Rend. Lincei Mat. Appl. 29 (2018), 289–296
DOI 10.4171/RLM/805

Number Theory — *On the existence of covers of* $\mathbb{P}_1$ *associated to certain permutations*, by Pietro Corvaja and Umberto Zannier, communicated on November 10, 2017.

Abstract. — In this short note we prove the impossibility of realizing finite topological covers of the Riemann sphere minus three points, associated to certain explicit combinatorial (permutation) data. This comes from a question of M. Zieve and falls in the framework of the so-called "Hurwitz problem", asking for a "simple" description of the combinatorial data which can be so realized.

Key words: Permutations, covers (of curves), branching

Mathematics Subject Classification: 14H57, 05E99

1. Introduction

The present brief note is concerned with the existence (and description) of certain finite connected covers of $\mathbb{P}_1\backslash\{0,1,\infty\}$ (where by $\mathbb{P}_1$ we shall always mean $\mathbb{P}_1(\mathbb{C})$).

It is well known that any such *topological* cover may be in fact realized as a cover of Riemann surfaces, and that it may be compactified as a branched cover of $\mathbb{P}_1$ by a compact Riemann surface; in turn, this yields a cover of complete smooth complex algebraic curves.

It is also well known (see [5], [6]) that every such cover, of degree say n, corresponds up to isomorphism to a triple of permutations $\sigma_0, \sigma_1, \sigma_\infty \in \mathscr{S}_n$, taken up to conjugacy by a single element of $\mathscr{S}_n$, such that

(i) σ_0, σ_1, σ_∞ generate a transitive subgroup of $\mathscr{S}_n$ and
(ii) $\sigma_0\sigma_1\sigma_\infty = 1$.[1]

Moreover, the cycle decompositions of these permutations correspond to the respective branchings above 0, 1, ∞, in the sense that the cycles which appear represent the inertia groups, thus the lengths being equal to the respective ramification indices. In this way we obtain three partitions of the degree n as sum of

[1] Indeed, the group generated by the permutations is a homomorphic image of $\pi_1(\mathbb{P}_1 - \{0,1,\infty\})$, which is a free group on two generators; then the quotient of the universal cover of $(\mathbb{P}_1 - \{0,1,\infty\})$ by the action of the kernel of the said homomorphism yields the Galois closure of the topological cover in question, the cover itself then corresponds to the stabiliser of a point in the permutation action.

positive integers. The set of data of these partitions is usually referred to as a *branching type*.

One may also extend this to covers of $\mathbb{P}_1$ branched above more than three points.

It is an open problem attributed to Hurwitz to 'describe' in simple terms all the possible branching types which may occur, the problem being significant (for several reasons, including especially *Belyi's Theorem*) already in the special but important case of three branching points, which shall be the only case appearing below.

Several papers obtained some necessary or sufficient conditions, and we do not try here to give any sort of complete account on this; but see for instance the paper [2] by the two of us and C. Petronio, where we give a number of references and where examples appear showing that occasionally there may be subtle arithmetical restrictions for a triple to occur.

Recently, M. Zieve and a group of collaborators went ahead with this problem (also for more than three permutations). In particular, they listed certain infinite families of triples and quadruples, for both the *existence* and *non-existence* situations. For instance, by an ingenious argument they could exclude the branching types of degree $2m$, with four branch points, when the cycle decomposition of three of the permutation is of type $(2, 2, \ldots, 2)$ (m times) whereas the fourth one is of type $(1, 3, 2, \ldots, 2)$.[2]

Zieve considered some other infinite families of branching types, this time with three branch points, for which experimental evidence suggested impossibility, which however had not yet been demonstrably excluded. Here are the three families in question, where m denotes any positive integer, and where for instance by "$[1^3, 2^m, 5]$" we mean a permutation whose cycle structure consists of three fixed points, m transpositions and a 5-cycle.

$$\deg = 3m: \quad [3^m], [3^m], [2, 4, 3^{m-2}]; \tag{1}$$

$$\deg = 4m: \quad [2^{2m}], [4^m], [3, 5, 4^{m-2}]; \tag{2}$$

$$\deg = 6m: \quad [2^{3m}], [3^{2m}], [5, 7, 6^{m-2}]. \tag{3}$$

The first and main purpose of this paper is to prove the impossibility of these branching types, as expected by Zieve:

THEOREM 1.1. *The branching types represented in* (1), (2), (3) *are all impossible: in each case, given any integer* $m > 0$ *there do not exist permutations* σ_0, σ_1, σ_∞ *with the respective cycle structure and satisfying* (ii) *above.*

We note at once that we need not assume (i) above to obtain the impossibility: as we shall repeat in the proof, given permutations with those data and satisfying

[2] Zieve tells us that his impossibility proof depends on the fact that *if the cycle decomposition of two permutations involves only transpositions then in their product every length appears an even number of times.*

(ii), the transitivity of the action would be achieved in all the three cases by restricting to an appropriate orbit.

Our method is extremely simple, just a 'trick', and we briefly comment below on it. Also, we shall illustrate another simple application of a similar principle, this time not to an impossibility proof, but to single out a certain property of the corresponding covers. For this, we shall consider covers with branching type $[3^m]$, $[3^m]$, $[3^m]$, hence somewhat similar to (1). Such covers however are well known and our purpose here is only to show another instance of the same trick.

We give a description of them which leads to rather complete results concerning e.g. the Galois closure of the covers and the fields of definition of the involved curves (now of genus 1). In general, the fields of definition of the covers have been studied in particular in connection with the theory of the so-called *dessins d'enfants*, emphasised by Grothendieck. The present case is one of the few where information can be obtained which can be considered satisfactory. (See [1] for the study of covers which includes our special one.)

Before stating our result, let F denote the (Fermat) elliptic curve defined affinely by

$$F : u^3 = f(1-f), \tag{4}$$

where we choose the point at infinity as origin. Note the equation $(2f-1)^2 = 4u^3 + 1$. This curve has Complex Multiplication by a primitive cubic root of unity θ, with $End(F) \cong \mathbb{Z}[\theta] =: \mathcal{O}$. We have:

THEOREM 1.2. *For each integer m, there is a connected cover $E \to \mathbb{P}_1$ of degree $3m$, with branching type $[3^m]$, $[3^m]$, $[3^m]$. All such covers have E of genus 1 and factor as $E \xrightarrow{\phi} F \xrightarrow{f} \mathbb{P}_1$. In particular, $E \cong F/\Phi$ for a finite subgroup $\Phi \subset F(\mathbb{C})$ of order m. In this isomorphism, the Galois closure of $E/\mathbb{P}_1$ is $F/\Phi \cap \theta\Phi \cap \theta^2\Phi$, so $E/\mathbb{P}_1$ is Galois if $E \cong F$. Also, the degree over $\mathbb{P}_1$ of the Galois closure is at most $3m^2$.*

Conversely, given a rational map $g : E \to F$ of degree m, where E has genus 1, the composed cover $f \circ g$ (of degree $3m$) has the said branching type.

REMARK 1.3. In particular, the description of these covers amounts to describe the isogenies $E \to F$ and the representation $E \cong F/\Phi$ allows to count easily the number of non isomorphic covers of given degree. Also, any isogeny can be factored as a multiplication map by an integer, and a cyclic isogeny. Then, basic theory of Complex Multiplication allows to describe their fields of definition. Here the situation is different depending on the residue class of primes p modulo 3. Just to mention an instance, take a cyclic isogeny of degree p. If $p \equiv 1 \pmod 3$ the isogeny is is either an endomorpishm (defined over $\mathbb{Q}(\theta)$), or the field of definition has degree $p-1$; if instead $p \equiv 2 \pmod 3$, the field of definition has degree $p+1$.

As another instance of what can be said, when $m = x^2 + xy + y^2$ for integers x, y there is always a cover as above of degree m, with E isomorphic to F, so

defined over $\mathbb{Q}$. (The cover map however shall be defined in general only over $\mathbb{Q}(\theta)$.)

See also [2] for other examples related to Complex Multiplication, which appears to give rise to quite peculiar constraints. Moreover, as detailed in [2] for CM by i (rather than θ), the corresponding covers of $\mathbb{P}_1$ by curves of genus 1 give rise, through appropriate substitutions, to other covers $\mathbb{P}_1 \to \mathbb{P}_1$, again unbranched outside 0, 1, ∞ and with special branching types.

Note finally that, as generally happens, the degree of the Galois closure is the order of the subgroup generated in $\mathscr{S}_n$ by the three permutations in question.

1.1. About the methods

In principle, the Hurwitz problem is of a purely combinatorial nature, on permutations of a finite set (as is the above theorem). However experience has shown (see e.g. [2]) that sometimes other, more involved, methods are required to deal with these issues. Naturally this reflects the geometrical significance of the structures which underly the existence of the permutations in question: this has a purely topological aspect, but also a metrical one, an analytical one, and an algebro-geometrical one. For instance certain proofs rely on the fact that the permutations correspond to certain triangulation of compact topological surfaces.

Our proof method is very simple to describe, relying on basic properties of elliptic curves. A completely different, rather longer and more complicated, approach has been suggested in [4], depending on pure topology. After the present note was conceived, Zieve brought to our attention the paper [3], relying on the viewpoint of triangulations. Such paper apparently is concerned with different problems, but it turns out that the impossibility one of the above three patterns falls as a corollary.[3]

2. Proofs

2.1. Proof of Theorem 1.1

Proof. Let us start by showing the impossibility of the branching type (1). If this is realisable, we would have three permutations a, b, c on $\{1, 2, \dots, 3m\}$, with cycle structures resp. $[3^m]$, $[3^m]$, $[2, 4, 3^{m-2}]$ and such that $abc = 1$.

First, note that we may reduce to the case when the group generated by a, b, c acts transitively on $\{1, 2, \dots, 3m\}$. In fact, since the group contains e.g. a, which has order 3 and no fixed points, each orbit of the group has cardinality divisible by 3; then there must exist an orbit containing both cyclic orbits of c of lengths coprime with 3, i.e. the orbits of lengths 2, 4, and it now suffices to replace the set $\{1, 2, \dots, 3m\}$ with this orbit.

[3] The paper [3] also uses elliptic curves to present a possible proof of a certain *holonomy theorem*; this has surely some analogy with our method; however our argument is far more direct and avoids appeal to such a theorem. The main methods of [3] are of purely geometrical nature.

Now, by what has been recalled above, the said cycle structure corresponds to a branched cover $f : E \to \mathbb{P}_1$, where E is a smooth complex curve, and f is a rational map of degree $3m$, unbranched outside $\{0, 1, \infty\}$, with the said branching type above the three points.

For the genus g of E, the Hurwitz formula gives $2g - 2 = -6m + (3m - m) + (3m - m) + (3m - (m - 2) - 2) = 0$, hence $g = 1$.

The main point is to look now at the divisors $\mathrm{div}(f)$, $\mathrm{div}(f - 1)$, $\mathrm{div}(\mathrm{d}f)$. All of these divisors are linearly equivalent to 0, the first two by definition, the last one because E has genus 1 (hence there is on it a differential with 0 divisor).

Let us then write

$$\mathrm{div}(f) = 3A - 3C, \quad \mathrm{div}(f - 1) = 2P + 4Q + 3B - 3C,$$

where P, Q are the (distinct) points on E corresponding to the cycles of length 2, 4, and where A, B, C are certain positive divisors of degrees resp. m, $m - 2$, m.

Then we immediately find that $\mathrm{div}(\mathrm{d}f) \geq 2A + P + 3Q + 2B - 4C$. But the right side has degree 0 so there must be equality; this is a crucial point in the proof.

All of this implies that at the level of linear equivalence, denoted $\sim$, we have

$$3A \sim 3C, \quad 2P + 4Q + 3B \sim 3C, \quad 2A + P + 3Q + 2B \sim 4C.$$

Summing the first two of these relations, doubling, and subtracting three times the third we obtain $P \sim Q$, which is impossible.

For the branching type (2) things are similar. As above we obtain positive divisors A, B, C of degrees resp. $2m$, $m - 2$, m and points $P \neq Q$ on a smooth curve of genus 1 such that

$$2A \sim 4C, \quad 3P + 5Q + 4B \sim 4C, \quad A + 2P + 4Q + 3B \sim 5C.$$

Multiplying the third by four and subtracting the second multiplied by three and the first multiplied by two we obtain again $P \sim Q$, a contradiction.

Finally, arguing in a completely similar way, for the branching type (3) we first obtain

$$2A \sim 3C, \quad 5P + 7Q + 6B \sim 3C, \quad A + 4P + 6Q + 5B \sim 4C,$$

for divisors A, B, C of degrees resp. $3m$, $m - 2$, $2m$ and points $P \neq Q$ on E, of genus 1.

Summing the triple of the first with five times the second and subtracting six times the third, we obtain once more $P \sim Q$, which is impossible.

This concludes the proof of Theorem 1.1. □

REMARK 2.1. Since the assertion of Theorem 1.1 regards merely permutations, it would be desirable, and an amusing challenge, to obtain a 'direct' proof, involving only combinatorial and algebraic properties of $\mathscr{S}_n$. Our proof is simple but relying on somewhat demanding tools, like Riemann Existence Theorem. A

more elementary proof is in [4]. However, this relies on topology, so again does not represent exactly what we are thinking of; moreover, it is not very short and requires familiarity with certain topological configurations which one can 'draw' but which are not easy to describe otherwise.

2.2. *Proof of Theorem 1.2*

PROOF. For any integer $m > 0$ the existence of a connected cover of $\mathbb{P}_1$ with the branching type $[3^m]$, $[3^m]$, $[3^m]$ may be established just by producing the corresponding three permutations in $\mathscr{S}_{3m}$, as illustrated above. Here is a possibility:

$$\begin{aligned}(5)\qquad &(1,2,3)(4,5,6)\dots(3m-2,3m-1,3m)\\ &\quad\cdot(2,3,4)(5,6,7)\dots(3m-1,3m,1)\\ &=(2,1,3m)(5,4,3)\dots(3m-1,3m-2,3m-3).\end{aligned}$$

However our argument gives more, and we can produce and describe quite explicitly all of the covers with the said branching type.

Let then $f : E \to \mathbb{P}_1$ be one such (connected) cover, of degree $3m$. A calculation as in the the proof of Theorem 1.1 shows that E has genus 1, so becomes an elliptic curve if we choose an origin, and we do this by choosing a marked pole of f.

Note that the Fermat curve F of equation (4) corresponds to the case $m = 1$, and to complete the proof of the theorem we have to show that our cover map f factors through F; in turn, for this it suffices to show that there is a function $u \in \mathbb{C}(E)$ satisfying $u^3 = f(f-1)$. To prove this last claim, we use the same simple argument as in the proof of the former theorem.

Write the divisors of f and $f-1$ in the shape $\operatorname{div}(f) = 3A - 3C$, $\operatorname{div}(f-1) = 3B - 3C$, where A, B, C are positive divisors on E of degree m, which we can do because of the branching conditions.

Then, as in the proof of Theorem 1.1, we find that $\operatorname{div}(\mathrm{d}f) = 2A + 2B - 4C$, so we obtain the linear equivalences

$$3A \sim 3B \sim 3C, \quad 2A + 2B \sim 4C.$$

Summing the first two, we deduce that $3(A+B) \sim 6C$, whence, subtracting the third, $A + B \sim 2C$. Therefore there is a rational function u on E with $\operatorname{div}(u) = A + B - 2C$. But then $\operatorname{div}(u^3) = 3A + 3B - 6C = \operatorname{div}(f(f-1))$. Hence $u^3/f(f-1)$ is a constant, which we may assume to be 1 by rescaling u, as required.

REMARK 2.2. Another proof of the said claim is as follows. We have the map $\pi : (u, f) \mapsto f$ on F. If $f : E \to \mathbb{P}_1$ does not factor as asserted, then the fiber product $X := F \times_{\pi,f} E$ over $\mathbb{P}_1$, with respect to the maps π, f, would be an irreducible curve, and let $\tilde{X}$ denote a complete smooth model of it. The branching conditions ensure that the projection $\tilde{X} \to F$ would be unramified, so that $\tilde{X}$ would have genus 1 and after a suitable choice of the origin would become an

elliptic curve isogenous to F. Now, the kernel of the isogeny would be a subgroup of $\tilde{X}$ of order $3m$, and the fiber product situation shows that this would contain the kernel of the isogeny $\tilde{X} \to E$ of degree 3: for otherwise the map $\tilde{X} \to F$ would induce on E an unramified map of degree $3m$, which would be f, a contradiction. But then after all we would find the sought factorisation of f through F.

Conversely, it is immediately checked that composing any isogeny $E \to F$ with the f-map on F we obtain a cover $E \to \mathbb{P}_1$ with the required branching type.

To conclude the proof of Theorem 1.2, we have only to inspect the Galois closure of a cover with the branching type in question. We have proved that the cover factors as $E \xrightarrow{\phi} F \xrightarrow{f} \mathbb{P}_1$. As in the statement, we find that E is isogenous to F through ϕ (of degree m) and there is an isogeny $\hat{\phi} : F \to E$ dual to ϕ, hence with the same degree m and such that $\phi \circ \hat{\phi} = [m]$ (the multiplication-by-m map on F). If $\Phi := \ker \hat{\phi}$, we find $E \cong F/\Phi$.

Now, we contend that the composite cover $f \circ \phi \circ \hat{\phi} = f \circ [m] : F \to \mathbb{P}_1$ is Galois. Indeed, it suffices to show that each automorphism of $f : F \to \mathbb{P}_1$ extends to an automorphism of $f \circ [m] : F \to F \to \mathbb{P}_1$. This is clear, because any automorphism of the first degree-3 cover is induced by θ on F (in fact, $f \circ \theta = f$). But then it suffices to consider θ on the 'top' F, and observe that $[m]$, θ commute.

From this, all the other observations follow from simple Galois theory, since E is an intermediate cover. □

As a final remark, we also note that the Galois group of the last cover is a semidirect product $(\mathbb{Z}/(m))^2 \rtimes \mathbb{Z}/(3)$, represented as a group of affine transformations $x \mapsto \theta^r x + u$, for $x \in F$, $r \in \mathbb{Z}/(3)$ and $u \in F$ a torsion point of order m. This also allows to recover explicitly the three permutations through actions on suitable sets of points. (See also [2] for similar considerations concerning however Complex Multiplication by i.)

References

[1] Paula B. Cohen (now Paula Tretkoff), *Dessins d'enfant and Shimura varieties*, in The Grothendieck Theory of Dessins d'Enfants, L. Schneps Ed., London Math. Soc. LNS, 200, Cambridge Univ. Press, 1994.

[2] P. Corvaja - C. Petronio - U. Zannier, *On certain permutation groups and sums of two squares*, Elem. Math. 67 (2012), 169–181.

[3] I. Izmestiev - R. B. Kusner - G. Rote - B. Springborn - J. M. Sullivan, *There is no triangulation of the torus with vertex degrees* $5, 6, \ldots, 6, 7$ *and related results: geometric proofs for combinatorial theorems.*, Geom. Dedicata 166 (2013), 15–29.

[4] T. Ferragut - C. Petronio, *Elementary solution of an infinite sequence of instances in the Hurwitz Problem*, Rend. Lincei Mat. Appl. 29 (2018), 297–307.

[5] J-P. Serre, *Topics in Galois Theory*, Research Notes in Mathematics, Vol. 1, Jones and Bartlett, Boston MA, 1992.

[6] H. VOLKLEIN, *Groups as Galois Groups*, Cambridge Studies in Advanced Mathematics, Vol. 53, Cambridge Univ. Press, Cambridge, 1996.
[7] M. ZIEVE ET AL., work in progress.

Received 19 May 2017,
and in revised form 18 August 2017.

Pietro Corvaja
Dipartimento di Scienze Matematiche, Informatiche e Fisiche
Università degli Studi di Udine
Via delle Scienze, 206
33100 Udine, Italy
pietro.corvaja@uniud.it

Umberto Zannier
Scuola Normale Superiore
Palazzo della Carovana
Piazza dei Cavalieri 7
56126 Pisa, Italy
umberto.zannier@sns.it