

## *The group of automorphisms of the Fermat curve*

MARBY BOLAÑOS ORTIZ, MARIBEL DÍAZ, MARTHA ROMERO ROJAS\*

Universidad del Cauca, Departamento de Matemáticas, Popayán, Colombia.

**Abstract.** In his paper, “The group of automorphisms of the Fermat curve” (see [7]), Tzermias proved that the automorphism group of the projective Fermat curves in characteristic 0 is the semidirect product of the direct sum of 2 copies of the cyclic group of order  $n$  and the symmetric group on 3 letters. In this paper we present an alternative proof of this fact accessible to someone with basic knowledge of Riemann surfaces and group theory. Also we include the geometric correspondence of the action.

**Keywords:** Riemann surfaces, automorphisms.

**MSC2010:** 14H37, 14H55, 14R20, 30F10.

### *El grupo de automorfismos de las curvas de Fermat*

**Resumen.** Pavlos Tzermias en su artículo “The group of automorphisms of the Fermat curve” (ver [7]), prueba que el grupo de automorfismos de las curvas de Fermat proyectivas en característica 0 es el producto semidirecto de la suma directa de 2 copias del grupo cíclico de orden  $n$  y el grupo simétrico de 3 letras. En este artículo se presenta una prueba alternativa de este hecho accesible para alguien con conocimientos básicos en superficies de Riemann y teoría de grupos. Además, se incluye la correspondencia geométrica de la acción.

**Palabras clave:** Superficies de Riemann, automorfismos.

### **1. Introduction**

If  $\mathcal{S}$  is a Riemann surface, then we denote by  $Aut(\mathcal{S})$  its group of conformal automorphisms. If  $F(x, y, z)$  is a nonsingular homogeneous polynomial, then the projective plane curve  $\mathcal{W}$ , which is the zero locus in  $\mathbb{C}\mathbb{P}^2$ , is a compact Riemann surface. The automorphism group of an algebraic curve is one of its most important invariants. Such a group

---

\*E-mail: [mjromero@unicauca.edu.co](mailto:mjromero@unicauca.edu.co)

Received: 11 February 2016, Accepted: 03 May 2016.

To cite this article: M. Bolaños Ortiz, M. Díaz, M. Romero Rojas, The group of automorphisms of the Fermat curve, *Rev. Integr. Temas Mat.* 34 (2016), No. 2, 133–138.

is finite, except for rational and elliptic curves. The construction and classification of curves with large automorphism groups with respect to their genera has been considered a relevant problem in algebraic geometry. A landmark paper in this direction is [3], in which Hurwitz proved his bound  $|Aut(\mathcal{W})| \leq 84(g(\mathcal{W}) - 1)$ , valid for any complex (projective, geometrically irreducible) algebraic curve  $\mathcal{W}$  of genus  $g \geq 2$ . The Hurwitz bound is attained by the Klein quartic. For a long time, various authors sought to find Riemann surfaces with a finite automorphism group attaining a given bound. Macbeath in [5] showed that there are infinite values of  $g$  (the genus) for which the Hurwitz bound is attained, and also infinite values of  $g$  for which the bound isn't attained. Thus, group theory is an essential tool in this area. In fact, groups provide a unifying framework for topics such as geometric symmetry, permutations, matrix arithmetic and more. Group theory is vital in many areas of mathematics (algebra, number theory, geometry, harmonic analysis, representation theory, geometric mechanics) and in areas of science such as theoretical physics and quantum chemistry.

In this paper we focus on the (projective) nonsingular plane algebraic curve  $F(n) = \{[X:Y:Z] \in \mathbb{CP}^2 : X^n + Y^n + Z^n = 0\}$ ,  $n \geq 4$ , called the  $n$ th Fermat curve. In [7], Tzermias proved that the automorphism group of  $F(n)$  is a semidirect product of the direct sum of 2 copies of the cyclic group  $\mathbb{Z}_n$  of the order  $n$ , and the symmetric group on 3 letters  $S_3$ . Leopoldt did the same in his paper [4], including the cases over fields of positive characteristic. Here, we will give an alternative proof of this fact from a different point view. We also study some geometric properties of  $F(n)$ , and we shall describe the geometric action of its automorphism group.

## 2. Preliminaries

We start recalling some known results about group actions.

An abstract finite group  $G$  acts on genus  $g \geq 2$  if it is (isomorphic to) a group of automorphisms of some compact Riemann surface of genus  $g$ . We say that  $G$  acts as a full group on genus  $g$  if  $G$  is the full automorphism group of some compact Riemann surface of genus  $g$ .

Suppose that  $G$  acts on genus  $g$  and let  $\mathcal{W}$  be a compact Riemann surface of genus  $g$ , for which  $G \subseteq Aut(\mathcal{W})$ . We write  $G = \Gamma/\Lambda$  when  $\Gamma$  and  $\Lambda$  are Fuchsian groups, and  $\Lambda$  is a normal subgroup of  $\Gamma$ , with signature  $(g; -)$ . If  $\Gamma$  has signature  $(\gamma; m_1, m_2, \dots, m_r)$ , we say that  $G$  acts on genus  $g$  with signature  $(\gamma; m_1, m_2, \dots, m_r)$ ; and if  $G = Aut(\mathcal{W})$ , we say that  $G$  acts as full automorphism group on genus  $g$  with signature  $(\gamma; m_1, m_2, \dots, m_r)$ .  $G$  may act with different signatures on the same genus  $g$ .

If  $G$  is a finite group of conformal automorphisms of the compact Riemann surface  $\mathcal{W}$ , we will denote by  $\mathcal{W}/G$  the quotient Riemann surface. The branched covering  $\pi_G : \mathcal{W} \rightarrow \mathcal{W}/G$  may be partially characterized by a vector of numbers  $(\gamma; m_1, m_2, \dots, m_r)$ , called signature (or branching data) of  $G$  on  $\mathcal{W}$ , where  $\gamma$  is the genus of  $\mathcal{W}/G$ ,  $r \leq 2\gamma + 2$  is the number of branch values of the covering and the  $m_i$  are positive integers associated to the branch values on  $\mathcal{W}/G$  (they represent the degree of

injectivity of  $\pi_G$  at that point). The Riemann-Hurwitz formula (see [6])

$$2g - 2 = |G| \left[ 2\gamma - 2 + \sum_{i=1}^r \left( 1 - \frac{1}{m_i} \right) \right] \tag{1}$$

must be satisfied by the integers  $m_1, m_2, \dots, m_r$  in the signature. This imposes restrictions on  $|G|$  and the branching data that can occur.

Broughton, in his paper [2], define a generating  $(\gamma; m_1, m_2, \dots, m_r)$ -vector as follows.

**Definition 2.1.** A  $2\gamma + r$  tuple  $(a_1, a_2, \dots, a_\gamma, b_1, b_2, \dots, b_\gamma, c_1, c_2, \dots, c_r)$  of elements of  $G$  is called a generating  $(\gamma; m_1, m_2, \dots, m_r)$ -vector if it satisfies:

1.  $G = \langle a_1, a_2, \dots, a_\gamma, b_1, b_2, \dots, b_\gamma, c_1, c_2, \dots, c_r \rangle$ ,
2.  $\text{order}(c_i) = m_i$ ,
3.  $\prod_{i=1}^{\gamma} [a_i, b_i] \prod_{j=1}^r c_j = 1$ .

The following theorem is the basic theorem translating the topological problem of constructing group actions to a problem in finite group theory (see [1], [2], [8]).

**Theorem 2.2. Riemann’s existence Theorem**

A finite group  $G$  acts on a Riemann surface  $\mathcal{W}$  of genus  $g$ , with signature  $(\gamma; m_1, m_2, \dots, m_r)$ , if and only if

1. The Riemann-Hurwitz formula is satisfied;
2.  $G$  has a generating  $(\gamma; m_1, m_2, \dots, m_r)$ -vector.

**3. Fermat curves**

Let  $n \geq 4$ . The projective Fermat curve of degree  $n$  over  $\mathbb{C}$  is the algebraic non singular curve

$$F(n) = \{[X : Y : Z] \in \mathbb{C}\mathbb{P}^2 : X^n + Y^n + Z^n = 0\}.$$

It is well known that  $F(n)$  is a smooth compact Riemann surface of genus  $g(F(n)) = \frac{(n-1)(n-2)}{2}$ .

We are interested in finding the automorphisms group of the projective Fermat curve of degree  $n$  over  $\mathbb{C}$ . Let  $G = \text{Aut}(F(n))$  be the group of automorphisms of  $F(n)$ . Then  $G$  is a finite group; in fact,  $|G| \leq 48n(n-3)$ . Let  $\omega = e^{\frac{2\pi}{n}i}$  be a  $n$ th primitive root of unity and let  $\phi_i : F(n) \rightarrow F(n)$ ,  $i=1,2,3,4$ , be a function given by :

$$\begin{aligned} \phi_1([X : Y : Z]) &= [Y, X, Z], \\ \phi_2([X : Y : Z]) &= [Z, X, Y], \\ \phi_3([X : Y : Z]) &= [\omega X : Y : Z], \\ \phi_4([X : Y : Z]) &= [X : \omega Y : Z]. \end{aligned}$$

Then for each  $i$ ,  $\phi_i$  is an automorphism of  $F(n)$ . It is clear that  $\langle \phi_1, \phi_2 \rangle \leq G$  is isomorphic to  $S_3$ , the symmetric group on 3 letters. Also  $\langle \phi_3, \phi_4 \rangle \leq G$  is isomorphic to  $\mathbb{Z}_n \times \mathbb{Z}_n$ . From now on, we will use the notation  $S_3$  and  $\mathbb{Z}_n \times \mathbb{Z}_n$  to refer to the above subgroups of  $G$ .

Let  $H$  be the subgroup of  $G$  generated by  $S_3$  and  $\mathbb{Z}_n \times \mathbb{Z}_n$ . It is easily seen that  $S_3 \cap (\mathbb{Z}_n \times \mathbb{Z}_n) = \{1\}$ . Also

$$\phi_1(\phi_3(\phi_1^{-1}([X:Y:Z]))) = \phi_4([X:Y:Z]); \quad \phi_1(\phi_4(\phi_1^{-1}([X:Y:Z]))) = \phi_3([X:Y:Z]);$$

$$\phi_2(\phi_3(\phi_2^{-1}([X:Y:Z]))) = \phi_4([X:Y:Z]); \quad \phi_2(\phi_4(\phi_2^{-1}([X:Y:Z]))) = \phi_3^{-1}(\phi_4^{-1}([X:Y:Z])).$$

Then  $\mathbb{Z}_n \times \mathbb{Z}_n$  is a normal subgroup of  $H$ . Therefore,  $H \cong (\mathbb{Z}_n \times \mathbb{Z}_n) \rtimes S_3$  and  $|H| = 6n^2$ .

The following theorem was proved in [7]; here we shall prove the same theorem from another point of view.

**Theorem 3.1.** *Let  $n \geq 4$  and  $G$  the automorphism group of  $F(n)$ . Then  $G = H$ .*

*Proof.* On one hand, since  $H \leq G$  and  $|H| = 6n^2$ , we get  $|G| = 6n^2m$ , for some positive integer  $m$ . On the other hand,  $G$  acts in  $F(n)$  and we will denote by  $F(n)/G$  the quotient Riemann surface. Let  $\pi : F(n) \rightarrow F(n)/G$  be the natural projection and let  $r_i$  be the corresponding ramification indices. Then, by the Riemann-Hurwitz formula (1), we have

$$n(n-3) = 6n^2m \left( 2g(F(n)/G) - 2 + \sum_{i=1}^r \left( 1 - \frac{1}{r_i} \right) \right),$$

where  $r \geq 0$ ,  $r_i \geq 2$ , for  $i = 1, 2, \dots, r$ . Also, we have  $g(F(n)/G) = 0$ . Indeed, if  $g(F(n)/G) \geq 1$ , then  $n-3 \geq 3nm$ , which is absurd. So we obtain

$$n-3 = 6nm \left( -2 + \sum_{i=1}^r \left( 1 - \frac{1}{r_i} \right) \right). \quad (2)$$

As  $n \geq 4$ , we have  $n-3 > 0$ , so  $R = \sum_{i=1}^r \left( 1 - \frac{1}{r_i} \right) > 2$ . It is clear that  $r \geq 3$ . Moreover we can see that each point in the set  $S = \{[X:Y:Z] \in F(n) : XYZ = 0\}$  is fixed by a subgroup of size  $2n$ . First, we can see that the points  $[X:Y:Z] \in F(n)$  such that not all its entries are non-zero are in the same orbit. In fact, if  $X = 0$ , then  $(Y/Z)^n = -1$ , so we have  $n$  points  $[0 : e^{i\pi/n}\omega^j : 1]$ , with  $j = 0, 1, \dots, n-1$ ; if  $Y = 0$ , we get the points  $[e^{i\pi/n}\omega^j : 0 : 1]$ ,  $j = 0, 1, \dots, n-1$ ; and if  $Z = 0$ ,  $[e^{i\pi/n}\omega^j : 1 : 0]$ ,  $j = 0, 1, \dots, n-1$ . These points belong to the same orbit, since  $\phi_4([0 : e^{i\pi/n}\omega^j : 1]) = [0 : e^{i\pi/n}\omega^{j+1} : 1]$ ,  $\phi_1([0 : e^{i\pi/n}\omega^j : 1]) = [e^{i\pi/n}\omega^j : 0 : 1]$  and  $\phi_2^{-1}([0 : e^{i\pi/n}\omega^j : 1]) = [e^{i\pi/n}\omega^j : 1 : 0]$ . Thus, if  $p \in S$ , then  $p$  is fixed by a subgroup of  $H$  of order  $2n$  (for example, the stabilizer subgroup of  $p = [0 : e^{i\pi/n} : 1]$  is  $H_p = \langle \varphi_1 \rangle$ , where  $\varphi_1[X:Y:Z] = [X : \omega Z : Y]$ ); then the stabilizer subgroup of  $p$ ,  $G_p$ , has order at least  $2n$ , and therefore  $r_i \geq 2n$ , for some  $i = 1, \dots, r$ . We can assume  $r_1 \geq 2n$ .

If  $r \geq 4$ , we have  $R \geq \frac{7}{8} + (r-1) - \sum_{i=2}^r \frac{1}{r_i} \geq \frac{7}{8} + \frac{r-1}{2} \geq \frac{7}{8} + \frac{3}{2} = \frac{19}{8}$ , because  $r_i \geq 2$ , for  $i = 2, 3, \dots, r$ . Then, replacing in (2), we get  $n-3 > 2nm$ , which is impossible. Therefore  $r = 3$ .

As  $R = 3 - (\frac{1}{r_1} + \frac{1}{r_2} + \frac{1}{r_3}) > 2$ , then we can't have  $r_i = 2$  for more than one value of  $i = 1, 2, 3$ .

Summarizing, we have that the signature of the action of  $G$  in  $F(n)$  is  $(0; r_1, r_2, r_3)$ , with  $r_1 \geq 2n, r_2 \geq 3$  and  $r_3 \geq 2$ .

Replacing in the 2 we obtain

$$n - 3 = 6nm \left( 1 - \left( \frac{1}{r_1} + \frac{1}{r_2} + \frac{1}{r_3} \right) \right) \geq 6nm \left( \frac{1}{6} - \frac{1}{2n} \right), \text{ then } n - 3 \geq (n - 3)m;$$

thus  $m = 1$ , and  $G = H$  is claimed, also the signature of action of  $G$  in  $F(n)$  is  $(0; 2n, 3, 2)$ .  $\square$

In the following section, we describe the action of  $G = (\mathbb{Z}_n \times \mathbb{Z}_n) \rtimes S_3$  in the projective Fermat curve  $F(n)$ ,  $n \geq 4$ .

#### 4. Geometric correspondence

As has been seen here, the automorphism group,  $G$ , of the projective Fermat curve is generated by the automorphisms  $\phi_1([X : Y : Z]) = [Y, X, Z]$ ,  $\phi_2([X : Y : Z]) = [Z : X : Y]$ ,  $\phi_3([X : Y : Z]) = [\omega X : Y : Z]$  and  $\phi_4([X : Y : Z]) = [X : \omega Y : Z]$ , and acts in  $F(n)$  with signature  $(0; 2n, 3, 2)$ . In this section we will give a realization of the ramification type  $(0; 2n, 3, 2)$  by finding a set of generators of  $G$  that satisfy the signature.

**Proposition 4.1.** *Let  $n \geq 4$  and  $a = \phi_4\phi_3\phi_2^{-1}\phi_1$ ,  $b = \phi_2\phi_3$  and  $c = \phi_1\phi_2^{-1}$  elements of  $G$ . Then  $G$  acts in  $F(n)$  with signature  $(0; 2n, 3, 2)$  and  $(a, b, c)$  is a generating vector of type  $(0; 2n, 3, 2)$ .*

*Proof.* As we saw before, the signature  $(0; 2n, 3, 2)$ , satisfies Riemann-Hurwitz formula (see (1)). As  $a, b, c \in G$ ,  $\langle a, b, c \rangle \leq G$  and

$$\begin{aligned} a([X : Y : Z]) &= \phi_4\phi_3\phi_2^{-1}\phi_1([X : Y : Z]) \\ &= \phi_4(\phi_3(\phi_2^{-1}([Y : X : Z]))) \\ &= \phi_4(\phi_3([X : Z : Y])) \\ &= \phi_4([\omega X : \omega Z : Y]) = [X : Z : \omega^{-1}Y], \end{aligned}$$

$$\begin{aligned} b([X : Y : Z]) &= \phi_2\phi_3([X : Y : Z]) \\ &= \phi_2([\omega X : Y : Z]) = [Z : \omega X : Y], \end{aligned}$$

$$\begin{aligned} c([X : Y : Z]) &= \phi_1\phi_2^{-1}([X : Y : Z]) \\ &= \phi_1(\phi_2^{-1}([X : Y : Z])) = \phi_1([Y : Z : X]) = [Z : Y : X], \end{aligned}$$

we get that  $|a| = 2n, |b| = 3, |c| = 2$ . Moreover,  $abc = 1$ . In fact

$$\begin{aligned} abc([X : Y : Z]) &= a(b([Z : Y : X])) \\ &= a([X, \omega Z, Y]) = [X : Y : Z]. \end{aligned}$$

Finally, we will prove that  $G = \langle a, b, c \rangle$ . Since  $a^{-1}([X : Y : Z]) = [X, \omega Z, Y]$  and  $b^2([X : Y : Z]) = [Y, \omega Z, \omega X]$ , we get

$$\begin{aligned} acb^2([X : Y : Z]) &= a(c([Y, \omega Z, \omega X])) \\ &= a([\omega X : \omega Z : Y]) = [\omega X : Y : Z] = \phi_3([X : Y : Z]), \end{aligned}$$

$$\begin{aligned} a^{-1}b^2cb([X : Y : Z]) &= a^{-1}(b^2(c([Z : \omega X : Y]))) \\ &= a^{-1}(b^2([Y : \omega X : Z])) = a^{-1}([X : Z : Y]) \\ &= [X : \omega Y : Z] = \phi_4([X : Y : Z]), \end{aligned}$$

$$\begin{aligned} b\phi_3^{-1}[X : Y : Z] &= b([\omega^{-1}X : Y : Z]) \\ &= [Z : X : Y] = \phi_2([X : Y : Z]), \end{aligned}$$

$$\begin{aligned} \phi_2^{-1}c([X : Y : Z]) &= \phi_2^{-1}([Z : Y : X]) \\ &= [Y : X : Z] = \phi_1([X : Y : Z]). \end{aligned}$$

Hence  $\langle a, b, c \rangle = G$ . Thus, according to the Riemann's existence Theorem 2.2,  $(a, b, c)$  is a generating vector of type  $(0; 2n, 3, 2)$ .  $\square$

### Acknowledgements

We are grateful to a referee for their careful reading and valuable suggestions and comments. We also thank Universidad del Cauca for support through Proyecto VRI 2488.

### References

- [1] Bauer I., Garion S. and Vdovina A., *Beauville surfaces and groups*, Springer Proc. Math. Stat. 123, Springer, Cham, 2015.
- [2] Broughton S.A., "Classifying finite group actions on surfaces of low genus", *J. Pure Appl. Algebra* 69 (1991), No. 3, 233–270.
- [3] Hurwitz A., "Ueber algebraische Gebilde mit eindeutigen Transformationen in sich", *Math. Ann.* 41 (1892), No. 3, 403–442.
- [4] Leopoldt H.-W., "Über die Automorphismengruppe des Fermatkörpers", *J. Number Theory* 56 (1996), No. 2, 256–282.
- [5] Macbeath A.M., "On a theorem of Hurwitz", *Proc. Glasgow Math. Assoc.* 5 (1961), 90–96.
- [6] Miranda R., *Algebraic curves and Riemann surfaces*, Graduate Studies in Mathematics 5, American Mathematical Society, Providence, RI, 1995.
- [7] Tzermias P., "The group of automorphisms of the Fermat curve", *J. Number Theory* 53 (1995), No. 1, 173–178.
- [8] Volklein H., *Groups as Galois groups. An introduction*, Cambridge Studies in Advanced Mathematics 53, Cambridge University Press, Cambridge, 1996.