Arch. Math. 104 (2015), 145–155

0003-889X/15/020145-11
published online January 29, 2015
DOI 10.1007/s00013-015-0724-y

Archiv der Mathematik

The group algebra decomposition of Fermat curves of prime degree

Patricio Barraza and Anita M. Rojas

Abstract. We describe the action of the full automorphisms group on the Fermat curve of degree N. For N prime, we obtain the group algebra decomposition of the corresponding Jacobian variety.

Mathematics Subject Classification. 14H40, 14H30.

Keywords. Isotypical decomposition, Jacobian variety, Fermat curves.

1. Introduction. Let S be a compact Riemann surface and G a non-trivial group of automorphisms of S. There are two representations of G associated to the action of G on S. Namely the *rational* (in what follows denoted by $\rho_{\mathbb{Q}}$) and the *analytic* representations, which are on $H_1(S, \mathbb{Q})$ (first homology group) and on $H^{1,0}(S, \mathbb{C})$ (analytic differentials) respectively. For the Fermat curve $\mathcal{F}_N$, the decomposition of both representations can be computed [2].

The action of G on S induces an action on the Jacobian variety JS of S. In [5] there was given a relationship between the rational irreducible representations of G and the G-invariant factors in the isotypical decomposition of an arbitrary abelian variety A with an action of a finite group G. In this way the group algebra decomposition of JS is obtained:

$$JS \sim J(S/G) \times B_2^{u_2} \times \cdots \times B_r^{u_r}. \tag{1.1}$$

This equation gives us a generic decomposition for a Jacobian with the action of a group G. The dimensions of the subvarieties B_i depend on the geometry of the action of G on S; they were computed in [7] in terms of the geometric signature for the action (see Section 2.2).

Let $N \geq 4$ be a natural number, and denote by $\mathcal{F}_N$ the Riemann surface given by the complex projective algebraic curve $x^N + y^N + z^N = 0$, known as the Fermat Curve of degree N. We compute the group algebra decomposition

Partially supported by Fondecyt Grant 1140507

for its Jacobian variety $J\mathcal{F}_N$ considering the action of its full automorphisms group. To decompose the Jacobian variety of a Fermat curve has been of interest to geometers and number theorists for quite some time. In [1] the Fermat curve $\mathcal{F}_N$ is decomposed using techniques of number theory, into a product of subvarieties of CM-type. The question of when such subvarieties are isogenous is answered, and under some additional conditions on N it is determined whether they are simple. This decomposition corresponds to the group algebra decomposition considering the subgroup $H = (\mathbb{Z}/N)^2$ of the full automorphisms group G_N. For $N = p$ a prime number, the author decomposes $J\mathcal{F}_p$ into $p-2$ factors of dimension $\frac{p-1}{2}$, describing which of these subvarieties are simple. Our decomposition, which considers the full group of automorphisms G_N, further decomposes some of the factors determining which are isogenous. For instance for $p = 7$, in [1] $J\mathcal{F}_7$ is decomposed as a product of five threefolds, three of them simple. Considering the full group G_N, we determine that $J\mathcal{F}_7 \sim E^6 \times T^3$, with E an elliptic curve and T a threefold.

2. Preliminaries. Let S be a Riemann surface S of genus g. We say that the group G acts on S if G is isomorphic to a subgroup of the analytical automorphism group $\mathrm{Aut}(S)$ of S. Let $\pi_G : S \to S/G$ denote the branched covering of S to S/G associated to the action of G on S. A ramification point $P \in S$ is a point where π_G has multiplicity $n \geq 2$. In other words, a point whose stabilizer has order n. The image of a ramification point of multiplicity n is called a branch point of degree n.

The geometric information about the action of G on S is partially encoded in the *geometric signature*. This is a tuple $\sigma = (\gamma; [n_1, C_1], \ldots, [n_t, C_t])$, where γ is the genus of the quotient curve S/G, each C_j is a conjugacy class of cyclic subgroups of G, n_j denotes the number of branch points $y \in S/G$ whose preimages in S are fixed by a subgroup in the class C_j, and $\sum_{j=1}^{t} n_j$ is the number of branch points of $\pi_G : S \to S/G$, see [7] for details.

2.1. Rational representation $\rho_{\mathbb{Q}}$. According to [7], if G is acting on S with geometric signature σ as above, then for each non trivial complex irreducible representation $\theta_i : G \to GL(V_i)$, its multiplicity s_i in the isotypical decomposition of $\rho_{\mathbb{Q}} \otimes \mathbb{C}$ is given by

$$s_i = 2\dim(V_i)(\gamma - 1) + \sum_{k=1}^{t} n_k(\dim(V_i) - \dim(\mathrm{Fix}_{G_k}(V_i))), \tag{2.1}$$

where G_k is a representative of the conjugacy class C_k.

2.2. Lange–Recillas decomposition [5]. Let S be a Riemann surface of genus $g \geq 2$ with a faithful action of a finite group G denoted by $\rho : G \to \mathrm{Aut}(S)$. This action induces a homomorphism $\mathbb{Q}[G] \to \mathrm{End}_{\mathbb{Q}}(JS)$ of the rational group algebra $\mathbb{Q}[G]$ into the endomorphism algebra $\mathrm{End}_{\mathbb{Q}}(JS)$ of the Jacobian of S, in a natural way.

Let $\mathbb{Q}[G] = Q_1 \times \cdots \times Q_r$ denote the decomposition of $\mathbb{Q}[G]$ into a product of simple $\mathbb{Q}$-algebras Q_i. The algebras Q_i correspond bijectively to the rational irreducible representations W_i of G. So for any irreducible rational representation W_i of G, there is a uniquely determined central idempotent e_{W_i} in $\mathbb{Q}[G]$ defining an abelian subvariety $A_i := \mathrm{Im}(ne_{W_i})$ of JS, where n is any positive integer such that $ne_{W_i} \in \mathrm{End}(JS)$. The addition map

$$\mu : A_1 \times \cdots \times A_r \to JS \tag{2.2}$$

is an isogeny. The isogeny (2.2) is called the *isotypical decomposition* (or the G-equivariant decomposition) of JS. The subvarieties A_i are called *isotypical components* of JS.

The decomposition of every $Q_i = L_1 \times \cdots \times L_{u_i}$ into a product of (isomorphic) minimal left ideals gives a further decomposition of the Jacobian which is called *the group algebra decomposition*. There are idempotents, not uniquely determined, $f_{i1}, \ldots, f_{iu_i} \in Q_i$ such that $e_i = f_{i1} + \cdots + f_{iu_i}$ [3], where $u_i = \frac{\dim V_i}{m_i}$, and $m_i = m_{V_i}$ is the Schur index of the representation V_i. As before, define for each f_{ij} a subvariety $B_{ij} := \mathrm{Im}(nf_{ij})$. As all these subvarieties are isogenous, we write $B_i = B_{i1}$ obtaining (1.1).

According to [7], if G is acting on S with geometric signature $\sigma = (\gamma; [n_1, C_1], \ldots, [n_t, C_t])$, the dimension of the subvarieties B_i of (1.1) associated to a non trivial rational irreducible representation W_i, is given by

$$\dim B_i = k_i \left(\dim V_i(\gamma - 1) + \frac{1}{2} \sum_{k=1}^{t} n_k \left(\dim V_i - \dim \mathrm{Fix}_{G_k} V_i \right) \right) \tag{2.3}$$

where G_k is a representative of the conjugacy class C_k, $\dim V_i$ is the dimension of a complex irreducible representation V_i associated to W_i, $K_i = \mathbb{Q}(\chi_{V_i}(g) : g \in G)$, m_i is the Schur index of V_i, and $k_i = m_i[K_i : \mathbb{Q}]$.

2.3. The full group of automorphisms of $\mathcal{F}_N$. It is known that the genus of $\mathcal{F}_N$ is $g = \dfrac{(N-1)(N-2)}{2}$. Concerning its full automorphisms group, we have the following result [6].

Proposition 2.1. *Let $\omega = e^{i\frac{2\pi}{N}}$ be a primitive n-th root of the unity. Then*

1. *The full group of automorphisms $Aut(\mathcal{F}_N)$ of $\mathcal{F}_N$ is generated by the maps in (2.4):*

$$\begin{aligned} &F_1(x, y, z) = (x, \omega y, z), F_2(x, y, z) = (\omega x, y, z), \\ &F_3(x, y, z) = (y, x, z), F_4(x, y, z) = (z, x, y). \end{aligned} \tag{2.4}$$

2. *Let $G_N := (\mu_N \times \mu_N) \rtimes S_3$, where $\mu_N = \langle \omega \rangle$ is the group of n-th roots of unity, and the action of $S_3 = \langle a, b : a^3, b^2, abab \rangle$ on $\mu_N \times \mu_N$ is given by $a(\omega, 1)a^2 = (1, \omega), b(\omega, 1)b = (1, \omega), a(1, \omega)a^2 = (\omega, 1)^{-1}(1, \omega)^{-1}$. Then $\mathrm{Aut}(\mathcal{F}_N) \cong G_N$. In fact an isomorphism $\Phi : G_N \to \mathrm{Aut}(\mathcal{F}_N)$ is given by $(1, \omega) \mapsto F_1, (\omega, 1) \mapsto F_2, b \mapsto F_3, a \mapsto F_4$.*

In what follows we identify G_N with $\mathrm{Aut}(\mathcal{F}_N)$ using Φ.

Table 1. Ramification points and stabilizer for the action of G_N on $\mathcal{F}_N$

Point	Stabilizer
$(\sqrt[N]{2}e^{i\frac{\pi}{N}}, 1, 1)$	$\langle ba\rangle$
$(e^{i\frac{2\pi}{3N}})^2, e^{i\frac{2\pi}{3N}}, 1)$	$\langle(\omega, 1)a\rangle$
$(0, e^{i\frac{\pi}{N}}, 1)$	$\langle(\omega, \omega)ba\rangle$

2.4. Description of the action of $G_N = (\mu_N \times \mu_N) \rtimes S_3$ on $\mathcal{F}_N$. We describe the canonical covering $\pi : \mathcal{F}_N \to \mathcal{F}_N/G_N$.

Proposition 2.2. *The geometric signature for the action of its full group of automorphisms G_N on $\mathcal{F}_N$ is $(0; [1, \overline{\langle ba\rangle}], [1, \overline{\langle(w, 1)a\rangle}], [1, \overline{\langle(w, w)ba\rangle}])$. Ramification points and their stabilizers are given in Table 1.*

Proof. With the notation of Proposition 2.1, each $f \in \mathrm{Aut}(\mathcal{F}_N)$ is of the form $f = (\omega^k, \omega^j)\sigma$, for some $k, j \in \mathbb{Z}/N$ and $\sigma \in S_3$. The elements of S_3 act on $\mathcal{F}_N$ as follows:

$$1(x, y, z) = (x, y, z), ba(x, y, z) = (x, z, y), ab(x, y, z) = (z, y, x),$$
$$b(x, y, z) = (y, x, z), a(x, y, z) = (z, x, y), a^2(x, y, z) = (y, z, x).$$

The set of points in $\mathcal{F}_N$ having any zero coordinate are all in the same orbit. In fact we have:

(1) $(0, y, z) \in \mathcal{F}_N$ if and only if $(0, y, z) = (0, e^{i\frac{\pi}{N}}\omega^k, 1)$, for some $k \in \mathbb{Z}/N$.
(2) $(x, 0, z) \in \mathcal{F}_N$ if and only if $(x, 0, z) = (e^{i\frac{\pi}{N}}\omega^k, 0, 1)$, for some $k \in \mathbb{Z}/N$.
(3) $(x, y, 0) \in \mathcal{F}_N$ if and only if $(x, y, 0) = (e^{i\frac{\pi}{N}}\omega^k, 1, 0)$, for some $k \in \mathbb{Z}/N$.

Note that for all j, k we have $(1, \omega^{j-k})(0, e^{i\frac{\pi}{N}}\omega^k, 1) = (0, e^{i\frac{\pi}{N}}\omega^j, 1)$, thus points of type (1) are in the same orbit. Moreover, as $b(x, 0, z) = (0, x, z)$ and $a(x, y, 0) = (0, x, y)$, points of type (2) and (3) are also in this orbit. Therefore this orbit has size $3N$. Since $\mid G \mid= 6N^2$, we have a branch point of degree $2N$. Finally, the stabilizer of $(0, e^{i\frac{\pi}{N}}, 1)$ is $(\omega, \omega)ba$, which gives part of the geometric signature.

On the other hand, we have that $ab(1, \sqrt[N]{2}e^{i\frac{\pi}{N}}, 1) = (1, \sqrt[N]{2}e^{i\frac{\pi}{N}}, 1)$, thus we have another branch point of degree 2. Finally observe that $(1, \omega)a \in \mathrm{Stab}(e^{-\frac{4\pi i}{3N}}, 1, e^{-\frac{2\pi i}{3N}})$, so we have one last branch point of degree 3. We verify that these points are all the branch points for the covering $\pi : \mathcal{F}_N \to \mathcal{F}_N/G_N$ using the Riemann-Hurwitz equation. If there are r points with multiplicities $t_1, .., t_r > 1$ and γ is the genus of the quotient, we have

$$\frac{(N-1)(N-2)}{2} = (\gamma - 1)6N^2 + 1 + \frac{6N^2}{2}\left(3 - \frac{1}{2N} - \frac{1}{2} - \frac{1}{3} + r - \sum_{j=1}^{r}\frac{1}{t_j}\right),$$

hence

$$3N^2\left(r - \sum_{j=1}^{r}\frac{1}{t_j}\right) = \frac{-\gamma 12N^2}{2},$$

but $3N^2\left(r-\sum_{j=1}^{r}\frac{1}{t_j}\right) > 0$ and $\dfrac{-\gamma 12N^2}{2} \leq 0$, which is a contradiction. Therefore

$$\frac{(N-1)(N-2)}{2} = (\gamma-1)6N^2 + 1 + \frac{6N^2}{2}\left(3 - \frac{1}{2N} - \frac{1}{2} - \frac{1}{3}\right),$$

hence $\gamma = 0$. □

3. Complex irreducible representations of G_N. To study the group algebra decomposition (1.1) of the Jacobian variety $J\mathcal{F}_N$ of $\mathcal{F}_N$, we need to know the complex irreducible representations of G_N. We use the method known as *little groups method* of Wigner and Mackey [8, 8.2] to compute them.

Proposition 3.1. *The group G_N of automorphisms of $\mathcal{F}_N$, given in Proposition 2.1, has the following complex irreducible representations.*

1. *If 3 divides N, then G_N has 6 irreducible representations of degree 1, 3 of degree 2, $2(N-3)$ of degree 3, and $\frac{N^2-3N+6}{6}$ of degree 6.*
2. *If 3 does not divide N, then G_N has 2 irreducible representations of degree 1, 1 of degree 2, $2(N-1)$ of degree 3, and $\frac{(N-2)(N-1)}{6}$ of degree 6.*

Moreover, these representations are explicitly shown in Table 2, where 'diag' means diagonal matrix, and $(\alpha,\beta) \in \{1,\dots,N-1\}^2$ is such that $\alpha \neq \beta$ and N does not divide $\beta + 2\alpha$ or $\alpha + 2\beta$. We denote by Λ the set of these pairs.

4. Group algebra decomposition of $J\mathcal{F}_N$, for N prime. We are interested in showing the group algebra decomposition (1.1) of the Jacobian variety $J\mathcal{F}_N$ associated to $\mathcal{F}_N$. The restriction on N becomes necessary when we compute the degree of the extension field $K_{\alpha,\beta} := \mathbb{Q}(\chi_{\rho_{\alpha,\beta}}(g) : g \in G_N)$ over $\mathbb{Q}$, see (2.3). The decomposition of $\rho_{\mathbb{Q}}$ can be obtained for arbitrary N.

4.1. Decomposition of $\rho_{\mathbb{Q}}$, for the action of G_N on $\mathcal{F}_N$.

Theorem 4.1. *Let the notation be as above, in particular representations are given in Table 2. Then the decomposition of the rational representation $\rho_{\mathbb{Q}} \otimes \mathbb{C}$ associated to the action of G_N on $\mathcal{F}_N$ depends on N in the following way.*

1. *If N is even and 3 does not divide N, the rational representation decomposes into a sum of $N-2$ irreducible representations of degree 3 and $\frac{(N-2)(N-4)}{6}$ irreducible representations of degree 6, namely:*

$$\bigoplus_{\alpha\in\{1,\dots,N-1\}\setminus\{\frac{N}{2}\}} \rho_\alpha^- \oplus \bigoplus_{(\alpha,\beta)\in\Lambda,\alpha+\beta\not\equiv 0(N)} \rho_{\alpha,\beta}$$

2. *If N is odd and 3 does not divide N, the rational representation decomposes into a sum of $N-1$ irreducible representations of degree 3 and $\frac{(N-1)(N-5)}{6}$ irreducible representations of degree 6, namely:*

$$\bigoplus_{\alpha\in\{1,\dots,N-1\}} \rho_\alpha^- \oplus \bigoplus_{(\alpha,\beta)\in\Lambda,\alpha+\beta\not\equiv 0(N)} \rho_{\alpha,\beta}$$

Table 2. Representations of G_N given on its generators

Label	Generators of S_3	Generators of $\mu_N \times \mu_N$
ρ_1	$a \to 1, b \to 1$	$(\omega,1) \to 1, (1,\omega) \to 1$
ρ_2	$a \to 1, b \to -1$	$(\omega,1) \to 1, (1,\omega) \to 1$
ρ_3	$a \to \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$,	$(\omega,1) \to \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$,
	$b \to \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$	$(1,\omega) \to \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
ρ_α^+	$a \to \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$,	$(\omega,1) \to \begin{pmatrix} \omega^\alpha & 0 & 0 \\ 0 & \omega^\alpha & 0 \\ 0 & 0 & \omega^{-2\alpha} \end{pmatrix}$,
	$b \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$	$(1,\omega) \to \begin{pmatrix} \omega^\alpha & 0 & 0 \\ 0 & \omega^{-2\alpha} & 0 \\ 0 & 0 & \omega^\alpha \end{pmatrix}$
		$\alpha \in \{1,..,N-1\} \setminus \{\frac{N}{3}, \frac{2N}{3}\}$
ρ_α^-	$a \to \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$,	$(\omega,1) \to \begin{pmatrix} \omega^\alpha & 0 & 0 \\ 0 & \omega^\alpha & 0 \\ 0 & 0 & \omega^{-2\alpha} \end{pmatrix}$,
	$b \to \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}$	$(1,\omega) \to \begin{pmatrix} \omega^\alpha & 0 & 0 \\ 0 & \omega^{-2\alpha} & 0 \\ 0 & 0 & \omega^\alpha \end{pmatrix}$
		$\alpha \in \{1,..,N-1\} \setminus \{\frac{N}{3}, \frac{2N}{3}\}$
$\rho^1_{\frac{N}{3}}$	$a \to 1, b \to 1$	$(\omega,1) \to \omega^{\frac{N}{3}}, (1,\omega) \to \omega^{\frac{N}{3}}$
$\rho^2_{\frac{N}{3}}$	$a \to 1, b \to -1$	$(\omega,1) \to \omega^{\frac{N}{3}}, (1,\omega) \to \omega^{\frac{N}{3}}$
$\rho^3_{\frac{N}{3}}$	$a \to \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$,	$(\omega,1) \to \begin{pmatrix} \omega^{\frac{N}{3}} & 0 \\ 0 & \omega^{\frac{N}{3}} \end{pmatrix}$,
	$b \to \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$	$(1,\omega) \to \begin{pmatrix} \omega^{\frac{N}{3}} & 0 \\ 0 & \omega^{\frac{N}{3}} \end{pmatrix}$
$\rho^1_{\frac{2N}{3}}$	$a \to 1, b \to 1$	$(\omega,1) \to \omega^{\frac{2N}{3}}, (1,\omega) \to \omega^{\frac{2N}{3}}$
$\rho^2_{\frac{2N}{3}}$	$a \to 1, b \to -1$	$(\omega,1) \to \omega^{\frac{2N}{3}}, (1,\omega) \to \omega^{\frac{2N}{3}}$
$\rho^3_{\frac{2N}{3}}$	$a \to \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$,	$(\omega,1) \to \begin{pmatrix} \omega^{\frac{2N}{3}} & 0 \\ 0 & \omega^{\frac{2N}{3}} \end{pmatrix}$,
	$b \to \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$	$(1,\omega) \to \begin{pmatrix} \omega^{\frac{2N}{3}} & 0 \\ 0 & \omega^{\frac{2N}{3}} \end{pmatrix}$

Table 2. Table 2 continued

Label	Generators of S_3	Generators of $\mu_N \times \mu_N$
$\rho_{\alpha,\beta}$	$a \to \begin{pmatrix} 0&0&1&0&0&0\\ 1&0&0&0&0&0\\ 0&1&0&0&0&0\\ 0&0&0&0&1&0\\ 0&0&0&0&0&1\\ 0&0&0&1&0&0 \end{pmatrix}$,	$(\omega,1) \to \mathrm{diag}(\omega^{\alpha},\omega^{\beta},\omega^{-\alpha-\beta},\omega^{\beta},\omega^{-\alpha-\beta},\omega^{\alpha})$,
	$b \to \begin{pmatrix} 0&0&0&1&0&0\\ 0&0&0&0&1&0\\ 0&0&0&0&0&1\\ 1&0&0&0&0&0\\ 0&1&0&0&0&0\\ 0&0&1&0&0&0 \end{pmatrix}$	$(1,\omega) \to \mathrm{diag}(\omega^{\beta},\omega^{-\alpha-\beta},\omega^{\alpha},\omega^{\alpha},\omega^{\beta},\omega^{-\alpha-\beta})$

3. *If N is even and 3 divides N, the rational representation decomposes into a sum of $N-4$ irreducible representations of degree 3, $\frac{N^2-6N+12}{6}$ irreducible representations of degree 6, and 2 of degree 1, namely:*

$$\bigoplus_{\alpha\in\{1,\ldots,N-1\}\setminus\{\frac{N}{3},\frac{N}{2},\frac{2N}{3}\}} \rho_\alpha^- \oplus \bigoplus_{(\alpha,\beta)\in\Lambda,\alpha+\beta\not\equiv 0(N)} \rho_{\alpha,\beta} \oplus \left(\rho^2_{\frac{N}{3}}\right) \oplus \left(\rho^2_{\frac{2N}{3}}\right)$$

4. *If N is odd and 3 divides N, the rational representation decomposes into a sum of $N-3$ irreducible representations of degree 3, $\frac{(N-3)^2}{6}$ irreducible representations of degree 6, and 2 of degree 1, namely :*

$$\bigoplus_{\alpha\in\{1,\ldots,N-1\}\setminus\{\frac{N}{3},\frac{2N}{3}\}} \rho_\alpha^- \oplus \bigoplus_{(\alpha,\beta)\in\Lambda,\alpha+\beta\not\equiv 0(N)} \rho_{\alpha,\beta} \oplus \left(\rho^2_{\frac{N}{3}}\right) \oplus \left(\rho^2_{\frac{2N}{3}}\right)$$

The proof of Theorem 4.1 is a straightforward computation using Theorem 2.1, see [2] for details.

4.2. Subvarieties of the group algebra decomposition for $J\mathcal{F}_N$. According to (2.3), we need to compute the Schur index and the degree $[\mathbb{Q}(\chi_{\rho_i}(g) : g \in G_N) : \mathbb{Q}]$ for the irreducible representations ρ_i decomposing $\rho_{\mathbb{Q}} \otimes \mathbb{C}$ (Theorem 4.1).

Proposition 4.2. *The Schur index of each representation ρ_α^- and $\rho_{\alpha,\beta}$ is 1.*

Proof. These representations are induced by irreducible representations of degree 1 of $H_1 = \mu_N \times \mu_N\langle b\rangle \le G_N$ and $H_2 = \mu_N \times \mu_N \le G_N$, respectively; both subgroups have a complement in G_N. From Proposition [4, X.8] we obtain that the Schur index of the corresponding induced representations divide 1. □

Lemma 4.3. *Let χ be the character of the representation ρ_α^-, $\alpha \in \{1,\ldots,N-1\}\setminus\{\frac{N}{2},\frac{N}{3},\frac{2N}{3}\}$. Then*

$$[\mathbb{Q}(\chi(g) : g \in G) : \mathbb{Q}] = \varphi\left(\frac{N}{\gcd(N,\alpha)}\right).$$

Proof. We will prove that $\mathbb{Q}(\chi(g) : g \in G) = \mathbb{Q}(2\omega^{\alpha} + \omega^{-2\alpha}) = \mathbb{Q}(\omega^{\alpha})$. The proposition follows from the fact that ω^{α} is a $\left(\frac{N}{\gcd(N,\alpha)}\right)$ – primitive root of unity.

Let $\tau = \omega^{\alpha}$ be a $\left(\frac{N}{\gcd(N,\alpha)}\right)$ – primitive root of unity. We have the following extension of fields $\mathbb{Q}(\tau) \supset \mathbb{Q}(\chi(g) : g \in G) \supset \mathbb{Q}(2\tau + \tau^{-2})$, hence it is sufficient to prove that $\mathbb{Q}(\tau) = \mathbb{Q}(2\tau + \tau^{-2})$. Since $\mathbb{Q}(\tau) \supset \mathbb{Q}$ is Galois, we will prove that $\mathrm{Gal}_{\mathbb{Q}(2\tau+\tau^{-2})}(\mathbb{Q}(\tau)) = \{Id\}$. Suppose we have $\sigma \in \mathrm{Gal}_{\mathbb{Q}(2\tau+\tau^{-2})}(\mathbb{Q}(\tau)) \setminus \{Id\}$, hence $\sigma(\tau) = \tau^r$, for some $r \neq 1$. Thus $\sigma(2\tau + \tau^{-2}) = 2\tau^r + \tau^{-2r} = 2\tau + \tau^{-2}$. Hence

$$2(\tau^r - \tau) = \frac{1}{\tau^2} - \frac{1}{\tau^{2r}} = \frac{\tau^{2r} - \tau^2}{\tau^2\tau^{2r}} = \frac{(\tau^r - \tau)(\tau^r + \tau)}{\tau^2\tau^{2r}}$$

and $2 = \frac{\tau^r + \tau}{\tau^2\tau^{2r}}$. Furthermore $\mid \tau^r + \tau \mid = 2 = \mid \tau^r \mid + \mid \tau \mid$, then $\tau^r = \lambda\tau$ for some $\lambda \in \mathbb{R}$, where $\mid \lambda \mid = 1$. If $\lambda = -1$, then $\tau^r + \tau = 0$, which is impossible. If $\lambda = 1$, then $\tau^r = \tau$, which is not possible. Thus $\mathrm{Gal}_{\mathbb{Q}(2\tau+\tau^{-2})}(\mathbb{Q}(\tau)) = \{Id\}$. □

We recall (Table 2) that Λ is a set of pairs $(\alpha, \beta) \in \{1, \ldots, N-1\}^2$ indexing the irreducible representations of degree 6 of G. At this point we need to restrict N to prime numbers.

Lemma 4.4. *Let $N > 6$ be a prime, $(\alpha, \beta) \in \Lambda$ be a pair such that $\alpha + \beta \not\equiv 0(N)$, and $K_{\alpha,\beta}$ as before. Then*

$$[K_{\alpha,\beta} : \mathbb{Q}] = \begin{cases} \frac{N-1}{3} & \text{if } \alpha \equiv r\beta(N) \quad \text{for some } r \in \mathbb{Z} \text{ where } r^3 \equiv 1(N) \\ N-1 & \text{otherwise} \end{cases}$$

Proof. We will consider two cases. First consider $N \equiv 1(3)$. Since N is prime, by Cauchy's theorem, there exists $r \not\equiv 1(N)$ such that $r^3 \equiv 1(N)$. Let $\alpha \equiv r\beta(N)$ be an integer. We will show that $\mid \mathrm{Gal}_{K_{\alpha,\beta}} \mathbb{Q}(\omega) \mid = 3$.

Let $\sigma \in \mathrm{Gal}_{\mathbb{Q}} \mathbb{Q}(\omega)$ be the automorphism given by $\sigma(\omega) = \omega^r$, then $\mid \sigma \mid = 3$. We will prove that $\langle \sigma \rangle = \mathrm{Gal}_{K_{\alpha,\beta}} \mathbb{Q}(\omega)$.

Consider $\sigma' \in \mathrm{Gal}_{K_{\alpha,\beta}} \mathbb{Q}(\omega)$, hence $\sigma'(\omega) = \omega^s$, for some $s \in \mathbb{Z}$. We must show that $\sigma' \in \langle \sigma \rangle$, that is $s \equiv 1(N)$ or $s \equiv r(N)$ or $s \equiv r^2(N)$. N is prime and $r \not\equiv 1(N)$, hence if $r^3 - 1 \equiv (r-1)(r^2 + r + 1) \equiv 0(N)$ then $r^2 + r + 1 \equiv 0(N)$.

Let $\gamma = -\alpha - \beta$, multiplying by β we have $\beta + \beta r + \beta r^2 \equiv \beta + \beta r + \alpha r(N)$. Adding α we conclude $\alpha \equiv \alpha + \beta + \beta r + \alpha r \equiv (\alpha + \beta)(1 + r) \equiv -\gamma(1 + r)(N)$. Equivalently, $r\beta \equiv -\gamma - \gamma r(N)$ so that $\gamma \equiv -\gamma r - r\beta \equiv \alpha r(N)$. Thus $r\gamma \equiv \beta(N)$.

On the other hand, $\chi(\omega, 1) = 2\omega^{\alpha} + 2\omega^{\beta} + 2\omega^{-\alpha-\beta} \in K_{\alpha,\beta}$, then $\omega^{\alpha} + \omega^{\beta} + \omega^{\gamma} = \omega^{s\alpha} + \omega^{s\beta} + \omega^{s\gamma}$, but since $N > 6$, we must have equal elements in the set $\{\omega^{\alpha}, \omega^{\beta}, \omega^{\gamma}, \omega^{s\alpha}, \omega^{s\beta}, \omega^{s\gamma}\}$, otherwise they are part of a basis for $\mathbb{Q}(\omega)$ and linearly dependent. As α, β, and γ are different form each other, we have three cases:

1. $\alpha \in \{s\alpha, s\beta, s\gamma\}$. If $\alpha = s\alpha$, then $s = 1$. If $\alpha = s\beta$, then $r\beta = s\beta$, hence $r = s$. If $\alpha = s\gamma$, then $\gamma = r\alpha = rs\gamma$ and hence $rs = 1$, that is $s = r^2$.
2. $\beta \in \{s\alpha, s\beta, s\gamma\}$. If $\beta = s\alpha$, then $\beta = sr\beta$ and hence $rs = 1$, that is $\sigma' = \sigma^2$. If $\beta = s\beta$, then $s = 1$. If $\beta = s\gamma$, then $r\beta = rs\gamma = s\beta$ and hence $r = s$.

3. $\gamma \in \{s\alpha, s\beta, s\gamma\}$. If $\gamma = s\alpha$, then $r\alpha = s\alpha$ and hence $r = s$. If $\gamma = s\beta$, then $r\gamma = rs\beta$ and hence $rs = 1$, that is $s = r^2$. If $\gamma = s\gamma$, then $s = 1$.

If $\alpha \not\equiv r\beta(N)$ for each r with $r^3 \equiv 1(N)$, then we must show that $\mathrm{Gal}_K\,\mathbb{Q}(\omega) = \{Id\}$. Suppose $\sigma \in \mathrm{Gal}_K\,\mathbb{Q}(\omega)\backslash\{Id\}$, that is $\sigma(\omega) = \omega^s$, where $s \not\equiv 1(N)$. By the previous analysis, we have the following cases:

1. $\alpha = s\beta$. If $\beta = s\gamma$, then $\gamma = s\alpha$. Hence $\gamma = s\alpha = s^2\beta = s^3\gamma$, that is $s^3 \equiv 1(N)$, which is impossible.
   If $\beta = s\alpha$, then $\gamma = s\gamma$. Hence $s = 1$, which is a contradiction.
2. $\alpha = s\gamma$. Then $\beta = s\alpha$ and $\gamma = s\beta$. Hence $\beta = s^2\gamma = s^3\beta$, that is $s^3 \equiv 1$, which is impossible.
3. $\gamma = s\alpha$. Then $\beta = s\gamma$ and $\alpha = s\beta$. Hence $\gamma = s^3\gamma$, that is $s^3 \equiv 1$, which is impossible.

□

Theorem 4.5. *Let $N > 4$ be a prime:*

1. *If $N \equiv -1(3)$ the isotypical decomposition of $J\mathcal{F}_N$ is given by*

$$J\mathcal{F}_N \sim B_0^3 \times B_1^6 \times \cdots \times B_{\frac{N-5}{6}}^6.$$

The subvariety B_0 corresponds to the $\mathbb{Q}-$irreducible representation of G_N associated to ρ_α^-, for any α. B_0 is of dimension $\frac{N-1}{2}$.

For $i > 0$, the subvariety B_i corresponds to the $\mathbb{Q}-$irreducible representation of G_N associated to $\rho_{\alpha,\beta}$ appearing in the decomposition of $\rho_\mathbb{Q} \otimes \mathbb{C}$ (see Theorem 4.1). B_i is of dimension $\frac{N-1}{2}$.

2. *If $N \equiv 1(3)$,the isotypical decomposition of $J\mathcal{F}_N$ is given by*

$$J\mathcal{F}_N \sim B^6 \times B_0^3 \times B_1^6 \times \cdots \times B_{\frac{N-7}{6}}^6.$$

The subvariety B corresponds to the $\mathbb{Q}-$irreducible representation of G associated to the representations of degree 6 appearing in the decomposition of $\rho_\mathbb{Q} \otimes \mathbb{C}$ (see Theorem 4.1). They have Galois group $\mathrm{Gal}_\mathbb{Q}\,K_{\alpha,\beta}$ of order $\frac{N-1}{3}$, therefore B is of dimension $\frac{N-1}{6}$.

The subvariety B_0 corresponds to the $\mathbb{Q}-$irreducible representation of G_N associated to ρ_α^-, for any α. B_0 is of dimension $\frac{N-1}{2}$.

For $i > 0$, the subvariety B_i corresponds to the irreducible representation of G over $\mathbb{Q}$ associated to the representations of degree 6 appearing in the decomposition of $\rho_\mathbb{Q} \otimes \mathbb{C}$ (see Theorem 4.1), they have Galois group $\mathrm{Gal}_\mathbb{Q}\,K_{\alpha,\beta}$ of order $N-1$. Therefore these varieties are of dimension $\frac{N-1}{2}$.

Proof. For each ρ_α^- the corresponding Galois group $\mathrm{Gal}_\mathbb{Q}\,K_\alpha$ is of order $N-1$ and the other potencial representations of degree 3 do not appear in the rational representation (see Theorem 4.1). We have that the representations ρ_α^- are in one Galois orbit of size $N-1$, the corresponding subvariety B_0 is of dimension $\frac{N-1}{2}$, and its factor is B_0^3.

If $N \not\equiv 1(3)$, there exist s subvarieties associated to the s orbits of the action of $\mathrm{Gal}_\mathbb{Q}\,K$, of order $N-1$, on the irreducible representations of degree 6 which appear in the rational representation (see Theorem 4.1), each subvariety is of dimension $\frac{N-1}{2}$ and appears with multiplicity 6.

Thus $J\mathcal{F}_N \sim B_0^3 \times B_1^6 \times \cdots \times B_s^6$. Comparing with the dimension of $J\mathcal{F}_N$, we have

$$\frac{(N-1)(N-2)}{2} = 3\frac{N-1}{2} + s\left(6\frac{N-1}{2}\right),$$

equivalently $s = \frac{N-5}{6}$.

If $N \equiv 1(3)$, then there exists an element of order 3 on the group $\mathbb{Z}/N^*$, that is there exists $r_0 \neq 1$ with $r_0^3 \equiv 1(N)$ and hence there exists $r_1 \neq 1, r_0$ with $r_1^3 \equiv 1(N)$. Then the $2(N-1)$ pairs $(r_0\beta, \beta)$ and $(r_1\beta, \beta)$ are such that the corresponding representation appears in the rational representation and have Galois group $\mathrm{Gal}_{\mathbb{Q}K}$ of order $\frac{N-1}{3}$. We have $\frac{N-1}{3}$ representations of degree 6, which must be grouped into orbits of size $\frac{N-1}{3}$, then we have only one Galois orbit. Therefore there is only one subvariety B associated to them, it is of dimension $\frac{N-1}{6}$, and its factor is B^6. Finally, there are s subvarieties associated to the s orbits corresponding to the representations of degree 6 with Galois group $\mathrm{Gal}_{\mathbb{Q}}\, K_{\alpha,\beta}$ of order $N-1$. Each subvariety is of dimension $\frac{N-1}{2}$ and appears with multiplicity 6. Thus

$$J\mathcal{F}_N \sim B_0^3 \times B^6 \times B_1^6 \cdots \times B_s^6,$$

comparing with the dimension of $J\mathcal{F}_N$, we have that

$$\frac{(N-1)(N-2)}{2} = 3\frac{N-1}{2} + 6\frac{N-1}{6} + s\left(6\frac{N-1}{2}\right),$$

equivalently $s = \frac{N-7}{6}$. □

Acknowledgements. We would like to thank the referee for some valuable suggestions.

References

[1] N. Aoki, Simple factors of the Jacobian of a Fermat curve and the Picard number of a product of Fermat curves, Am. J. Math. **113** (1991), 779–833.

[2] P. Barraza, Curvas de Fermat y descomposición de objetos asociados, Master thesis, Pontificia Universidad Católica de Chile, (2009).

[3] A. Carocca and R. Rodrguez, E. Jacobians with groups actions and rational idempotents, J. Algebra **306** (2006), 322–343.

[4] I. Isaacs , Character theory of finite groups, Corrected reprint of the 1976 original [Academic Press, New York; MR0460423]. AMS Chelsea Publishing, Providence, RI, 2006. xii+310 pp. ISBN: 978-0-8218-4229-4; 0-8218-4229-3.

[5] H. Lange and S. Recillas, Abelian varieties with group action, J. Reine Angew. Math. **575** (2004), 135–155.

[6] P. Tzermias, The group of automorphisms of the Fermat curve, J. Number Theory **53** (1995), 173–178.

[7] A. M. Rojas Group actions on Jacobian varieties. Rev. Mat. Iberoam, **23** (2007), 397–420.

[8] J.-P. Serre, Linear representations of finite groups, Translated from the second French edition by Leonard L. Scott. Graduate Texts in Mathematics, Vol. 42. Springer-Verlag, New York-Heidelberg, 1977, ISBN: 0-387-90190-6.

Patricio Barraza
Universidad Técnica Federico Santa María
Casilla 110-V
Valparaíso
Chile.
e-mail: patricio.barraza@usm.cl

Anita M. Rojas
Departamento de Matemáticas, Facultad de Ciencias,
Universidad de Chile
Las Palmeras 3425 Ñuñoa
Santiago, Chile.
e-mail: anirojas@u.uchile.cl

Received: 30 July 2014
Revised: 2 January 2015