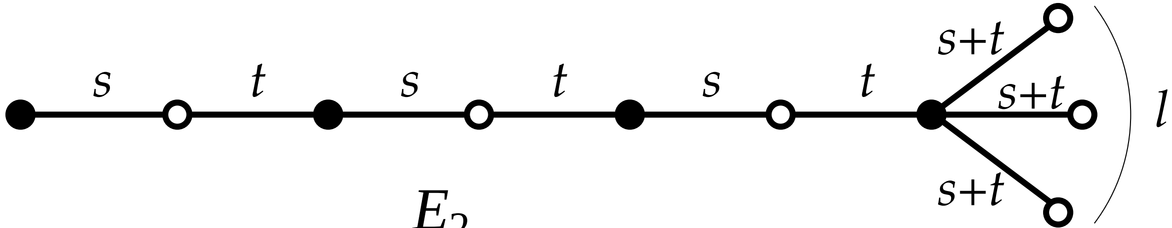
B



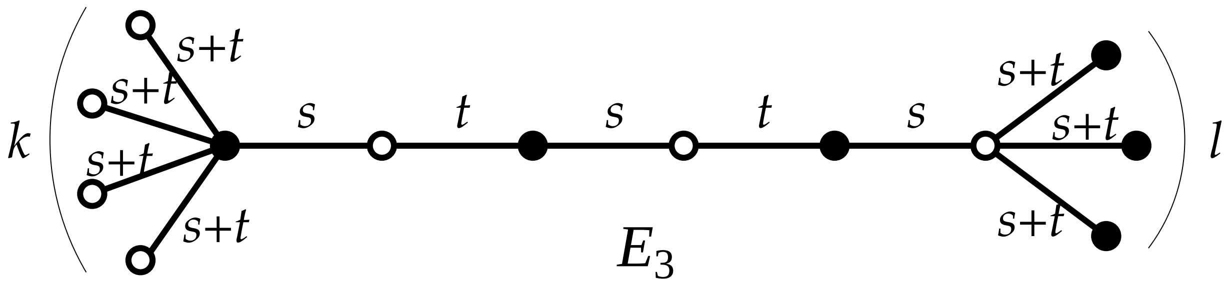
D


s t s t s
s+t s+t s+t
l

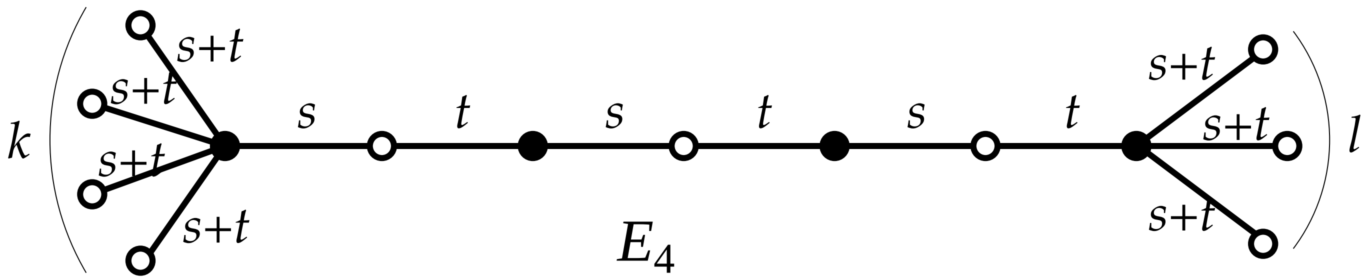
E_1


s t s t s t
s+t s+t s+t
l

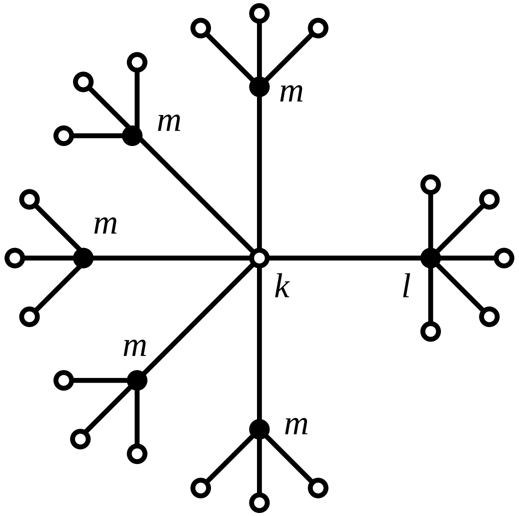
E_2


k
s+t s+t s+t s+t
s t s t s
s+t s+t s+t
l

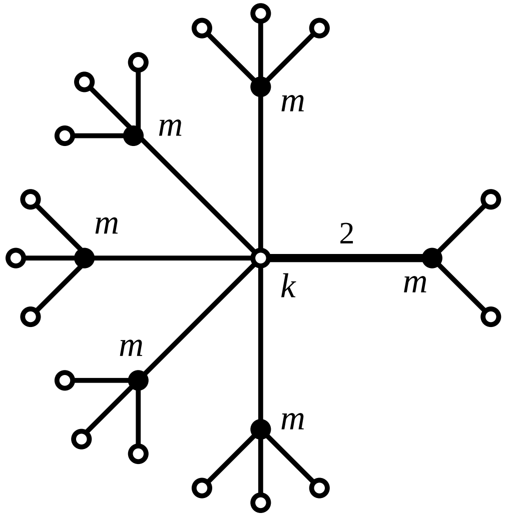
E_3


k
s+t s+t s+t s+t
s t s t s t
s+t s+t s+t
l

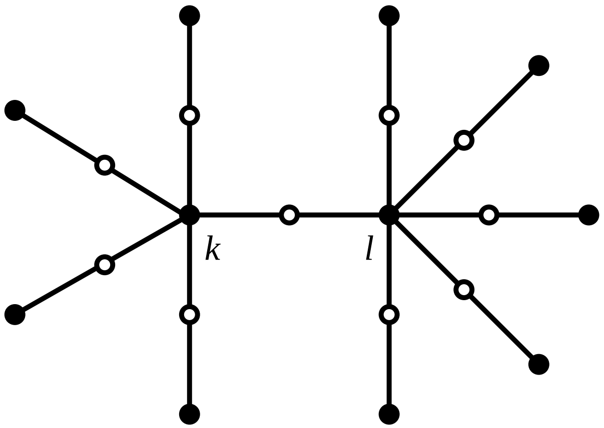
E_4



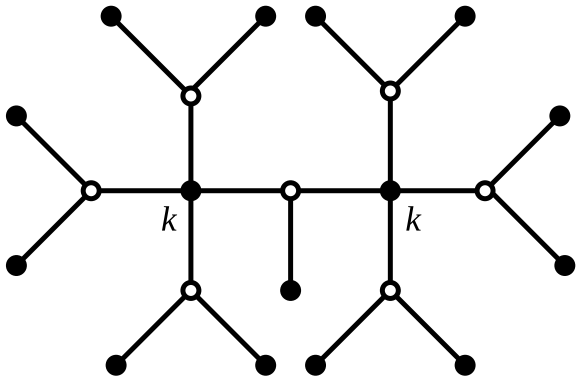
F



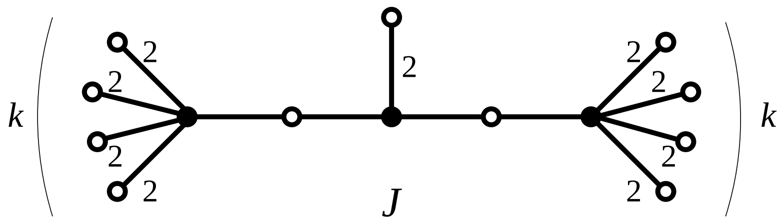
G



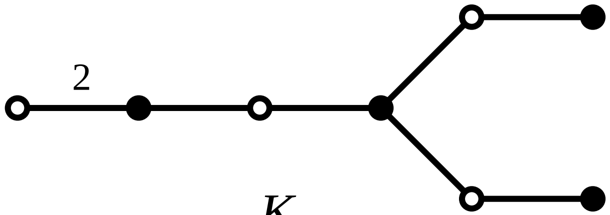
H



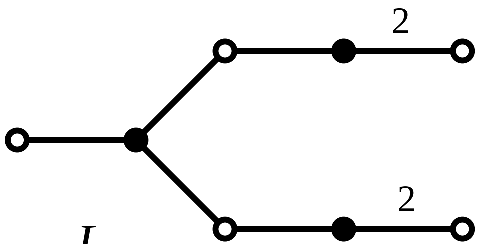
I



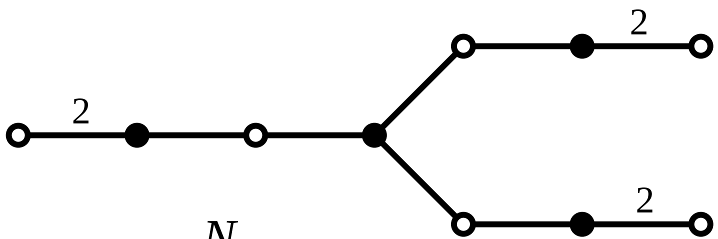
J



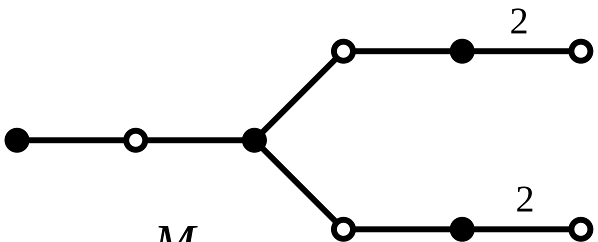
K



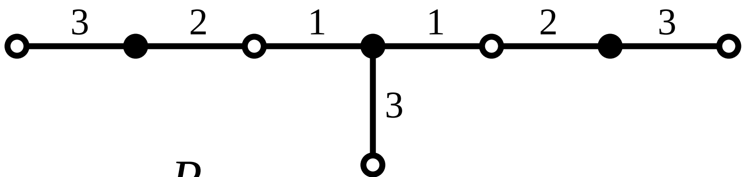
L



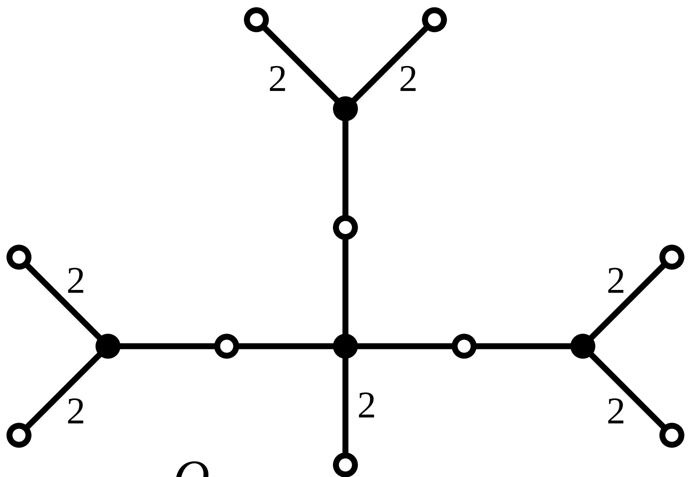
N



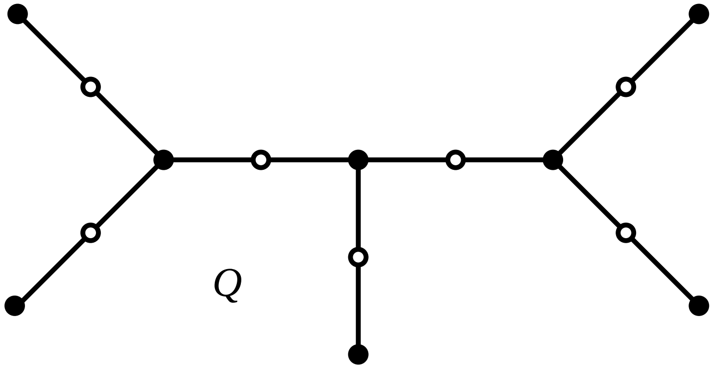
M



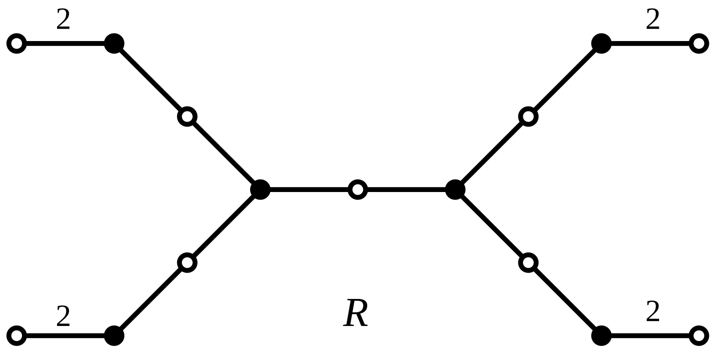
P



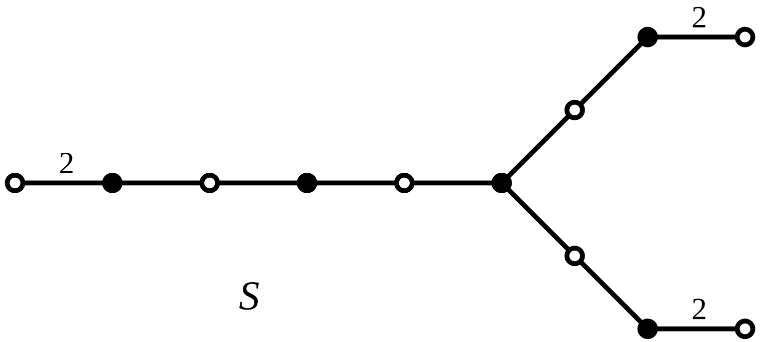
O



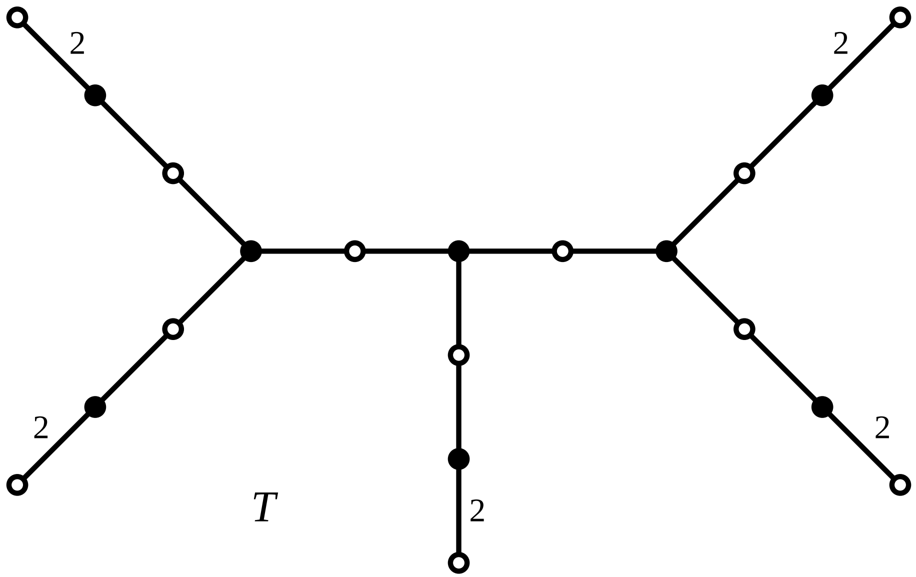
Q



R



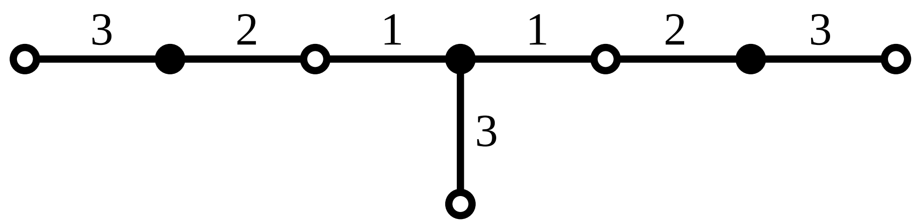
S



T

Third result (F. Pakovich, A. Z.): Belyi functions for all unitrees are computed.

Example



$$
\begin{aligned}
P &= (x^3 + 9x + 9)^5 \\
Q &= (x^5 + 15x^3 + 15x^2 + 45x + 90)^3 \\
R &= -27\,(15x^8 + 395x^6 + 423x^5 + 3\,330x^4 + 7\,290x^3 \\
&\quad + 11\,880x^2 + 29\,565x + 24\,813)
\end{aligned}
$$

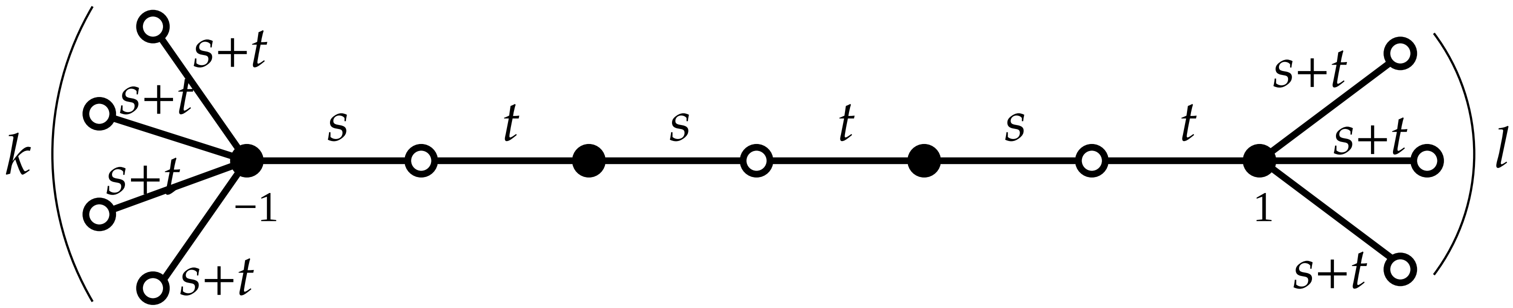
Difficult to find but trivial to verify. . .

For infinite series the situation is much more complicated.

- One has to compute a lot of examples;
- to guess a general pattern;
- and to prove that the suggested solution is indeed true,

and every stage is non-trivial.

An example follows. . .



$$
\begin{aligned}
m_1 &= l(s+t)+t \\
m_2 &= k(s+t)+s \\
p &= \text{number of black vertices of degree } s+t \\
q &= \text{number of white vertices (all of them are of degree } s+t) \\
a &= l + \ t/(s+t) \\
b &= k + \ s/(s+t)
\end{aligned}
$$

$$
\begin{aligned}
P &= \left(\frac{x-1}{2}\right)^{m_1} \cdot \left(\frac{x+1}{2}\right)^{m_2} \cdot J_p(a,b,x)^{s+t} \\
Q &= J_q(-a,-b,x)^{s+t}
\end{aligned}
$$

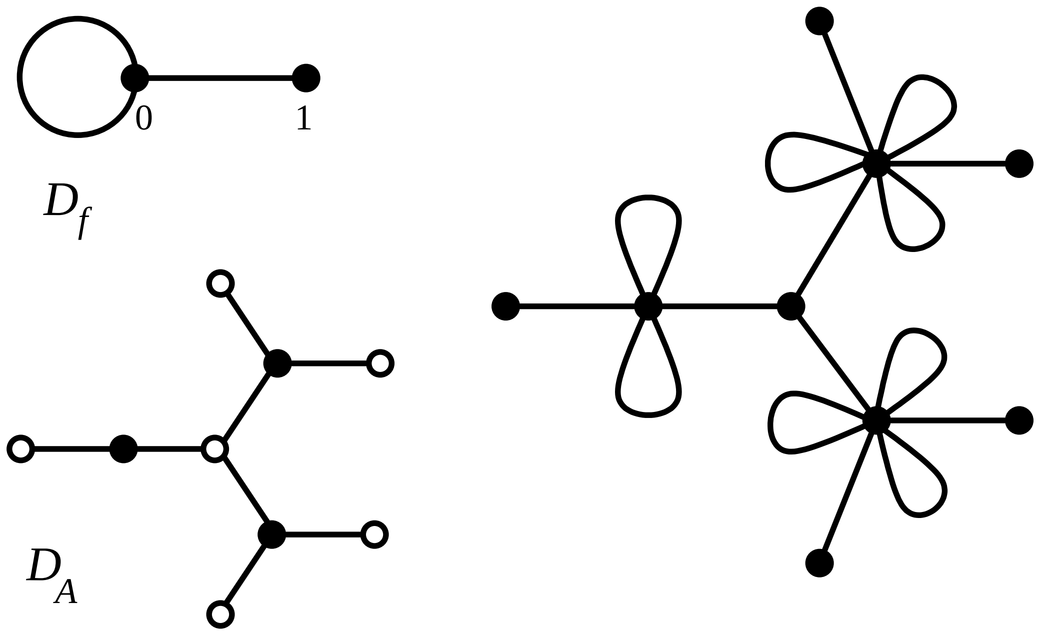
Here J_p and J_q are Jacobi polynomials of degrees p and q.
Notice the negative parameters $-a$ and $-b$ in J_q.

Among the polynomials for infinite series there are quite a few "cut-off" hypergeometric series.

But we did not uncover any general structure.

The uniqueness of the tree is a sufficient but not necessary condition for being defined over $\mathbb{Q}$.

Example: A composition of two unitrees.



D_F where

$F(t) = f(A(t))$

$$f = -\frac{64\,x^3(x-1)}{8\,x+1}, \qquad A = \frac{1}{5^5}\cdot(t^2+4)^3(3\,t+8)^2\,.$$

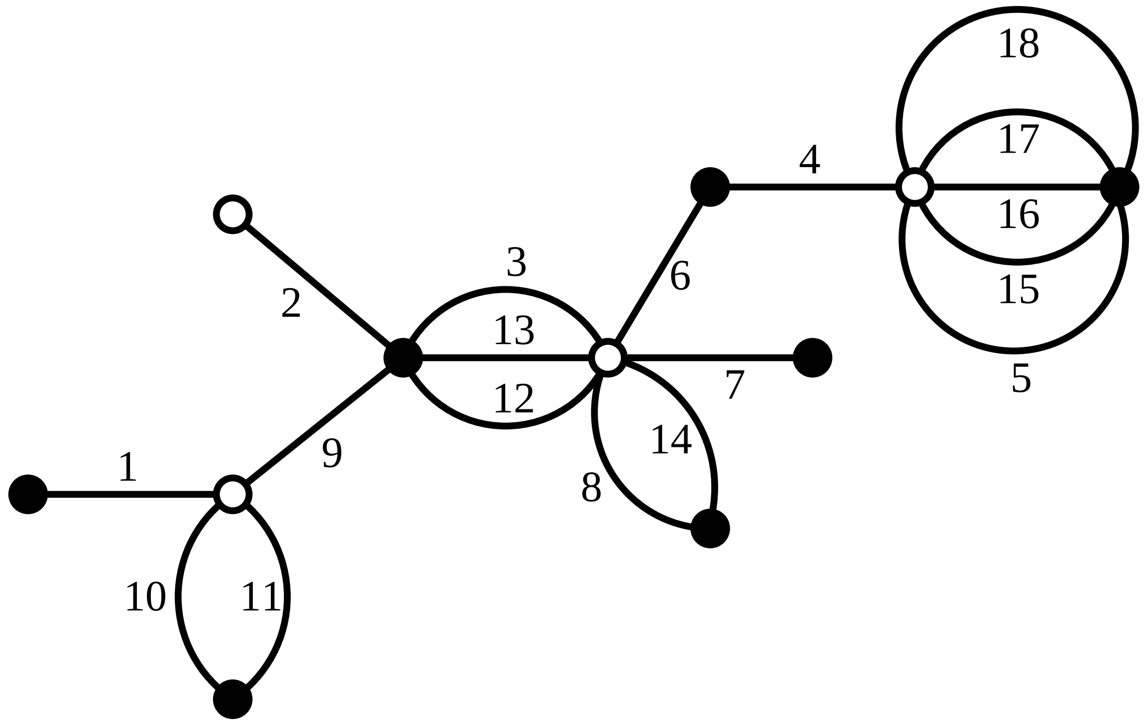
VI. Groups

A rational function $f : \overline{\mathbb{C}} \to \overline{\mathbb{C}}$ may be considered as a **ramified covering** of the Riemann sphere by itself.

The monodromy group is an invariant of the Galois action.

It is well-known that **a covering is a composition of two or more coverings of smaller degrees if and only if its monodromy group is imprimitive** (Ritt's Theorem).

The monodromy group can be found using the picture:

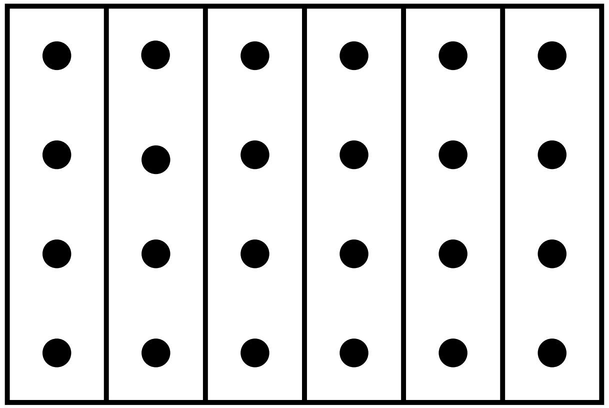


$$a = (2, 9, 12, 13, 3)(4, 6)(5, 18, 17, 16, 15)(8, 14)(10, 11)$$

$$b = (1, 10, 11, 9)(3, 13, 12, 8, 14, 7, 6)(4, 5, 15, 16, 17, 18)$$

Monodromy group: $\boxed{G = \langle a, b \rangle}$

Definition. A permutation group acting on n points is *imprimitive* if the set of points can be subdivided into m blocks of equal size, $1 < m < n$, such that an image of a block under the action of any element of the group is once again a block.



Otherwise the group is called *primitive*.

The groups S_n and A_n are primitive. For p prime all groups of degree p are primitive.

Primitive groups are few...

Degree	2	3	4	5	6	7	8	9	10	11	12	13	14
Primitive	1	2	2	5	4	7	7	11	9	8	6	9	4
Transitive	1	2	5	5	16	7	50	34	45	8	301	9	63

Degree	15	16	17	18	19	20	21	22	23
Primitive	6	22	10	4	8	4	9	4	7
Transitive	104	1954	10	983	8	1117	164	59	7

Degree	24	25	26	27	28	29	30	31
Primitive	5	28	7	15	14	8	4	12
Transitive	25000	211	96	2392	1854	8	5712	12

Degree	32
Primitive	5
Transitive	2 801 324

Fourth result: (N. Adrianov, A. Z.) Complete classification of primitive monodromy groups of weighted trees:

Proposition. Beside the symmetric and alternating groups S_n and A_n for all n, and the cyclic and dihedral groups C_p and D_{2p} for p prime, there are finitely many primitive monodromy groups of weighted trees. Namely, there are:

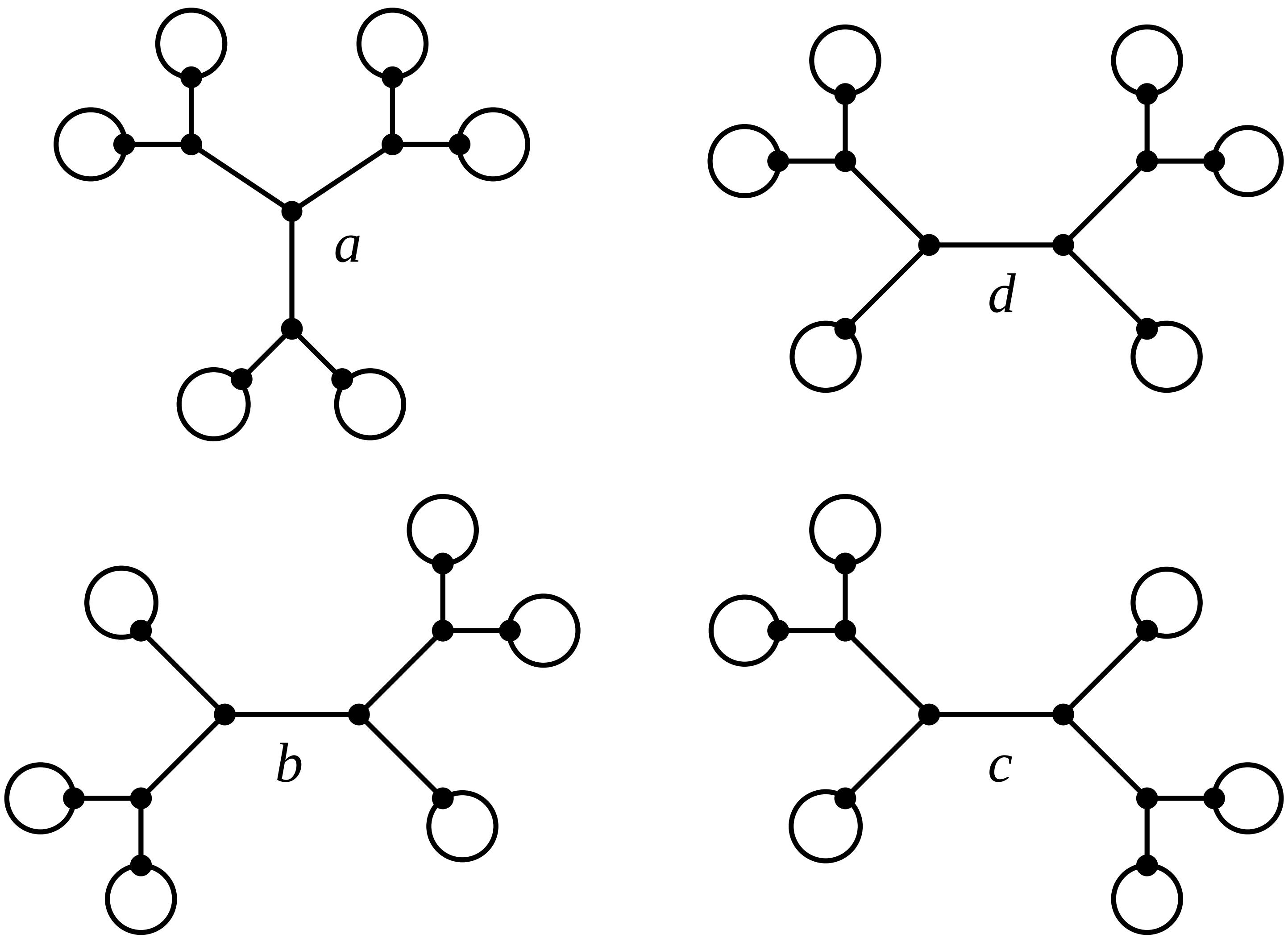
- 184 trees (up to a color exchange);
- 85 Galois orbits;
- 34 groups;
- the highest degree of a group from this list is 32.

Weight	Group	Order	Orbits	Trees
5	$AGL_1(5)$	20	1	2
6	$PSL_2(5)$	60	2	2
	$PGL_2(5)$	120	7	7
7	$AGL_1(7)$	42	1	2
	$PSL_3(2)$	168	2	4
8	$A\Gamma L_1(8)$	168	1	4
	$PSL_2(7)$	168	2	2
	$PGL_2(7)$	336	6	7
	$ASL_3(2)$	1 344	6	14
9	$A\Gamma L_1(9)$	144	1	2
	$AGL_2(3)$	432	2	4
	$PSL_2(8)$	504	3	3
	$P\Gamma L_2(8)$	1 512	4	10
10	$PGL_2(9)$	720	3	3
	$P\Gamma L_2(9)$	1 440	2	2
11	$PSL_2(11)$	660	1	2
	M_{11}	7 920	1	2
12	$PGL_2(11)$	1 320	2	4
	M_{11}	7 920	3	10
	M_{12}	95 040	9	20

Weight	**Group**	**Order**	**Orbits**	**Trees**
13	$\mathrm{PSL}_3(3)$	5 616	3	12
14	$\mathrm{PSL}_2(13)$	1 092	1	1
	$\mathrm{PGL}_2(13)$	2 184	2	4
15	$\mathrm{PSL}_4(2)$	20 160	3	6
16	$\mathrm{A\Gamma L}_2(4)$	5 760	1	2
	$\mathrm{AGL}_4(2)$	322 560	4	12
17	$\mathrm{PSL}_2(16)$	4 080	1	1
	$\mathrm{PSL}_2(16) \rtimes C_2$	8 160	1	1
20	$\mathrm{PGL}_2(19)$	6 840	1	3
21	$\mathrm{P\Gamma L}_3(4)$	120 960	1	2
23	M_{23}	10 200 960	1	4
24	M_{24}	244 823 040	5	18
31	$\mathrm{PSL}_5(2)$	9 999 360	1	6
32	$\mathrm{ASL}_5(2)$	319 979 520	1	6
Total	**34**	—	**85***	**184**

*For certain orbits we are not entirely sure that the "orbit" in question is indeed a single orbit and not a union of several orbits.

VII. A sample of beautiful examples



Computation of Belyi functions:

(a)	B. Birch, 1965	defined over $\mathbb{Q}$
(d)	N. Elkies, 2000	defined over $\mathbb{Q}$
(b,c)	T. Shioda, 2004	defined over $\mathbb{Q}(\sqrt{-3})$

The theory of dessins d'enfants does not make computations any easier. It just predicts that in the above case there exist exactly four non equivalent solutions. Moreover:

- one of them is defined over $\mathbb{Q}$, and its Belyi function is a function in x^3;

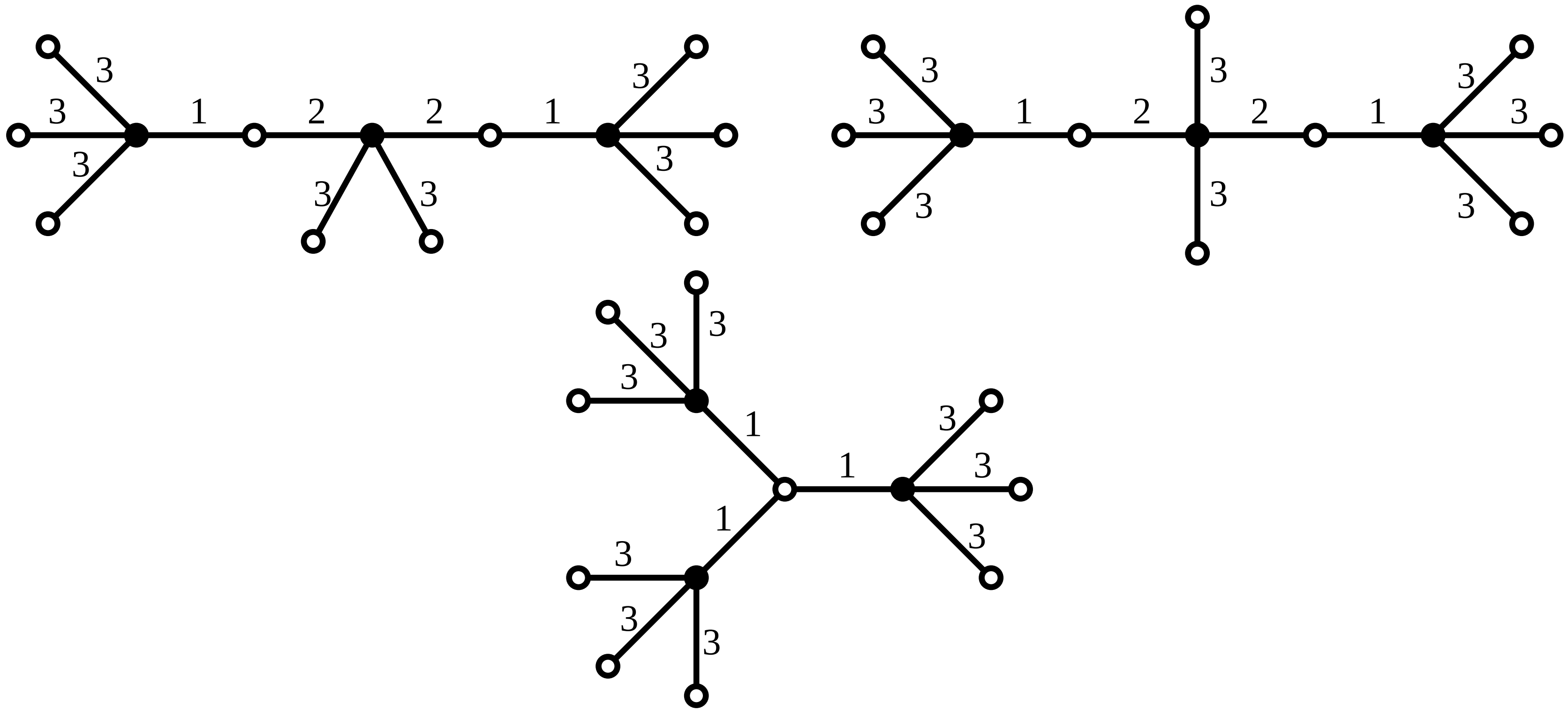
- another one is defined over $\mathbb{Q}$;

- the two remaining solutions constitute a Galois orbit defined over an imaginary quadratic field, and their Belyi functions are functions in x^2.

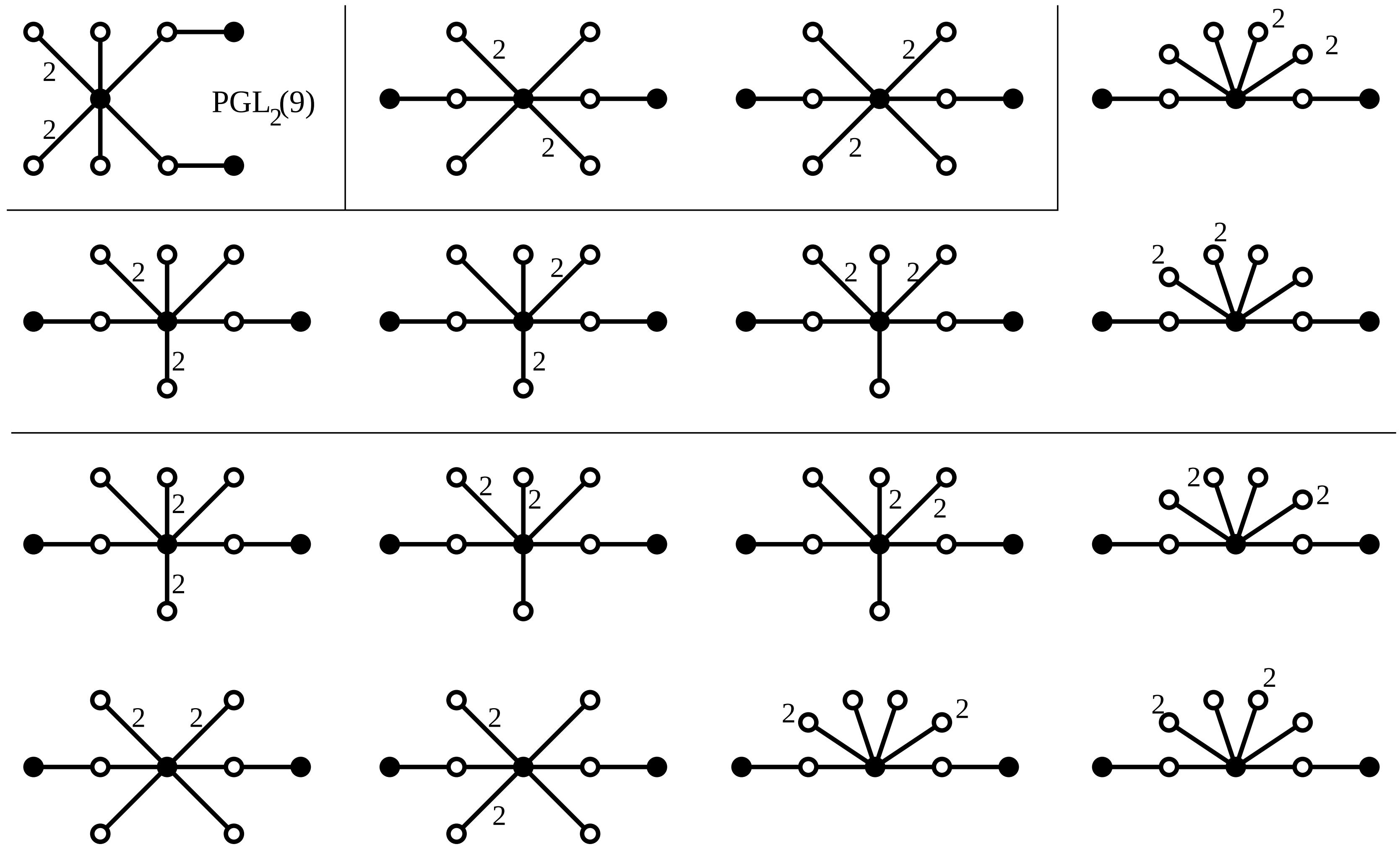
All that can be said without any computation, only by looking at the pictures.

Maybe the time gap of 35 years between the statement of the problem for $A^3 - B^2$ (1965) and the example of Elkies (2000) is explained by the fact that nobody knew that such an example exists. The search was blind.

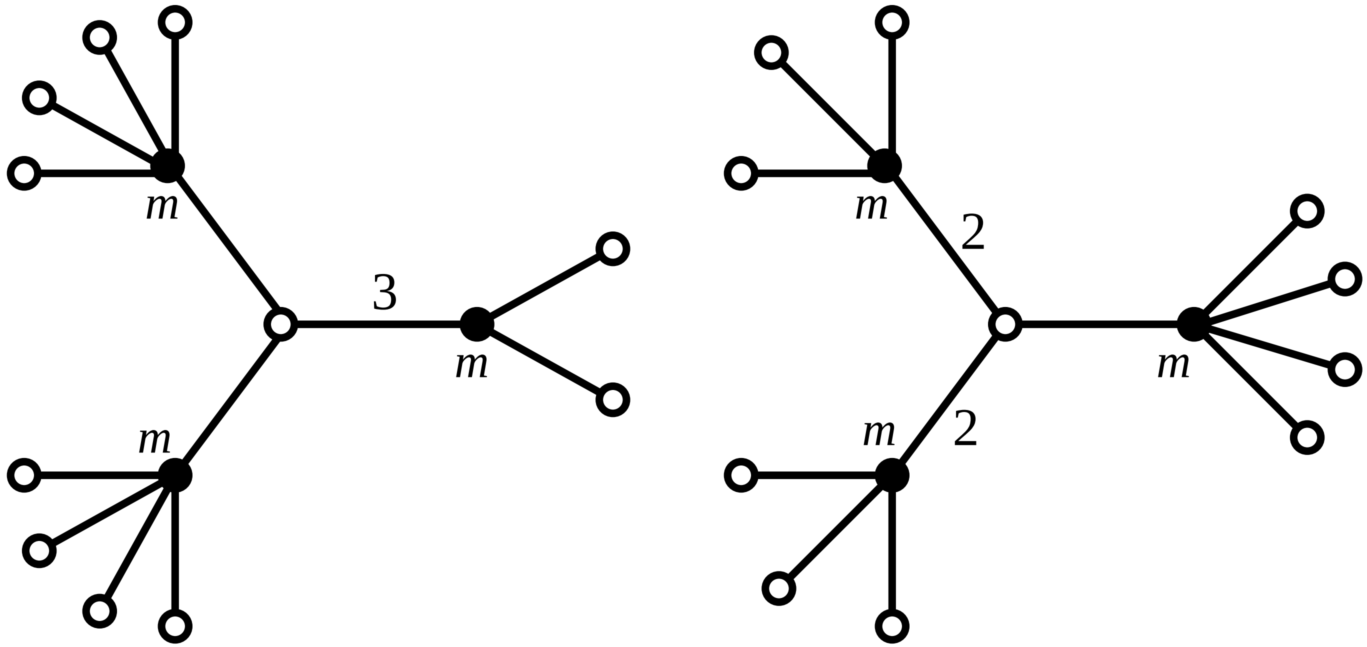
Here all three dessins are defined over $\mathbb{Q}$:



Note that all black degrees are equal to 10 and all white degrees are equal to 3. Therefore, this example corresponds to the minimum degree problem for $A^{10} - B^3$.



Weight $n = 10$, vertex degrees $(8^1 1^2, 2^4 1^2)$.
16 trees, 4 Galois orbits.
The sizes of orbits: 1 (group $\mathrm{PGL}_2(9)$), 2 (symmetry), 5, 8. The monodromy group of the $5 + 8 = 13$ maps is S_{10}. Five of them are self-dual, the other eight are not.



Weight $3m$, vertex degrees $(m^3, 5^1 1^{3m-5})$.

- either one orbit over a real quadratic field;
- or two orbits over $\mathbb{Q}$.

Computation gives the field $\mathbb{Q}(\sqrt{\Delta})$ where

$$\Delta = 3\,(2m-1)\,(3m-2).$$

Question: can $\Delta = 3\,(2m-1)\,(3m-2)$ **be a perfect square?**

1. $2m-1$ and $3m-2$ are coprime:

$$\begin{aligned} 3m-2 &= 1\cdot(2m-1)+(m-1), \\ 2m-1 &= 2\cdot(m-1)+1. \end{aligned}$$

2. Only $2m-1$ can be divisible by 3 ($3m-2$ cannot).

3. Hence, $3\,(2m-1)$ and $3m-2$ must both be squares.

4. Denoting

$$6m-3 = a^2, \qquad 3m-2 = b^2$$

we get

$$a^2 - 2b^2 = 1.$$

Pell equation ! (Plus the condition of a being a multiple of 3.)

Pell's name was attributed to this equation by error...

- Pythagoras (VI before J. C.): $a^2 - 2b^2 = 0$
- Brahmagupta (VII)
- Bhaskara II (XII)
- Narayana Pandit (XIV)
- Brouncker (XVII)
- Fermat, Euler, Lagrange, Abel, ... (XVII–XIX)
- Dirichlet (XIX)

Infinitely many solutions. For every other solution of the Pell equation the parameter a is divisible by 3.

First values of the parameter $m = \dfrac{a^2+3}{6}$ (vertex degree):

$$1\,634,\ 1\,884\,962,\ 2\,175\,243\,842,\ \ldots$$

Growth exponent: $(17+12\sqrt{2})^2 \approx 1154$.

VIII. Enumeration

Proposition (A. Z.) Let a_n be the number of rooted trees of weight n, and let $f(t) = \sum_{n\geq 0} a_n t^n$. Then

$$f(t) = \frac{1 - t - \sqrt{1 - 6\,t + 5\,t^2}}{2\,t}$$
$$= 1 + t + 3\,t^2 + 10\,t^3 + 36\,t^4 + 137\,t^5 + 543\,t^6 + 2219\,t^7 + \ldots$$

Recurrence:

$$a_0 = 1, \quad a_1 = 1, \quad a_{n+1} = a_n + \sum_{k=0}^{n} a_k a_{n-k} \quad \text{for} \quad n \geq 1.$$

Asymptotic: $a_n \sim \frac{1}{2}\sqrt{\frac{5}{\pi}} \cdot 5^n\, n^{-3/2}$.

Sequence A002212 of the "On-Line Encyclopedia of Integer Sequences". It has many different interpretations.

Let $b_{m,n}$ be the number of rooted trees of weight n with m edges, and let $h(s,t) = \sum_{m,n\geq 0} b_{m,n} s^m t^n$. Then

$$
\begin{aligned}
h(s,t) &= \frac{1 - t - \sqrt{1 - (2+4s)\,t + (1+4s)\,t^2}}{2st} \\
&= 1 + st + (s + 2s^2)\,t^2 + (s + 4s^2 + 5s^3)\,t^3 \\
&\quad + (s + 6s^2 + 15s^3 + 14s^4)\,t^4 + \dots
\end{aligned}
$$

Explicit formula for $b_{m,n}$:

$$
b_{m,n} = \binom{n-1}{m-1} \cdot \frac{1}{m+1} \binom{2m}{m}.
$$

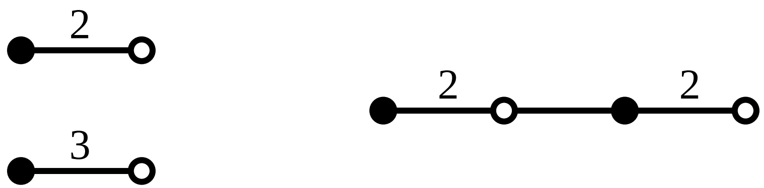
We would like to have an

> **explicit formula for the number of rooted weighted trees corresponding to a given pair of partitions (α, β)**

and which would

> **avoid inclusion-exclusion**.

Difficulty: the same pair of partitions can be realized by a tree and by a forest:



For **ordinary trees** this difficulty does not exist, and the needed formula does exist (Tutte, 1964).

Thank you !